**ACCORDO PER IL TRATTAMENTO DI DATI PERSONALI**

**(ai sensi dell’art. 28 del Reg. UE 679/2016 in materia di protezione dei dati personali)**

# Tra:

# Agenzia regionale per lo sviluppo rurale – ERSA, di seguito ERSA*[[1]](#footnote-2)*, con sede e domicilio fiscale in Gorizia (GO), all’indirizzo Via del Montesanto, 17, codice fiscale e partita IVA: 00485650311, rappresentata ai fini del presente atto dal Direttore di Servizio/Direttore dell’OPR FVG …………………………., giusta delega al trattamento dei dati di cui al Decreto del Direttore generale sostituto di ERSA del 2 febbraio 2024, n. 41, di seguito Titolare

# E:

# … *inserire i riferimenti del soggetto nominato in qualità di responsabile trattamento dati* di seguito Responsabile

# Visti:

* il regolamento (UE) n. 679/2016 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), di seguito GDPR, il quale all’articolo 4, paragrafo 1, stabilisce quanto segue:

- punto 2), concernente la definizione di “trattamento”, quale qualsiasi operazione o insieme di operazioni, compiute con o senza l’ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l’organizzazione, la strutturazione, la conservazione, l’adattamento o la modifica, l’estrazione, la consultazione, l’uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l’interconnessione, la limitazione, la cancellazione o la distruzione;

- punto 7), concernente il “Titolare del trattamento”, quale persona fisica o giuridica, autorità pubblica, servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;

- punto 8) concernente il Responsabile del trattamento, quale persona fisica o giuridica, autorità pubblica, servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

* in particolare, l’articolo 28 del GDPR il quale dispone, *“1. Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest’ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto adeguate misure tecniche e organizzative in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell’interessato. … 3. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico …. che vincoli il responsabile del trattamento al titolare del trattamento …“;*
* il decreto legislativo 30 giugno 2003, n.196 recante il “Codice in materia di protezione dei dati personali”;
* il contratto stipulato in data ……. tra ERSA e ………il quale ha ad oggetto lo svolgimento, da parte di quest’ultimo, del servizio ………..…;

# PREMESSO CHE

* ERSA è Titolare del trattamento dei dati personali connessi allo svolgimento del servizio oggetto del contratto sopra richiamato e detti dati saranno trattati dal Responsabile per le finalità di cui all’articolo 1 del presente accordo;
* il Responsabile deve procedere al trattamento nel pieno rispetto delle previsioni legislative vigenti nonché nei limiti stabiliti dal presente documento e secondo le istruzioni impartite da ERSA per iscritto con il presente atto o con eventuali atti successivi;
* il Responsabile dichiara e garantisce di possedere competenze e conoscenze tecniche in relazione alle finalità e modalità di trattamento, alle misure di sicurezza da adottare a garanzia della riservatezza, completezza ed integrità dei dati personali trattati, alla normativa italiana ed europea in materia di protezione dei dati personali, e di possedere i requisiti di affidabilità idonei a garantire il rispetto delle disposizioni normative in materia;

**TANTO PREMESSO**

Le Parti disciplinano il reciproco rapporto di “responsabilità” di cui all’art. 28 del GDPR secondo le condizioni contrattuali e le istruzioni di seguito riportate, che vengono accettate dalle Parti medesime con la firma in calce.

**1. Scopo del presente documento e oggetto del trattamento.**

Il presente atto ha lo scopo di garantire il pieno rispetto delle previsioni legislative vigenti in materia di protezione dei dati personali, con particolare riferimento all'articolo 28, paragrafi 3 e 4, del GDPR, tenendo inoltre conto dei provvedimenti e dei comunicati ufficiali emessi dall'Autorità Garante per la Protezione dei Dati Personali, in relazione ai trattamenti effettuati dal Responsabile per adempiere agli obblighi derivanti dal contratto sopra richiamato, nonché da norme di legge e regolamento correlate.

