ACCORDO PER IL TRATTAMENTO DEI DATI PERSONALI

ai sensi dell'art. 28 del regolamento (UE) 2016/679 (GDPR)

TRA

Automobile Club Udine, ente pubblico non economico a base associativa, con sede in Udine, Viale Tricesimo n. 46, codice fiscale e partita IVA n. 00160740304, nella persona del direttore, dott.ssa Maddalena Valli (di seguito "AC")

E

Fornitore, con sede legale in , partita IVA n. , nella persona di [nome e cognome], in qualità di [legale rappresentante] (di seguito "responsabile")

(l'AC e il responsabile congiuntamente le "Parti")

PREMESSE

a) A decorrere dal 25 maggio 2018 è direttamente applicabile il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito, il "GDPR").

b) L'AC è un ente pubblico non economico a base associativa, federato all'Automobile Club d'Italia, che persegue le finalità e svolge le attività previste dallo Statuto dell'ACI.

c) Le Parti sono vincolate da un contratto [stipulato in data ...] avente ad oggetto _____, in forza del quale il responsabile svolge per conto dell'AC le attività descritte nell'Allegato 1 al presente accordo.

d) L'esecuzione delle attività oggetto del contratto principale comporta necessariamente il trattamento, da parte del responsabile, di dati personali di cui l'AC è titolare del trattamento, con conseguente necessità di disciplinare compiutamente il rapporto tra le Parti ai sensi dell'art. 28 del GDPR.

e) L'art. 28, paragrafo 3, del GDPR prevede che i trattamenti da parte di un responsabile del trattamento siano disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

f) L'AC ha verificato che il responsabile presenta garanzie sufficienti, in particolare in termini di conoscenza specialistica, esperienza, capacità, affidabilità e risorse, per mettere in atto le misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti degli interessati.

DEFINIZIONI

Ai fini del presente accordo, oltre ai termini definiti nel GDPR e nelle premesse, si intendono:

- **"Normativa privacy"**: il GDPR, il d.lgs. 196/2003 come modificato dal d.lgs. 101/2018, nonché qualsiasi altra normativa sulla protezione dei dati personali applicabile, ivi compresi i provvedimenti, le linee guida e le opinioni del Garante per la protezione dei dati personali, del Comitato europeo per la protezione dei dati (EDPB) e di ogni altra autorità competente;
- **"Misure di sicurezza"**: le misure di sicurezza tecniche e organizzative e ogni altro obbligo previsto dalla normativa privacy al fine di garantire la sicurezza e la riservatezza dei dati personali, ivi comprese le attività da compiere in caso di violazione dei dati personali;
- **"Sub-responsabile"**: la persona giuridica, l'ente, l'impresa individuale o il libero professionista incaricato dal responsabile di eseguire specifiche attività di trattamento dei dati personali ai sensi dell'art. 28, paragrafo 4, del GDPR;
- **"Violazione dei dati personali"**: ogni violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, ai sensi dell'art. 4, n. 12, del GDPR;
- **"Incaricati"**: le persone fisiche autorizzate al trattamento dei dati personali sotto l'autorità diretta del responsabile, ai sensi dell'art. 29 del GDPR e dell'art. 2-quaterdecies del d.lgs. 196/2003;
- **"Amministratore di sistema"**: la figura preposta alla gestione e alla manutenzione dei sistemi informatici utilizzati per il trattamento dei dati personali, come individuata dal provvedimento del Garante del 27 novembre 2008, e successive modificazioni.

TUTTO CIÒ PREMESSO

le premesse e le definizioni costituiscono parte integrante e sostanziale del presente accordo. Le Parti convengono e stipulano quanto segue.

Art. 1 – Oggetto e ambito del trattamento

1.1. Con il presente accordo l'AC designa il responsabile, ai sensi dell'art. 28 del GDPR, quale responsabile del trattamento in relazione ai dati personali di cui l'AC è titolare.

