Allegato 1 decreto n. 96 del 31/08/2023 – Schema convenzione ARTEA - CAA Centri di AssistenzaAgricola anno 2023/2025.

DE SANTIS FRANCESCA
AGENZIA REGIONALE TOSCANA
EROGAZIONI AGRICOLTURA
31.08.2023 13:05:50 UTC

CONVENZIONE

tra

Agenzia Regionale Toscana per le Erogazioni in Agricoltura, in seguito denominata "Agenzia", C.F. 05096020481, con sede legale in Firenze -Via Ruggero Bardazzi n. 19/21- rappresentata dal Dott. _____, ivi domiciliato per la sua carica, non in proprio ma nella qualità di Direttore e l.r.p.t. di ARTEA, in forza del D.P.G.R. n. 60 del 9.3.2021,

e

Centro Autorizzato di Assistenza Agricola_____s.r.l., che per brevità sarà di seguito denominato "CAA", con sede legale in_____, via_____, C.F.- P.IVA _____, PEC_____, autorizzato dalla Regione _____ con decreto_____n._____del_____, rappresentato da_____, domiciliato per la sua carica presso la sede legale della società, in qualità di l.r.p.t. e _____,

VISTI, in relazione alla PAC 2014/2021:

- il regolamento (UE) n. 1306/2013 del Parlamento Europeo e del Consiglio, sul finanziamento, sulla gestione e sul monitoraggio della politica agricola comune e che abroga i regolamenti del Consiglio (CEE) n. 352/78, (CE) n. 165/94, (CE) n. 2799/98, (CE) n. 814/2000, (CE) n. 1290/2005 e (CE) n. 485/2008 e i regolamenti delegati e di esecuzione al regolamento medesimo riferiti;
- il regolamento delegato n. (UE) 907/2014 della Commissione dell'11 marzo 2014 che integra il regolamento (UE) n. 1306/2013 del Parlamento Europeo e del Consiglio per quanto riguarda gli organismi pagatori e altri organismi, la gestione finanziaria, la liquidazione dei conti, le cauzioni e l'uso dell'euro e che abroga il regolamento (CE) n. 885/2006;
- il regolamento delegato (UE) n. 640/2014 della Commissione che integra il regolamento (UE) n. 1306/2013 del Parlamento europeo e del Consiglio per quanto riguarda il Sistema Integrato di Gestione e Controllo e le condizioni per il rifiuto o la revoca di pagamenti nonché le sanzioni amministrative applicabili ai pagamenti diretti, al sostegno allo sviluppo rurale e alla condizionalità;
- il regolamento di esecuzione (UE) n. 809/2014 della Commissione del 17 luglio 2014 recante modalità di applicazione del regolamento (UE) n. 1306/2013 del Parlamento Europeo e del

Consiglio per quanto riguarda il Sistema Integrato di Gestione e Controllo, le misure di sviluppo rurale e la condizionalità e che prevede una introduzione graduale della domanda grafica a partire dal 2016;

- il regolamento (UE) n. 908/2014 della Commissione del 06 agosto 2014, recante modalità di applicazione del regolamento (UE) n. 1306/2013 del Parlamento Europeo e del Consiglio per quanto riguarda gli organismi pagatori e altri organismi, la gestione finanziaria laliquidazione dei conti, le norme sui controlli, le cauzioni e la trasparenza;
- il regolamento (UE) n. 1305/2013 sul sostegno allo sviluppo rurale da parte del Fondo europeo agricolo per lo sviluppo rurale (FEASR), e che abroga il regolamento (CE) n. 1698/2005 del Consiglio e i regolamenti delegati e di esecuzione al regolamento medesimo riferiti;
- il regolamento (UE) n. 1307/2013 recante norme sui pagamenti diretti agli agricoltori nell'ambito dei regimi di sostegno previsti dalla politica agricola comune, che abroga il regolamento (CE) n. 73/2009 del Consiglio;
- il regolamento delegato (UE) n. 639/2014 della Commissione dell'11 marzo 2014 che integra il regolamento (UE) n. 1307/2013 del Parlamento Europeo e del Consiglio recante norme sui pagamenti diretti agli agricoltori nell'ambito dei regimi di sostegno previsti dalla politica agricola comune e che modifica l'allegato X di tale regolamento;
- il regolamento (UE) n. 508/2014 del 15 maggio 2014 che abroga il regolamento CE n. 1198/2006 relativo al Fondo Europeo per la Pesca (FEP);
- il regolamento (UE) n. 1308/2013 recante organizzazione comune dei mercati dei prodotti agricoli, che abroga il regolamento (CE) n. 1234/2007;
- il regolamento (UE) n. 1303/2013 recante disposizioni comuni sul Fondo europeo di sviluppo regionale, sul Fondo sociale europeo, sul Fondo di coesione, sul Fondo europeo agricolo per lo sviluppo rurale e sul Fondo europeo per gli affari marittimi e la pesca e disposizioni generali sul Fondo europeo di sviluppo regionale, sul Fondo sociale europeo, sul Fondo di coesione e sul Fondo europeo per gli affari marittimi e la pesca, e che abroga il regolamento (CE) n. 1083/2006 del Consiglio;
- il regolamento (UE) n. 2393/2017 del Parlamento europeo e del Consiglio, del 13 dicembre 2017, che modifica i regolamenti (UE) n. 1305/2013 sul sostegno allo sviluppo ruraleda parte del Fondo europeo agricolo per lo sviluppo rurale (FEASR), (UE) n. 1306/2013 sul finanziamento, sulla gestione e sul monitoraggio della politica agricola comune, (UE) n. 1307/2013 recante norme sui pagamenti diretti agli agricoltori nell'ambito dei regimi di sostegno previsti dalla politica agricola comune, (UE) n. 1308/2013 recante organizzazione comune dei mercati dei prodotti agricoli e (UE) n. 652/2014 che fissa le disposizioni per la gestione delle spese relative

alla filiera alimentare, alla salute e al benessere degli animali, alla sanità delle piante e al materiale riproduttivo vegetale;

VISTO che il Consiglio ha formalmente adottato la nuova PAC per il periodo 2023/2027 e che i tre regolamenti che compongono il pacchetto di riforma della PAC sono stati firmati dal Consiglio e dalla Commissione e pubblicati nella G.U. il 6.12.2021, e sono entrati in vigore in data 1.1.2023;

VISTI, in relazione alla nuova PAC 2023/2027, in particolare:

- il regolamento (UE) 2021/2115 del Parlamento europeo e del Consiglio del 2 dicembre 2021 recante norme sul sostegno ai piani strategici che gli Stati membri devono redigere nell'ambito della politica agricola comune (piani strategici della PAC) e finanziati dal Fondo europeo agricolo di garanzia (FEAGA) e dal Fondo europeo agricolo per lo sviluppo rurale (FEASR) e che abroga i regolamenti (UE) n. 1305/2013 e (UE) n. 1307/2013;
- il regolamento (UE) 2021/2116 del Parlamento europeo e del Consiglio del 2 dicembre 2021sul finanziamento, sulla gestione e sul monitoraggio della politica agricola;
- il regolamento (UE) 2021/2117 del Parlamento europeo e del Consiglio del 2 dicembre 2021 che modifica i regolamenti (UE) n. 1308/2013 recante organizzazione comune dei mercati dei prodotti agricoli, (UE) n. 1151/2012 sui regimi di qualità dei prodotti agricoli e alimentari, (UE) n. 251/2014 concernente la definizione, la designazione, la presentazione, l'etichettatura e la protezione delle indicazioni geografiche dei prodotti vitivinicoli aromatizzati e (UE) n. 228/2013 recante misure specifiche nel settore dell'agricoltura a favore delle regioni ultra periferiche dell'Unione;
- il regolamento delegato (UE) 2022/126 della Commissione del 7 dicembre 2021 che integra il regolamento (UE) 2021/2115 del Parlamento europeo e del Consiglio con requisiti aggiuntivi per taluni tipi di intervento specificati dagli Stati membri nei rispettivi piani strategici della PAC per il periodo dal 2023 al 2027 a norma di tale regolamento, nonché per le norme relative alla percentuale per la norma 1 in materia di buone condizioni agronomiche e ambientali (BCAA);
- regolamento delegato (UE) 2022/127 della Commissione del 7 dicembre 2021 che integra il regolamento (UE) 2021/2116 del Parlamento europeo e del Consiglio con norme concernenti gli organismi pagatori e altri organismi, la gestione finanziaria, la liquidazione dei conti, le cauzioni e l'uso dell'euro;
- regolamento di esecuzione (UE) 2022/128 della Commissione del 21 dicembre 2021 recante modalità di applicazione del regolamento (UE) 2021/2116 del Parlamento europeo e del Consiglio per quanto riguarda gli organismi pagatori e altri organismi, la gestione finanziaria, la

liquidazione dei conti, i controlli, le cauzioni e la trasparenza;

- regolamento di esecuzione (UE) 2022/129 della Commissione del 21 dicembre 2021 che stabilisce norme relative ai tipi di intervento riguardanti i semi oleaginosi, il cotone e i sottoprodotti della vinificazione a norma del regolamento (UE) 2021/2115 del Parlamento europeo e del Consiglio e ai requisiti in materia di informazione, pubblicità e visibilità inerenti al sostegno dell'Unione e ai piani strategici della PAC;

VISTO il decreto legislativo 21 maggio 2018 n. 74 (Riorganizzazione dell'Agenzia per le erogazioni in agricoltura - AGEA e per il riordino del sistema dei controlli nel settore agroalimentare, in attuazione dell'articolo 15 della legge 28 luglio 2016, n. 154), ed in particolare l'art. 6 che disciplina l'attività dei Centri Autorizzati di assistenza agricola (CAA);

VISTO il decreto del Presidente della Repubblica 1° dicembre 1999, n. 503, con il quale è stato emanato il "Regolamento recante norme per l'istituzione della Carta dell'agricoltore e del pescatore e dell'anagrafe delle aziende agricole, in attuazione dell'articolo 14, comma 3, del decreto legislativo 30 aprile 1998, n. 173";

VISTO il decreto legislativo 29 marzo 2004, n. 99 (Disposizioni in materia di soggetti e attività, integrità aziendale e semplificazione amministrativa in agricoltura, a norma dell'articolo 1, comma 2, lettere d), f), g), l), ee), della legge 7 marzo 2003, n. 38) che detta le regole per la semplificazione amministrativa in agricoltura e la gestione del fascicolo aziendale elettronico;

VISTO il Decreto del Ministero delle Politiche Agricole del 27/03/2008 "Riforma dei centri autorizzati di assistenza agricola", che definisce i requisiti minimi di garanzia e di funzionamento per le attività dei centri autorizzati di assistenza agricola e abroga il decreto MiPAAF 27 marzo 2001;

VISTO il decreto MiPAAF relativo alla semplificazione della gestione della PAC 2014-2020 n. 162 del 12 gennaio 2015;

VISTO il decreto MiPAAF n. 5465 del 07 giugno 2018 recante "*Attuazione regolamento Omnibus - Pagamenti diretti";*

VISTO il decreto-legge 3 ottobre 2006, n. 262, convertito in legge 24 novembre 2006, n. 286 (Conversione in legge, con modificazioni, del decreto-legge 3 ottobre 2006, n. 262, recante disposizioni urgenti in materia tributaria e finanziaria) che prevede che le richieste di contributi agricoli presentati agli organismi pagatori debbano contenere anche gli elementi utili a consentire l'aggiornamento del

catasto terreni, ivi compresi quelli relativi ai fabbricati inclusi nell'azienda agricola, al fine di risultare sostitutive delle dichiarazioni di variazione colturale da rendere al catasto stesso;

VISTO il Regolamento (CEE) del 4 marzo 1991, n. 595, relativo alle irregolarità ed al recupero delle somme indebitamente pagate nell'ambito del finanziamento della politica agricola comune, nonché all'instaurazione di un sistema di informazione in questo settore;

VISTO il Regolamento (CE) dell'11 novembre 1996, n. 2185, recante le disposizioni generali supplementari, a norma dell'art.10 del Reg. 2988/95 e relativo ai controlli ed alle verifiche sul posto effettuati dalla Commissione ai fini della tutela degli interessi finanziari delle Comunità europee contro le frodi ed altre irregolarità;

VISTA la legge 24 novembre 1981, n.689 "Modifiche al sistema penale", in particolare l'art.13 che conferisce i poteri agli organi addetti al controllo;

VISTA la legge 23 dicembre 1986, n.898 "Conversione in legge, con modificazioni, del decreto-legge 27 ottobre 1986, n. 701, recante misure urgenti in materia di controlli degli aiuti comunitari alla produzione dell'olio di oliva. Sanzioni amministrative e penali in materia di aiuti comunitari nel settore agricolo";

VISTO il D.P.R. 14/11/2002, n. 313 "Testo unico delle disposizioni legislative e regolamentari in materia di casellario giudiziale, di casellario giudiziale europeo, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti" ed in particolare gli artt. 9, 11, 30, 31 e 32 nonché il Codice Antimafia d.lgs 159/2011;

VISTO il regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;

VISTO il decreto legislativo 30 giugno 2003, n. 196, come modificato dal decreto legislativo 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)".

VISTO il decreto legislativo 18 maggio 2018, n. 51, di "*Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche*

con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio", con particolare riferimento all'articolo 47 ("*Modalità di trattamento e flussi di dati da parte delle Forze di polizia*");

VISTO il decreto del Presidente della Repubblica 15 gennaio 2018, n. 15, recante "*Regolamento a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia"* e, in particolare, l'articolo 13, comma 1, in base al quale "*La comunicazione di dati personali a pubbliche amministrazioni o enti pubblici è consentita esclusivamente nei casi previsti da disposizioni di legge o di regolamento o, nel rispetto dei principi richiamati dall'articolo 4, quando è necessaria per l'adempimento di uno specifico compito istituzionale dell'organo, ufficio o comando e i dati personali sono necessari per lo svolgimento dei compiti istituzionali del ricevente*";

VISTA la legge 7 agosto 1990 n. 241 recante "*Nuove norme in materia di procedimenti amministrativi e di diritto di accesso ai documenti amministrativi*";

VISTO il decreto legislativo 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale);

VISTO il decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 (Disposizioni legislative in materia di documentazione amministrativa);

VISTA legge regionale Toscana del 19 novembre 1999, n. 60 (Agenzia Regionale Toscana per le Erogazioni in Agricoltura - ARTEA) istitutiva di ARTEA e in particolare l'art.5 "Affidamento di servizi e delega di funzioni";

VISTA la legge regionale Toscana del 9 febbraio 1998, n. 11 (Norme per lo snellimento e la semplificazione dell'attività amministrativa in materia di agricoltura, foreste, caccia e pesca);

VISTA la legge regionale Toscana 8 marzo 2000 n. 23 (Istituzione dell'anagrafe regionale delle aziende agricole, norme per la semplificazione dei procedimenti amministrativi ed altre norme in materia di agricoltura), relativa all'istituzione dell'Anagrafe regionale delle aziende agricole;

VISTA la legge regionale Toscana 27 luglio 2007, n. 45 (Norme in materia di imprenditore ed imprenditrice agricola e di impresa agricola);

VISTE le Circolari AGEA Coordinamento vigenti, contenenti le istruzioni per l'aggiornamento e la

conservazione del fascicolo aziendale e successive integrazioni e modifiche (ad oggi Circolare n. 210 del 20/04/2005, come integrata dalle successive Circolari del 2016 e del 2018);

VISTE le procedure per la costituzione ed aggiornamento del fascicolo aziendale nel Sistema Informativo di ARTEA e per la gestione della Dichiarazione Unica Aziendale (DUA) adottate con il decreto di ARTEA n. 70 del 30 giugno 2016;

VISTO il Manuale Operativo per il Riconoscimento dei Centri di Assistenza Agricola e per i Controlli delle Sedi Operative, approvato da Regione Toscana con decreto dirigenziale di Regione Toscana 18/12/2013, n. 5564 (Approvazione del Manuale operativo riconoscimento centri di assistenza agricola (CAA) e controlli strutture operative);

VISTO il regolamento di ARTEA per la disciplina del diritto di accesso documentale e civico approvato con decreto del Direttore ARTEA 12 gennaio 2023, n. 3 (Approvazione del regolamento per la disciplina del diritto di accesso documentale e civico);

VISTO il Manuale dell'Anagrafe ARTEA come pubblicato sul sito istituzionale di ARTEA;

VISTO lo standard ISO/IEC 27001:2013 che definisce i requisiti per impostare e gestire un Sistema di gestione della sicurezza delle informazioni e considerato che ARTEA ha conseguito la Certificazione ISO 27001 (Certificazione n. 2151.2019 del 17/12/2019 rilasciata da CISQ con scadenza 16/12/2022) relativamente al Sistema di Gestione della Sicurezza delle Informazioni, ai sensi delle disposizioni del regolamento delegato n. 907/2014 della Commissione Europea;

DATO atto che ARTEA sta perseguendo l'obiettivo della certificazione ISO 37001 sull'anticorruzione;

VISTI, quindi:
- il decreto del Direttore n.17 del 07/02/2023 che approva l'aggiornamento del documento "Data Protection Policy di ARTEA – modello Organizzativo" e modifica il decreto ARTEA n.136 del 22/10/2019;
- il decreto del sottoscritto dirigente n.26 del 24/02/2023 che approva la politica "Sistemi di gestione per la prevenzione della corruzione", pubblicato in Amministrazione Trasparente;
- il decreto del Direttore n. 27 del 03/03/2023 che approva la "Strategia per la prevenzione della corruzione" per l'anno 2023, quale allegato parte integrante e sostanziale del PIAO della Regione Toscana, approvato con delibera di Giunta Regionale n.299 del 27/03/2023;
- il decreto del sottoscritto dirigente n. 30 del 13/03/2023 che approva la Policy e l'autocertificazione

sul conflitto di interessi, rilevanti anche ai fini ISO 27001 e ISO 37001, alla quale sono vincolati anche i CAA;

- il decreto del sottoscritto dirigente n. 43 del 04/04/2023 che approva l'autocertificazione per i fornitori di ARTEA sui requisiti art. 80 d.lgs. 50/2016 ai fini ISO 37001, alla quale sono vincolati anche i CAA e relative società di servizi;
- il decreto del sottoscritto dirigente n. 85 del 26/07/2023 che fissa il termine del 30 settembre 2023 per la sottoscrizione della nuova dichiarazione sul conflitto di interessi approvata con il citato decreto n.30/2023;

CONSIDERATO che l'Agenzia, sulla base del riconoscimento della qualità di Organismo Pagatore ai sensi del regolamento delegato (UE) 2022/127 della Commissione, può delegare l'esecuzione dei compiti ad essa affidati eccezion fatta per il pagamento degli aiuti comunitari.

In caso di delega, come previsto nell'Allegato I al regolamento delegato (UE) 2022/127 della Commissione, devono essere soddisfatte le seguenti condizioni:

a) un accordo scritto tra l'organismo pagatore e tale organismo deve specificare, oltre ai compiti delegati, la natura delle informazioni e dei documenti giustificativi da presentare all'organismo pagatore, nonché i termini entro i quali devono essere forniti. L'accordo deve consentire all'organismo pagatore di rispettare i criteri per il riconoscimento;
b) l'organismo pagatore resta in ogni caso responsabile dell'efficace gestione dei fondi di cui trattasi; esso rimane l'unico responsabile della legittimità e regolarità delle operazioni sottostanti, compresa la tutela degli interessi finanziari dell'Unione, e ad esso compete dichiarare alla Commissione la spesa corrispondente e contabilizzarla;
c) le responsabilità e gli obblighi dell'altro organismo, segnatamente per il controllo e la verifica del rispetto della normativa dell'Unione, vanno chiaramente definiti;
d) l'organismo pagatore garantisce che l'organismo delegato dispone di sistemi efficaci per espletare in maniera soddisfacente i compiti che gli sono assegnati;
e) l'organismo delegato conferma esplicitamente all'organismo pagatore che espleta effettivamente i compiti suddetti e descrive i mezzi utilizzati;
f) l'organismo pagatore sottopone periodicamente a verifica i compiti delegati per accertarsi che l'operato dell'organismo sia di livello soddisfacente e conforme alla normativa dell'Unione.

CONSIDERATO che ai sensi dell'art. 2 del DM del 27 marzo 2008, il CAA può svolgere le attività delegate di servizio sulla base di apposite convenzioni stipulate con gli Organismi pagatori;

CONSIDERATO che i regolamenti comunitari in materia prescrivono l'istituzione di un Sistema

Integrato di Gestione e Controllo, comprendente, tra l'altro, una base dati informatizzata, nella quale devono essere registrati i dati desunti dalle domande di aiuto e dai controlli effettuati;

CONSIDERATO che il d.p.r. 503/1999 istituisce all'articolo 9 il fascicolo aziendale quale modello riepilogativo dei dati aziendali contenuti nel Sistema Integrato di Gestione e Controllo nonché strumento per l'aggiornamento dei dati presenti;

CONSIDERATO che l'aggiornamento del Sistema Integrato di Gestione e Controllo e in particolare del fascicolo aziendale, integrato con i dati dell'art. 66, regolamento (UE) 2021/2116, ai sensi dell'art. 13 del d.lgs. 99/2004, può essere effettuato, oltre che dai soggetti di cui all'art. 6 comma 1 lettera a) del d.p.r. 503/99, anche dai Centri di Assistenza Agricola sulla base di apposite convenzioni stipulate con gli organismi pagatori, in coerenza con quanto disposto dall'art. 2 del Decreto del Ministero delle politiche agricole, alimentari e forestali del 27 marzo 2008 e dall'art. 4 del Decreto Ministero delle politiche agricole, alimentari e forestali del 12 gennaio 2015 n. 162;

CONSIDERATO che l'Autorità di gestione per l'attuazione del Programma di Sviluppo Rurale e l'Agenzia, nell'esercizio delle proprie competenze, utilizzano le informazioni contenute nel fascicolo aziendale elettronico, istituito al fine di assicurare il processo di semplificazione amministrativa per il produttore e di certezza documentale dei pagamenti autorizzati;

CONSIDERATO che l'Agenzia, nell'ambito delle proprie competenze ed in accordo con gli atti di programmazione regionale e la normativa regionale, deve provvedere alla definizione delle procedure necessarie alla semplificazione amministrativa;

CONSIDERATO che l'Agenzia, nell'esercizio delle funzioni rese ai sensi della l.r. 23/2000, ha interesse ad integrare il fascicolo aziendale dei produttori che intendano presentare istanze e/o accedere ai benefici previsti dalla normativa comunitaria, nazionale e regionale con la documentazione necessaria a supporto delle procedure conformemente a quanto previsto dalla normativa di riferimento e dal Manuale dell'Anagrafe di ARTEA;

CONSIDERATO che l'Agenzia, nell'esercizio delle proprie competenze ed alla luce dell'esperienza maturata nel corso dell'ultimo trascorso periodo di operatività convenzionata con i CAA, ritiene che debba proseguire la delega ai CAA per la gestione del fascicolo aziendale e che debba essere rafforzata la celerità e la rapidità nella diffusione delle comunicazioni relative all'attività dell'Agenzia garantendo un adeguato livello operativo di raccordo verso le strutture periferiche dei CAA, laddove le stesse necessitino, per numero e/o dislocazione territoriale, di un adeguato coordinamento regionale;

CONSIDERATO che in Toscana il fascicolo aziendale è il presupposto per la presentazione delle istanze da parte del produttore - per esempio, alle procedure per la richiesta del carburante ad accisa agevolata (UMA), per l'ottenimento del requisito di imprenditore agricolo professionale (IAP), per l'avvio dell'attività agrituristica (relazione agrituristica) e per le richieste di documentazione in campo biologico (PAP) nonché per la notifica attività con il metodo biologico - ed elemento base per il controllo propedeutico al pagamento degli aiuti comunitari e nazionali, nonché per gli altri procedimenti di settore. Inoltre, il fascicolo aziendale contiene tutte le informazioni in forma alfanumerica e grafica concernenti la compagine e consistenza aziendale, richieste dalla normativa comunitaria e nazionale in materia di Sistema Integrato di Gestione e Controllo (SIGC) di cui al regolamento (UE) 2021/2116. Il fascicolo contiene altresì le informazioni di cuiall'art. 3, commi 1, 2 e 3 del decreto MiPAAF 12 gennaio 2015, n. 162, comprese quelle riferite al "Registro Nazionale Titoli" e agli albi a cui l'azienda può essere iscritta;

CONSIDERATO, altresì, che la Regione Toscana ha adottato la domanda grafica, già a partire dal 2016, per la totalità dei procedimenti a superficie inerenti alla PAC primo e secondo pilastro e per altri procedimenti regionali connessi (UMA, IAP, Biologico, relazione agrituristica, etc.) richiedendo ai CAA un impegno complesso per la diffusione e corretta gestione delle procedure di tenuta del fascicolo legate alla domanda grafica;

CONSIDERATO che, per quanto indicato al punto precedente, Regione Toscana intende destinare alla presente Convenzione risorse destinate ai CAA al fine anche di compensare l'impegno richiesto per lo svolgimento delle specifiche attività collegate al fascicolo e previste dalla Regione stessa;

Tutto ciò premesso si conviene e si stipula quanto segue:

Articolo 1
Premesse e definizioni

1. Le premesse sono parte integrante e sostanziale della presente Convenzione.
2. Ai fini della presente Convenzione, si intende per:

- *CAA:* il soggetto rispondente ai requisiti di cui al Decreto del Ministero delle Politiche Agricole Alimentari e Forestali del 27 marzo 2008 e riconosciuto con provvedimento della regione competente per territorio;
- *Fascicolo aziendale*: il fascicolo costituito ai sensi dell'art. 9 del DPR 503/1999 e descritto all'art. 3 del decreto MiPAAF del 12 gennaio 2015, n. 162;

- *Gestione del fascicolo aziendale:* la costituzione e l'aggiornamento del fascicolo aziendale che rappresenta riferimento obbligatorio per tutti i procedimenti inerenti il settore agricolo.
- *Sedi operativ*e: le sedi, riconosciute con provvedimento regionale della regione competente per territorio, ricadenti nell'ambito di competenza dell'Organismo Pagatore ARTEA per tipologia di aiuto e territorio, mediante le quali il CAA svolge le proprie attività. Presso le sedi operative sono istallate le apparecchiature occorrenti per l'espletamento dei compiti affidati al CAA con la presente Convenzione e dettagliati nelle circolari/istruzioni operative di campagna;
- *Strutture operative*: le sedi operative presso le quali sono disponibili gli archivi cartacei;
- *Sportelli*: le sedi operative presso cui non sono presenti gli archivi cartacei, ma che rispondono ai criteri individuati dal decreto MiPAAF del 27 marzo 2008;
- *Mandato*: mandato al CAA sottoscritto dal produttore, rilasciato ai sensi dell'art. 14 del decreto MiPAAF del 27 marzo 2008 e conforme al modello di cui all'Allegato 6 della presente Convenzione;
- *Delega*: delega scritta rilasciata dal produttore al CAA per le ulteriori attività che il CAA può svolgere ai sensi della normativa vigente, diverse da quelle oggetto della presente Convenzione;
- *Procedure*: circolari e istruzioni operative emanate da AGEA Coordinamento e da ARTEA in merito ai contenuti ed alle modalità di costituzione e aggiornamento del fascicolo;
- *CUDOC*: codice univoco rilasciato dal Sistema Informativo ARTEA che indentifica ogni documento inserito nel fascicolo aziendale.