Il trattamento di dati effettuati dal Responsabile per l’adempimento del contratto riguarda le seguenti finalità e categorie di dati:

1. i trattamenti sono svolti al fine di *… .. indicare finalità* ed ogni altra finalità indispensabile a dare esecuzione al contratto/convenzione descritto in premessa;
2. i dati trattati in ragione delle attività di cui al suddetto contratto hanno ad oggetto dati di natura personale, quali *… ad esempio: dati anagrafici, dati che consentono l'identificazione indiretta, di residenza/domicilio, recapiti telefonici, caselle di posta elettronica, numero di conto corrente bancario, dati catastali, benefici/sovvenzioni richieste ed ottenute*;
3. le categorie di interessati sono ….

**2. Durata e cessazione del presente accordo. Disposizioni per la restituzione o la cancellazione dei dati personali.**

Ogni trattamento dei dati succitati, da effettuarsi solamente in conformità alle finalità sopra riportate, dovrà essere limitato al tempo necessario a dare esecuzione al contratto richiamato in premessa. ERSA avrà, comunque, sempre la facoltà di revocare l’incarico conferito al Responsabile, qualora si verifichi la cessazione, per qualsiasi causa intervenuta, del contratto in premessa, dandone semplice comunicazione scritta al Responsabile.

Al termine delle operazioni di trattamento affidate, nonché all’atto della cessazione per qualsiasi causa del contratto in premessa, il Responsabile sarà tenuto a restituire a ERSA, in formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali oggetto del trattamento. Successivamente il Responsabile dovrà provvedere alla loro integrale distruzione salvo i casi in cui la conservazione dei dati sia richiesta da norme di legge od altri fini (contabili, fiscali, ecc.). Se richiesto, il Responsabile provvederà a rilasciare a ERSA apposita dichiarazione per iscritto contenente l’attestazione che presso il Responsabile non esista alcuna copia dei dati personali e delle informazioni di titolarità di ERSA.

La validità del presente accordo si intende altresì estesa ad ulteriori, eventuali, proroghe del contratto; ogni altra pattuizione resta pienamente confermata e impregiudicata.

**3. Istruzioni fornite da ERSA al Responsabile ai sensi dell’art. 28 par. 3 del GDPR.**

Nello svolgimento dell’incarico, in merito ai trattamenti che dovranno essere effettuati, il Responsabile dovrà dare applicazione alle disposizioni previste dal GDPR, in particolare dovrà:

* al fine di garantire il rispetto del principio della “Protezione dei dati fin dalla progettazione e protezione predefinita” di cui all’articolo 25 del GDPR, il Responsabile si impegna a determinare i mezzi del trattamento e a mettere in atto le misure tecniche e organizzative adeguate, di cui all’articolo 32 del GDPR, prima dell’inizio delle attività;
* il Responsabile dovrà eseguire i trattamenti connessi alle funzioni ad esso attribuite e comunque non incompatibili con le finalità per cui i dati sono stati raccolti. Qualora sorgesse la necessità di effettuare trattamenti su dati personali diversi ed eccezionali rispetto a quelli normalmente eseguiti, il Responsabile dovrà informare ERSA del trattamento ed il Responsabile della Protezione dei Dati (RPD) di ERSA;
* il Responsabile dovrà attivare le necessarie procedure per identificare ed istruire le persone autorizzate al trattamento dei dati personali ed organizzare i loro compiti in maniera che le singole operazioni di trattamento risultino coerenti con le disposizioni di cui al presente accordo, facendo anche in modo che, sulla base delle istruzioni operative loro impartite, i trattamenti non si discostino dalle finalità istituzionali per cui i dati sono stati raccolti e trattati. Il Responsabile garantirà, inoltre, che le persone autorizzate al trattamento siano vincolate da un obbligo, legalmente assunto, di riservatezza;
* il Responsabile si attiverà per garantire l’adozione delle misure di sicurezza di cui all’articolo 32 del GDPR. In particolare, tenuto conto della natura, dell’oggetto, del contesto e delle finalità del trattamento e, sulla base delle risultanze dell'analisi dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall’accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati, porrà in essere le opportune azioni organizzative per l'ottimizzazione di tali misure di sicurezza, per garantire un livello di sicurezza adeguato al rischio. Tali misure comprendono, tra le altre:
1. la pseudonimizzazione e la cifratura dei dati personali;
2. misure idonee a garantire la riservatezza, l’integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
3. misure idonee a garantire la capacità di ripristinare tempestivamente la disponibilità e l’accesso ai dati personali in caso di incidente fisico o tecnico;
4. procedure per testare, verificare e valutare regolarmente l’efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;
* il Responsabile mette a disposizione di ERSA tutte le informazioni necessarie a dimostrare il rispetto degli obblighi stabiliti nel presente documento e che derivano direttamente dal GDPR. Su richiesta di ERSA, il Responsabile consente e contribuisce alle attività di revisione delle attività di trattamento, a intervalli ragionevoli o se vi sono indicazioni di inosservanza;
* il Responsabile è tenuto ad informare di ogni violazione di dati personali (cd. data breach) ERSA ed il Responsabile della Protezione dei Dati (RPD) di ERSA, senza ingiustificato ritardo e comunque entro 24 ore dal momento in cui ne venga a conoscenza, secondo le linee guida adottate con decreto del Direttore generale sostituto di ERSA del 29 marzo 2021, n. 25 recante “Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, articolo 33. Notifica di una violazione dei dati personali all’Autorità di controllo. Approvazione delle “Linee guida per la notifica della violazione dei dati personali “Data Breach” per gli uffici dell’Agenzia regionale per lo sviluppo rurale – ERSA”, allegato al presente accordo. Tale notifica – da effettuarsi tramite PEC da inviare sia all’indirizzo PEC di ERSA ersa@certregione.fvg.it sia all'indirizzo email: ersa@ersa.fvg.it – deve essere accompagnata da ogni documentazione utile, ai sensi degli articoli 33 e 34 del GDPR, per permettere a ERSA, ove ritenuto necessario, di notificare questa violazione all’Autorità Garante per la protezione dei dati personali o darne comunicazione agli interessati, entro il termine di 72 ore da quando ERSA ne è venuta a conoscenza. Nel caso in cui ERSA debba fornire informazioni aggiuntive alla suddetta Autorità Garante, il Responsabile supporterà ERSA nella misura in cui le informazioni richieste o necessarie per l’Autorità Garante siano esclusivamente in possesso del Responsabile o di suoi eventuali sub-Responsabili;
* il Responsabile, su eventuale richiesta di ERSA, è tenuto inoltre ad assistere quest’ultima nello svolgimento della valutazione d’impatto sulla protezione dei dati, conformemente a quanto prescritto dall’articolo 35 del GDPR e nella eventuale consultazione del Garante per la protezione dei dati personali, prevista dall’articolo 36 del GDPR;
* il Responsabile, qualora riceva istanze degli interessati in esercizio dei loro diritti di cui dall’articolo 15 all’articolo 22 del GDPR, è tenuto a:
1. darne tempestiva comunicazione scritta a ERSA o al Responsabile della Protezione dei Dati (RPD) di ERSA, allegando copia della richiesta;
2. valutare con ERSA e con il Responsabile della Protezione dei Dati (RPD) di ERSA la legittimità delle richieste;
3. coordinarsi con ERSA e con il Responsabile della Protezione dei Dati (RPD) di ERSA al fine di soddisfare le richieste ritenute legittime;
* il Responsabile garantisce gli adempimenti e le incombenze anche formali verso l’Autorità Garante quando richiesto e nei limiti dovuti, disponendosi a collaborare tempestivamente, per quanto di competenza, sia con ERSA sia con l’Autorità. In particolare:
1. fornisce informazioni sulle operazioni di trattamento svolte;
2. consente l’accesso alle banche dati oggetto delle operazioni di trattamento;
3. consente l’effettuazione di controlli;
4. compie quanto necessario per una tempestiva esecuzione dei provvedimenti inibitori, di natura temporanea;
* durante l’esecuzione del contratto richiamato in premessa, nell’eventualità di qualsivoglia modifica della normativa in materia di protezione dei dati personali, che generi nuovi requisiti (ivi incluse nuove misure di sicurezza di natura fisica, logica o organizzativa), il Responsabile si impegna a collaborare, nei limiti delle proprie competenze tecniche/organizzative e delle proprie risorse, con ERSA affinché siano sviluppate, adottate ed implementate misure correttive di adeguamento ai nuovi requisiti;
* il Responsabile informerà prontamente ERSA qualora, per qualunque motivo, non sia in grado di rispettare le istruzioni sopra riportate.