1.2. L'ambito del trattamento consentito è quello strettamente connesso e funzionale all'esecuzione del contratto principale ed è descritto in dettaglio nell'Allegato 1 al presente accordo, che ne forma parte integrante e sostanziale, con specifico riferimento a:

- la natura e le finalità del trattamento;

- le tipologie di dati personali trattati;
- le categorie di interessati;
- le operazioni di trattamento.

1.3. Ogni trattamento di dati personali eseguito dal responsabile o dai sub-responsabili, direttamente o tramite i propri incaricati, che non sia strettamente connesso alle attività oggetto del contratto principale, non è ricompreso nel presente accordo e costituisce trattamento autonomo di cui il responsabile è tenuto a rispondere in via esclusiva.

Art. 2 – Durata

2.1. Il presente accordo produce i propri effetti dalla data della sua sottoscrizione e rimarrà in vigore per tutta la durata del contratto principale, ivi compresi eventuali rinnovi, proroghe o periodi di prosecuzione del servizio.

2.2. In caso di cessazione del contratto principale, a qualunque titolo e per qualunque ragione, il responsabile provvederà senza ritardo a cessare ogni trattamento dei dati personali, fatta eccezione per la conservazione temporanea in attesa della restituzione all'AC, e procederà secondo quanto previsto al successivo art. 12.

Art. 3 – Obblighi generali del responsabile

3.1. Il responsabile si impegna a trattare i dati personali esclusivamente ai fini dell'esecuzione del contratto principale, nei limiti e secondo le modalità stabilite dal presente accordo e dalla normativa privacy, attenendosi strettamente alle istruzioni documentate impartite dall'AC.

3.2. Il responsabile informa immediatamente per iscritto l'AC qualora ritenga che un'istruzione violi la normativa privacy o qualsiasi altra disposizione normativa applicabile.

3.3. Il responsabile si impegna in particolare a:

a) trattare esclusivamente i dati personali strettamente necessari per dare corretta e piena esecuzione al contratto principale, nel rispetto del principio di minimizzazione di cui all'art. 5, paragrafo 1, lettera c), del GDPR;
b) trattare i dati personali in modo lecito, secondo correttezza e in piena osservanza dei principi di cui all'art. 5 del GDPR;
c) non trasferire, modificare, comunicare, diffondere o consentire la divulgazione dei dati personali a terzi se non in conformità alle istruzioni documentate dell'AC, salvo che il trattamento sia richiesto dal diritto dell'Unione o dalla legislazione nazionale cui è soggetto il responsabile;
d) non agire quale titolare autonomo del trattamento in relazione ai dati personali trattati per conto dell'AC;
e) assistere e collaborare con l'AC in caso di richieste da parte delle autorità competenti, degli interessati e al fine di conformarsi agli obblighi derivanti dalla normativa privacy;
f) mettere a disposizione dell'AC tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 del GDPR;
g) comunicare tempestivamente all'AC ogni informazione che possa incidere sulla sussistenza delle garanzie prescritte dall'art. 28, paragrafo 1, del GDPR.

Art. 4 – Personale autorizzato al trattamento

4.1. Il responsabile si impegna a consentire il trattamento dei dati personali unicamente a persone autorizzate per iscritto che operino sotto la propria autorità e che:

a) per esperienza, capacità e formazione risultino idonee ad assicurare il rispetto della normativa privacy;
b) siano state debitamente informate e istruite circa gli obblighi previsti dalla normativa privacy e dal presente accordo;
c) abbiano ricevuto specifiche istruzioni operative sulle precauzioni da adottare per garantire la sicurezza e la riservatezza dei dati personali;
d) siano state istruite circa le procedure da rispettare in caso di violazione dei dati personali;
e) siano vincolate a obblighi contrattuali o normativi di riservatezza in relazione a tutte le informazioni conosciute nell'esecuzione del contratto principale;
f) ricevano periodica e adeguata formazione in materia di protezione dei dati personali.

4.2. Il responsabile garantisce che, alla cessazione del rapporto di lavoro o di collaborazione con un incaricato, questi cessi immediatamente ogni trattamento dei dati personali e non conservi nella propria disponibilità, a qualunque titolo e in qualunque formato, copia dei dati.

Art. 5 – Misure di sicurezza

5.1. Tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il responsabile mette in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio, ai sensi dell'art. 32 del GDPR.