Articolo 2
Oggetto della Convenzione e funzioni delegate ai CAA

1. Oggetto della presente Convenzione sono le funzioni di ARTEA delegate ai CAA oltre alle ulteriori disposizioni in materia di controlli, sanzioni, responsabilità.
2. Sono delegate ai CAA, ai sensi del regolamento (UE) n. 127/2022, le funzioni inerenti l'acquisizione delle informazioni per la costituzione e l'aggiornamento del fascicolo aziendale, la conservazione e la custodia dei fascicoli aziendali, i cui dati confluiscono nel Sistema Informativo ARTEA e di conseguenza nel Sistema Informativo Agricolo Nazionale gestito da AGEA (SIAN), nel rispetto delle disposizioni contenute nel decreto MiPAAF del 12 gennaio 2015, n. 162, nelle Circolari vigenti di AGEA Coordinamento in materia di fascicolo aziendale e titoli di conduzione delle superfici e nelle circolari/istruzioni operative di campagna definite da ARTEA e da AGEA Coordinamento.
3. Ai fini della presente Convenzione, quindi, ai CAA sono delegate in particolare le seguenti attività:
   a) l'identificazione univoca del produttore mandante, ai fini del pieno rispetto del paragrafo 1,

lettera d), dell'articolo 66 del regolamento (UE) 2021/2116;

b) l'acquisizione della documentazione idonea, conformemente ai manuali procedimentali pubblicati nel Sistema Informativo ARTEA ed alle circolari AGEA, ad attestare l'esistenza di titoli di conduzione dei terreni dell'azienda per quanto riguarda le aziende agricole. Per i soggetti diversi dagli agricoltori, viene costituito un fascicolo semplificato il cui contenuto informativo e documentale obbligatorio è limitato alle informazioni anagrafiche e, ove pertinenti ai procedimenti attivati, le informazioni riferite alle lettere di cui al comma 2 dell'articolo 3 del DM 162 del 2015, a seconda del soggetto richiedente e dei procedimenti attivati;
c) l'eventuale acquisizione delle istanze delle aziende con riferimento alle quali il CAA detiene il fascicolo aziendale e che le aziende intendono presentare per il tramite del CAA medesimo. Nello svolgimento di tale operatività il CAA non svolge alcuna attività di valutazione amministrativa. Il CAA inserisce nel Sistema Informativo i dati forniti dalla azienda al fine della presentazione delle istanze sulla base delle istruzioni e circolari fornite da ARTEA previa identificazione del firmatario;
d) la custodia presso le sedi operative della documentazione acquisita nel fascicolo, in originale o in copia a seconda della natura del documento;
e) la verifica della presenza, della completezza e conformità formale dei documenti da inserire nei fascicoli dei produttori, nonché la perfetta rispondenza dei dati registrati in Anagrafe ARTEA rispetto a quelli risultanti dai documenti cartacei acquisiti nel fascicolo, in conformità a quanto prescritto dalla normativa comunitaria, nazionale, regionale nonché dai relativi manuali procedimentali pubblicati nel Sistema Informativo ARTEA ed alle circolari AGEA;
f) il trattamento delle anomalie di domande e dichiarazioni risultanti dai controlli effettuati e riferibili al mancato aggiornamento dei documenti contenuti nel fascicolo aziendale;
g) l'interfaccia verso l'azienda mandataria per approfondimenti e verifiche, attinenti il contenuto del fascicolo, e inerenti procedimenti istruttori di competenza di ARTEA o di altri Enti;
h) l'aggiornamento del fascicolo con le informazioni rese dai titolari dei fascicoli e necessarie per la sua completezza.

4. I CAA hanno la responsabilità dell'identificazione del produttore e dell'accertamento del titolo di conduzione dell'azienda, della corretta immissione dei dati, del rispetto per quanto di competenza delle disposizioni della normativa dell'Unione europea applicabile, nonché la facoltà di accedere alle banche dati del SIAN, secondo le modalità previste a tale scopo. Il trattamento dei dati relativi ai propri utenti che abbiano rilasciato delega espressa in tal senso avviene nel rispetto della normativa nazionale e dell'Unione europea in materia di protezione dei dati personali.

5. L'Agenzia si riserva la facoltà di affidare al CAA ulteriori attività in relazione a funzioni proprie o ad

essa delegate da altre amministrazioni. L'eventuale ulteriore affidamento è oggetto di un atto integrativo della presente Convenzione con il quale saranno stabilite le ulteriori risorse da destinare.
6. È esclusa dall'applicazione della presente Convenzione ogni altra attività, anche di assistenza alla presentazione delle domande/istanze di aiuto, non oggetto della presente delega e qui non espressamente regolata, che il CAA svolge in autonomia in favore delle aziende, sulla base della normativa vigente.
7. Il CAA, nel rispetto del principio di separazione tra funzioni delegate e funzioni non delegate, garantisce autonomia di gestione tra le suddette funzioni.

Art. 2 bis
(Supporto rendicontazione misure PSR Investimenti Enti)

1. Ai sensi dell'art. 2 comma 5 della presente Convenzione, nella Programmazione 2023/2025 ARTEA delega ai CAA l'attività di supporto volta ad agevolare la rendicontazione delle misure PSR Investimenti Enti, in accordo con Anci Toscana.
2. Per tale attività di sperimentazione relativa al 2022, sono state riconosciute risorse aggiuntive in virtù della delibera di Giunta n. 898 del 01/08/2022 e del successivo decreto n. 16463 del 12/08/2022 ed è stato conseguentemente stipulato apposito Accordo Integrativo della Convenzione;
3. Per la Programmazione 2023/2025 si rimanda agli appositi accordi integrativi per la definizione delle modalità operative, previa definizione delle risorse dedicate da parte della Giunta.

Articolo 3
Obblighi del CAA

1. Per lo svolgimento delle attività delegate di cui all'articolo 2, il CAA garantisce il perdurante possesso dei requisiti minimi di garanzia, di funzionamento ed i requisiti soggettivi e oggettivi così come stabiliti dal D.M. 27 marzo 2008 e ss.mm. e dalle norme europee, interne e regionali vigenti. Salva ogni ulteriore responsabilità ed onere ascrivibili ai CAA, la carenza dei requisiti accertata a norma della presente Convenzione, o anche di uno solo dei suddetti requisiti, comporta la risoluzione della presente Convenzione, ai sensi dell'art. 1456 c.c. L'accertata perdita dei requisiti minimi di garanzia e funzionamento comporta, altresì, l'attivazione della procedura di revoca dell'autorizzazione, ai sensi dell'art. 11 del D.M. 27 marzo 2008, della presente Convenzione e del Manuale Operativo.
2. Ai fini dell'adempimento delle sole funzioni oggetto della presente Convenzione, il CAA assicura che dette funzioni siano svolte in maniera autonoma e distinta rispetto alle altre funzioni proprie del CAA non oggetto della presente delega, in modo da consentire ad ARTEA un controllo diretto sulle

funzioni delegate, senza rischio di interferenza. A tal fine il CAA dedica alle funzioni delegate locali, attrezzature e risorse specificamente individuate e controllabili ai sensi dell'art. 11 del DM 27.3.2008.

3. Il CAA si impegna, altresì, ad operare in conformità al d.lgs. n. 74/2018, al Regolamento delegato (UE) n. 127/2022, al D.M. 27 marzo 2008, al Regolamento (UE) 679/2016, ai manuali procedimentali specifici pubblicati nel Sistema Operativo ARTEA, alle Circolari AGEA, al Manuale Operativo per il Riconoscimento dei Centri di Assistenza Agricole e per i Controlli delle Sedi Operative approvato con Decreto della Regione Toscana, al vigente Codice di Comportamento dei dipendenti regionali, per quanto applicabile, nonché alla certificazione ISO 27001 e a quanto richiesto per l'acquisizione della certificazione ISO 37001 da parte di ARTEA;

4. In particolare, i CAA hanno la responsabilità dell'identificazione del produttore e dell'accertamento del titolo di conduzione dell'azienda – conformemente a quanto indicato dalla normativa vigente e dalle circolari applicabili - della corretta immissione dei dati, del rispetto per quanto di competenza delle disposizioni della normativa dell'Unione europea applicabile, nonché la facoltà di accedere alle banche dati del SIAN, secondo le modalità previste a tale scopo.

5. Il CAA assicura il rispetto dei requisiti obbligatori inerenti all'organizzazione, la gestione del personale e la tenuta e gestione dei fascicoli.

6. Il CAA riconosce che la sottoscrizione della presente Convenzione costituisce accettazione espressa della delega di funzioni rilasciata da ARTEA per lo svolgimento dei compiti di cui all'art. 2, confermando esplicitamente ad ARTEA di essere in grado di espletare i compiti connessi ad esso delegati, ai sensi dell'Allegato I al Reg. (UE) 127/2022. A tal fine con la relazione annuale di cui al successivo art. 4 il CAA descrive i mezzi utilizzati ed il personale destinato allo svolgimento delle funzioni delegate con la presente Convenzione. La mancata ottemperanza al disposto del comma 1 comporta la responsabilità del CAA ai fini di quanto stabilito al successivo articolo 17.

7. Il CAA si impegna inoltre ad inviare la "Relazione annuale" e la certificazione di bilancio ovvero le risultanze dell'audit interno di cui all'art. 11 comma 4 lettera d) del decreto ministeriale MiPAAF 27 marzo 2008.

8. In presenza di richieste di accesso agli atti documentale e civico presentate presso le proprie sedi operative, il CAA si impegna a trasmetterle tempestivamente per PEC ad ARTEA per consentire all'Agenzia di rispondere nel rispetto dei termini previsti dalla normativa. Di tale trasmissione è data comunicazione all'interessato. Nel caso in cui l'Agenzia sia condannata al risarcimento di danni per il mancato rispetto dei termini e nel caso in cui il ritardo sia imputabile all'inerzia del CAA nella trasmissione dell'istanza, ARTEA si rivarrà sulla garanzia fidejussoria di cui al successivo art. 24.

Articolo 4
Monitoraggio e reporting obbligatorio dei CAA

1. Il CAA si impegna altresì ad inviare, oltre ad eventuali relazioni periodiche richieste, la "Relazione annuale", conformemente allo schema fornito da ARTEA, firmata digitalmente dal rappresentante legale del CAA e inoltrata tramite PEC entro il 30 aprile dell'anno successivo a quello di riferimento, nella quale specifica le risorse umane e strumentali destinate espressamente e specificamente, nel rispetto dell'art. 2 comma 7 della Convenzione, all'esercizio delle funzioni delegate. Inoltre, ai fini del mantenimento dei requisiti di riconoscimento, il CAA si impegna a inoltrare all'Agenzia, entro il 31 dicembre dell'anno successivo a quello di riferimento, la certificazione di bilancio ovvero le risultanze dell'audit ai sensi dell'art. 11 comma 4 lettera d) del decreto ministeriale MiPAAF 27 marzo 2008.
2. La violazione degli obblighi previsti al primo comma - relativamente all'invio della "Relazione annuale" e della certificazione di bilancio ovvero delle risultanze dell'audit - fa sorgere la responsabilità del CAA ai sensi dell'art. 17 della presente Convenzione.

Articolo 5
Società di servizi e strutture periferiche del CAA

1. Il CAA ha facoltà di espletare gli adempimenti previsti nella presente Convenzione sia direttamente sia tramite le proprie società di servizi ai sensi dell'art. 12 del decreto MiPAAF 27 marzo 2008. Tutti i requisiti, le condizioni, gli obblighi e i controlli applicabili ai CAA sulla base delle norme vigenti e della presente Convenzione, si applicano anche alle rispettive società di servizi.
2. Nel caso in cui il CAA si avvalga di società di servizi, al momento della sottoscrizione della presente Convenzione, il CAA comunica ad ARTEA l'elenco delle società che opereranno sul territorio toscano.
3. Attraverso le sue strutture centrali e/o periferiche, il CAA assicura il coordinamento di tutte le strutture operative afferenti al CAA e garantisce la diffusione celere e capillare delle comunicazioni e delle indicazioni operative, sollevando l'Agenzia dall'onere di svolgere comunicazioni dirette alle singole strutture.
4. I responsabili individuati e nominati ai sensi dell'art. 25 della presente Convenzione devono garantire:
   a) la propria presenza alle riunioni di informazione e coordinamento previste dall'Agenzia;
   b) l'attività di diffusione coordinata a tutte le strutture operative afferenti al CAA delle indicazioni emanate dall'Agenzia;
   c) gli adempimenti, all'interno delle proprie strutture operative, di cui all'art. 7, 22 e 23 della presente Convenzione e il coordinamento del personale a tal fine.
5. Ai fini della presente Convenzione, la responsabilità delle attività svolte dalle società di servizi

rimane interamente a carico del CAA.

Articolo 6

Tenuta del fascicolo aziendale

1. Il fascicolo può essere costituito da documenti cartacei opportunamente registrati ed archiviati e/o da documenti digitali registrati e archiviati nell'Anagrafe ARTEA. Ogni nuovo documento inserito in fascicolo deve essere scansionato e inserito nel corrispondente ID del fascicolo digitale. A tal fine per ogni ID facente parte del fascicolo è predisposta la scansione obbligatoria quale requisito essenziale per la creazione e la certificazione del documento.

2. I documenti da conservare obbligatoriamente in cartaceo e in originale sono tutti i documenti depositati presso il CAA che per loro natura devono essere acquisiti in originale, come ad esempio le dichiarazioni rilasciate ai sensi degli articoli 46 e 47 del D.P.R 445/2000.

3. Il CAA si impegna a costituire, aggiornare, conservare e custodire presso le proprie strutture operative il fascicolo aziendale secondo le modalità previste dal Manuale dell'Anagrafe di ARTEA, dai manuali procedimentali pubblicati nel Sistema Informativo ARTEA e dalle circolari AGEA vigenti, dal successivo articolo 22 in merito al trattamento dei dati personali e conformemente alle indicazioni contenute nella DPA di cui all'Allegato 1.

Articolo 7
Codici di comportamento e gestione conflitti di interessi

1. Ai sensi dell'art. 2 del D.P.R. n. 62/2013 (Codice di comportamento dei dipendenti pubblici) e dell'art. 2 del Codice di comportamento dei dipendenti di Regione Toscana (D.G.R. n. 978/2019 e successive modifiche), tali codici di comportamento si applicano – per quanto compatibili – ai CAA ed a tutti i loro dipendenti, amministratori, sindaci e a tutti i loro collaboratori o consulenti, con qualsiasi tipologia di contratto o incarico.
2. Salve le specifiche responsabilità anche disciplinari previste dai contratti collettivi ed individuali di lavoro, la violazione degli obblighi derivanti dai codici di comportamento indicati nel primo comma e di quelli posti dal presente articolo comporta, ove siano accertate responsabilità ascrivibili al CAA stesso o alle società di servizi di cui si avvale, la risoluzione della presente Convenzione, ai sensi di quanto previsto dall'art. 2, secondo comma, Codice di comportamento dei dipendenti di Regione Toscana e dall'art. 2, comma terzo, del D.P.R. 62/2013.
3. In particolare, i CAA sono tenuti al rispetto rigoroso delle norme in materia di prevenzione dei

conflitti di interessi (attuale e anche meramente potenziale) e di obbligo di astensione, così come definiti dagli artt. 6 e 7 del Codice di comportamento dei dipendenti di Regione Toscana e dagli art. 6 e 7 del D.P.R. 62/2013, nonché dalle norme europee, segnatamente dall'articolo 61 del Regolamento (UE, Euratom) 2018/1046 e dal Reg. (UE) 127/2022.

4. A tale fine i CAA devono rispettare la Policy di ARTEA e compilare ogni anno nel rispetto del termine assegnato l'autocertificazione di cui al Decreto dirigenziale di ARTEA n. 30/2023 tramite il Sistema Informativo.

5. Oltre alle situazioni di cui all'art. 7 del Codice di comportamento dei dipendenti di Regione Toscana, costituiscono altresì situazioni di conflitto di interessi:

a. l'eventuale adesione ad associazioni e ad altre organizzazioni i cui interessi siano coinvolti dallo svolgimento delle attività istituzionale dell'Agenzia, esclusi i partiti politici;
b. le eventuali partecipazioni finanziarie e patrimoniali che possano porre il personale del CAA in situazioni di conflitto di interesse con la funzione svolta presso il CAA;
c. l'aver intrattenuto negli ultimi tre anni prima dell'inizio del rapporto di lavoro con il CAA rapporti diretti o indiretti di collaborazione o consulenza, comunque denominati ed in qualunque modo retribuiti con aziende agricole mandanti del CAA;
d. l'aver concluso accordi o negozi ovvero stipulato contratti a titolo privato o per conto dell'amministrazione, con aziende agricole mandanti del CAA

6. Il CAA si impegna a portare a conoscenza di tutto il personale impiegato nell'espletamento dell'attività di cui alla presente Convenzione l'obbligo di attenersi al Codice di Comportamento dei dipendenti regionali e l'obbligo di astensione, conseguente ad ogni dichiarazione di presenza di conflitto di interessi attuale o potenziale. Il CAA informa tutto il personale in ordine agli obblighi di dichiarazione di conflitti di interessi, con particolare attenzione alla relativa segnalazione – da effettuarsi tramite l'apposita procedura predisposta sul Sistema Informativo di ARTEA – resa almeno una volta all'anno e da rinnovare tempestivamente ogniqualvolta il personale si trovi in una nuova condizione di confitto di interessi.

7. Ai fini del coordinamento e della formazione in materia di conflitto di interessi ai sensi dell'art. 25, nonché del rispetto delle procedure adottate da ARTEA per la gestione e monitoraggio del conflitto di interesse, il CAA nomina il proprio responsabile del conflitto di interessi e lo comunica tempestivamente ad ARTEA. Il responsabile del conflitto di interessi utilizza tutti gli strumenti messi a disposizione da ARTEA, inclusi quelli informatici, per il monitoraggio, il coordinamento e la gestione del conflitto di interessi e delle relative dichiarazioni obbligatorie.

Articolo 8
Mandato

1. Ai fini della costituzione, custodia, aggiornamento e gestione del fascicolo aziendale, il CAA opera sulla base di un mandato sottoscritto dal produttore, rilasciato ai sensi dell'art. 14 del decreto MIPAAF 27 marzo 2008. Il mandato deve essere conforme al modello di cui all'Allegato 6 della presente Convenzione e deve essere provvisto di data di sottoscrizione, indicazione della durata e corredato di valido documento di riconoscimento.

2. Il CAA provvede alla registrazione nel Sistema Informativo ARTEA del mandato, secondo le istruzioni fornite da ARTEA.

3. Il mandato è valido fino alla sottoscrizione di un nuovo mandato presso un altro CAA. La sottoscrizione di un nuovo mandato comporta la revoca automatica del precedente. Le modalità di notifica della revoca al CAA precedente sono stabilite nelle procedure fornite da ARTEA.

4. In caso di registrazione di un nuovo mandato conferito ad altro CAA, il CAA mandatario precedente garantisce, su richiesta scritta del produttore, la restituzione del fascicolo, ad esclusione del mandato che rimane in originale presso il CAA, al produttore stesso o ad un suo procuratore speciale con procura notarile, entro 30 giorni dalla comunicazione inviata tramite PEC o raccomandata A/R , avendo cura di trattenere copia di tutta la documentazione in esso contenuta, fermo restando l'immutata validità probatoria delle informazioni certificate risultanti nel Sistema Informativo e contenute nel fascicolo elettronico.

5. Il CAA mandatario non è responsabile dell'inserimento di titoli di conduzione da parte del CAA precedente ancorché i suddetti titoli siano in corso di validità al momento della presa in carico del fascicolo. Resta tuttavia l'obbligo per il nuovo CAA mandatario di verificare tempestivamente la conformità formale e l'idoneità della documentazione contenuta nel fascicolo predisposto dal CAA precedente, che, al momento dell'acquisizione del mandato, sia ancora funzionale allo svolgimento dei procedimenti di qualsiasi natura con le Pubbliche Amministrazioni.

6. Il CAA non ha facoltà di recedere dal mandato del produttore, salvo nel caso in cui il produttore abbia tenuto comportamenti manifestamente non corretti, minando il rapporto di fiducia necessario con CAA mandatario.

7. Nei casi in cui il mandato venga revocato, sono inibite al CAA nel sistema di ARTEA le funzioni di aggiornamento del fascicolo aziendale. Rimane salva le facoltà di consultazione del fascicolo.