Solamente nel caso in cui il contratto indicato in premessa comporti lo svolgimento di attività di natura informatica e sistemistica sui sistemi ed infrastrutture di ERSA, accesso a servizi e piattaforme web, in ossequio alla deliberazione del Garante per la protezione dei dati personali *“Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008”* (in G.U. n. 300 del 24 dicembre 2008) e smi., il Responsabile dovrà altresì:

1. Nominare quali “Amministratori di sistema” i propri dipendenti e/o collaboratori che avranno accesso e tratteranno dati ed informazioni di ERSA. La nomina ad Amministratore dovrà avvenire previa valutazione delle caratteristiche di esperienza, capacità e affidabilità dei soggetti designati;
2. La succitata nomina, redatta obbligatoriamente in forma iscritta, dovrà fornire almeno le seguenti istruzioni:
* curare un sistema di registrazione degli accessi al sistema informativo di ERSA da parte dei propri incaricati o collaboratori, in modo che le registrazioni (access log) consentano di identificare, anche indirettamente, il soggetto che ha avuto accesso al sistema, i dati temporali e la descrizione dell'evento. Tali dati dovranno essere conservati con modalità che ne garantiscano l’immodificabilità;
* attenersi all'applicazione delle misure organizzative, fisiche, procedurali e logiche sulla sicurezza con particolare riferimento a quanto specificato nell’art. 32 del Reg. Ue 679/2016 adottando "appropriate misure tecniche e organizzative" per assicurare "un livello di sicurezza adeguato al rischio " (art. 32, par. 1 Reg. Ue 679/2016) rispetto la tipologia e la mole di dati trattati;
* informare tempestivamente ERSA di ogni violazione di dati personali che possa compromettere le libertà e i diritti dei soggetti interessati, in particolare coadiuvare ERSA nelle comunicazioni all’Autorità di controllo competente ed ai soggetti interessati secondo le disposizioni dell’art. 33 e 34 del Reg. UE 679/2016 senza ingiustificato ritardo e, ove possibile, entro 48 ore dal momento in cui ne è venuto a conoscenza;
* se del caso, predisporre e sottoporre a ERSA un programma degli interventi ritenuti utili per migliorare gli aspetti legati alla sicurezza dei dati e dei sistemi;
* comunicare immediatamente a ERSA, e comunque non oltre le 24 ore successive al loro ricevimento, ogni richiesta, ordine o attività di controllo da parte del Garante per la protezione dei dati personali o dell’Autorità Giudiziaria, ai sensi degli articoli 152 e da 157 a 160 del D.Lgs. 196/2003;
* rispondere tempestivamente ed in modo esaustivo alle richieste e ai questionari eventualmente inviati da ERSA per monitorare e vigilare sulle misure di sicurezza poste in essere e, più in generale, sull’applicazione del Reg. UE 679/2016;
* in caso di manutenzioni del sistema, qualora sia effettuato un back up informatico che comporti il salvataggio dei dati su supporti o in cloud, adottare misure di prevenzione dal rischio di sottrazione o accesso non autorizzato e cancellare il back up a conclusione dei lavori.

**4. Garanzie prestate dal Responsabile.**

Il Responsabile garantisce che i dati saranno custoditi e controllati in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di loro distribuzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità del contratto.

Tali dati dovranno essere trattati dal Responsabile esclusivamente al fine di adempiere alle obbligazioni che le derivano dal contratto. Conseguentemente i dati non saranno:

1. utilizzati in proprio e comunque per finalità diverse da quelle riportate all’articolo 1;
2. oggetto di cessione o di concessione d'uso a terzi, totale o parziale, a qualsiasi titolo;
3. duplicati o riprodotti, in proprio, per finalità diverse da quelle riportate all’articolo 1.