5.2. Le misure tecniche e organizzative adottate dal responsabile sono descritte nell'Allegato 4 al presente accordo, che ne costituisce parte integrante e sostanziale.

5.3. Il responsabile si impegna a riesaminare e, ove necessario, aggiornare le misure di sicurezza con periodicità almeno annuale ovvero ogniqualvolta intervengano significativi mutamenti del contesto di rischio, dandone comunicazione all'AC.

5.4. Su richiesta dell'AC, il responsabile conferma per iscritto il rispetto delle misure di cui all'Allegato 4 ovvero ne comunica le modifiche intervenute.

Art. 6 – Sub-responsabili del trattamento

6.1. L'AC autorizza il responsabile a ricorrere a sub-responsabili per l'esecuzione di specifiche attività di trattamento connesse al contratto principale. L'elenco dei sub-responsabili autorizzati è riportato nell'Allegato 2 al presente accordo.

6.2. Il responsabile informa preventivamente per iscritto l'AC di eventuali modifiche riguardanti l'aggiunta o la sostituzione di sub-responsabili, concedendo all'AC un termine non inferiore a quindici (15) giorni per opporsi a tali modifiche. In mancanza di opposizione scritta entro detto termine, la nomina si intende autorizzata.

6.3. Qualora ricorra a sub-responsabili, il responsabile si impegna a:

a) selezionare sub-responsabili che per esperienza, capacità e affidabilità forniscano garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate;

b) stipulare con ciascun sub-responsabile, ai sensi dell'art. 28, paragrafo 4, del GDPR, un contratto o altro atto giuridico che imponga obblighi equivalenti a quelli contenuti nel presente accordo;

c) aggiornare tempestivamente l'Allegato 2;

d) notificare prontamente all'AC eventuali violazioni degli obblighi di protezione dei dati da parte di un sub-responsabile.

6.4. Il responsabile rimane pienamente responsabile nei confronti dell'AC per l'adempimento degli obblighi del sub-responsabile, ai sensi dell'art. 28, paragrafo 4, secondo periodo, del GDPR.

Art. 7 – Violazione dei dati personali

7.1. Nell'ipotesi in cui si verifichi o si sospetti ragionevolmente una violazione dei dati personali, il responsabile ne informa l'AC senza ingiustificato ritardo e, in ogni caso, entro ventiquattro (24) ore dal momento in cui ne sia venuto a conoscenza, inviando una comunicazione scritta redatta utilizzando il modulo di cui all'Allegato 3.

7.2. La comunicazione di cui al comma precedente deve contenere almeno:

a) la descrizione della natura della violazione, compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati personali coinvolti;

b) il nome e i dati di contatto del punto di riferimento presso il responsabile dal quale ottenere ulteriori informazioni;

c) la descrizione del rischio stimato e delle probabili conseguenze della violazione;

d) la descrizione delle misure adottate o proposte per porre rimedio alla violazione e per attenuarne i possibili effetti negativi.

7.3. Il responsabile collabora con l'AC e adotta ogni misura ragionevole per assistere nelle attività di indagine, contenimento e risoluzione della violazione, fornendo tutte le informazioni necessarie per consentire all'AC di adempiere agli obblighi di notifica di cui agli artt. 33 e 34 del GDPR.

7.4. Il responsabile non informa terzi in merito alla violazione senza la preventiva autorizzazione scritta dell'AC, salvo che ciò sia richiesto dal diritto dell'Unione o dalla legislazione nazionale. In tale ultima ipotesi, il responsabile informa preventivamente l'AC dell'obbligo giuridico e considera eventuali sue osservazioni prima di procedere alla notifica.

Art. 8 – Diritti degli interessati

8.1. Tenuto conto della natura del trattamento, il responsabile assiste l'AC con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, ai fini dell'adempimento dell'obbligo di dare seguito alle richieste di esercizio dei diritti degli interessati di cui agli artt. 15-22 del GDPR.