Articolo 9
Attività del CAA ulteriore e diversa dalle funzioni delegate, esclusa dalla presente Convenzione

1. Le altre attività, ulteriori e diverse dalle funzioni delegate di cui all'art. 2, svolte dal CAA in favore delle Aziende ed escluse perciò dall'applicazione della presente Convenzione ai sensi dell'art. 2, sono regolate tramite delega ai sensi dell'art 1, ovvero un apposito atto distinto dal mandato di cui al precedente art. 8 stipulato fra il CAA mandatario ed il mandante per lo svolgimento delle attività delegate da ARTEA ai CAA sulla base della Convenzione vigente.
2. È comunque riconosciuto al CAA l'accesso al Sistema Informativo dell'Agenzia per lo svolgimento di ulteriori attività, ai sensi della normativa vigente, per le quali sia funzionale l'accesso al Sistema Informativo e previa acquisizione di specifica delega da parte dell'azienda.

Articolo 10
Requisiti di capacità operativa

1. Dal momento della sottoscrizione della presente Convenzione, e per tutta la durata della stessa, i CAA devono possedere, mantenere e garantire i requisiti di capacità operativa, di sicurezza nella gestione, di qualità del servizio, così come definiti nell'Allegato A del Manuale operativo riconoscimento e controlli sedi CAA dei controlli approvato dalla Regione.

Articolo 11
Responsabilità ed obblighi di ARTEA

1. L'Agenzia si impegna per sé e per le proprie strutture operative:

a) a mettere a disposizione, in tempo utile, tutta la manualistica e le disposizioni attuative che i CAA devono osservare nell'attività di loro competenza;
b) a garantire, in tempo utile, l'attività di formazione ed informazione necessaria per migliorare e standardizzare l'esercizio delle attività affidate ai CAA;
c) a mettere tempestivamente a disposizione del CAA i dati delle domande o le informazioni riferite alle dichiarazioni, presenti nelle proprie banche dati e relative ai beneficiari di cui il CAA è mandatario, per i soli fini di cui alla presente Convenzione;
d) a mettere a disposizione del CAA strumenti di verifica e controllo sul lavoro eseguito per le funzioni previste dalla presente Convenzione.

2. L'Agenzia assicura l'efficienza del proprio Sistema Informativo. Al CAA non potrà essere imputata alcuna responsabilità per gli accertati ritardi e/o errori derivanti da interruzioni e/o disfunzioni del servizio erogato dal sistema stesso.

3. L'Agenzia individua sin d'ora quale interfaccia operativo per il fascicolo elettronico, il responsabile del Settore competente sul Sistema Informativo di ARTEA.

4. L'Agenzia si riserva di predisporre le necessarie integrazioni e/o modificazioni ai propri manuali che si rendessero necessarie e di darne tempestivo avviso al CAA, che si impegna ad osservarle.

5. L'Agenzia assicura il corretto flusso informativo sull'iter e sullo stato delle domande e delle istanze presentate al CAA mandatario e all'utente stesso o suo delegato.

Articolo 12
Corrispettivi

1. Verrà riconosciuto al CAA un corrispettivo per le seguenti attività:

a) tenuta del fascicolo aziendale ai sensi del precedente art. 6;

b) attività di coordinamento ai sensi del precedente art. 5;

c) specifiche attività connesse ad altri procedimenti regionali (UMA, IAP, Biologico, relazione agrituristica, etc.).

2. Per le eventuali ulteriori attività affidate al CAA, di cui all'art. 2 comma 5, queste saranno oggetto di apposito atto integrativo alla Convenzione contenente la descrizione delle attività stesse, delle procedure e dei corrispettivi.

3. Per la tenuta del fascicolo aziendale l'importo verrà erogato per ogni fascicolo gestito, validato e del quale è riconoscibile l'azienda mandante. Si precisa che per "fascicolo gestito, validato e del quale è riconoscibile l'azienda mandante" si intende:

- fascicolo gestito = il fascicolo deve essere stato movimentato (quindi deve essere presente almeno una domanda o un'istanza) nel corso dell'anno di riferimento delcompenso erogato;
- fascicolo validato = il fascicolo risulta validato quando è presente almeno una scheda di validazione (piano colturale grafico) nel corso dell'anno di riferimento.
- fascicolo del quale è riconoscibile l'azienda mandante = nel fascicolo informatico deve essere obbligatoriamente compilato l'ID 6. In assenza di questo requisito il fascicolo non verrà conteggiato.

4. Il corrispettivo per l'attività di coordinamento di cui all'art. 5 è riconosciuto neicasi ove la gestione annuale dell'attività sul territorio toscano si riferisca:

- ad un numero dei fascicoli superiore a 1.000;
- al coordinamento di unità di personale superiore a 15;
- ad una presenza territoriale delle strutture operative su almeno i 2/3 delle province toscane (7 province su 10).

Articolo 13
Definizione risorse

1. La definizione delle risorse per l'erogazione dei compensi viene definita annualmente. Tale definizione viene formalizzata con un atto integrativo della presente Convenzione efa riferimento:

a) alle risorse regionali, da determinare tutti gli anni entro il 31 gennaio, così articolate:

- importo per i fascicoli e ettari grafici;
- importo per le attività di coordinamento per i CAA che gestiscono un numero rilevante di fascicoli e siano diffusi sul territorio regionale, secondo i criteri di cui al precedente art. 12 comma 4;
- eventuale importo a fascicolo per compensare la specificità delle attività regionali di cui all'art. 12 comma 1 lett. C) e la digitalizzazione dei fascicoli di cui all'art. 6 comma 3 della presente Convenzione;
- importo per le ulteriori funzioni delegate di cui all'art. 2 comma 5, ivi comprese quelle di cui all'art. 2 bis, della presente Convenzione;

b) all'eventuale trasferimento della quota riconosciuta da AGEA, se prevista, per l'annualità interessata coni criteri definiti dalla stessa a livello nazionale;

2. In ogni caso, l'erogazione dei corrispettivi dovuti annualmente è subordinata all'effettivo trasferimento dei fondi ad ARTEA da parte di Regione Toscana e da parte di AGEA coordinamento, se previsti.

3. L'erogazione dei corrispettivi avverrà presuntivamente entro il 31 marzo dell'anno successivo quello di riferimento e in ogni caso non prima dell'effettivo trasferimento dei fondi ad ARTEA da parte dei soggetti di cui al comma precedente. Entro 60 gg dalla data di trasferimento delle risorse da parte di Regione Toscana e/o da parte di AGEA se previste, ARTEA provvede ad adottare il decreto di accertamento delle somme spettanti al CAA, sulla base del quale il CAA potrà emettere fattura.

Entro la scadenza del 30 settembre di ogni anno, potranno essere liquidate nell'anno di riferimento fino a due anticipazioni, non superiori comunque all' 80% del contributo complessivo in riferimento al dato storico dell'anno precedente.

4. I pagamenti conseguenti all'attuazione della presente convenzione, anche a seguito di contenzioso giurisdizionale o arbitrale, verranno effettuati entro 60 giorni dalla data di ricevimento della fattura. Ogni ritardo da parte del soggetto obbligato, che ecceda i termini sopra indicati, darà luogo automaticamente al pagamento di interessi di cui all'art. 1284, comma 1, c.c.

Articolo 14
Risorse finanziarie anno 2023

1. Per l'anno 2023 la quantificazione delle risorse finanziarie necessarie per il riconoscimento dei corrispettivi delle attività di cui al precedente articolo, viene così definita:

a) quota regionale per i fascicoli validi ai sensi dell'art. 12 comma 3 della presente Convenzione pari a Euro 10,00 a fascicolo;

b) quota regionale per ettari grafici collegati ai fascicoli riconosciuti;

c) eventuali risorse per le ulteriori funzioni delegate di cui all'art. 2 comma 5, ivi comprese quelle di cui all'art. 2 bis, della presente Convenzione;

d) eventuali importi riconosciuti da AGEA ad ARTEA stanziati per l'anno 2023, secondo i criteri di ripartizione adottati da AGEA;

e) riconoscimento regionale per le attività di cui all'art. 5, secondo i requisiti di cui all'art. 12 comma 4, pari a Euro 40.260,00 IVA inclusa e di un ulteriore 40%, per un totale di Euro 56.364,00 IVA inclusa, in presenza di un numero di fascicoli superiore a 10.000, coordinamento di unità di personale superiore a 20 e presenza territoriale delle strutture operative su almeno il 90% delle province toscane (9 su 10);

2. Alle attività di cui al precedente comma 1 lettere a) b), c) e e) viene destinato un importo complessivo individuato annualmente dalla Regione Toscana.

3. A tale importo concorrono:

- i residui delle precedenti convenzioni AGEA-ARTEA, presenti nella disponibilità del bilancio ARTEA se presenti;
- le risorse rese disponibili da Regione Toscana sul proprio bilancio.

4. Il totale erogato per le attività di cui ai punti a), b), c) e e) non può in nessun caso superare l'importo di cui al precedente punto 2;

5. Il totale delle risorse destinato a compensare il precedente punto 1 lettera b) è definito dal totale delle risorse rimanenti dopo aver individuato gli importi destinati ai punti a), c) e e);

6. Gli importi destinati al precedente comma 1 lettera c) verranno distribuiti in base a criteri definiti con uno specifico atto integrativo della presente Convenzione.

Articolo 15
Controlli e sanzioni

1. Il CAA prende atto che le sedi operative ed i fascicoli dei produttori mandanti, intestatari di un

fascicolo aziendale e/o richiedenti benefici, sono soggetti ai controlli amministrativi ed in loco disposti dalle diverse istituzioni e servizi dell'Unione Europea, dal MASAF, dall'Organismo di Certificazione designato ai sensi dell'articolo 12 del regolamento (UE) 2021/2116, dalle Regioni e Province autonome, dall'Organismo di Coordinamento e dagli Organismi pagatori in applicazione del SIGC, nonché da altri enti e società delegate al controllo da parte degli organismo sopracitati in applicazione della normativa comunitaria, nazionale e regionale vigente.

2. L'attività di controllo predisposta da ARTEA e da Regione Toscana si svolge secondo le indicazioni fornite dalla presente Convenzione e dal Manuale Operativo per il Riconoscimento dei Centri di Assistenza Agricola e Controlli Strutture Operative.

3. L'Agenzia sottopone al controllo:

a. la documentazione relativa al Fascicolo, utilizzando la check list presenti nel Manuale Operativo per il Riconoscimento dei Centri di Assistenza Agricola e per i Controlli delle Sedi Operative;
b. le procedure operative di svolgimento dei compiti;
c. il mantenimento dei requisiti previsti dalla normativa vigente nonché dalla presente Convenzione e dal Manuale Operativo per il Riconoscimento dei Centri di Assistenza Agricola e Controlli Strutture Operative utilizzando la check list presenti nel Manuale Operativo per il Riconoscimento dei Centri di Assistenza Agricola e per i Controlli delle Sedi Operative;
d. ogni quant'altro specifico compito che il CAA è tenuto a svolgere in attuazione dell'articolo 2.

4. Per i procedimenti di controllo amministrativo ordinario, sono stabiliti i seguenti presupposti:

a. il procedimento di controllo è stabilito dal Manuale Operativo per il Riconoscimento dei Centri di Assistenza Agricola e Controlli Strutture Operative, riconosciuto con decreto dirigenziale di Regione Toscana;
b. il controllo viene effettuato su un campione di sedi operative individuate secondo i criteri stabiliti nel predetto Manuale;
c. il controllo deve essere effettuato su un numero rappresentativo di fascicoli movimentati dalla sede operativa del CAA;
d. il procedimento di controllo deve perfezionarsi entro l'anno successivo a quello di riferimento;

il procedimento di controllo ha per oggetto sia il riscontro di irregolarità nel fascicolo aziendale, come definite nelle circolari, anche in considerazione delle conseguenze che ne siano derivate, sia il mantenimento dei requisiti organizzativi e di funzionamento delle sedi operative del CAA indicati nella presente Convenzione e nel Manuale Operativo per il Riconoscimento dei Centri di Assistenza Agricola e Controlli Strutture Operative e nella normativa vigente.

5. In ogni caso, ARTEA conserva la facoltà di sottoporre a controllo puntuale ed estemporaneo le sedi

dei CAA ogniqualvolta sussistano fondati motivi, fattori di rischio o indizi di irregolarità in ordine ai compiti affidati ai CAA dalla presente Convenzione o al possesso da parte dei CAA dei requisiti soggettivi, oggettivi e di garanzia previsti per i CAA dalle norme interne ed europee vigenti. Tali controlli possono avvenire in ogni momento ed anche in riferimento ad annualità pregresse e le eventuali anomalie verranno gestite secondo le indicazioni fornite in sede di controllo.

6. Le situazioni di conflitto emerse da tali comunicazioni possono essere considerate fattori di rischio significativi per l'individuazione delle aziende soggette a controllo ovvero per stabilire da parte dell'Agenzia specifiche prescrizioni.

7. ARTEA informa tempestivamente la Regione quando - all'esito dei controlli di cui al presente articolo - emerga il mancato possesso anche di uno solo dei requisiti di cui al D.M. del 27 marzo 2008, inclusi i requisiti soggettivi, oggettivi e di garanzia, nonché dei requisiti previsti nella presente Convenzione e nel Manuale Operativo per il Riconoscimento dei Centri di Assistenza Agricola e Controlli Strutture Operative.

8. È riconosciuta ad ARTEA la facoltà di diffidare il CAA a regolarizzare la posizione della sede operativa interessata entro il termine di 30 giorni. Per il superamento delle anomalie sanabili in merito al fascicolo, il CAA aggiorna i documenti forniti dall'azienda.

9. ARTEA non riconoscerà al CAA il corrispettivo di cui al precedente articolo 12 comma 1 lett. a) per la gestione dei fascicoli che presentano almeno una irregolarità al momento del controllo, imputabile al CAA stesso. L'esclusione dal riconoscimento del corrispettivo con riferimento agli anni in cui è stata riscontrata la/le irregolarità in sede di controllo avviene anche nel caso in cui le anomalie vengano sanate. Nel caso in cui le anomalie imputabili al CAA e riscontrate al momento del controllo non siano sanate nei 30 giorni successivi all'invio dell'esito del controllo, i fascicoli irregolari verranno esclusi dai corrispettivi anche degli anni successivi quello di riferimento del controllo fino alla risoluzione delle anomalie, comunicata dal CAA al personale addetto controlli tramite e-mail.

10. In caso di mancata regolarizzazione nei termini suddetti è riconosciuta ad ARTEA la facoltà di inibire l'attività della sede operativa interessata, conformemente a quanto disposto dalle norme vigenti, esclusivamente nel caso le anomalie siano imputabili al CAA e non siano risolvibili.

11. Salve le eventuali o ulteriori responsabilità ai sensi della presente Convenzione e delle norme vigenti, qualora all'esito dei controlli effettuati ai sensi del presente articolo sia riscontrata la violazione delle obbligazioni di cui alla presente Convenzione ovvero ai manuali procedimentali pubblicati nel Sistema Informativo ARTEA ed alle circolari AGEA, saranno altresì applicate le sanzioni previste dall'Allegato 2, secondo le relative modalità operative. In particolare, qualora in base ai controlli effettuati sull'archivio dei documenti sia riscontrata la mancata corrispondenza tra i dati del Sistema

Informativo, la documentazione archiviata e quella elencata nelle domande o dichiarazioni delle aziende e tali anomalie siano imputabili al CAA, anche con effetti incidenti sul calcolo del premio/contributo richiesto, saranno applicate le sanzioni previste dall'Allegato 2.

Articolo 16
Risoluzione espressa e revoca

1. Nel caso in cui, a seguito dell'attività di vigilanza di cui all'art. 11 del DM 27 marzo 2008 e dei controlli effettuati da ARTEA a norma della presente Convenzione venga riscontrata in capo al CAA e/o alle società di cui esso si avvale la carenza dei requisiti di cui agli artt. 7 e 8 del DM 27 marzo 2008, si dispone la risoluzione della presente Convenzione, ai sensi dell'art. 2, comma 3, del DM 27 marzo 2008.

2. L'ente vigilante può altresì revocare l'autorizzazione precedentemente concessa al CAA in tutte le seguenti ipotesi:

a) perdita totale o parziale dei requisiti minimi di garanzia e funzionamento stabiliti dalle norme vigenti;
b) qualora nello svolgimento dell'attività affidata vengano commesse gravi e ripetute violazioni alle disposizioni previste dalla normativa comunitaria, nazionale e regionale;
c) quando non siano osservati le prescrizioni e gli obblighi posti dalla Convenzione presente;
d) quando non sussistano i requisiti oggettivi di cui all'art. 3 e dell'art. 10;
e) quando il CAA non produca con cadenza annuale alla Regione e ad ARTEA la certificazione del bilancio annuale da parte di società di revisione a ciò abilitate ovvero la relazione della funzione della revisione interna secondo i requisiti stabiliti dalla Associazione italiana Internal auditor.

3. Qualora al CAA, ai sensi dell'articolo 12, comma 3 del DM 27 marzo 2008, venga revocato il riconoscimento per gravi violazioni di legge o per gravi e/o ripetute inosservanze della Convenzione, nonché delle prescrizioni e degli obblighi imposti dalla Regione, dall'Organismo di Coordinamento o dall'Organismo Pagatore, ovvero il CAA cessi di operare a seguito di scissione, cessata attività, ecc., il rapporto convenzionale è risolto a totale danno del CAA, con eventuale rivalsa sulle garanzieassicurative.

4. Qualora, ai sensi del DM MIPAAF 28/03/2008, venga comunicato all'Agenzia l'avvio di un procedimento di contestazione a carico del CAA per la revocadell'autorizzazione, l'Agenzia si riserva di diffidare il CAA dall'accoglimento di nuove domande e dichiarazioni. In tal caso quest'ultimo è tenuto a dare le opportune informazioni agli utenti per orientarli verso altre strutture abilitate al ricevimento.

5. È compito di ARTEA definire nei propri manuali le modalità per assicurare nei confronti dei soggetti

interessati il regolare svolgimento dell'iter delle pratiche connesse al proprio fascicolo aziendale, a seguito di provvedimentidi revoca e di sospensione nei confronti del CAA.

Articolo 17
Responsabilità,-penali e altre ipotesi di risoluzione

1. Fermo restando quanto previsto all'articolo 3, le responsabilità derivanti dalla presente Convenzione non escludono la risarcibilità degli eventuali ulteriori specifici danni connessi a particolari comportamenti posti in essere dal CAA nell'espletamento delle attività delegate in forza della stessa Convenzione nei confronti dei produttori mandanti e dell'Organismo Pagatore.

2. Il CAA risponde e garantisce sotto il profilo amministrativo e civile della regolarità e legittimità dell'operato, sia proprio che delle società di servizio di cui può avvalersi ai sensi dell'art 12 del decreto MiPAAF 27 marzo 2008, fatta salva la responsabilità dell'azienda mandante circa la correttezza delle informazioni dei documenti forniti al CAA.

3. Il CAA è impegnato al rispetto dell'art. 1375 c.c., la cui violazione, concretizzando la fattispecie di abuso del diritto, costituisce inadempimento contrattuale.

4. Qualora l'Agenzia sia condannata al pagamento di somme di denaro o a qualunque altra forma di risarcimento in conseguenza di inadempimenti da parte del CAA, l'Agenzia provvede a rivalersi nei confronti del CAA ricorrendo alla garanzia assicurativa di cui all'articolo 5 del DM 27 marzo 2008, e successive modificazioni e integrazioni fatta salva l'ulteriore rivalsa fino a concorrenza dell'onere sopportato.

5. Qualora, in sede di appuramento e di liquidazione dei conti, con decisione della Commissione Europea, vengano stabilite riduzioni degli anticipi a carico dell'Agenzia per spese effettuate oltre i termini o le scadenze regolamentari e qualora tali riduzioni siano imputabili all'esito negativo dei controlli sulle funzioni attribuite dalla presente Convenzione al CAA, in quanto in contrasto con i manuali procedimentali dell'Agenzia o con le circolari AGEA, ARTEA provvede a rivalersi sulla garanzia prestata, per tutti i danni diretti ed indiretti provocati dal CAA nello svolgimento dell'attività nel limite del massimale assicurato.

6. In caso di tentativi di accesso non autorizzato e/o di forzatura del SistemaInformativo da parte di un singolo operatore CAA si provvederà a disabilitare l'utenza dalla quale risultano effettuati i tentativi di accesso e/o la forzatura; nel caso il CAA non fornisca idonea motivazione del comportamento, si provvederà all'ulteriore disabilitazione degli accessi per la sede CAA, periferica o centrale, dalla quale risulta effettuata la violazione.

7. Qualora le violazioni del Sistema Informativo siano dolosamente preordinate al fine di ricavare benefici per sé o per altri o di recare danno ad altri, ovvero per altri gravi inadempienze indicate dall'Agenzia, si riconosce ad ARTEA la facoltà di risoluzione di diritto della presente Convenzione, salvo il risarcimento dei danni.

Articolo 18
Potere sostitutivo, sospensione cautelare, avocazione

1. Nel caso in cui si renda necessario interrompere l'operatività del CAA o di una sua sede operativa, l'Agenzia si riserva la facoltà di avocare a sé, ai sensi del successivo comma 5 del presente articolo, le funzioni svolte dalla sede operativa fino a quando non saranno completamente rimosse le condizioni di irregolarità.
2. L'esercizio della facoltà di sostituzione di cui al successivo comma 3, comporta la conseguente riduzione o annullamento dei corrispettivi di cui all'art. 12. La definizione di corrispettivi sarà individuata con riferimento dalla data di notifica del provvedimento di sostituzione in misura proporzionale al numero di giorni per i quali l'Agenzia è costretta ad operare in sostituzione.
3. Qualora nell'ambito di controlli o indagini di Polizia Giudiziaria, delle istituzioni comunitarie (Corte dei Conti Europea e Commissione Europea, OLAF) o dell'Agenzia stessa, a uno o più operatori del CAA e/o al responsabile di sede (assimilato, ai fini del presente articolo, agli operatori) siano personalmente contestate violazioni gravi e circostanziate di carattere penale, nell'adempimento delle procedure di aggiornamento del fascicolo aziendale e/o di presentazione delle domande di contributo nazionale e/o comunitario, cui il CAA è tenuto a dare esecuzione dalla data di sottoscrizione della presente Convenzione, ARTEA procede alla sospensione cautelativa dell'utenza sul Sistema Informativo ARTEA dell'operatore coinvolto, con contestuale avviso al CAA di provvedere affinché la disattivazione non provochi disservizio ai mandanti. L'Agenzia comunica al rispettivo CAA di appartenenza la sospensione cautelativa degli operatori cui sia stato contestato un uso improprio dell'accesso al Sistema Informativo ARTEA. Nel caso di condanna definitiva, ARTEA metterà in campo ogni misura idonea affinché il soggetto interessato non possa più operare per qualsiasi CAA. L'Organismo Pagatore si obbliga a riattivare tempestivamente l'utenza sul Sistema Informativo ARTEA dell'operatore sospeso, entro dieci giorni dalla comunicazione del provvedimento di archiviazione e/o di qualsiasi altro provvedimento adottato in favore dello stesso dall'Autorità giudiziaria e/o amministrativa competente che escluda ogni responsabilità in merito alle contestazioni che hanno dato origine alprovvedimento di sospensione.
4. La sospensione del riconoscimento comporta la sospensione dell'esecuzione del rapporto

contrattuale.

5. L'Agenzia si riserva la facoltà, per giustificati motivi ed in qualsiasi fase dell'istruttoria, di avocare alla propria competente struttura, la gestione del fascicolo aziendale. Di tale volontà viene data notizia al CAA interessato mediante PEC. Il CAA si impegna a fornire all'Agenzia tutte le notizie necessarie ad una tempestiva ed efficiente gestione della pratica ed a trasmettere, o consegnare, gli eventuali fascicoli domanda/dichiarazioni correlati nelle modalità stabilite dall'Agenzia.