Il Responsabile si impegna a non cedere, non consegnare, non copiare, non riprodurre, non comunicare, non divulgare, non rendere disponibili in qualsiasi modo o a qualsiasi titolo a terzi, le informazioni acquisite nell'esecuzione dei servizi resi a favore di ERSA.

Il Responsabile garantisce la tenuta di un Registro delle attività di Trattamento effettuate sotto la propria responsabilità, in conformità a quanto stabilito dall’articolo 30 del GDPR.

**5. Responsabili ulteriori del trattamento**

Il Responsabile si impegna a rispettare le condizioni indicate nei paragrafi 2 e 4 dell’articolo 28 del GDPR per ricorrere ad altro eventuale responsabile del trattamento. In particolare, il Responsabile ha la facoltà di ricorrere alla nomina di ulteriori Responsabili del trattamento ad esso subordinati nell’ambito dell’attività svolta in esecuzione del contratto. Qualora il Responsabile eserciti detta facoltà è tenuta ad informare preventivamente ERSA del trattamento mediante trasmissione via pec all’indirizzo ersa@certregione.fvg.it, al fine di consentire a quest’ultima di manifestare formale opposizione entro 15 giorni dalla ricezione della suddetta comunicazione. Decorso detto termine, il Responsabile potrà procedere alla nomina di ulteriori Responsabili del trattamento, a condizione che su tali soggetti siano imposti gli stessi obblighi in materia di protezione dei dati contenuti nel presente accordo, con particolare riferimento alle garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti del GDPR.

**6. Trasferimento dei dati personali al di fuori dello Spazio Economico Europeo (SEE)**

Qualunque trasferimento di dati verso un paese terzo o un'organizzazione internazionale da parte del Responsabile del trattamento è effettuato soltanto a seguito di autorizzazione scritta rilasciata da ERSA, nel rispetto del capo V del Reg. UE 679/2016. Qualora il Responsabile del trattamento ricorra a un sub-responsabile del trattamento per l'esecuzione di specifiche attività di trattamento e tali attività comportino il trasferimento di dati personali extra UE, il Responsabile del trattamento e il sub-responsabile del trattamento devono garantire il rispetto del capo V del Reg. UE 679/2016 utilizzando le clausole contrattuali tipo adottate dalla Commissione conformemente all'articolo 46, paragrafo 2, del Reg. UE 679/2016.

**7. Foro Competente ed ulteriori disposizioni**

Questo accordo è stipulato e governato dalle leggi italiane. Ogni e qualsiasi controversia relativa all’esecuzione e all’interpretazione di esso sarà devoluta alla competenza del Foro di xxxxx ad esclusione di ogni altro foro anche concorrente.

In caso di contraddizione tra il presente accordo e le disposizioni di accordi correlati, vigenti tra le Parti al momento dell'accettazione del presente documento, o conclusi successivamente, prevalgono le disposizioni del presente accordo.

Resta inteso che il presente Accordo non comporta alcun diritto del Responsabile ad uno specifico compenso e/o indennità e/o rimborso derivante dal medesimo.

Qualsiasi comunicazione inerente il presente accordo viene trasmessa dal Responsabile a ERSA all’indirizzo Pec ersa@certregione.fvg.it

**8. Informativa sul trattamento dei dati personali**

Se richiesto dal Titolare, il Responsabile fornisce all’interessato il modello di informativa predisposto dal Titolare medesimo. Il Responsabile si attiene alle istruzioni fornite dal Titolare per la consegna dell’informativa, garantendo in ogni caso modalità che conservino la prova dell’avvenuta consegna.

Per ERSA Il Responsabile del trattamento

Il Direttore del servizio/Direttore dell’OPR FVG

……………………………………………….. ………………………………………….

 *(sottoscritto digitalmente ai sensi del D.Lgs. 82/2005 e s.m.i.)*

1. *Nel caso di accordo sottoscritto dal Direttore dell’OPR FVG personalizzare con i riferimenti dell’OPR FVG, compresi gli indirizzi PEC, mail e di sede.* [↑](#footnote-ref-2)