8.2. Il responsabile notifica per iscritto all'AC, entro sette (7) giorni dal ricevimento, qualsivoglia richiesta di esercizio dei diritti degli interessati relativa ai dati personali trattati nell'ambito del presente accordo. Il responsabile non dà autonomamente seguito a tali richieste, salvo diversa istruzione scritta dell'AC.

8.3. Il responsabile collabora con l'AC affinché le richieste degli interessati siano riscontrate nei termini e secondo le modalità previste dalla normativa privacy.

Art. 9 – Valutazione d'impatto e consultazione preventiva

9.1. Il responsabile fornisce all'AC assistenza ragionevole, tenuto conto della natura del trattamento e delle informazioni a propria disposizione, qualora l'AC proceda a una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35 del GDPR e, se del caso, alla consultazione preventiva ai sensi dell'art. 36 del GDPR, limitatamente ai trattamenti di cui al presente accordo.

Art. 10 – Registro delle attività di trattamento

10.1. In conformità all'art. 30, paragrafo 2, del GDPR, il responsabile si impegna a tenere un registro aggiornato di tutte le categorie di attività relative al trattamento svolte per conto dell'AC.

10.2. Il responsabile fornisce all'AC, a richiesta, copia del registro di cui al comma precedente, limitatamente ai trattamenti di cui al presente accordo, e tutte le informazioni necessarie affinché l'AC possa predisporre e mantenere aggiornato il proprio registro dei trattamenti.

Art. 11 – Trasferimento dei dati personali

11.1. Il responsabile non trasferisce né consente che i sub-responsabili trasferiscano i dati personali di cui al presente accordo verso paesi terzi al di fuori dello Spazio economico europeo (SEE), salvo previa autorizzazione scritta dell'AC.

11.2. In assenza di una decisione di adeguatezza ai sensi dell'art. 45 del GDPR relativa al paese terzo di destinazione, il trasferimento può avvenire esclusivamente sulla base delle garanzie adeguate di cui all'art. 46 del GDPR o, in via eccezionale, delle deroghe di cui all'art. 49 del GDPR.

Art. 12 – Restituzione e cancellazione dei dati

12.1. Al termine del trattamento, per qualsiasi ragione, il responsabile, su scelta dell'AC, provvede entro trenta (30) giorni a:

a) restituire all'AC una copia completa di tutti i dati personali su supporto idoneo e in un formato strutturato, di uso comune e leggibile da dispositivo automatico;

b) cancellare in modo sicuro e irreversibile tutte le copie dei dati personali trattati, ivi incluse eventuali copie detenute dai sub-responsabili.

12.2. Il responsabile può conservare i dati personali esclusivamente nella misura e per il periodo richiesto dal diritto dell'Unione o dalla legislazione nazionale, a condizione che garantisca la riservatezza dei dati e che gli stessi siano trattati esclusivamente per le finalità prescritte dalla legge. Resta in ogni caso salvo il diritto del responsabile di conservare la documentazione, analogica e digitale, necessaria per l'esercizio, la difesa o la tutela di un proprio diritto in ogni sede.

Art. 13 – Attività di verifica e audit

13.1. Il responsabile mette a disposizione dell'AC tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 del GDPR e consente e contribuisce alle attività di revisione, comprese le ispezioni, realizzate dall'AC o da un altro soggetto da quest'ultimo incaricato.

13.2. L'AC ha il diritto di accedere, direttamente o tramite propri incaricati, con un preavviso minimo di sette (7) giorni lavorativi, ai locali e alle componenti del sistema informativo utilizzati dal responsabile e dai sub-responsabili per il trattamento dei dati personali di cui al presente accordo, al fine di verificare la conformità alla normativa privacy e al presente accordo.

13.3. Le attività di audit sono a cura e spese dell'AC. Il responsabile informa immediatamente l'AC qualora ritenga che un'istruzione impartita nell'ambito delle attività di audit violi la normativa privacy o altre disposizioni normative applicabili.