Articolo 19
Durata

1. La presente Convenzione ha durata dalla data della sottoscrizione fino al 31 dicembre 2025, ferma restando l'attività compiuta dal CAA nelle more della stipula della stessa per l'anno 2023.

2. I corrispettivi per gli anni 2024 e 2025 saranno definiti annualmente con un successivo atto integrativo della presente Convenzione, secondo quanto stabilito dall'art. 13.

3. Le parti si impegnano reciprocamente a verificare lo stato delle attività di cui alla presente Convenzione almeno ogni anno e comunque a richiesta di una delle parti.

4. La Convenzione potrà essere integrata e modificata in relazione ad eventuali modifiche normative sopravvenute nel corso della sua vigenza o qualora se ne riscontri la necessità o l'opportunità.

Articolo 20
Recesso del CAA

1. La volontà di recesso anticipato deve essere comunicata formalmente dal CAA almeno tre mesi prima tramite PEC.

2. Allo scopo di garantire la continuità della prestazione, la facoltà di recesso del CAA è subordinata alla conclusione delle attività in corso.

Articolo 21
Accesso ai locali del CAA e alla documentazione

1. Il CAA e le Sedi operative consentono, ai fini dell'espletamento dei compiti di vigilanza spettanti all'Agenzia, l'accesso ai locali ed alla documentazione acquisita e custodita per l'espletamento dei servizi affidati.

2. Allo scopo di far fronte alle eventuali richieste formulate da parte delle istituzioni comunitarie, anche in occasione di verifiche e ispezioni, il CAA si impegna a rendere disponibili tutte le informazioni

inerenti allo stato delle procedure, nonché eventuali motivazioni del totale, parziale o mancato pagamento degli aiuti imputabile al CAA mandatario.
3. Il CAA garantisce l'accesso ai propri locali e a tutta la documentazione inerente i procedimenti di cui alla presente Convenzione al personale incaricato dall'Agenzia delle attività di controllo ed al personale dell'organismo di certificazione ed ai funzionari designati dell'Unione Europea nonché a fornire il necessario supporto alla suddetta attività.
4. Il CAA riconosce all'Agenzia il diritto di acquisire, in qualsiasi momento, copia di tutti gli atti che il CAA e le sedi operative sono tenuti a conservare a seguito della presentazione delle dichiarazioni e delle domande di aiuto da parte dei produttori.

Articolo 22
Trattamento dei dati personali

1. Il CAA è nominato responsabile esterno del trattamento dati, rimanendo ARTEA titolare del trattamento. Le rispettive funzioni e modalità del trattamento sono disciplinate all'interno di apposita DPA di cui all'Allegato 1.

Articolo 23
Certificazione ISO 27001 e ISO 37001

1. ARTEA, ai sensi delle disposizioni del regolamento delegato 2022/127 della Commissione Europea, ha ottenuto la certificazione per la Gestione della sicurezza delle informazioni per l'erogazione di servizi, aiuti, contributi, premi ed altre agevolazioni pubbliche previsti da disposizioni comunitarie nazionali e regionali ISO 27001. La certificazione ottenuta si applica ai servizi e ai processi gestiti per l'autorizzazione, la contabilizzazione e l'esecuzione dei pagamenti degli aiuti previsti dalla Politica Agricola Comunitaria.

2. In accordo a tale Sistema di Gestione, con la sottoscrizione della presente Convenzione il CAA assicura i requisiti di sicurezza delle informazioni acquisite, comunicate, archiviate, processate, o in ogni modo gestite e relative al rapporto di collaborazione con ARTEA stessa, secondo le disposizioni presenti nell'Allegato 5 che forma parte integrante della presente Convenzione.

3. La Certificazione ISO 27001 non si estende al CAA.
4. ARTEA sta perseguendo l'obiettivo della certificazione ISO 37001. Con la stipula della presente Convenzione il CAA si impegna al rispetto della Politica per la prevenzione della corruzione approvata

da ARTEA, alla sottoscrizione dell'autocertificazione sul conflitto di interessi anche ai fini ISO 37001 di cui all'Allegato 3 e dell'autocertificazione dei fornitori anche ai fini ISO 37001 di cui all'Allegato 4.

Articolo 24
Polizza assicurativa R.C.

1. Alla stipula della presente Convenzione il CAA deve depositare presso l'Agenzia apposita polizza assicurativa per la responsabilità civile, stipulata ai sensi dell'art. 5 del decreto MiPAAF 27/03/2008 al fine di garantire danni diretti ed indiretti provocati nello svolgimento dell'attività agli organismi pagatori, agli utenti del servizio e agli enti pubblici affidatari delle funzioni di cui all'art. 2, comma 1 letteraa) l.r. 11/1998.
2. Entro il 31 dicembre di ciascun anno il CAA deve presentare la copia della polizza relativa all'anno successivo, nonché copia della ricevuta dell'avvenuto pagamento della prima rata del premio riferito all'anno in questione. Le copie dell'avvenuto pagamento delle rate successive, dovranno essere presentate entro 20 giorni dalla relativa scadenza.
3. La garanzia assicurativa dispiega i suoi effetti per l'intera durata del rapporto contrattuale e per i tre anni successivi alla cessazione dello stesso.
4. Il massimale annuo di garanzia è stabilito dal D.M. 27 marzo 2008.

Articolo 25
Nomina responsabile tecnico e responsabile del conflitto di interessi

1. Ai sensi dell'art. 7 comma 4 del decreto MiPAAF 27 marzo 2008 ed in attuazione di quanto previsto dalla presente Convenzione, ai fini e per lo svolgimento delle attività previste dalla presente Convenzione, il CAA dichiara di aver nominato il Responsabile Tecnico nella persona di _____ in possesso di tutti requisiti richiesti dal DM sopra citato. Nel sistema informativo ARTEA il Responsabile Tecnico assume il ruolo di Responsabile delle utenze, come già previsto nel Manuale operativo riconoscimento centri di assistenza agricola e controlli sedi operative approvato con decreto del dirigente regionale n. 5564 del 18 dicembre 2013.
2. Ai sensi della presente Convenzione, il CAA dichiara di aver nominato Responsabile del conflitto di interessi _____.

Articolo 26
Foro competente

1. Le controversie nascenti dalla presente Convenzione o con la stessa connesse sono devolute alla

competenza del Foro di Firenze.

Articolo 27
Imposte

1. La presente Convenzione tra ARTEA ed il CAA è soggetta ad imposta di bollo ai sensi dell'art. 2 del dpr 26 ottobre 1972 n. 642 (Disciplina dell'imposta di bollo).
2. Le parti concordano che il pagamento dell'imposta di bollo di cui al comma 1 sia a carico del CAA.
3. Il presente atto sarà registrato in caso di uso, ai sensi degli artt.5 e 6 del dpr 26 aprile 1986, n.131 (Testo unico delle disposizioni concernenti l'imposta di registro), a cura e spese della parte richiedente la registrazione.

Articolo 28
Disposizioni di rinvio

1. Per quanto non espressamente previsto nella presente Convenzione, si rinvia alla l.r. 9 febbraio 1998 n. 11 (Norme per lo snellimento e la semplificazione dell'attività amministrativa in materia di agricoltura, foreste, caccia e pesca, e alledisposizioni disciplinanti la materia) e successive modifiche.

Letto approvato e sottoscritto
Firenze, il _____

Centro Autorizzato Assistenza Agricola

_____

Agenzia Regionale Toscana per le Erogazioni in Agricoltura
(Il Direttore)

_____

ALLEGATI

Allegato 1 - Data Protection Policy. Modello organizzativo ARTEA

Allegato 2 - Controlli e sanzionamento

Allegato 3 - Autocertificazione conflitto di interessi e n.d.a. ISO 27001 e ISO 37001

Allegato 4 - Autocertificazione fornitori sui requisiti ex art. 80 Codice Contratti e ISO 37001

Allegato 5 - Accordi/clausole per la sicurezza delle informazioni (ISO 27001)

Allegato 6 - Modello di mandato

Allegato 1 - Data Protection Policy. Modello organizzativo ARTEA

Indice

1. Scopo del documento

Il presente documento definisce il modello organizzativo della struttura amministrativa di ARTEA per la compliance con il regolamento europeo 2016/679 denominato GDPR. Nello specifico prende in esame le figure organizzative, i processi, ruoli e le responsabilità previste dal GDPR per perseguire l'obiettivo di garantire un adeguato livello di protezione nella gestione di dati personali, e descrivere come debba mutare l'assetto organizzativo dell'ente al fine di garantire nel trattamento dei dati personali la tutela dei diritti di libertà delle persone.

Si articola quindi in una breve descrizione di cosa richiede l'attuazione del GDPR, quali processi aggiuntivi debbano essere posti in essere e come questi si rapportino con i procedimenti in essere.

A tale documento di definizione del modello organizzativo seguiranno le linee guida per l'attuazione dei processi GDPR individuati.

2. Obiettivo del documento

Il GDPR riforma il precedente impianto normativo in materia di protezione dei dati personali – Codice Privacy, inserendo come innovativo elemento cardine il principio di Accountability (o "Responsabilizzazione") in capo al Titolare, e di eventuali Responsabili o Contitolari del trattamento, nell'adozione di misure tecniche ed organizzative adeguate ed efficaci, con l'onere di dimostrare la conformità delle attività di trattamento al GDPR stesso, garantendo la tutela ai diritti dell'interessato, nonché mettendo in atto procedure per riesaminare e aggiornare le misure stesse.

In tale contesto assume rilievo il cambio di approccio richiesto dal Regolamento al "tema privacy" da parte del Titolare del trattamento, oggi chiamato a rimodulare i processi di gestione dei dati personali secondo i principi di Data Protection "by design" e "by default", per avere la certezza che le misure tecniche e organizzative siano adottate ed integrate fin dalla progettazione (ideazione) del trattamento; per valutare i rischi di minacce che possono generare violazioni dei dati personali (come riporta l'art. 1 § 2 del GDPR "il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali"); per dare priorità agli interventi, per avere la garanzia della liceità del trattamento, per monitorare costantemente le misure di sicurezza ed i trattamenti, per rendere i collaboratori, nella qualità di soggetti autorizzati, consapevoli del valore del dato attraverso la formazione e la corretta applicazione di istruzioni ad hoc ed, infine, per garantire che quest'ultimi si impegnino alla riservatezza o che abbiano un adeguato obbligo legale di riservatezza.

Pertanto, diventa prioritaria la riorganizzazione dell'Agenzia cercando di ridistribuire compiti e responsabilità tra i soggetti coinvolti nel trattamento dei dati personali (vedi Titolare del trattamento, Responsabile del trattamento, persona istruita e autorizzata – ex incaricato del trattamento nel codice privacy) con la particolare attenzione di armonizzare il tutto con il nuovo ruolo DPO, introdotto dal GDPR.

Il presente elaborato vuole fornire le linee guida su come configurare il nuovo assetto organizzativo in materia di protezione dei dati personali.

3. Approccio di responsabilizzazione sostanziale

In riferimento alle specifiche novità introdotte dal GDPR – così come evidenziato in precedenza - si determina un approccio di responsabilizzazione sostanziale, con l'espressa indicazione di una "Data Protection compliance" basata su metodologie di valutazione del rischio e che deve essere integrata nei processi dell'Agenzia.

In altri termini, il Regolamento impone un "approccio preventivo, proattivo e non più reattivo", con focus su obblighi e comportamenti che prevengano in modo effettivo il possibile evento di danno, configurandosi sulle specificità dei diversi trattamenti cui si riferiscono.

4. Titolare del trattamento

Lo sviluppo delle considerazioni riportate nel paragrafo precedente ha poi generato la previsione specificamente contenuta nell'art. 24 del Regolamento 2016/679, rubricato "Responsabilità del titolare del trattamento" in cui, per l'appunto, è previsto che, il titolare del trattamento metta in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento sia effettuato conformemente al presente regolamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

In questo quadro, si delinea un sistema organizzativo ai fini dell'applicazione del GDPR in cui il Titolare assume il ruolo di principale attore del sistema del trattamento. Come indicato dal considerando n. 74, il Titolare del trattamento assume la responsabilità generale per qualsiasi trattamento di dati personali che effettui direttamente o che altri abbiano effettuato per suo conto.

Infatti, l'art. 5 del GDPR attribuisce direttamente ai titolari del trattamento il compito di assicurare, ed essere in grado di comprovare, il rispetto dei principi applicabili al trattamento dei dati personali.

Il titolare, per rispettare il principio di accountability, deve assicurare che i dati siano sempre:

a. trattati secondo "liceità, correttezza e trasparenza"
b. raccolti per "finalità determinate, esplicite e legittime"
c. adeguati, pertinenti e limitati rispetto alle finalità
d. esatti
e. limitati nella conservazione
f. trattati garantendo sicurezza e integrità.

Per l'individuazione del titolare si deve fare riferimento – in base a quanto previsto dall'art. 4 del GDPR – alla "persona giuridica, autorità pubblica, servizio o di altro organismo" che determina le finalità e i mezzi del trattamento di dati personali, autonomamente o in regime di contitolarità.

Con riferimento ad un Ente, va specificato che la necessaria identificazione della "persona giuridica, autorità pubblica, servizio o di altro organismo" quale titolare o contitolare del trattamento non preclude l'applicazione dei principi generali in materia di formazione della volontà dell'ente e di delega di funzioni, nel senso che la volontà del "titolare/contitolari" sarà formata, anche agli effetti della disciplina della protezione dei dati, tenendo conto delle ordinarie attribuzioni degli organi previsti dall'atto costitutivo.

In tal senso, sono da considerare tutte le caratteristiche specifiche che influiscono sul processo di determinazione delle finalità e dei mezzi del trattamento di dati personali.

In conclusione, le specifiche del modello organizzativo amministrativo adottato costituiscono l'elemento qualificante per determinare le scelte della volontà (e le modalità di esercizio delle stesse) attraverso la struttura amministrativa che le compete, incluse quelle relative alle finalità e ai mezzi del trattamento di dati personali.

5. Data Protection Officer (DPO)

Il Data Protection Officer – DPO –, altrimenti noto come Responsabile della protezione dei dati, è una nuova figura di riferimento, per tutto ciò che attiene la materia di protezione dei dati personali, e si

affianca al Titolare o al Responsabile del trattamento e nei rapporti esterni con le Autorità di controllo e con gli Interessati.
Il DPO è una figura la cui nomina è obbligatoria, tra l'altro, per gli enti pubblici.
Il DPO è parte dell'organizzazione Data Protection dell'Ente, di cui non necessariamente deve essere un dipendente, ben potendo tale ruolo essere assolto da un soggetto esterno identificato dal Titolare o dal Responsabile del trattamento.
Il Gruppo di lavoro art. 29, costituito da tutti i rappresentanti dei Garanti europei, ha più volte ribadito l'importanza della figura del DPO quale pilastro della responsabilizzazione che agisce quale coordinatore della conformità al GDPR.
Il DPO è incaricato, dal Titolare del trattamento, di svolgere almeno i seguenti compiti e funzioni:
a. informare e fornire consulenza al titolare del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal regolamento (UE) 2016/679, nonché da altre disposizioni nazionali o dell'Unione relative alla protezione dei dati;
b. sorvegliare l'osservanza del regolamento (UE) 2016/679, di altre disposizioni nazionali o dell'Unione relative alla protezione dei dati nonché delle politiche del titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c. fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del regolamento (UE) 2016/679;
d. cooperare con il Garante per la protezione dei dati personali;
e. fungere da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del regolamento europeo, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.
f. fungere da punto di contatto per gli interessati, per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.
Il DPO riferisce direttamente al titolare del trattamento.
Non possono essere nominati DPO o componenti dell'Ufficio DPO soggetti che ricoprono ruoli nell'organizzazione che possono determinare potenziali conflitti d'interesse o il mancato rispetto dei principi di controllo, con particolare attenzione al principio della separazione delle funzioni.
Il DPO e i componenti dell'Ufficio del DPO non possono rivestire ruoli che comportino la definizione di finalità e mezzi di trattamento, né può ricevere istruzioni dal Titolare sulle modalità di esecuzione dei propri compiti.
Il Titolare del trattamento e il Responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.
Il sistema dei flussi informativi è strutturato in base ai seguenti punti principali:
a. ogni dirigente, posizione organizzativa e/o altre eventuali figure di coordinamento sono tenuti a comunicare all'ufficio del DPO ogni evento rilevante ai fini dell'applicazione del GDPR
b. i responsabili della Struttura organizzativa interna per la sicurezza dei trattamenti con mezzi elettronici e della Struttura organizzativa per la sicurezza dei trattamenti cartacei devono comunicare tempestivamente al DPO le evidenze di ogni attività di controllo e/o di altra natura rilevante ai fini dell'applicazione del GDPR.
c. i dati di contatto del DPO da pubblicare dovranno ricomprendere le informazioni che possono consentire agli interessati e al Garante di raggiungerlo con facilità: recapito postale, numero telefonico

dedicato e/o indirizzo mail dedicato

d. il primo riferimento operativo per le richieste degli interessati è l'URP, cui sono delegate le attività di comunicazione di front end.

e. le richieste più specifiche che richiedono un parere da parte dell'ufficio del DPO, avvengono per via telematica secondo le indicazioni riportate sul sito dell'organizzazione di riferimento alla sezione Data Protection Officer – Contatti.

In relazione al ruolo previsto dal legislatore europeo che configura il DPO come un consulente indipendente, il compito del DPO nell'ambito delle attività di verifica è quello di vigilare affinché il sistema dei controlli preventivi (l'insieme delle misure di sicurezza tecniche e organizzative e ogni altro presidio di controllo applicato dall'Agenzia) nel suo complesso sia adeguato a mitigare i rischi riferibili al diritto alla protezione dei dati personali e a mantenere nel tempo la propria efficacia nel mantenere a livello accettabile i rischi di volta in volta rilevati e/o emergenti. Per tale attività si avvale del Security Manager.

In sostanza, non competono al DPO i controlli operativi sull'osservanza del regolamento. Per controlli operativi si intendono quei controlli sull'operato dei dipendenti assegnati alla struttura di cui il dirigente è responsabile.

I controlli operativi spettano ai dirigenti, o ai loro delegati a norma del contratto di lavoro, in riferimento ai trattamenti di dati personali svolti nel settore di cui sono responsabili. Per tali attività di controllo in merito alla correttezza delle operazioni e non dei comportamenti, possono avvalersi del supporto dei Data Protection Specialist.

Le evidenze di tutti i controlli e di ogni altra attività di verifica effettuata, rilevante ai fini del GDPR, devono essere comunicate al DPO.

In riferimento alle evidenze dei controlli svolti, alle eventuali segnalazioni ricevute, alla verifica di documentazione e/o ad ogni altra informazione acquisita rilevante ai fini del GDPR, il DPO può:

a. riservarsi di chiedere approfondimenti ai soggetti competenti per i controlli

b. intervenire con una pluralità di azioni idonee a favorire l'osservanza delle prescrizioni del GDPR (a titolo esemplificativo, si vedano le ipotesi di intervento in ordine al controllo del registro dei trattamenti, così come indicate nelle Indicazioni Operative per il Registro delle attività di trattamento)

c. disporre ulteriori controlli ai fini del processo di accountability – da effettuarsi dall'Ufficio del DPO o da altri soggetti specificatamente designati dal DPO stesso - negli ambiti di competenza assegnati dal legislatore europeo (sorvegliare l'osservanza del regolamento, nonché delle altre disposizioni europee o di diritto interno in materia di protezione dati; sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e attività di controllo)

Nel rispetto di quanto disposto dall'art. 39, secondo paragrafo, del GDPR ("Nell'eseguire i propri compiti, il DPO considera debitamente i rischi inerenti al trattamento…") il DPO può definire un ordine di priorità nelle attività da svolgere in relazione a quelle che hanno come ambiti di riferimento quelli che presentino maggiori rischi in termini di protezione di dati (c.d. Piano attività Risk Based).

Allo scopo di svolgere le proprie funzioni, il DPO può:

a. partecipare agli incontri organizzati dall'Agenzia, valutando quali attività rivestono rilevanza per il corretto svolgimento dei propri compiti. A tal fine, in osservanza al principio di Data Protection by Design, ogni qualvolta siano in trattazione argomenti e attività che comportano trattamento di dati personali, occorre, secondo le regole organizzative dell'ente, darne comunicazione al DPO, che valuterà se e come intervenire.

b. accedere a tutta la documentazione e a tutte le sedi dell'Agenzia per lo svolgimento dei propri

compiti

c. Il DPO – ai sensi dell'art. 38 del GDPR - deve essere dotato delle risorse necessarie per lo svolgimento efficace dei propri compiti, così come indicati all'art. 39 del GDPR, per accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.

Ciò implica che:

a) sia fornito supporto attivo alle funzioni del DPO da parte dei referenti dell'Agenzia,

b) siano assegnate adeguate risorse (finanziarie, infrastrutture - sede, attrezzature, strumentazione - e personale)

c) sia comunicata ufficialmente la nomina del DPO sia esternamente (comunicazione all'Autorità Garante, informative agli interessati ex art. 13 GDPR) che a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell'Agenzia.

d) sia garantita la collaborazione da parte dell'Agenzia così da fornire al DPO supporto, informazioni e input essenziali.

e) sia assicurata da parte della Direzione Generale la formazione permanente dei componenti dell'Ufficio del DPO e dei data protection specialist, in modo che possano curare il loro aggiornamento con riguardo agli sviluppi nel settore della protezione dati.

Nel rispetto delle procedure dell'Agenzia applicabili, il DPO provvederà a trasmettere la propria richiesta di budget periodico, opportunamente motivata, al Titolare o ad altro organo delegato dal Titolare.

In riferimento al budget assegnato, il DPO svolgerà in autonomia le proprie attività, con il potere di intervenire – impiegando le risorse necessarie – anche per attività non incluse nella richiesta di budget, se ritenute indispensabili per il rispetto della normativa.

6. Responsabile del trattamento

Il Regolamento definisce il Responsabile del trattamento come la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare (art. 4, § 8; art. 28).

L'approccio basato sul rischio e misure di accountability del GDPR influenza anche la figura del Responsabile del trattamento, al quale sono assegnati nuovi compiti e che condivide in certa misura le responsabilità del Titolare, in riferimento al risarcimento del danno a terzi, ed è oggetto di autonome sanzioni amministrative.

Il Responsabile risponde per danno se non ha adempiuto agli obblighi previsti dal regolamento, ma anche se ha agito senza rispettare le istruzioni del Titolare.

Il Responsabile è soggetto anche a obblighi risarcitori per mancanze ad esso ascrivibili e, in caso disattenda le istruzioni del titolare al punto da individuare - con i dati che ha ricevuto in affidamento - proprie finalità del trattamento, diventa a sua volta Titolare autonomo, con conseguente applicazione del quadro di riferimento - anche sanzionatorio - ben più "pesante", rispetto a quello relativo ad una semplice violazione degli obblighi contrattuali assunti con il Titolare.

Il Responsabile del trattamento deve presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate – in primis agli standard stabiliti dal titolare - in modo tale che il trattamento soddisfi i requisiti previsti dal GDPR e garantisca la tutela dei diritti dell'interessato.

I trattamenti svolti da un Responsabile devono essere disciplinati da un contratto o altro atto giuridico stipulato con il titolare. Il contratto deve regolare gli elementi essenziali del trattamento di dati personali curato dal Responsabile, con particolare riferimento a:

a. materia disciplinata

b. durata del trattamento/i,
c. natura e finalità del trattamento/i,
d. tipo di dati personali
e. categorie degli interessati coinvolti,
f. nonché a tutti gli altri elementi indicizzati all'art. 28, comma 3, GDPR

definendo in modo chiaro quali siano gli obblighi e i diritti del titolare e quali quelli del responsabile, tendo nel debito conto l'attività di controllo propria del Titolare.

7. Autorizzati

Ai fini di individuare gli "autorizzati", al trattamento dei dati personali, si deve far riferimento alle seguenti disposizioni del GDPR:

1. trattasi innanzitutto di persone soggette alla "autorità diretta del Titolare o del Responsabile" (art. 4, § 10)
2. Che non possono trattare dati personali del titolare per il quale operano se non dietro istruzione fornita dal Titolare o dal Responsabile del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri (artt. 29 e 32 § 4)

Quindi per trattare i dati bisogna essere soggetti istruiti e autorizzati.

8. La compliance al GDPR

Passiamo a definire come le figure previste dal GDPR si mappano con ruoli e responsabilità dell'organizzazione dell'Agenzia, per rispondere al dettato regolamentare europeo. Segue un breve riepilogo delle figure previste dal GDPR.

8.1 Le figure e le responsabilità nell'organizzazione

Il Regolamento europeo 2016/679 (GDPR) richiede che le organizzazioni adottino una struttura (ruoli e funzioni) e procedimenti che garantiscano intrinsecamente, così come previsto all'art. 1 (C1-14, C170, C172), la protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché la libera circolazione di tali dati, proteggendo i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.

Questo in quanto le finalità sono la protezione per l'affermazione di diritti delle persone fisiche, commisurata alla riduzione dei rischi derivanti dall'uso improprio o illecito di dati personali.

A tale scopo il GDPR introduce figure organizzative, con ruoli e responsabilità precisi, e fissa alcuni principi organizzativi atti a vincolare i comportamenti in modo che siano coerenti con le finalità del regolamento stesso.

8.2 Figure previste esplicitamente o implicitamente dal regolamento

Titolare del Trattamento dati, art. 24 GDPR (C74-C78) (in inglese Controller) è colui che ha la responsabilità, fra le altre, di mettere in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare (principio della accountability), che il trattamento è effettuato in modo conforme al regolamento. A lui è demandata in via diretta o indiretta la tutela dei diritti e delle libertà fondamentali della persona fisica a cui si riferiscono i dati personali che vengono trattati. Decide in ordine a finalità e mezzi (questi ultimi parzialmente delegabili a responsabili) dei trattamenti di propria competenza e ha la responsabilità di tenuta del registro dei trattamenti ex art. 30 GDPR (C82).

Delegato del titolare, Art .2-quaterdecies, comma 1, d.lgs. 196/2003 è la persona fisica delegata, con

atto espresso dal Titolare, a svolgere le sue funzioni a norma del GDPR.
Responsabile del Trattamento, Art. 28 GDPR (C81) (in inglese Processor) Persona fisica o giuridica, diversa dal Titolare ed esterna all'organizzazione dello stesso, che eventualmente effettua trattamenti per conto del Titolare. Il rapporto fra Titolare e Responsabile, ove previsto, deve essere regolato da apposito contratto o altro atto bilaterale. Al Titolare spetta l'onere e la responsabilità di indicare al responsabile le modalità di trattamento e le relative istruzioni, nonché di controllare che siano rispettate.
Gli autorizzati, art .2-quaterdecies, comma 2, d.lgs. 196/2003 sono le persone autorizzate dal titolare al trattamento dei dati: al Titolare compete di dare, oltre che l'autorizzazione, anche le istruzioni e un'adeguata formazione in merito alle misure da adottare nella esecuzione del trattamento.
Data Protection Specialist, figura implicitamente prevista dal GDPR, quando prevede e mette in capo al titolare, responsabilità e attività che prefigurano competenze tecniche specialistiche, non riconducibili direttamente alle competenze richieste per svolgere il ruolo di Titolare. In particolare la valutazione dei rischi (DPIA Art. 35 C84, C89-C93, C95), l'individuazione dei trattamenti partendo dai processi dell'organizzazione e andandone ad individuare i riferimenti che ne determinano la liceità, la determinazione della misura dei rischi di natura tecnica ed organizzativa, ecc. Una figura che abbia competenze organizzative, giuridiche e tecnologiche, o coadiuvata da altre, per essere in grado di supportare la struttura nei rapporti con strutture specialistiche, interne o esterne all'organizzazione, referenti per le specifiche competenze.
Security manager/Data Security Officer, figura implicitamente prevista dal GDPR, per garantire quanto previsto alla sezione 2 "sicurezza dei dati personali", per supportare il Titolare nei suoi compiti di supervisione e controllo delle misure di sicurezza adottate, per determinarne la loro adeguatezza nel tempo e per garantire il rispetto del principio di separazione delle responsabilità fra chi le misure le deve attuare, il Responsabile/i della sicurezza IT dell'organizzazione o il Responsabile del trattamento, e chi invece deve controllarle.
Il DPO (Data Protection Officer), o Responsabile della protezione dei dati, previsto sezione 4 del GDPR art. 37-39. Svolge azione di promozione, consulenza e verifica per il corretto comportamento organizzativo in ottemperanza al regolamento. Mantiene relazioni con l'autorità garante e funge da punto di contatto con gli interessati per agevolare l'esercizio dei loro diritti.
L'ufficio del DPO, struttura non esplicitamente prevista nel GDPR ma derivante dall'esigenza: di essere un punto di competenza multidisciplinare a supporto del Titolare e suoi delegati, di essere punto di contatto con gli interessati, di essere punto di riferimento organizzativo di supporto alle interlocuzioni con il Garante.

8.3 Come si mappa l'organizzazione GDPR con l'organizzazione di ARTEA

ARTEA assume, a norma dell'Art. 4 punto 7 del GDPR, il ruolo di Titolare dei trattamenti afferenti alle finalità dell'ARTEA, nella persona del Direttore.
Con decreto del Direttore n. 92 del 9 settembre 2022, relativo all'approvazione della nuova macrostruttura dell'Agenzia con decorrenza 12 settembre 2022, è stato costituito il Settore "Affari Generali, Supporto giuridico e contabilizzazione" al quale è assegnata la competenza in materia di privacy. Conseguentemente viene individuato un pool di Data Protection Specialists, collocati organizzativamente all'interno del Settore suddetto, che fornisce adeguato supporto alla Direzione e ai settori dell'Agenzia, al fine di verificare e garantire il rispetto dei principi e dei procedimenti per la compliance al GDPR.
I nominativi dei Data Protection Specialists vengono individuati con apposito Ordine di Servizio e

comunicati al DPO.
I Dirigenti assumono, a seguito del decreto del direttore n. 97/2018, la figura di Delegato del Titolare per i trattamenti di loro diretta responsabilità.
ARTEA, con decreto del direttore n. 77/2022, si è avvalsa della facoltà prevista dall'art. 37, paragrafo 3, del regolamento europeo, di procedere alla nomina condivisa del DPO individuato dalla Regione Toscana nella figura del Consorzio METIS con delibera di Giunta n. 755 del 26 giugno 2022.
ARTEA con decreto del direttore n. 70/2022 ha di nominato quale Security Manager di ARTEA la dott.ssa Stefania Bove responsabile della PO "Programmi di monitoraggio applicativo".
Uno o più dirigenti possono configurarsi, per conto di ARTEA, come responsabili per trattamenti di un titolare diverso dall'Agenzia.
I Dipendenti, a seguito di un processo autorizzativo da parte dei dirigenti nel loro ruolo di Titolari che integra l'autorizzazione generale e le istruzioni di cui al decreto del Direttore n. 97/2018, associando loro, nel caso di procedure IT, i diritti di accesso ed elaborazione dei dati o assegnando loro funzioni per il trattamento di dati personali presenti in documenti o archivi cartacei, vengono associati ai trattamenti tramite registrazione nel registro dei trattamenti e assumono il ruolo di Autorizzati al trattamento. In tale fase il Titolare, può fornire se lo ritiene utile, ulteriori informazioni e istruzioni utili al dipendente, al fine di consentirgli di svolgere il suo ruolo nella piena consapevolezza del suo operato.
Dipendenti opportunamente formati, assumono e assolvono, alle dirette dipendenze del direttore generale, alla funzione di Data Protection Specialist.

9. I Processi GDPR

La compliance al GDPR si sostanzia nella messa in atto di un modello organizzativo che si innervi nella realtà organizzativa dell'Ente e di processi specifici finalizzati alla costante verifica dei dati trattati e della adeguatezza delle misure adottate e commisurate alla valutazione dei rischi. Altro aspetto che la compliance deve garantire è l'esercizio dei diritti degli interessati.

9.1 Processo: Data protection by design e by default

Questo processo riguarda il rispetto di quanto disposto art. 25 del GDPR, ed è rappresentato da tutte quelle analisi e valutazioni da effettuare al momento della emissione di un qualsivoglia atto che comporti come conseguenza un trattamento di dati personali. Nel caso in cui l'atto prefiguri il trattamento di dati personali devono essere valutati, al livello di granularità commisurato alla tipologia di atto, i seguenti aspetti:

a. Individuazione del trattamento sotteso e del processo organizzativo che si va a ipotizzare o realizzare, modificare, integrare,
b. I soggetti organizzativi coinvolti e le differenti figure dell'organizzazione GDPR,
c. Le relative misure di sicurezza.

Tale processo deve essere vincolante nella produzione di un qualsivoglia atto.
Pertanto si procede alla modifica della procedura dell'iter di approvazione degli atti al fine di inserire, a cura del dirigente promotore, una fase di verifica degli impatti GDPR dell'atto, così che se l'atto prefigura il trattamento dei dati personali, l'atto deve essere obbligatoriamente corredato di informazioni aggiuntive ai sensi della disciplina in materia di protezione dei dati personali. Tale processo è descritto nel documento "Linee guida per la Data Protection by design e by default".

9.2 Processo: Mantenimento del registro dei trattamenti

L'art. 30 del GDPR (C82) pone in capo al Titolare la responsabilità di tenere un registro delle attività di trattamento: pertanto nell'organizzazione dell'Agenzia tale responsabilità si trasferisce per delega ai dirigenti, nell'ambito dell'esercizio delle loro competenze e dei rispettivi ruoli gerarchici, per effetto del decreto n. 97/2018.

Il registro dei trattamenti viene gestito con apposita procedura IT che deve garantire:

1. il ciclo di vita del trattamento,
2. il collegamento con l'organizzazione dell'Agenzia al fine di mantenere allineate le strutture, le competenze e le persone a seguito di variazioni organizzative, quali cambio di dirigenti, cambio di competenze delle strutture, cambio di personale autorizzato, ecc.
3. il collegamento con i processi produttivi dell'Agenzia in quanto i trattamenti sono segmenti di tali processi finalizzati al trattamento di dati personali. Il riferimento al processo risulta importante in quanto è sulla base del processo, e non del singolo trattamento, che risulta opportuno fare la valutazione dei rischi e la esecuzione di vere e proprie DPIA. Analizzando i singoli trattamenti, può accadere di sottovalutare o sopravvalutare rischi, o di dover eseguire più DPIA, una per ogni trattamento, con dispendio di costi e tempi, quando sarebbe stato possibile farla una sola volta sull'intero processo (in senso conforme, art 35 comma 1): "… Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi").
4. Il collegamento con gli asset, intesi come applicazioni IT, basi di dati e strutture tecnologiche di supporto, ma anche archivi cartacei e relativi supporti, al fine di determinare le misure di sicurezza
5. Il collegamento con le procedure di assegnazione dei diritti di accesso a dati e funzioni al fine di riportare sui trattamenti correlati, i nominativi degli autorizzati e i relativi privilegi nel trattamento. La gestione degli autorizzati su procedimenti non digitalizzati richiederà l'inserimento manuale degli autorizzati.

Questo prefigura un aggiornamento della procedura IT di gestione dei trattamenti in una logica di processo garante della rappresentazione fedele della realtà.

La gestione dei trattamenti e la loro registrazione nei fatti si configura come un sotto-processo del processo di Data Protection by Design.

Per la descrizione di dettaglio si rimanda alle "linee guida per il mantenimento del registro dei trattamenti" (Data protection policy relativa alla gestione dei processi GDPR).

9.3 Processo: Formulazione e gestione della DPIA

Il GDPR all'art.35, in coerenza con il principio di sostanziale responsabilizzazione, basato sull'analisi dei rischi, prevede lo strumento della DPIA quale processo mirato alla valutazione degli impatti conseguenti ai rischi rilevati e alla determinazione delle misure finalizzate alla loro riduzione.

La DPIA viene individuata come processo obbligatorio in tutti quei casi in cui, in particolare con l'uso delle di nuove tecnologie, si può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Il Garante Nazionale con provvedimento n. 467 del 11 Ottobre 2018 (Pubblicato sulla Gazzetta Ufficiale n. 269 del 19 novembre 2018) ha individuato, così come previsto all'art. 35 comma 4 del GDPR, le tipologie di trattamenti per i quali la DPIA è un adempimento obbligatorio:

1) Trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso App, relativi ad "aspetti riguardanti il rendimento professionale, la situazione economica, la

salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato.

2) Trattamenti automatizzati finalizzati ad assumere decisioni che producono “effetti giuridici” oppure che incidono “in modo analogo significativamente” sull’interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l’utilizzo di dati registrati in una centrale rischi).

3) Trattamenti che prevedono un utilizzo sistematico di dati per l’osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell’informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d’uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.

4) Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull’esercizio di un diritto fondamentale (quali i dati sull’ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell’interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).

5) Trattamenti effettuati nell’ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell’attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn.3,7 e8).

6) Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).

7) Trattamenti effettuati attraverso l’uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogni qualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01.

8) Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.

9) Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l’incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment).

10) Trattamenti di categorie particolari di dati ai sensi dell’art. 9 oppure di dati relativi a condanne penali e a reati di cui all’art. 10 interconnessi con altri dati personali raccolti per finalità diverse.

11) Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell’attività di trattamento.

12) Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell’attività di trattamento.

La decisione o meno di effettuare una DPIA e il suo svolgimento è in capo al titolare o suo delegato che

si consulta con il DPO.
I contenuti minimi di una valutazione di impatto sono descritti all'art. 35 comma 7 del GDPR a cui si rimanda.
Il Titolare nello svolgimento della DPIA, se del caso, così come previsto all'art. 35 comma 9 richiede il parere degli interessati o dei loro rappresentanti.
In sintesi il processo di DPIA è competenza del Titolare o suo delegato, che si avvale della consultazione con il DPO ed è mirato ad evidenziare e documentare in modo chiaro i rischi, le misure di sicurezza adottate per mitigarli e i rischi residui. La DPIA è mantenuta aggiornata dal Titolare allorquando si modifichi il processo, intervengano incidenti che mettano in luce possibili debolezze del sistema non considerate, si evidenzino minacce non prese in considerazione, ecc.
La formulazione della DPIA si configura come un sotto-processo del processo di Data Protection by Design da mettere in atto qualora la tematica in questione la richieda.

9.4 Processo: Gestione degli incidenti

È bene che siano definite delle figure per il presidio del processo di raccolta, gestione e analisi degli incidenti fra cui anche il processo di Data Breach previsto dal GDPR.
Il Security Manager assistito dai data protection specialist provvede a:

a. mantenere un registro degli incidenti
b. valutare l'impatto sulla continuità del servizio coordinandosi con l'eventuale responsabile della continuità operativa
c. supervisionare il gruppo di intervento e gli specialisti nelle attività di contrasto degli incidenti durante le fasi di emergenza
d. segnalare al DPO possibili vulnerabilità e/o incidenti in ambito di trattamento di informazioni personali
e. analizzare lo storico degli incidenti insieme agli specialisti al fine di identificare delle soluzioni stabili in grado di contrastare le vulnerabilità emerse
f. comunicare al Responsabile della sicurezza (quando presente) o hai responsabili dello sviluppo dei sistemi informativi o delle infrastrutture, la sintesi delle vulnerabilità emerse dal registro degli incidenti e le soluzioni intraprese per il loro contrasto
g. supportare il Titolare del trattamento (o a suo delegato) e il DPO nel processo di notifica del Data Breach al Garante e alle altre autorità competenti.
h. supportare il Titolare del trattamento (o suo delegato) e il DPO nel valutare la necessità di procedere anche alla comunicazione dell'incidente a tutti gli Interessati.

9.5 Processo Accountability

In riferimento all'approccio di responsabilizzazione sostanziale introdotto dal GDPR si determinano rilevanti ulteriori novità anche in merito al sistema organizzativo nel suo complesso.
Il Regolamento, come già indicato in precedenza, prevede espressamente una compliance basata su metodologie di valutazione del rischio e che deve essere integrata nei processi dell'Agenzia.
In altri termini, rispetto al Codice Privacy, si passa dalla richiesta di una somma di adempimenti obbligatori ad un approccio per processi e ad una protezione dei dati personali in ottica Risk Based.
L'approccio per processi favorisce la visione globale dell'organizzazione, rappresentandola attraverso un insieme di processi tra loro interconnessi.
Per un'efficace applicazione del GDPR e del rispetto del principio di accountability, in particolare, è

opportuno che il sistema organizzativo includa la rilevazione dei processi che evidenzi il complesso delle attività svolte, la loro sequenza e le modalità con cui sono corrispondentemente effettuate.
Adempimenti rilevanti ai fini GDPR quali il censimento dei trattamenti dei dati personali, la correlata predisposizione del registro dei trattamenti e il mantenimento dello stesso aggiornato e allineato ad ogni eventuale nuovo trattamento avviato e/o variazione intervenuta nei trattamenti preesistenti implicano che tutte le attività svolte dall'Agenzia siano analizzate e siano continuamente monitorate.
L'efficacia di tali analisi può essere maggiore se condotta con il supporto preventivo della mappatura dei processi, in modo da poter più facilmente identificare gli ambiti di attività effettivamente svolte e ogni eventuale trattamento correlato che, in ragione della natura e delle peculiarità dell'attività stessa, risultano potenzialmente esposti a rischi rispetto al diritto alla protezione dei dati personali.
Peraltro, già altre norme – tra cui la Legge 190/2012 ("Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione") – richiedono un modello organizzativo che includa un approccio per processi, ai fini di meglio identificare e prevenire i rischi verso cui sono potenzialmente esposte le attività dell'Agenzia.
In considerazione di quanto sopraindicato, è opportuno che – in occasione dell'applicazione del GDPR – l'Agenzia implementi il proprio sistema organizzativo con l'approccio per processi, condizione basilare per l'impostazione e la conduzione delle attività di monitoraggio e di accountability.
In particolare, riveste particolare importanza l'identificazione e mappatura dei processi in modo unitario, a prescindere dall'istanza contingente che ne motiva la realizzazione (quali l'applicazione di una specifica norma o la risposta ad una puntuale esigenza gestionale).
Infatti, i processi – rappresentando come effettivamente sono svolte le attività dell'Agenzia – se declinati con un approccio unitario (valido per tutta l'Agenzia e per tutte le casistiche applicative) e con la stessa metodologia di rilevazione consentono una più semplice individuazione delle responsabilità, dei potenziali rischi cui sono esposti gli obiettivi di ogni processo e del livello di adeguatezza delle misure di sicurezza, di prevenzione e/o di controllo esistenti.
Inoltre, lo stesso "linguaggio" consente per ogni processo - da un lato - la confrontabilità del grado di rilevanza dei diversi rischi, indipendentemente dall'ambito operativo in cui possono manifestarsi e dall'altro, la rilevazione di ogni misura tecnica e organizzativa applicata ai fini della mitigazione dei rischi rilevati, con la conseguente possibilità di razionalizzare le misure di prevenzione.
In conclusione, l'approccio unitario per processi riveste un ruolo cruciale per l'implementazione e l'aggiornamento di un Sistema Organizzativo in grado di realizzare una gestione dei rischi efficace ed efficiente.
Il Modello organizzativo richiesto dal GDPR rientra nella categoria dei Compliance Program, cioè di modelli organizzativi atti alla prevenzione di rischi di compliance cui è esposto l'Ente.
Per rischio di compliance si intende il rischio di incorrere in sanzioni, subire perdite o danni reputazionali in conseguenza della mancata osservanza di leggi, regolamenti o provvedimenti.
Il Modello per l'applicazione del GDPR, come gli altri Compliance Program, prevede per la propria realizzazione 2 macrofasi:

a. Risk Assessment (identificazione e valutazione dei rischi)
b. Verifica ed eventuale implementazione del Sistema dei controlli (idonei a prevenire i rischi individuati nella macrofase 1).

Il Sistema dei controlli, con riferimento al GDPR, può essere correlato alle misure tecniche e organizzative adeguate a garantire che il trattamento è effettuato in conformità al Regolamento stesso.
Il Sistema dei controlli, o Sistema di controllo interno, in base ai framework di riferimento più diffusi è

composto da diversi elementi di controllo generale. Inoltre, le componenti del Sistema di controllo interno devono integrarsi tra loro nel rispetto di una serie di principi di controllo.
Il Sistema organizzativo costituisce uno degli elementi di rilievo del Sistema di controllo interno: tener in considerazione le correlazioni del Sistema organizzativo con gli altri componenti del Sistema di controllo interno può consentire di:

a. rafforzare la capacità di mitigazione dei rischi delle misure organizzative
b. ampliare lo spettro di compensazione/adattamento delle misure organizzative rispetto ad eventuali criticità – temporanee o durature – delle misure tecniche per la prevenzione dei rischi
c. favorire un approccio coordinato all'applicazione dei diversi Compliance Program e, conseguentemente, la loro efficacia di prevenzione dei rischi individuati.

Il principio di accountability sancito dal regolamento europeo in materia di protezione dei dati richiede che l'organizzazione e i processi, siano impostati in modo tale a rendere possibile la attività di "rendere conto" delle misure messe in atto per la protezione dei dati.
Principio che si lega fortemente con l'altro della data protection by design in quanto se nella progettazione di nuove iniziative si tiene presente la tematica della protezione dei dati fin dall'inizio e aggiornata nel tempo, l'attività di rendicontazione delle scelte diviene una logica conseguenza della lettura delle decisioni prese e delle relative motivazioni. Se così non fosse e si dovesse rendere conto di quanto fatto solo a valle della rilevazione degli incidenti, ovviamente richiederebbe una ricerca a ritroso non certo agevole sia nel risultato sia nei tempi mettendo il Titolare e tutta l'organizzazione in situazioni sanzionabili a norma del GDPR.
L'organizzazione dell'Agenzia può essere chiamata a rendere conto in varie circostanze:

a) su istanza del Garante in attività ispettiva o a seguito di segnalazioni o denunce
b) su istanza degli interessati nell'esercizio dei loro diritti
c) su istanza del DPO in attività di monitoraggio o a seguito di segnalazioni da parte degli interessati.

In particolare l'attività di "rendere conto" si sostanzia:

1) individuazione del processo in esame
2) rispetto dei principi generali applicabili ai trattamenti,
3) Misure di sicurezza messe in atto sulla base del processo di valutazione degli effetti (danni) sulle libertà e i diritti individuali delle persone fisiche, dei rischi, delle minacce e della probabilità di accadimento.

All'interno del Processo di Data Protection by design and by default, è prevista la costituzione di un dossier data protection per ogni processo che tiene traccia delle scelte, delle misure e delle motivazioni che hanno portato alla loro determinazione. Il dossier è tenuto aggiornato come risorsa condivisa dalle diverse figure responsabili dei vari ambiti.
Questo sia che sia stata effettuata a norma dell'art. 35 (C84, C89-C93, C95) una specifica DPIA, sia che non sia stata effettuata in quanto ritenuta non necessaria.

9.6 Processo: Garanzia e tutela dei diritti degli interessati

Il GDPR dedica l'intero Capo III ai diritti dell'interessato ed in particolare:

1. art. 12 trasparenza e modalità attraverso le quali l'interessato viene emesso a conoscenza di come può esercitare i suoi diritti,
2. art. 13 e 14 Le informazioni che devono essere fornite all'interessato e le relative modalità
3. art. 15 i diritti di accesso dell'interessato alla conoscenza di quali dati che a lui si riferiscono

sono in possesso del titolare, i relativi trattamenti e quanto a questi è correlato in termini di misure di sicurezza.