Art. 14 – Amministratori di sistema

14.1. Ove il responsabile gestisca sistemi informatici utilizzati per i trattamenti oggetto del presente accordo, con riferimento al provvedimento del Garante del 27 novembre 2008, e successive modificazioni, il responsabile si impegna a:

a) garantire che i sistemi informatici utilizzati nell'esecuzione del contratto principale siano gestiti esclusivamente da personale nominato quale amministratore di sistema, in possesso dei requisiti di esperienza, capacità e affidabilità richiesti dal predetto provvedimento;
b) mantenere a disposizione dell'AC un elenco aggiornato dei soggetti designati quali amministratori di sistema;
c) verificare con cadenza almeno annuale l'operato degli amministratori di sistema, in modo da controllare la rispondenza alle istruzioni impartite;
d) registrare gli accessi logici ai sistemi informatici effettuati dagli amministratori di sistema, conservando i relativi log per un periodo non inferiore a sei mesi.

Art. 15 – Responsabilità e manleva

15.1. La responsabilità per i danni derivanti dal trattamento dei dati personali oggetto del presente accordo è disciplinata dall'art. 82 del GDPR, ivi incluse le disposizioni in materia di solidarietà (paragrafo 4), regresso (paragrafo 5) ed esonero (paragrafo 3).

15.2. Fermo restando quanto previsto dal contratto principale, e a integrazione della manleva ivi contenuta, il responsabile si obbliga a manlevare e tenere indenne l'AC da ogni danno, costo, onere e spesa, ivi comprese le spese legali, derivanti da sanzioni comminate ai sensi dell'art. 83 del GDPR ovvero da richieste risarcitorie, reclami, azioni o procedimenti promossi da interessati, terzi o autorità competenti, nella misura in cui siano riconducibili a violazioni della normativa privacy imputabili al responsabile, ai sub-responsabili da esso designati o ai rispettivi incaricati.

15.3. Il responsabile si impegna a collaborare attivamente con l'AC in ogni procedimento, giudiziale o amministrativo, relativo ai dati personali trattati nell'ambito del presente accordo.

Art. 16 – Corrispettivo

16.1. Gli obblighi del responsabile derivanti dal presente accordo si intendono ricompresi nel corrispettivo previsto dal contratto principale. Nessun corrispettivo ulteriore è dovuto al responsabile in relazione alle attività oggetto del presente accordo, salvo diverso accordo scritto tra le Parti.

Art. 17 – Comunicazioni

17.1. Ogni comunicazione tra le Parti relativa al presente accordo dovrà essere effettuata per iscritto tramite posta elettronica certificata (PEC) ai seguenti indirizzi:

- Per l'AC: automobileclubudine@legalmail.it
- Per il responsabile: [indirizzo PEC di Fornitore]

17.2. Le comunicazioni inviate a mezzo PEC saranno considerate efficaci al momento dell'effettiva ricezione, se ricevute in un giorno lavorativo; diversamente, nel giorno lavorativo immediatamente successivo.

Art. 18 – Disposizioni finali

18.1. Il presente accordo è regolato dalla legge italiana. Per ogni controversia derivante dal presente accordo è esclusivamente competente il Foro di Udine.

18.2. In caso di contrasto tra il presente accordo e il contratto principale, il presente accordo prevale con riferimento alle questioni relative al trattamento dei dati personali.

18.3. Le Parti si impegnano a modificare il presente accordo in conseguenza di modifiche della normativa privacy, ivi compresi provvedimenti, linee guida od opinioni delle autorità competenti, che rendano necessario un adeguamento.

18.4. L'eventuale invalidità o inefficacia di una o più clausole del presente accordo non comporta l'invalidità delle restanti, che rimangono pienamente valide ed efficaci.

18.5. Il presente accordo e i relativi allegati sostituiscono integralmente ogni precedente intesa tra le Parti in materia di protezione dei dati personali con riferimento ai servizi oggetto del contratto principale.