4. art. 16 il diritto di rettifica
5. art. 17 il diritto alla cancellazione (oblio)
6. art.18 il diritto di limitazione del trattamento
7. art.19 obbligo di notifica da parte del Titolare all'interessato in caso di rettifica, cancellazione, limitazioni
8. art. 20 Portabilità dei dati, la possibilità cioè, di richiedere e ottenere su adeguato supporto tecnologico e in formati elaborabili i dati detenuti dal Titolare.
9. art. 21 opposizione al proseguimento di un trattamento
10. art. 22 l'interessato ha il diritto di non essere sottoposto ad un processo automatizzato che produca effetti giuridici che lo riguardano o che incida sulla sua persona, salvo i casi previsti al comma 2 dello stesso articolo.

I diritti richiamati, a norma dell'art. 23 (C73) e per le motivazioni espresse nello stesso articolo, possono subire delle limitazioni.

In estrema sintesi il processo prevede l'informazione preventiva dell'interessato, la richiesta del consenso dove applicabile, come misure antecedenti l'avvio del trattamento con riguardo ad una persona fisica e il diritto della stessa di poter intervenire, con modalità certe e tempi definiti, nell'ambito dei trattamenti e relativi dati che lo riguardano, sia per acquisirne la conoscenza sia per richiedere eventuali misure fra quelle previste dal regolamento.

10. Modello organizzativo da adottare

Come evidenziato, nell'organizzazione Data Protection esistono alcuni ruoli e funzioni chiaramente identificati in capo a determinate istanze organizzative, così come sono chiaramente identificati i processi che sostengono la compliance organizzativa al GDPR.

Ferme restanti le competenze e i vincoli dei diversi soggetti nei rispettivi ruoli, vengono individuate le nuove strutture di supporto e la loro collocazione organizzativa per la gestione dei processi.

Le competenze e le figure di supporto sono quelle riconducibili ai Data Protection Specialist e quelle dell'ufficio del DPO.

Nel seguito si prendono i processi GDPR e per ciascuno di essi si descrivono i compiti nei diversi livelli organizzativi.

10.1 Data Protection by design and by default

Tale processo riguarda la "formazione degli atti" da cui discendono trattamenti di dati personali e la realizzazione di sistemi automatizzati o meno che attuano indirizzi e scelte definiti in tali atti.

Al fine di presidiare il processo di formazione degli atti in modo che sia compliant con il GDPR, i data protection specialist hanno il compito di supportare i dirigenti nel definire, per ogni atto di loro competenza, se è coinvolta o meno la problematica della protezione di dati personali, e se nel caso aggiornare l'atto con quanto necessario ad impostare gli elementi di data protection e seguire l'evoluzione susseguente l'adozione dell'atto stesso. Tale personale costituisce l'interfaccia organizzativa e naturale con il DPO e con l'ufficio del DPO.

Gli atti, saranno centralmente verificati dall'ufficio del DPO che provvederà a formalizzare rilievi e procederà a fare attività di monitoraggio attraverso il Direttore di ARTEA Per quanto attiene le richieste di pareri verso il DPO nelle diverse fasi di formazione degli atti, che nascono in Agenzia,

questa può avvalersi, dei data protection specialist per il supporto diretto e di interlocuzione verso il DPO.

10.1.1 Mantenimento del registro dei trattamenti

Il censimento dei trattamenti e il conseguente aggiornamento del registro è competenza del singolo dirigente in quanto delegato dal Titolare, e le figure di data protection specialist, supportano i dirigenti, nella definizione di nuovi trattamenti nella modifica di trattamenti esistenti e nella compilazione del registro.

10.1.2 Valutazione Impatto (DPIA)

La valutazione di impatto rappresenta una componente fondamentale del processo di data protection by design e by default e costituisce un documento aggiuntivo che va ad aggiungersi alla formazione corretta di atti che per natura dei loro contenuti riguardano trattamenti di "dati particolari".
Il DPO assicura, a norma dell'art.35 punto 2 e art. 39 lettera c) del GDPR, supporto di consulenza alla redazione delle DPIA. La formulazione della DPIA è competenza dei dirigenti delegati che la redigono avvalendosi delle competenze specifiche, dei data protection specialist e dell'ufficio del DPO.
Pertanto i data protection specialist con il supporto dell'ufficio del DPO o di assistenza esterna (contratti di servizio, convenzioni con università, ecc.), hanno il compito di affiancare i dirigenti nella esecuzione della DPIA.

10.2 Accountability

Premesso che:
a) l'attività di accountability a norma del regolamento è in carico al titolare o suo delegato e quindi in capo ad ogni dirigente, che per questo compito si avvale di strutture centralizzate quali il Security Manager e l'ufficio del DPO
b) l'attività di monitoraggio tecnico è in carico al security manager e all'ufficio del DPO per le valutazioni del caso, e coinvolge per i suoi effetti la struttura del Responsabile.
In tale contesto il ruolo dei singoli dirigenti è quello di offrire il massimo supporto, in maniera diretta o attraverso i Data Protection Specialist, all'ufficio del DPO e al DPO stesso in tutte quelle fasi in cui possa venir richiesto dal Garante o dagli interessati, informazioni in merito ai processi messi in atto al fine di garantire il pieno rispetto del GDPR

10.3 Monitoraggio, controllo misure di sicurezza e gestione degli incidenti

Tale processo è gestito centralmente dalle strutture del Security Manager, dall'ufficio del DPO e dalle strutture tecniche di riferimento, per la gestione dei sistemi o degli archivi cartacei.

10.4 Informazione e Garanzia dei diritti degli interessati

L'informazione agli interessati risulta a carico del dirigente con il supporto consulenziale dell'ufficio del DPO cui spetta il compito di definire la modulistica standard. La garanzia dei diritti dell'interessato è in carico all'ufficio del DPO.

10.5 I compiti dei Data Protection Specialist

Sulla base di quanto sopra espresso si riepilogano i compiti dei Data Protection Specialist individuati dal Direttore dell'Agenzia che supportano le strutture, per tutte le questioni attinenti al trattamento dei

dati personali e rappresentano l'interlocutore operativo verso l'ufficio del DPO.
I Data Protection Specialist svolgono attività informativa nei confronti dell'Ufficio del DPO, perché quest'ultimo abbia tutti gli elementi e riscontri che – unitamente alle evidenze della documentazione richiesta dal GDPR – i trattamenti di dati personali svolti nell'ambito dell'Agenzia siano effettuati in conformità alle prescrizioni del GDPR e alle istruzioni del Titolare.
In particolare, in collaborazione con il Security Manager e l'ufficio del DPO, supportano i dirigenti dei Settori per i seguenti compiti:

a. l'aggiornamento della mappa dei processi,
b. la formazione degli atti al fine di garantire il principio di data protection by design (decreti, bandi gara, contratti, convenzioni, procedure, manuali...),
c. l'individuazione e registrazione corretta dei trattamenti,
d. in merito alle informative da dare agli interessati, sulla base delle indicazioni dell'ufficio DPO,
e. l'individuazione e valutazione dei rischi in fase preventiva e di DPIA, in accordo con l'ufficio del DPO,
f. la richiesta di intervento del Security Manager per individuare e valutare l'adeguatezza delle misure di sicurezza, sia in fase preventiva sia successiva ad attività di monitoraggio,
g. la richiesta di pareri al DPO e nelle risposte alle richieste dei cittadini,
h. la verifica che il personale sia informato e formato sui temi del GDPR e che gli autorizzati abbiano ricevuto e compreso le istruzioni, al fine di assicurare quanto previsto art. 39 lettera a) del GDPR e Art.2-quaterdecies decreto legislativo n. 196/2003,
i. la piena e fattiva collaborazione all'ufficio del DPO e al Security manager in caso di incidente/data breach e per tutte le azioni conseguenti,
j. la piena e fattiva collaborazione all'ufficio del DPO e al Security Manager in caso di ispezione o indagine delle autorità di controllo.

10.6 Rapporti fra DPO e il Titolare

Il DPO, nel caso rilevasse criticità di ordine generale in merito all'obiettivo di garantire la compliance al GDPR, provvede a segnalare al Titolare, ovvero il Direttore di ARTEA, le criticità organizzative e tecniche o le eventuali violazioni accertate, che possano comportare l'insorgere di una responsabilità in capo all'Agenzia per non conformità al GDPR.
Tali comunicazioni, su una base periodica e di necessità, riguardano ogni aspetto che il DPO ritiene di sottoporre al Titolare, ai fini della conformità al GDPR, tra cui si citano a titolo esemplificativo:

a. informazioni sul livello di adeguatezza della sicurezza e della capacità di prevenzione di trattamenti in violazione del Regolamento,
b. evidenze di ipotesi di trattamento a "rischio elevato",
c. istanze da presentare all'Autorità di controllo,
d. ispezioni da parte dell'Autorità di controllo,
e. criticità inerente alla protezione dei dati personali, anche in relazione ad eventuali segnalazioni esterne o interne ricevute dall'Agenzia.

11. Rapporto fra processi GDPR e Procedimenti amministrativo decisionali

Nella precedente sezione abbiamo esaminato i processi che il GDPR prevede nell'ambito di una organizzazione compliant, coerente ai suoi principi e ai suoi dettati. In questa sezione delle linee guida, individueremo le misure necessarie a rendere tali processi intrinsecamente connessi con i procedimenti

amministrativi dell'Agenzia al fine di non creare percorsi paralleli di difficile gestione e possibili disallineamenti fra i processi decisionali e attuativi e quelli di valutazione dei rischi in caso di trattamenti di dati personali.

11.1 Data Protection by design and by default

Come richiesto dal processo di Data Protection by Design, il tema della protezione dei dati personali deve essere preso in considerazione fin dal nascere di una nuova iniziativa.
Pertanto in ogni atto dell'amministrazione, occorre che sia data evidenza se negli effetti dell'atto vengono coinvolti processi e trattamenti relativi a dati personali. In questo caso il dirigente, nella sua funzione di “delegato del Titolare”, con il supporto dei Data Protection Specialist e la consulenza dell’ufficio del DPO, provvede ad aprire il "Dossier Data Protection", ed è responsabile della sua tenuta attraverso un aggiornamento costante.
Al fine di dare supporto a tale procedimento occorre:
- che sia modificata la procedura di gestione degli atti in modo da inserire a cura del dirigente se quell'atto ha rilevanza in materia di dati personali, e se sì alcuni dati descrittivi in termini di trattamenti, liceità degli stessi, caratteristiche dei dati stessi e numerosità e tipologia degli interessati, l'identificativo del dossier se esistente oppure la creazione di uno nuovo. Nel caso di atti che si riferiscono a dossier già attivati si dovrà rendere conto del fatto che il dossier è stato aggiornato con i documenti previsti nel processo di Data Protection by Design,
- che sia realizzato all'interno del sistema documentale il Dossier Data Protection per i diversi processi che verranno attivati.
Si ricorda che la gestione del Dossier è finalizzata a rendere agevole l’attività di accountability in quanto terrà traccia di tutti gli adempimenti fatti, di tutte le scelte fatte e delle relative motivazioni.
L’ufficio del DPO procede alla verifica preventiva della rispondenza al GDPR ed effettua un monitoraggio a campione sui decreti.

11.2 Mantenimento del registro dei trattamenti

I Dirigenti:
a) al momento della predisposizione di atti amministrativi individuano se quell'atto prefigura o interviene in processi che prevedono il trattamento di dati personali, nonché se è necessario prevedere la stipula di appositi data protection agreement in base alle regole dedicate ai rapporti DP con terze parti In tale caso con il supporto degli estensori e dei data protection specialist individuano i trattamenti e ne avviano la registrazione nell'apposito registro, aprono un Dossier Data Protection, rendono conto nell'atto dei nuovi trattamenti e del nuovo Dossier. Nel caso di atti che intervengono successivamente su trattamenti già individuati e/o Dossier già aperti, si procede alla verifica di quanto registrato nel registro dei trattamenti, si aggiorna se del caso il dossier, si dà atto, nell'atto, degli avvenuti aggiornamenti.
b) attraverso i Data Protection Specialist, e se ritenuto necessario, consultano il DPO per tutte le questioni riguardanti la individuazione dei trattamenti, delle loro caratteristiche e delle azioni da porre in essere per la loro corretta gestione nel tempo.

11.2.1 Richiesta pareri, formulazione e gestione della DPIA

I Dirigenti:
a) attraverso il supporto dei Data Protection Specialist dell’Agenzia e per mezzo dell’applicativo

dedicato "Richiesta Pareri", possono indirizzare all'attenzione del DPO la richiesta di pareri formali in merito a questioni riguardanti la protezione dei dati.

b) attraverso il coinvolgimento dei Data Protection Specialist predispongono nei casi previsti e con il supporto dell'"ufficio del DPO", la DPIA.

c) richiedono il parere del DPO a chiusura della DPIA.

d) aggiornano il Dossier Data Protection con la DPIA.

11.3 Monitoraggio Organizzativo e Accountability

Come evidenziato nelle precedenti sezioni elemento fondamentale per la compliance al GDPR è mettere in atto meccanismi organizzativi che rendano l'attività di protezione del dato, una attività, un pensiero corrente che accompagni l'operato di ogni dipendente con particolare riferimento all'azione dirigenziale che si assume la responsabilità derivante dal suo ruolo di delegato del titolare. Al tempo stesso i dirigenti devono essere messi in grado dall'amministrazione di poter svolgere con efficienza ed efficacia la loro responsabilità. In questa ottica Il DPO con il supporto del Direttore di ARTEA provvederà a redigere apposita relazione sull'adeguatezza dell'organizzazione ai compiti derivanti dall'attuazione del GDPR.

I Dirigenti devono:

a) in fase di monitoraggio da parte dell'ufficio del DPO, fornire la massima collaborazione tesa ad evidenziare problemi e ad individuare soluzioni,

b) in fase di segnalazioni da parte di interessati provvedere, con il supporto eventuale del DPO o del suo ufficio, a mettere in atto misure adeguate a rendere conto delle situazioni oggetto di segnalazione ed eventualmente a mettere in atto misure idonee alla risoluzione dei problemi evidenziati

c) in fase di ispezione o indagine del garante offrire tutta la collaborazione possibile.

11.4 Monitoraggio tecnologico, controllo misure di sicurezza e gestione degli incidenti

Il Monitoraggio tecnologico è in carico al Security Manager che provvede:

a) alla redazione e attuazione di un piano per le verifiche sulle misure di sicurezza messe in atto dai dirigenti responsabili nei sistemi e delle applicazioni IT dell'Agenzia o di fornitori esterni,

b) alla verifica della rispondenza delle misure di sicurezza in essere alle linee guida emesse dal DPO

c) alla relazione periodica sulle misure di sicurezza adottate evidenziando punti di criticità e proponendo remediation plan,

La gestione degli incidenti è in carico al Security Manager che:

a) registra l'incidente

b) avvisa il titolare dei trattamenti coinvolti nell'incidente

c) provvede ad una valutazione dell'incidente in termini di gravità con la collaborazione del dirigente/i coinvolto/i nel trattamento/i

d) Provvede a relazionare al DPO per la decisione relativa alla segnalazione al garante, alla segnalazione agli interessati, alla segnalazione all'autorità giudiziaria se trattasi di atto potenzialmente doloso.

I dirigenti responsabili per ambiti di competenza alla sicurezza IT o titolari di contratti in essere per la fornitura di servizi IT debbono assicurare:

a) tutte le condizioni idonee, di collaborazione e contrattuali verso fornitori (individuati come Responsabili) al fine di consentire un efficiente ed agevole lavoro del Security Manager,

b) l'attuazione del remediation plan indicato dal Security Manager nei tempi indicati nello stesso
c) fornire il supporto in caso di segnalazioni di incidenti al fine di comprendere la gravità degli stessi
d) la tempestiva segnalazione al security manager della evidenza di incidenti che possono aver coinvolto dati personali

11.5 Garanzia dei diritti degli interessati

I Dirigenti, al momento della definizione del trattamento identificano e mettono in atto le procedure idonee a fornire adeguata informativa agli interessati. Per la corretta individuazione dei contenuti e della forma dell'informativa il dirigente si avvale dei fac-simili messi a disposizione dall'ufficio del DPO, del supporto dei Data Protection Specialist dell'Agenzia o dell'ufficio del DPO.
Gli interessati tramite i punti di contatto pubblicati per l'interlocuzione con il titolare e il DPO e attraverso specifico modulo effettuano la richiesta, il DPO provvede alla risposta e a dare indicazioni alle strutture competenti al fine di dare fattiva e tempestiva risposta alle richieste.
Per tale obiettivo, occorre dare urgente attuazione alla previsione di istituire il "fascicolo del cittadino" come collezione delle banche dati o archivi nelle quali sono presenti i relativi dati personali.

12. Tabella riepilogativa attribuzione responsabilità e attività

Nella seguente tabella sono riassunti, per sommi, capi ruoli e relative responsabilità a seguito dell'applicazione del GDPR al modello organizzativo di ARTEA.
Per ogni componente dell'organizzazione è stato individuato: il ruolo assegnato in virtù del GDPR e degli atti di Giunta, e le attività che sono assegnate per la corretta gestione dei processi. Tale tabella è riepilogativa di quanto descritto in dettaglio nel documento Data Protection Policy.

Organizzazione	Ruoli e responsabilità in relazione al GDPR ed ai relativi processi
ARTEA	Ruolo GDPR: Assume, a norma dell'Art. 4 punto 7 del GDPR, il ruolo di Titolare dei trattamenti afferenti alle finalità di ARTEA, nella persona del Direttore. Processo Formazione degli atti (data protection by design/default) Approva atti di organizzazione o di indirizzo al fine di garantire la compliance al GDPR Processo Accountability Adozione di atti di organizzazione idonei a garantire la compliance al GDPR
Il Direttore	Ruolo GDPR: assume a seguito del decreto n. 97/2018 la figura di Titolare per i trattamenti di sua diretta responsabilità. Assolve, nelle forme più opportune, all'attuazione dell'organizzazione e dei processi in materia di data protection. Processo di formazione degli atti: L'organizzazione della direzione, attraverso i "Data Protection Specialist", realizza il supporto ai settori e posizioni dirigenziali individuali, al fine del rispetto dei principi e dei procedimenti per la compliance al GDPR. Processo di accountability Adotta di misure e direttive idonee a garantire la compliance al GDPR Processo di gestione degli incidenti Attua, su indicazione dell'ufficio del DPO o del security Manager, misure organizzative o tecniche tese a diminuire i rischi e le probabilità di incidente

	nell'ambito dei trattamenti di sua responsabilità. Processo dei diritti degli interessati Collabora attivamente con il DPO e l'Ufficio del DPO al fine di rispondere nei tempi previsti alle richieste degli interessati, del garante o dell'autorità giudiziaria.
I Dirigenti	Ruolo GDPR: Assumono, a seguito del decreto n. 97/2018, la figura di Delegato del Titolare per i trattamenti di loro diretta responsabilità. Processo di formazione degli atti: Cura la gestione del registro dei trattamenti. Predispone gli atti, esegue DPIA, emette indirizzi e istruzioni operativi per il personale in relazione e al rispetto del GDPR e della Policy dell'Agenzia, con il supporto dei data protection specialist, e se necessario con il supporto dell'ufficio del DPO Processo di Accountability Organizzazione della documentazione relativa ai trattamenti di cui sono titolari o responsabili in una logica di dossier che riassuma le decisioni prese e le relative motivazioni Processo di gestione degli incidenti Ricevono o rilevano incidenti che coinvolgono trattamenti di cui sono titolari, concorrono alla determinazione della gravità dell'incidente e determinano le comunicazioni da fare al garante, alla autorità giudiziaria, in collaborazione con l'ufficio del DPO e il security manager Processo dei diritti degli interessati Collaborano attivamente con il DPO e l'Ufficio del DPO al fine di rispondere nei tempi previsti alle richieste degli interessati, del garante o dell'autorità giudiziaria.
Data Protection Officer	Ruolo GDPR v.di art 38 e 39 del GDPR decreto di nomina n. 45/2018
Security Manager	Processo di formazione degli atti Offre supporto tecnico per gli aspetti inerenti la sicurezza IT in fase di DPIA. Processo di accountability Predispone ed esegue le verifiche periodiche sulle misure di sicurezza adottate, Processo di gestione degli incidenti Gestisce il registro degli incidenti e supporta le strutture competenti nelle diverse tipologie di comunicazione. decreto di nomina n. 97/2018
Ufficio del DPO	Processo di formazione degli atti: Gestisce il registro dei trattamenti per quanto attiene il rispetto al GDPR; verifica e supporta il titolare e i suoi delegati nella tenuta del registro dei trattamenti e nella corretta formulazione degli atti; garantisce adeguata consulenza giuridica, tecnologica e organizzativa nella formulazione delle DPIA, se richiesto, e nella formulazione di atti convenzionali, contratti o protocolli di intesa. Processo di Accountability Svolge attività di verifica connesse all'attuazione del principio di accountability e si avvale delle strutture dell'Agenzia ed in particolare del responsabile dei sistemi informativi, del responsabile delle Infrastrutture Information

	Technology, del Security IT manager e del responsabile del sistema di documentazione ed archivi per lo svolgimento delle stesse. Processo di gestione degli incidenti Rileva le segnalazioni degli incidenti e congiuntamente con il security manager e il titolare del trattamento ne predispone la valutazione e persegue le azioni necessarie in modo diretto o dando indicazioni per il loro assolvimento. Processo dei diritti degli interessati In carico all'ufficio del DPO che si avvale della collaborazione delle strutture regionali al fine del rispetto dei tempi
Data Protection Specialist V.di Modello organizzativo, per i compiti assegnati	Processo di formazione degli atti Forniscono consulenza alle strutture dell'Agenzia, nella individuazione dei trattamenti, nella formulazione delle DPIA, nella predisposizione di atti e convezioni che prefigurino dei rapporti inerenti la Data Protection. Svolgono attività di consulenza, di affiancamento per la corretta formulazione degli atti/decreti. Svolgono attività di consulenza insieme al DPO, su tutti gli aspetti che riguardano il GDPR. Supportano i dirigenti nella verifica di qualità del registro dei trattamenti. Processo di accountability Offrono consulenza ai settori nei processi di verifica e controllo, collaborando con il DPO e l'Ufficio del DPO Processo di gestione degli incidenti Ricevono comunicazione da parte dell'ufficio del DPO o del Security Manager di incidenti avvenuti o comunicano al security manager incidenti di cui vengono a conoscenza diretta, che coinvolgono trattamenti afferenti alla direzione, affiancano se necessario il dirigente, in collaborazione con l'ufficio del DPO e il security manager, nella determinazione della gravità dell'incidente e concorrono a determinare le comunicazioni da fare al garante, alla autorità giudiziaria, … Processo dei diritti degli interessati Collaborano attivamente con il DPO e l'Ufficio del DPO al fine di rispondere nei tempi previsti alle richieste degli interessati, del garante o dell'autorità giudiziaria.

Allegato 2 - Controlli e sanzionamento

1. Le modalità di estrazione delle sedi CAA e dei fascicoli da sottoporre a controllo sono riportate nel Manuale Operativo per il Riconoscimento dei Centri di Assistenza Agricole e per i Controlli delle Sedi Operative.
Ogni fascicolo viene controllato con le istanze relative all'anno di riferimento del controllo o agli anni precedenti se non presenti nello stesso anno.
2. In ogni fascicolo controllato verrà inserito:
- ID 1966 in caso di esito negativo
- ID 66 in caso di esito positivo
Comporta l'inserimento dell'ID 1966:
a) mancanza dell'ID 6 – Incarico tenuta fascicolo
b) mancanza del CUDOC sui documenti non scansionati
c) mancanza del documento di identità valido alla data della firma dell'ultima istanza se non firmata digitalmente
d) mancanza o non correttezza dei titoli di conduzione
e) mancanza della sottoscrizione nonché del documento di identità valido in relazione alle dichiarazioni presenti in fascicolo
f) mancanza dei documenti originali presenti in fascicolo
g) mancanza di firma e/o di un documento di identità valido allegato alle istanze ricevute
h) mancanza delle istanze presso la sede riconosciuta dove sono state presentate
i) altre irregolarità (da specificare)
L'inserimento dell'ID 1966 avviene anche se l'irregolarità è sanabile.
In tutti i casi in cui un fascicolo venga sanzionato con l'inserimento dell'ID 1966 negativo, ARTEA si impegna a comunicare tempestivamente al Responsabile Tecnico del CAA i fascicoli sanzionati e la motivazione. Il CAA verso i provvedimenti adottati potrà presentare eventuali memorie difensive.
3. In caso di inserimento di ID 1966 si applica una penale pari all'importo del pagamento unitario previsto, di cui all'art. 8 comma 3, per l'anno di riferimento del controllo.
4. Nel caso in cui le anomalie riscontrate al momento del controllo non siano sanate nei 30 giorni successivi alla comunicazione da parte di ARTEA, i fascicoli che presentano delle irregolarità vengono esclusi dai corrispettivi anche degli anni successivi quello di riferimento del controllo fino alla risoluzione delle anomalie, comunicata dal CAA al personale addetto ai controlli tramite e-mail.
5. Nel caso in cui venga riscontrata una percentuale superiore al 50% di fascicoli negativi rispetto al campione estratto per singola sede operativa, ovvero per gravi inadempienze stabilite insindacabilmente da ARTEA, oltre al mancato pagamento dell'importo previsto per le pratiche negative, ARTEA potrà:
a) nel caso in cui le irregolarità siano lievi, applicare una sanzione pari al 25% dell'importo relativo a tutti i fascicoli attivi per l'anno di riferimento del controllo per la sede operativa sottoposta a controllo;
b) nel caso in cui le irregolarità siano gravi, applicare una sanzione pari al 50% dell'importo relativo a tutti i fascicoli attivi per l'anno di riferimento del controllo per la sede operativa sottoposta a controllo;
c) nel caso in cui le irregolarità siano tali da comportare il ritiro del riconoscimento della sede operativa, applicare una sanzione pari al 100% dell'importo relativo a tutti i fascicoli attivi per l'anno di riferimento del controllo per la sede operativa sottoposta a controllo. Il ritiro del riconoscimento della sede operativa che può essere temporaneo o definitivo.

6. Nel caso di ritardo nello svolgimento dell'attività istruttoria per cause addebitabili al CAA, si applicherà, a partire dal giorno successivo alla scadenza fissata ed esclusi i giorni festivi, una penale giornaliera per ogni domanda in istruttoria consegnata in ritardo pari al 5% del compenso unitario pattuito, per un periodo massimo di 15 giorni lavorativi. Allo scadere dei 15 giorni non sarà dovuto alcun compenso.
7. In caso di violazione degli obblighi di cui agli articoli 2 comma 4 lettera f e 12 comma 8 della Convenzione generale si applica la penale pari al 5% dei compensi da erogare sul totale dei compensi CAA per l'anno di riferimento del controllo. Analoga penale sarà applicata anche in caso di ritardo superiore a 30 giorni nella trasmissione di dati, comunicazioni e relazioni.

Allegato 3 - Autocertificazione conflitto di interessi e n.d.a. ISO 27001 e ISO 37001

Dichiarazione sostitutiva ai sensi dell'art. 47 D.P.R. 445/2000
sul conflitto di interessi, anche potenziale, e dichiarazione sulla sicurezza delle informazioni

Il/La sottoscritto/a _____, C.F. _____
consapevole di quanto previsto dagli artt. 75 e 76 del D.P.R. 445/2000, in merito alle conseguenze penali derivanti da dichiarazioni mendaci, formazione o uso di atti falsi e loro esibizione,

DICHIARA

1. Conflitto di interessi

• di rientrare tra le seguenti categorie di soggetti tenuti a dichiarare il conflitto di interessi nei confronti di ARTEA (specificare quale):

- Dipendente di ARTEA;
- Soggetto non dipendente di ARTEA (a titolo esemplificativo ma non esaustivo dipendenti/operatori CAA, GAL, dipendenti e/o enti collegati di Regione Toscana che operano in Anagrafe, concessionari e appaltatori di ARTEA, soggetti comunque legati da un rapporto di servizio con ARTEA: _____;

• di aver preso conoscenza della policy di ARTEA in materia di "Prevenzione del rischio di conflitto di interesse", consultabile alla pagina home page/amministrazione trasparente/altri contenuti-conflitto d'interessi del sito di ARTEA;

• di NON trovarsi in situazioni di conflitto di interesse, anche potenziale, così come disciplinato dalla normativa interna ed europea vigente e meglio indicato nella citata Policy, in riferimento a beneficiari presenti nella Anagrafe di ARTEA e/o a soggetti fornitori di ARTEA non presenti in Anagrafe.

In caso di conflitto di interessi, anche potenziale, deve essere di seguito specificato il codice fiscale del soggetto nei cui confronti sussiste il conflitto:
_____
_____;

• di essere a conoscenza dell'obbligo di comunicazione di ogni variazione nella posizione del sottoscrivente, intervenuta successivamente alla presente dichiarazione, che dovrà essere tempestivamente comunicata al responsabile dell'ufficio di appartenenza, con contestuale aggiornamento della dichiarazione sostitutiva stessa;

• che il dirigente/responsabile della struttura di appartenenza, deputato al controllo della presente dichiarazione è _____ PEC: _____

• di essere a conoscenza dell'obbligo di rinnovare la presente dichiarazione al primo accesso annuale al Sistema Informativo di ARTEA e in ogni caso entro il 1° marzo di ogni anno, nel rispetto dei contenuti propri della Policy di cui sopra;

• di essere a conoscenza che verranno effettuati controlli sui soggetti tenuti a rendere la presente dichiarazione e che, in ogni caso, al mancato rinnovo della dichiarazione nei termini consegue la sospensione dell'autorizzazione all'accesso al sistema informativo fino alla sottoscrizione di una nuova dichiarazione;

• di essere a conoscenza del fatto che la comunicazione di conflitto dichiarato verrà registrata sul sistema informativo di ARTEA che raccoglie tutti i conflitti dichiarati.
In particolare, le comunicazioni di conflitto dei dipendenti di ARTEA saranno visibili dai dirigenti e dal direttore di ARTEA, mentre le comunicazioni di conflitto dichiarato da soggetti non dipendenti di ARTEA (a titolo esemplificativo ma non esaustivo **dipendenti/operatori** CAA, GAL, dipendenti e/o enti collegati di Regione Toscana che operano in Anagrafe, ovvero concessionari e appaltatori di ARTEA e/o soggetti comunque legati da un rapporto di servizio con ARTEA), saranno inviate altresì ai soggetti incaricati dei relativi controlli all'interno del rispettivo soggetto di appartenenza.

2. No disclosure agreement

Il sottoscritto, richiamati il DPR 62/2013, la DGR 978/2019 e le determine ANAC 12/2015 e 831/2016,

SI IMPEGNA INOLTRE

- a rispettare i principi enunciati nella Politica ISO per la Sicurezza dei dati e delle informazioni secondo la norma ISO 27001 e nella Politica per la Prevenzione della Corruzione di ARTEA secondo la norma ISO 37001, nonché nel Codice di Condotta per i dipendenti pubblici (documenti consultabili nelle apposite aree del sito di ARTEA);
- a mantenere la riservatezza ed a non divulgare qualsiasi informazione acquisita nel corso dello svolgimento dell'attività lavorativa e/o di collaborazione, indipendentemente dalla modalità di acquisizione (escluse naturalmente le informazioni di pubblico dominio);
- a dare immediata comunicazione di eventuali variazioni che, nel corso del rapporto di servizio, dovessero intervenire rispetto a quanto dichiarato nel presente atto.
- a produrre, su eventuale richiesta di ARTEA, per i dati non conservati presso una pubblica amministrazione, la documentazione idonea a confermare la veridicità dei dati dichiarati.

3. Privacy

Il sottoscritto dichiara di essere stato informato, ai sensi e per gli effetti di cui al Regolamento (UE) n. 679/2016, che i dati raccolti saranno trattati, anche con strumenti informatici, esclusivamente per le finalità per le quali la presente dichiarazione viene resa, così come indicato nell'informativa consultabile alla pagina dedicata alla Privacy.

In fede

Il/La Dichiarante _____

Data *Firma*

Allegato 4 - Autocertificazione fornitori sui requisiti ex art. 80 Codice Contratti e ISO 37001

DICHIARAZIONE SOSTITUTIVA DELL'ATTO DI NOTORIETÀ PER FORNITORI, ANCHE EX ART. 80 D.lgs. 50/2016

(*art. 47 del D.P.R. 28.12.2000, n. 445*)

Il/La sottoscritto/a _____nato/a a_____il_____

_____ residente a _____

_____in Via/Piazza_____

_____

nella sua qualità di_____e legale rappresentante della Società

_____

_____con sede legale in _____

_____

Via/Piazza_____

C.F. _____P.IVA n._____

e, limitatamente al comma 1, lettere a), b), b-bis), c), d), e), f), g) e al comma 2 anche in nome e per conto dei soggetti indicati nell'art. 80, comma 3, del D.lgs. n. 50/2016[1]

- **consapevole delle sanzioni penali previste dall'art. 76 del D.P.R. 28/12/2000, n. 445, nel caso di dichiarazioni mendaci, esibizione di atti falsi o contenenti dati non più corrispondenti al vero**

- **consapevole altresì che qualora emerga la non veridicità di una qualsiasi delle dichiarazioni ivi riportate, tutti i contratti sottoscritti tra la scrivente Società/Ditta e ARTEA si intenderanno risolti ipso jure ai sensi e per gli effetti dell'art. 1456 c.c.***

DICHIARA

l'inesistenza delle cause di esclusione dalla partecipazione ad una procedura d'appalto o concessione elencate nell'art.80 del D.lgs. n. 50/2016, ed in particolare:

1. che nei propri confronti e nei confronti dei soggetti sopra indicati non è stata pronunciata sentenza definitiva di condanna o emesso decreto penale di condanna divenuto irrevocabile, oppure

[1] I soggetti di cui all'art. 80, comma 3, sono i seguenti: il titolare e direttore tecnico, se si tratta di impresa individuale; un socio o il direttore tecnico, se si tratta di società in nome collettivo; i soci accomandatari o il direttore tecnico, se si tratta di società in accomandita semplice; i membri del consiglio di amministrazione cui sia stata conferita la legale rappresentanza, ivi compresi institori e procuratori generali, i membri degli organi con poteri di direzione o di vigilanza o i soggetti muniti di poteri di rappresentanza, di direzione o di controllo, il direttore tecnico o il socio unico persona fisica, ovvero il socio di maggioranza in caso di società con meno di quattro soci, se si tratta di altro tipo di società o consorzio; i soggetti cessati dalla carica nell'anno antecedente la data di pubblicazione del bando di gara o di invio della lettera d'invito.

sentenza di applicazione della pena su richiesta ai sensi dell'articolo 444 del codice di procedura penale per uno dei seguenti reati:

a) delitti, consumati o tentati, di cui agli articoli 416, 416-bis del codice penale ovvero delitti commessi avvalendosi delle condizioni previste dal predetto articolo 416-bis ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo, nonché' per i delitti, consumati o tentati, previsti dall'articolo 74 del decreto del Presidente della Repubblica 9 ottobre 1990, n. 309, dall'articolo 291quater del decreto del Presidente della Repubblica 23 gennaio 1973, n. 43 e dall'articolo 260 del decreto legislativo 3 aprile 2006, n. 152, in quanto riconducibili alla partecipazione a un'organizzazione criminale, quale definita all'articolo 2 della decisione quadro 2008/841/GAI del Consiglio;

b) delitti, consumati o tentati, di cui agli articoli 317, 318, 319, 319-ter, 319-quater, 320, 321, 322, 322bis, 346- bis, 353, 353-bis, 354, 355 e 356 del codice penale nonché all'articolo 2635 del codice civile;

b-bis) false comunicazioni sociali di cui agli articoli 2621 e 2622 del codice civile;

c) frode ai sensi dell'articolo 1 della Convenzione relativa alla tutela degli interessi finanziari delle Comunità europee;

d) delitti, consumati o tentati, commessi con finalità di terrorismo, anche internazionale, e di eversione
dell'ordine costituzionale reati terroristici o reati connessi alle attività terroristiche;

e) delitti di cui agli articoli 648-bis, 648-ter e 648-ter.1 del codice penale, riciclaggio di proventi di attività criminose o finanziamento del terrorismo, quali definiti all'articolo 1 del decreto legislativo 22 giugno 2007, n.109 e successive modificazioni;

f) sfruttamento del lavoro minorile e altre forme di tratta di esseri umani definite con il decreto legislativo 4marzo 2014, n. 24;

g) ogni altro delitto da cui derivi, quale pena accessoria, l'incapacità di contrattare con la pubblica amministrazione.

In caso contrario, dichiara nello spazio che segue le condanne riportate (indicare i soggetti specificando ruolo, imputazione e condanna)

2. che nei propri confronti e nei confronti dei soggetti sopra indicati non sussiste la causa di decadenza, di sospensione o di divieto previste dall'articolo 67 del decreto legislativo 6 settembre 2011, n. 159 o di un tentativo di infiltrazione mafiosa di cui all'articolo 84, comma 4, del medesimo decreto;

3. che l'operatore economico non ha commesso violazioni gravi, definitivamente accertate, rispetto agli obblighi relativi al pagamento delle imposte e tasse o dei contributi previdenziali, secondo la legislazione italiana o quella dello Stato in cui sono stabiliti[2] ed indica all'uopo i seguenti dati:

[2] Ai sensi dell'art. 80, comma 4, del D.lgs. n. 50/2016, "costituiscono gravi violazioni quelle che comportano un omesso pagamento di imposte e tasse superiore all'importo di cui all'articolo 48-bis, commi 1 e 2-bis del decreto del Presidente della Repubblica 29 settembre 1973, n. 602. Costituiscono violazioni definitivamente accertate quelle contenute in sentenze o atti amministrativi non più soggetti ad impugnazione. Costituiscono gravi violazioni in materia contributiva e previdenziale quelle ostative al rilascio del documento unico di regolarità contributiva (DURC), di cui all'articolo 8 del decreto del Ministero del lavoro e delle politiche sociali 30 gennaio 2015, pubblicato sulla Gazzetta Ufficiale n. 125 del 1° giugno 2015.Il presente comma non si applica quando l'operatore economico ha

- Ufficio Locale dell'Agenzia delle Entrate competente:

i. Indirizzo: _____

ii. numero di telefono: _____

iii. PEC, fax e/o e-mail: _____

- [*Se non iscritto all'INPS e/o INAIL*] Informazioni ai fini delle verifiche sulla regolarità contributiva previdenziale(*compilare sezione d'interesse*):

i. Posizione assicurativa INAIL: _____

cod. identificativo: _____

sede competente: _____

ovvero

ii. Posizione assicurativa INPS: _____

cod. identificativo: _____

sede competente:_____

ovvero

iii. Iscrizione altra cassa previdenziale:

cassa di appartenenza: _____

cod. identificativo: _____

Indirizzo: _____

4. che l'operatore economico non ha commesso gravi infrazioni debitamente accertate alle norme in materia di salute e sicurezza sul lavoro nonché agli obblighi di cui all'articolo 30, comma 3 del D.lgs. n. 50/2016;

5. che l'operatore economico non si trova in stato di fallimento, di liquidazione coatta, di concordato preventivo, salvo il caso di concordato con continuità aziendale, o nei cui riguardi non è in corso un procedimento per la dichiarazionedi una di tali situazioni, fermo restando quanto previsto dall'articolo 110 del D.lgs. n. 50/2016;

6. che l'operatore economico non si è reso colpevole di gravi illeciti professionali, tali da rendere dubbia la sua integrità o affidabilità nè ricorre nelle altre fattispecie di cui all'art. 80, lett. c-bis) e c-ter)[3];

7. che la propria partecipazione non determina una situazione di conflitto di interesse ai sensi dell'articolo 42, comma 2 del D.lgs. n. 50/2016, non diversamente risolvibile;

8. che la propria partecipazione non determina una distorsione della concorrenza derivante dal proprio precedente coinvolgimento nella preparazione della procedura d'appalto di cui all'articolo 67 del D.lgs. n. 50/2016 che non possa essere risolta con misure meno intrusive;

9. che l'operatore economico non è stato soggetto alla sanzione interdittiva di cui all'articolo 9,

---

ottemperato ai suoi obblighi pagando o impegnandosi in modo vincolante a pagare le imposte o i contributi previdenziali dovuti, compresi eventuali interessi o multe, purché il pagamento o l'impegno siano stati formalizzati prima della scadenza del termine per la presentazione delle domande".

[3] L'art. 80, comma 5, c-bis) e c-ter) prevede, tra le cause di esclusione: "c-bis) l'operatore economico abbia tentato di influenzare indebitamente il processo decisionale della stazione appaltante o di ottenere informazioni riservate a fini di proprio vantaggio oppure abbia fornito, anche per negligenza, informazioni false o fuorvianti suscettibili di influenzare le decisioni sull'esclusione, la selezione o l'aggiudicazione, ovvero abbia omesso le informazioni dovute ai fini del corretto svolgimento della procedura di selezione; c-ter) l'operatore economico abbia dimostrato significative o persistenti carenze nell'esecuzione di un precedente contratto di appalto o di concessione che ne hanno causato la risoluzione per inadempimento ovvero la condanna al risarcimento del danno o altre sanzioni comparabili; su tali circostanze la stazione appaltante motiva anche con riferimento al tempo trascorso dalla violazione e alla gravità della stessa;"

comma 2, lettera c) del D.lgs. n. 8 giugno 2001, n. 231 o ad altra sanzione che comporta il divieto di contrarre con la pubblica amministrazione, compresi i provvedimenti interdittivi di cui all'articolo 14 del D.lgs. n. 9 aprile 2008, n. 81 e che si trova in possesso dei requisiti d'idoneità di cui all'art. 26 del D.lgs. 81;

10. che l'operatore economico non ha presentato nella procedura di gara in corso e negli affidamenti di subappalti documentazioni non veritiere (art. 80, comma f-bis);

11. che l'operatore economico non è iscritto nel casellario informatico tenuto dall'Osservatorio dell'ANAC per aver presentato false dichiarazioni o falsa documentazione nelle procedure di gara e negli affidamenti di subappalti (art. 80, comma f-ter);

12. che l'operatore economico non è iscritto nel casellario informatico tenuto dall'Osservatorio dell'ANAC per aver presentato false dichiarazioni o falsa documentazione ai fini del rilascio dell'attestazione di qualificazione, per il periodo durante il quale perdura l'iscrizione;

13. che l'operatore economico non ha violato il divieto di intestazione fiduciaria di cui all'articolo 17 della legge 19 marzo 1990, n. 55;

14. che, ai sensi dell'art. 17 della legge 12.03.1999, n. 68:

(*Barrare la casella di interesse*)

☐ l'operatore economico è in regola con le norme che disciplinano il diritto al lavoro dei disabili poiché ha ottemperato alle disposizioni contenute nella Legge 68/99 o_____ _____(indicare la Legge Stato estero). Gli adempimenti sono stati eseguiti presso l'Ufficio _____ di_____Via_____fax_____ e-mail/PEC: _____

☐ l'operatore economico non è soggetto agli obblighi di assunzione obbligatoria previsti dalla Legge 68/99 per i seguenti motivi: [indicare i motivi di esenzione] _____

☐ in_____(Stato estero) non esiste una normativa sull'assunzione obbligatoria dei disabili;

15. che l'operatore economico: (*Barrare la casella di interesse*)

☐ non è stato vittima dei reati previsti e puniti dagli artt. 317 e 629 c.p., aggravati ai sensi dell'art. 7 del decreto
legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991 n. 203.

☐ è stato vittima dei suddetti reati ma hanno denunciato i fatti all'autorità giudiziaria;

☐ è stato vittima dei reati previsti e puniti dagli artt. 317 e 629 c.p., aggravati ai sensi dell'art. 7 del decreto legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991 n. 203, e non hanno denunciato i fatti all'autorità giudiziaria, in quanto ricorrono i casi previsti dall'art. 4, 1 comma, della legge 24 novembre 1981, n. 689.

16. (*Barrare la casella di interesse*)

☐ che l'operatore economico non si trova in alcuna situazione di controllo di cui all'articolo 2359 del codice civile o in una qualsiasi relazione, anche di fatto con alcun soggetto, se la situazione di controllo o la relazione comporti che le offerte sono imputabili ad un unico centro decisionale, e di aver formulato autonomamente l'offerta.

ovvero

☐ che l'operatore economico non è a conoscenza della partecipazione alla medesima procedura di soggetti che si trovano, rispetto ad essa, in una delle situazioni di controllo di cui all'articolo 2359 del codice civile, o in una qualsiasi relazione, anche di fatto con alcun soggetto, se la situazione di controllo o la relazione comporti che le offerte sono imputabili ad un unico centro decisionale e di aver formulato autonomamente l'offerta.

ovvero

☐ che l'operatore economico è a conoscenza della partecipazione alla medesima procedura di soggetti che si trovano, rispetto ad essa, in una delle situazioni di controllo di cui all'articolo 2359 o in una qualsiasi relazione, anche di fatto con alcun soggetto, se la situazione di controllo o la relazione comporti che le offerte sono imputabili ad un unico centro decisionale del codice civile, e di aver formulato autonomamente l'offerta.

DICHIARA altresì ai fini ISO 37001:2016
che la Società/Ditta individuale

- è iscritta alla Camera di Commercio di _____ n° iscrizione_____
- è iscritta all'INAIL (n° posizione INAIL) _____
- è iscritta all'INPS (n° matricola INPS) _____
- è in regola, quale sostituto di imposta, con il versamento delle ritenute fiscali IRPEF sui redditi di lavoro;
- è, altresì, in regola con il versamento dei contributi previdenziali ed assicurativi obbligatori per gli infortuni sul lavoro e per le malattie professionali dei lavoratori;
- non è stata oggetto, negli ultimi cinque anni dalla data della presente dichiarazione, di provvedimenti di sospensione o di interdizione ai sensi dell'art. 14 del D.lgs. n. 81/2008 (T.U. Sicurezza nei luoghi di lavoro);
- ha nominato [in data] il/la Sig./ra_____, con sede di lavoro a_____ ____quale Responsabile del Servizio Protezione e Prevenzione (RSPP) ai sensi e per gli effetti del citato T.U.;
- ha nominato [in data] quale medico competente (coordinatore) il/la Dott./Dott.ssa _____;
- di avere svolto la valutazione dei rischi ai sensi dell'art.17 del D.lgs. 81/08 e aver redatto il DVR;
- è in possesso dei requisiti di idoneità tecnico professionale previsti dalla legge per effettuare i lavori e/o i servizi oggetto dei possibili affidamenti da parte di ARTEA;
- non è stata destinataria di sanzioni, anche solo provvisorie o cautelari, previste dal Decreto Legislativo n. 231/2001 (Responsabilità amministrativa degli enti) e per i reati previsti nel capo I del titolo II del libro secondo del codice penale (delitti contro la pubblica amministrazione), negli ultimi cinque anni dalla data della presente dichiarazione;
- che nei confronti del sottoscritto legale rappresentante/amministratore alla data di sottoscrizione del contratto non è stata depositata sentenza, anche non definitiva, per taluno dei delitti previsti dal codice penale di seguito specificati:

- art 317 c.p. (reato di concussione); art 318 c.p. (Corruzione per l'esercizio della funzione); art 319 c.p.(Corruzione per un atto contrario ai doveri d'ufficio); art 319 bis c.p.c. (Circostanze aggravanti);

art. 319 ter c.p. (Corruzione in atti giudiziari); art 319 quater c.p.(circostanze aggravanti); art 320 c.p. (Corruzione di persona incaricata di un pubblico servizio); art. 322 c.p. (Istigazione alla corruzione); art. 322 bis c.p. (Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri della Corte penale internazionale e degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri); art. 346 bis (Traffico di influenze illecite); art 353 c.p.(Turbata libertà degli incanti), art 353 bis c.p. (Turbata libertà del procedimento di scelta del contraente; art 2635 c.c. (Corruzione tra privati);

- di essere in regola con la normativa antimafia;
- di aver preso visione e di attenersi alla politica per la prevenzione della corruzione di ARTEA ai sensi dello standard internazionale ISO 37001:2016, approvata con decreto ARTEA n. 26 del 24/02/2023, e, in particolare, di aver preso visione e di rispettare le prescrizioni contenute nella Strategia per la prevenzione della corruzione, contenuta nel PIAO della Regione Toscana, disponibile sul sito web della Agenzia; di non porre in essere azioni in contrasto con la L. 190/2012 e decreti collegati (D.lgs. 33/2013 e D.lgs. 39/2013), e comunque con la normativa vigente in materia;
- di aver preso visione e di attenersi alla politica per la sicurezza dei dati delle informazioni di ARTEA,disponibile sul sito web della Agenzia;
- di comunicare tempestivamente qualsiasi modifica alle dichiarazioni di cui ai punti precedenti.