Per l'Automobile Club Udine	**Per Fornitore**
Il direttore, dott.ssa Maddalena Valli _____	[nome, cognome e qualifica] _____

ALLEGATO 1

DESCRIZIONE DEI TRATTAMENTI

1. Tipologie di servizi e operazioni di trattamento

Il responsabile svolge, per conto dell'AC, le seguenti attività: consulenza in materia di salute e sicurezza nei luoghi di lavoro e funzioni di Responsabile del Servizio di Prevenzione e Protezione ai sensi del d.lgs. 81/2008. Le operazioni di trattamento comprendono:

a) raccolta, consultazione e conservazione dei dati del personale necessari alla valutazione dei rischi e alla predisposizione e all'aggiornamento del documento di valutazione dei rischi;
b) organizzazione, registrazione e documentazione della formazione e dell'addestramento del personale in materia di salute e sicurezza;
c) documentazione della consegna dei dispositivi di protezione individuale;
d) analisi degli infortuni e delle situazioni di rischio, limitatamente agli aspetti di prevenzione e protezione.

2. Categorie di interessati

I trattamenti possono riguardare, nei limiti delle singole attività svolte in esecuzione del contratto principale, le seguenti categorie di interessati:

- dipendenti e collaboratori dell'AC;
- altri lavoratori presenti nei luoghi di lavoro dell'AC, ove rilevante ai fini della valutazione dei rischi (es. personale di imprese terze).

3. Tipologie di dati personali trattati

3.1. Dati comuni

Dati identificativi e di contatto; mansione e inquadramento; dati relativi alla formazione e all'addestramento (attestati, esiti delle verifiche di apprendimento); dati relativi alla consegna dei dispositivi di protezione individuale.

3.2. Categorie particolari di dati personali (art. 9 GDPR)

Giudizi di idoneità alla mansione e relative limitazioni o prescrizioni comunicati dal medico competente, nonché informazioni relative a infortuni, limitatamente a quanto strettamente necessario all'esercizio delle funzioni di RSPP.

3.3. Dati relativi a condanne penali e reati (art. 10 GDPR)

Non sono trattati dati relativi a condanne penali e reati.

Nota: il trattamento delle categorie particolari di dati personali e dei dati relativi a condanne penali e reati è in ogni caso strettamente limitato a quanto necessario per l'esecuzione delle attività oggetto del contratto principale ed è effettuato nel rispetto delle condizioni di liceità previste dalla normativa applicabile.

4. Finalità del trattamento

Il responsabile tratta i dati personali esclusivamente per conto dell'AC, al fine di dare esecuzione al contratto principale. Le finalità del trattamento sono:

- adempimento degli obblighi in materia di salute e sicurezza nei luoghi di lavoro previsti dal d.lgs. 81/2008, con particolare riferimento alla valutazione dei rischi e all'individuazione delle misure di prevenzione e protezione;
- informazione, formazione e addestramento del personale.

Il responsabile non è autorizzato a trattare i dati per finalità proprie o ulteriori, né a comunicare i dati a terzi al di fuori delle ipotesi espressamente previste dal presente accordo e dalle istruzioni documentate dell'AC.

ALLEGATO 2

SUB-RESPONSABILI DEL TRATTAMENTO

Di seguito l'elenco dei sub-responsabili del trattamento autorizzati ai sensi dell'art. 6 del presente accordo:

Denominazione	**Sede**	**Attività di trattamento affidata**	**Dati trattati**
[da compilare]	[da compilare]	[da compilare]	[da compilare]
[da compilare]	[da compilare]	[da compilare]	[da compilare]

Ovvero, in alternativa:

☐ Alla data di sottoscrizione del presente accordo, il responsabile non ricorre a sub-responsabili del trattamento.

ALLEGATO 3

MODULO PER LA NOTIFICA DI VIOLAZIONI DEI DATI PERSONALI

Il presente modulo deve essere compilato e trasmesso all'AC entro 24 ore dalla conoscenza della violazione, ai sensi dell'art. 7 del presente accordo.

Campo	**Contenuto**
Data e ora della scoperta della violazione	
Data e ora stimate della violazione	
Descrizione della natura della violazione	
Categorie di interessati coinvolti	
Numero approssimativo di interessati coinvolti	
Categorie di dati personali coinvolti	

Numero approssimativo di registrazioni coinvolte	
Probabili conseguenze della violazione	
Misure adottate o proposte per porre rimedio alla violazione	
Misure adottate per attenuare gli effetti negativi	
Nome e dati di contatto del referente	

Data: _____ Firma del responsabile: _____

ALLEGATO 4

MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

1. Contesto del trattamento

L'attività è svolta in parte presso la sede dell'AC (sopralluoghi, riunioni, attività formative) e in parte presso la sede del responsabile, che conserva, su supporto cartaceo e informatico proprio, la documentazione necessaria all'incarico (es. documento di valutazione dei rischi, attestati e registri della formazione). Il responsabile non gestisce sistemi informatici dell'AC.