In fede,

Data e luogo [firma digitale del Titolare/ Legale Rappresentante]

***** Per accettazione espressa della clausola risolutiva espressa ex 1456 c.c. sopra menzionata, avente natura vessatoria,

Data e luogo [firma digitale del Titolare/ Legale Rappresentante]

Nota (1)
Nel caso in cui le dichiarazioni vengano rese anche per nome e per conto di tutti i soggetti di cui all'art. 80, comma 3, del D.lgs. n. 50/2016, è necessario indicare le generalità e il ruolo di questi soggetti.

Allegato 5 - Accordi/clausole per la sicurezza delle informazioni (ISO 27001)

ARTEA, ai sensi delle disposizioni del regolamento delegato n. 907/2014 della Commissione Europea, è certificata ISO 27001 relativamente al Sistema di Gestione della Sicurezza delle Informazioni.
La certificazione ottenuta si applica ai servizi e ai processi gestiti per l'autorizzazione, la contabilizzazione e l'esecuzione dei pagamenti degli aiuti previsti dalla Politica Agricola Comunitaria ma non si estende agli organismi delegati.
In tale caso le direttive impartite dalla Commissione Europea (Memorandum trasmesso al Comitato dei Fondi Agricoli D (2015) AGRI/2015/agri.ddg4.j.1(2015)1359224-IT-MEMO) dispongono che l'Organismo Pagatore preveda requisiti di sicurezza delle informazioni in tutti gli accordi conclusi con gli organismi delegati.
Per ARTEA la sicurezza delle informazioni ha come obiettivo primario la protezione dei dati e delle informazioni gestite, nonché la protezione della struttura tecnologica, fisica, logica ed organizzativa e dei Responsabili della loro gestione.
A tale fine ARTEA si è dotata di un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI), sviluppato secondo la normativa internazionale ISO/IEC 27001:2013.
In accordo a tale Sistema di Gestione, ARTEA chiede ai propri soggetti delegati (fornitori) di assicurare i requisiti di sicurezza delle informazioni acquisite, comunicate, archiviate, processate, o in ogni modo gestite e relative al rapporto di collaborazione con ARTEA stessa.
In particolare chiede che venga assicurata:

- la riservatezza: ovvero assicurarsi che le informazioni siano accessibili solo a coloro che sono autorizzati ad averne accesso;
- l'integrità: ovvero la salvaguardia della precisione e della completezza dell'informazione e del metodo di elaborazione;
- la disponibilità: ovvero l'assicurazione che gli utenti autorizzati abbiano accesso alle informazioni e ai beni quando richiesto e/o necessario.

Per meglio assicurare tali aspetti, ARTEA raccomanda ai propri fornitori e collaboratori di attuare gli aspetti di seguito descritti:

- Ruoli e responsabilità per la sicurezza delle informazioni > definire ed assegnare le responsabilità relative alla sicurezza delle informazioni;
- Consapevolezza, istruzione, formazione e addestramento sulla sicurezza delle informazioni > fornire a tutto il personale un'adeguata sensibilizzazione, formazione e addestramento, con aggiornamenti periodici, sulla sicurezza delle informazioni;
- Classificazione delle informazioni > definire come classificare le informazioni in relazione al loro valore, ai requisiti cogenti e alla criticità in caso di divulgazione o modifica non autorizzate;
- Trattamento degli asset > definire le modalità di gestione dei propri asset (computer, server, stampanti, dispositivi di rete, ecc.) in merito a installazione, manutenzione delle postazioni di lavoro (HW e SW), richieste di installazione di software aggiuntivo, presa in carico e gestione di segnalazioni e malfunzionamenti, ecc.;
- Politica di controllo degli accessi > definire una politica di controllo degli accessi ai sistemi informativi, sulla base dei compiti assegnati a ciascuna persona e di sicurezza delle informazioni;

- Sistema di gestione delle password > assicurare che i sistemi di gestione delle password siano interattivi e garantiscano password di qualità;
- Perimetro di sicurezza fisica > utilizzare dei sistemi di protezione degli accessi fisici, per proteggere le aree che contengono informazioni critiche e i sistemi di elaborazione delle informazioni;
- Manutenzione delle apparecchiature > manutenere correttamente le apparecchiature per assicurare la loro continua disponibilità e integrità;
- Controlli contro il malware (antivirus) > attuare controlli di individuazione, di prevenzione e di ripristino relativamente al malware, congiuntamente ad un'appropriata consapevolezza degli utenti in materia;
- Backup delle informazioni > effettuare regolari copie di backup delle informazioni, del software e delle immagini relative ai propri sistemi;
- Controlli di rete > gestire e controllare le reti e i relativi accessi per proteggere le informazioni nei sistemi e nelle applicazioni;
- Segnalazione degli incidenti relativi alla sicurezza delle informazioni > segnalare e gestire gli incidenti relativi alla sicurezza delle informazioni e classificarli per ottenere spunti di miglioramento

Requisiti di sicurezza ISO 27001

1. Premessa

Di seguito si definiscono i requisiti di sicurezza che devono essere rispettati dal CAA relativamente alla sicurezza delle informazioni gestite in nome e per conto dell'Organismo Pagatore.

2.Classificazione delle informazioni trattate

Le informazioni gestite dal CAA in nome e per conto dell'Organismo Pagatore, 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 al CAA, devono essere trattate nel rispetto della normativa vigente in tema di sicurezza e privacy e nel rispetto delle prescrizioni emanate da ARTEA.
Le informazioni trattate devono essere classificate secondo livelli differenti di riservatezza, integrità e disponibilità.
I livelli di classificazione individuati, in ordine crescente di sensibilità delle informazioni sono:

- pubblico (contenente informazioni che possono essere comunicate liberamente senza che vi possano essere conseguenze negative per ARTEA, es: albo beneficiari);
- ad uso interno (contenente informazioni che possono essere diffuse unicamente tra i dipendenti di ARTEA e tra il personale esterno che sia autorizzato per motivi strettamente necessari per poter svolgere incarichi assegnati. Es dati relativi alle domande e pagamenti);
- riservato (diffuse solo a personale interno / esterno attentamente identificato. Es atti giudiziari);
- strettamente riservato (documenti e le informazioni la cui diffusione potrebbe avere conseguenze significative sotto il profilo giuridico o legale per ARTEA ed essere rilevanti nello sviluppo di strategie di gestione.

3.Regole di protezione delle informazioni

A seconda del livello di classificazione le informazioni devono essere protette con adeguate regole di

gestione.
Nel seguito vengono definite le regole da rispettare per garantire la sicurezza delle informazioni nel corso del loro ciclo di vita, in accordo con i livelli di classificazione e i criteri definiti. Come indicazione di carattere generale, è necessario:

- rispettare regole tanto più stringenti quanto più alto è il livello di classificazione di un'informazione;
- prestare particolare attenzione al rispetto dei principi di necessità (i soggetti devono essere autorizzati a trattare le sole informazioni/ dati necessari allo svolgimento delle loro attività) e minimo privilegio (i soggetti devono avere i privilegi minimi per svolgere correttamente il proprio lavoro), soprattutto in caso di soggetti esterni;
- notificare, in caso di informazioni erroneamente condivise con una terza parte (es. qualora ci si accorgesse di non aver rispettato il principio di necessità), l'errata condivisione al mittente, richiedendo la cancellazione delle informazioni. Viceversa, in caso si entrasse in possesso di documenti dei quali non si è destinatari, avvisare il mittente del documento stesso e cancellarli;
- in caso di spedizioni (invio posta esterna) e di copie cartacee destinate a soggetti esterni, devono essere presenti a livello contrattuale le opportune clausole di riservatezza o atti equiparabili.

3.1 Generazione

La generazione di informazioni critiche è realizzata tramite la redazione, la trascrizione, la registrazione dei dati su un supporto e una etichettatura adeguata.

Formato cartaceo

Asset Labelling	Riservato	Ad uso interno	Pubblico
Stampa	Etichetta "Uso: Confidenziale" su tutte le pagine	Etichetta "Uso Interno" su tutte le pagine	n/a
Fax	Etichetta su ogni pagina, inclusa la copertina; Dichiarazione di responsabilità	Etichetta su ogni pagina, inclusa la copertina; Dichiarazione di responsabilità	n/a
Materiale di presentazioni	Etichetta "Uso: Confidenziale" su ogni slide	Etichetta "Uso: Interno" su ogni slide	n/a

Supporti rimovibili

Asset Labelling	Riservato	Ad uso interno	Pubblico
CD, DVD, Dispositivi USB	Etichetta "Uso: Confidenziale" sui supporti e sulla confezione esterna se applicabile	n/a	n/a

Formato elettronico

Asset Labelling	Riservato	Ad uso interno	Pubblico
Email	Marcare il messaggio come "Riservato" prima	Messaggio di dichiarazione di	n/a

	di inviarlo. Messaggio di dichiarazione di responsabilità nelle mail in partenza dal CAA	responsabilità nelle mail in partenza dal CAA	
Posta Elettronica Certificata (PEC)	Etichetta “Confidenziale” alla fine dell’Oggetto (“Subject”, Titolo) del messaggio email. Messaggio di dichiarazione di responsabilità nella PEC in partenza dal CAA	Messaggio di dichiarazione di responsabilità nella PEC in partenza dal CAA	n/a

3.2 Trasmissione

La comunicazione e la trasmissione delle informazioni prodotte e correttamente classificate, all'interno e/o all'esterno del CAA deve soddisfare i seguenti requisiti

Modalità	**Riservato**	**Ad uso interno**	**Pubblico**
Fax	Supervisionare fisicamente la trasmissione di fax; Indirizzare i fax a specifici destinatari; Verificare la trasmissione e dove possibile la ricevuta del facsimile del destinatario	Indirizzare i fax a specifici destinatari	n/a
Email aziendale	Non inoltrare a persone non già comprese nelle liste di destinatari primari o per conoscenza del messaggio originale ricevuto. Abilitare la ricevuta di ritorno	Non inoltrare a indirizzi non aziendali email senza rispettare i protocolli di sicurezza email	n/a
Email personale	Non usare email personali per la trasmissione di informazioni confidenziali	Non usare email personali per la trasmissione di informazioni ad uso Interno	n/a
Corriere	Utilizzare buste e contenitori sigillati e impermeabili; Indirizzare verso uno specifico destinatario; Tracciare la spedizione	Utilizzare buste e contenitori sigillati	n/a
Telefoni aziendali	Utilizzare postazioni sicure per le comunicazioni telefoniche	n/a	n/a
Telefoni personali	Non utilizzare dispositivi personali	Non utilizzare dispositivi personali	n/a
Messaggeria istantanea	Seguire i protocolli aziendali per l’uso di	n/a	n/a

	messaggeria istantanea		

3.3 Copia

La copia digitale o fisica delle informazioni prodotte/acquisite e correttamente classificate deve soddisfare i seguenti requisiti

Modalità	Riservato	Ad uso interno	Pubblico
Stampa	Solo individui autorizzati possono stampare informazioni per motivi di business; La stampa deve essere presidiata: chi stampa il documento deve essere presente presso la stampante durante la stampa e deve provvedere a rimuovere prontamente il documento dal cassetto di uscita della stampante.	Se la stampa avviene in uffici/piani condivisi con personale non CAA, eseguire una stampa protetta con PIN	n/a
Copia	Solo individui autorizzati possono copiare le informazioni per motivi di business. Se si effettuano copie, queste devono essere autorizzate, è necessario comunicare ai responsabili prima della loro creazione: - tipologia del documento prodotto; - data nella quale sono state fatte le copie; - numero di copie effettuate; - indirizzi, nel caso siano state distribuite. Il destinatario deve essere forzato a restituire la copia se richiesto. Le copie prodotte devono essere rimosse immediatamente dagli strumenti utilizzati per produrle e devono ricevere le stesse attenzioni riservate agli originali.	n/a	n/a

3.4 Conservazione

La conservazione delle informazioni deve soddisfare i seguenti requisiti.

Modalità	Riservato	Ad uso interno	Pubblico
Telefoni mobili aziendali e postazioni aziendali fisse e removibili (telefoni cellulari, PDA, laptop, desktop)	Proteggere i documenti/cartelle con password;	Proteggere i device con password	Non lasciare incustoditi i device in luoghi pubblici come aeroporti, aerei, ecc.
Dispositivi di archiviazione removibili e endpoint device (Hard Drive, CD/DVD, etc.)	Proteggere i documenti/cartelle con password; Metterli in sicurezza con blocchi o chiavi quando non utilizzati.	Proteggere i device con password	Non lasciare incustoditi i device in luoghi pubblici come aeroporti, aerei, ecc.
Dispositivi mobili e dispositivi di archiviazione removibili personali	Non archiviare informazioni gestite in nome e per conto di OPR	Non archiviare informazioni gestite in nome e per conto di OPR	n/a
Archivi cartacei	Conservare i documenti in casseforti o armadietti la cui apertura avviene tramite chiave o di combinazione numerica anche durante assenze brevi	Disporre la documentazione in armadietti o scrivanie; Gli archivi dovrebbero essere chiusi al termine della giornata lavorativa.	n/a

3.5 Distruzione

Nel caso sia necessario distruggere i documenti/file diversi da quelli di uso pubblico, è necessario utilizzare precauzioni per proteggere la riservatezza delle informazioni contenute, indipendentemente dal formato e dal supporto utilizzato.

Modalità	Riservato	Ad uso interno	Pubblico
Macchinari (fotocopiatrici, fax, ecc.)	Effettuare un ripristino dei settaggi allo stato di fabbrica; Ottenere l'approvazione manageriale prima che i macchinari siano donati e rimossi dalle sedi aziendali	Effettuare un ripristino dei settaggi allo stato di fabbrica; Ottenere l'approvazione manageriale prima che i macchinari siano donati e rimossi dalle sedi aziendali	Effettuare un ripristino dei settaggi allo stato di fabbrica; Ottenere l'approvazione manageriale prima che i macchinari siano donati e rimossi dalle sedi aziendali
Telefoni mobili aziendali e postazioni aziendali fisse e removibili (telefoni cellulari, PDA, laptop, desktop)	Cancellare o distruggere in modo sicuro i dispositivi	Cancellare o distruggere in modo sicuro i dispositivi	Cancellare o distruggere in modo sicuro i dispositivi
Supporti di	Cancellare o distruggere in	Cancellare tutte le vecchie	n/a

archiviazione removibili societari (Hard Drive, CD/DVD, etc.)	modo sicuro i dispositivi	copie precedenti	
Copie elettroniche di file	Assicurare la cancellazione di file dai supporti di memorizzazione	Cancellare tutte le vecchie copie precedenti	n/a

Allegato 6 - Modello di mandato

MANDATO

Il sottoscritto/a Cognome _____ Nome _____,
nato/a a _____, il _____
residente nel Comune di _____,
località _____,
via/piazza _____ , n. _____,
in qualità di titolare o legale rappresentante della seguente azienda, di seguito definita "mandante",
CUAA/C.F.-P.IVA_____denominazione_____,
costituita nella forma di [4] _____,
Tel._____fax_____Email_____
PEC_____

di seguito definito "mandante"

CONFERISCE MANDATO

al CAA _____, CF/P.IVA_____, con sede legale in via/piazza _____, di seguito definito "mandatario", che opera, se presenti, anche attraverso le sue strutture territoriali gestite dalle società di servizi con esso convenzionate, per lo svolgimento delle attività qui specificamente indicate e rientranti fra quelle previste dall'art. 6 comma 1 del d.lgs. 74/2018, del DM. 27/3/2008 e in conformità alla Convenzione ARTEA – CAA vigente.

In particolare, in forza del presente mandato, il CAA _____, si impegna a svolgere, a titolo gratuito, per conto del mandante, le seguenti attività:

1. **COSTITUIRE** il fascicolo aziendale previsto da ARTEA e/o da altro Organismo Pagatore e/o Ente pubblico e a procedere all'aggiornamento dei dati e delle informazioni in esso contenute;
2. **CONSERVARE** il fascicolo aziendale, con tutti i documenti ad esso inerenti, per tutto il tempo che le vigenti norme lo impongono, con espressa autorizzazione ad esibirlo e consegnarlo, per i dovuti controlli alle autorità di vigilanza preposte, così come previsto dal DM 27 Marzo 2008;
3. **TRASMETTERE** alla Regione, alle Amministrazioni Provinciali, alle Comunità Montane, ad ARTEA, ad altri Organismi Pagatori, agli altri Organismi della Pubblica Amministrazione, ai CAA nazionali di coordinamento in forza della Convenzione Quadro tra AGEA di coordinamento ed il CAA _____ nazionale ai fini dell'applicazione armonizzata della normativa comunitaria e nazionale e delle procedure di attuazione, le dichiarazioni previste dalla normativa comunitaria, nazionale e regionale;
4. **INTERROGARE** le banche dati del SIAN e degli Organismi Pagatori e/o dalle Regioni ed in particolare l'anagrafe nazionale delle aziende agricole di cui all'articolo 1 del DPR 1° dicembre 1999, n. 503 e del D.M. 12 gennaio 2015, ai fini della consultazione dello stato delle pratiche relative alla propria posizione;
5. **RICEVERE** per conto del mandante, dall'Organismo Pagatore della Toscana ARTEA o da altro Organismo Pagatore e dagli altri uffici preposti della P.A. nazionale e regionale,

[4] *Indicare se si tratta di impresa individuale o società. In caso di società specificare anche il tipo societario*.

comprese le ASL, dai CAA nazionali di coordinamento ed Enti privati documenti e dati, anche storici (su supporto cartaceo, magnetico e per via telematica) inerenti le domande di aiuto, premi, contributi ed agevolazioni previsti dalla regolamentazione comunitaria, nazionale e regionale, dal sottoscritto firmate e presentate per il tramite del CAA mandatario ed eventuali informazioni inerenti il Sistema Integrato di Gestione e Controllo;

6. **ACQUISIRE** dalle competenti amministrazioni e dai CAA nazionali di coordinamento informazioni sull'iter delle domande fondate sul fascicolo aziendale, compreso l'importo dei contributi, lo stato del procedimento di erogazione;
7. **VERIFICARE** la completezza dei dati e della documentazione fornita nonché l'effettiva erogazione degli aiuti, premi, contributi e agevolazioni e dei relativi importi;
8. **TRATTARE** eventuali anomalie di domande e dichiarazioni risultanti da controlli effettuati e riferibili al mancato aggiornamento dei documenti contenuti nel fascicolo aziendale;
9. **CORREGGERE**, **FORNIRE ASSISTENZA PER CORRETTIVE** di eventuali anomalie e criticità inerenti alla mancata riscossione degli importi riscontrate e/o segnalate durante gli iter istruttori, al fine della corretta e tempestiva erogazione dei contributi;
10. **DETENERE,** sulla base della documentazione fornita dal sottoscritto e laddove possibile, presso i propri uffici, la documentazione in formato digitale e/o cartaceo, in originale e/o in copia, riferita alle istanze presentate all'Organismo Pagatore ed agli altri uffici competenti della P.A., per il tramite del CAA mandatario.

Inoltre, il mandatario provvede a trasmettere i documenti e le informazioni necessari per la realizzazione di banche dati, archivi e schedari e per gli altri adempimenti relativi al Sistema Integrato di Gestione e Controllo, compresa l'immissione dei dati al SIAN, al SIART, all'interno dell'anagrafe aziendale di ARTEA e di altri Organismi Pagatori.

Il mandante

SI IMPEGNA

a prestare al CAA mandatario, per il tramite delle sue strutture territoriali, gestite se presenti dalle società di servizi con esso convenzionate, la necessaria collaborazione al fine di consentire ad esso l'esecuzione del presente mandato ed in particolare a:

1. fornire al CAA mandatario dati completi, veritieri, aggiornati e corredati di idonea documentazione a supporto;
2. fornire piena collaborazione al CAA per lo svolgimento delle attività di cui all'art. 2, comma 2 del D.M. 27 marzo 2008 (e ss. mm) e all'art. 6, comma quarto, d. lgs. 74/2018: in particolare, consentire al CAA l'accesso ai propri dati aziendali presenti nelle banche dati del SIAN – nei limiti di quanto è necessario per l'espletamento delle attività oggetto del presente mandato - gli accertamenti, le verifiche ed i controlli inerenti all'identificazione del mandante-produttore, il titolo di conduzione e la corretta immissione dei dati, così come previsto dall'art. 6, primo comma, lett. b) d. lgs. 74/2018.

Il mandante autorizza il mandatario all'accesso alle banche dati ed al trattamento dei suoi dati personali ivi contenuti, ai sensi del Reg. (UE) 679/2016, per le finalità e nei limiti dell'oggetto definito dal presente contratto di mandato.

Il sottoscritto dichiara, altresì, di aver preso visione della Carta Servizi del CAA _____ illustratagli in sede di sottoscrizione del presente mandato, ai sensi dell'art. 7, secondo comma, D.M. 27 marzo 2008 nonché di aver preso visione

dell'informativa agli interessati ai sensi dell'art. 13 del Regolamento UE n. 679/2016, pubblicata sul sito di ARTEA.

Nell'esecuzione del presente contratto il CAA _____ e le Società di Servizi con esso convenzionate non rispondono di errori e/o inadempimenti derivanti in tutto o in parte dalla mancata o tardiva acquisizione e consegna di informazioni e documenti, qualora l'omissione o il ritardo siano imputabili al mandante. La data di ricevimento della documentazione è attestata mediante apposizione sulla medesima di timbro con la data di pervenuto o rilascio di ricevuta.

DURATA E REVOCA DEL MANDATO

Il presente MANDATO ha durata annuale e si intende tacitamente rinnovato di anno in anno.
Il presente mandato può essere sempre revocato, mediante atto comunicato al CAA con lettera raccomandata a/r o tramite il seguente indirizzo PEC: _____.
Al riguardo dichiaro di essere consapevole che il CAA, in caso di revoca del mandato, è impegnato a completare gli adempimenti per tutte le pratiche in corso, fintanto che non sia intervenuta la chiusura di tutti i procedimenti amministrativi affidati ad esso in base al presente mandato e sempre che non intervengano disposizioni normative di senso contrario.
Dichiara inoltre di essere consapevole che la revoca del mandato ha efficacia dalla sottoscrizione di un nuovo mandato a favore di un altro CAA.

Per quanto non disciplinato dal presente atto, trovano applicazione, in quanto compatibili, le disposizioni contenute nel Codice Civile in materia di contratto di mandato, artt. 1703 e ss.

Luogo e data _____

Firma mandante _____

Timbro e firma CAA_____

È obbligatorio allegare alla presente richiesta copia di un documento di identità valido del mandante *(normativa inerente autocertificazione DPR 445/2000 e s.m.i.).*

Quadro B (*da compilare a cura del CAA*)

Prot._____

Data, _____

_____

(Timbro e firma del CAA)