2. Misure minime

Fermo restando l'obbligo di cui all'art. 5 del presente accordo di adottare misure adeguate al rischio, il responsabile garantisce in ogni caso che:

a) **accessi:** l'accesso ai dati sia consentito alle sole persone autorizzate e istruite, mediante credenziali personali e non condivise, protette da password di adeguata lunghezza e complessità; le abilitazioni siano revocate tempestivamente alla cessazione del rapporto e le postazioni si blocchino automaticamente in caso di inattività;

b) **documentazione cartacea:** sia custodita in armadi o locali chiusi, non sia lasciata incustodita e, quando non più necessaria, sia distrutta con modalità che ne impediscano la ricostruzione;

c) **sistemi:** siano utilizzati software e sistemi operativi supportati dal produttore, con aggiornamenti di sicurezza applicati tempestivamente e protezione antimalware e firewall attivi;

d) **backup:** i dati siano oggetto di copie di sicurezza periodiche, di cui almeno una conservata separatamente dai sistemi ordinari, in modo da consentirne il ripristino anche in caso di attacco informatico;

e) **dispositivi portatili:** computer portatili, smartphone e supporti rimovibili che contengono dati dell'AC siano protetti da cifratura e da credenziali di accesso;

f) **trasmissione:** le comunicazioni di dati con l'AC avvengano mediante canali sicuri (es. PEC, sistemi messi a disposizione dall'AC o dall'ACI, connessioni cifrate); le categorie particolari di dati siano trasmesse solo in forma protetta;

g) **strumenti di terzi:** i dati dell'AC non siano conservati o trattati su servizi o piattaforme di terzi (es. servizi cloud, posta elettronica personale, applicazioni di messaggistica) se non riconducibili a sub-responsabili autorizzati ai sensi dell'art. 6;

h) **formazione:** il personale sia periodicamente sensibilizzato sui principali rischi per la sicurezza dei dati, in particolare sui tentativi di frode informatica (es. phishing);

i) **conservazione:** i dati non siano copiati né conservati oltre quanto necessario all'esecuzione del contratto principale e siano cancellati con modalità sicure.

3. Misure ulteriori per i servizi informatici

Ove il responsabile gestisca sistemi informatici utilizzati per i trattamenti dell'AC, garantisce altresì che:

a) gli accessi da remoto e con privilegi amministrativi siano protetti con autenticazione a più fattori, salvo comprovata impossibilità tecnica;

b) a ciascun operatore siano attribuiti i soli privilegi necessari e le utenze amministrative siano distinte da quelle di uso ordinario;

c) siano rispettati gli obblighi di cui all'art. 14 del presente accordo;

d) gli interventi da remoto avvengano con strumenti sicuri, su richiesta dell'AC o nell'ambito di attività programmate, e siano documentati;

e) le copie di sicurezza comprendano almeno una copia non modificabile o non connessa alla rete e la possibilità di ripristino sia verificata almeno una volta all'anno;

f) le vulnerabilità note siano corrette tempestivamente, con priorità per quelle critiche;

g) i dati siano cifrati durante la trasmissione e, nei servizi in cloud, anche durante la conservazione;

h) i dati siano conservati all'interno dello Spazio economico europeo, salvo quanto previsto dall'art. 11;

i) siano previste modalità e tempi di ripristino del servizio in caso di incidente, indicati nel contratto principale o comunicati all'AC.

4. Documentazione del responsabile

Il responsabile può allegare o mettere a disposizione dell'AC la propria documentazione sulle misure adottate (ad esempio policy di sicurezza o certificazioni), che integra il presente allegato, e comunica all'AC ogni modifica che riduca in modo significativo il livello di protezione.