REGOLAMENTO INTERNO SULLA PROTEZIONE, IL TRATTAMENTO E LA CIRCOLAZIONE DEI DATI PERSONALI

Titolo I
Disposizioni generali
Art. 1
Definizioni

1. Ai fini del presente Regolamento si intende per:

a) **Archivio:** qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
b) **Autenticazione informatica:** insieme degli strumenti elettronici e delle procedure di verifica anche indiretta dell'identità;
c) **Codice della privacy:** il decreto legislativo 30 giugno 2003, n. 196 come modificato dal decreto legislativo 10 agosto 2018, n. 101.
d) **CONI:** Comitato Olimpico Nazionale Italiano di cui al decreto legislativo 23 luglio 1999, n. 242;
e) **Credenziali di autenticazione o di accesso:** dati e dispositivi, in possesso di una persona, da questi conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica.
f) **Data breach:** un incidente di sicurezza in cui Dati personali, protetti o riservati vengono consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato ovvero la divulgazione di dati personali in maniera illecita, involontaria o volontaria.
g) **Dato anonimo:** dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
h) **Dato giudiziario:** dato personale idoneo a rivelare i provvedimenti giudiziari penali ed amministrativi in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato (es.: provvedimenti di condanna definitivi, di proscioglimento, di non luogo a procedere per difetto di imputabilità, concernenti le pene, le misure di sicurezza, gli effetti penali della condanna, l'amnistia, l'indulto, la grazia, la dichiarazione di abitualità, di professionalità nel reato, di tendenza a delinquere, le pene accessorie, le misure alternative alla detenzione, la liberazione condizionale, ecc.).
i) **Dato identificativo:** dati personali che permettono l'identificazione dell'interessato;
j) **Dato personale:** qualsiasi informazione riguardante una persona fisica identificata o identificabile direttamente o indirettamente;
k) **Dato personale (categorie particolari di) o Dato sensibile**: i dati personali idonei a rilevare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rilevare lo stato di salute e la vita sessuale.
l) **Garante:** l'Autorità italiana Garante per la protezione dei dati personali.

m) **GDPR:** il Regolamento (UE) del Parlamento Europeo e del Consiglio Europeo del 27 aprile 2016.
n) **Interessato:** persona fisica identificata o identificabile, direttamente o indirettamente;
o) **Lavoratore:** le persone fisiche assunte alle dipendenze della Federazione ivi inclusi i lavoratori temporanei, intermittenti, i tirocinanti, gli stagisti ecc. Sono assimilati ai lavoratori i titolari di cariche istituzionali. Sono considerati lavoratori ai fine della anche quanti abbiano cessato la propria attività di collaborazione con FISE nella misura in cui i dati personali degli stessi rimangano nel possesso di FISE.
p) **Misure di sicurezza o di protezione:** complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti;
q) **Organizzazione internazionale:** un'organizzazione e gli organismi di Diritto Internazionale Pubblico ad essa subordinati o qualsiasi altro organismo istituto sulla base di un accordo fra due o più stati quali ad esempio il Comitato olimpico internazionale-CIO, la Federazione Equestre Internazionale - FEI, la World AntiDoping Agency – WADA, il Tribunale Arbitrale dello Sport - TAS.
r) **Profilo o livello di autorizzazione:** insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;
s) **Pseudonimizzazione:** trattamento di dati personali attribuibili all'interessato solo attraverso ulteriori informazioni aggiuntive, separatamente conservate e sottoposte ad adeguate misure tecniche che non ne consentano l'attribuzione ad una persona identificabile;
t) **Sistema di autorizzazione:** insieme di strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente;
u) **Strumenti elettronici:** elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
v) **Titolare:** Federazione Italiana Sport Equestri (di seguito FISE o "Federazione");
w) **Tracciabilità:** grado in cui i dati hanno attributi che forniscono una registrazione degli accessi ai dati e a tutte le modifiche effettuate ai dati in un contesto di utilizzo specifico;
x) **Trattamento:** qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di strumenti elettronici, processi automatizzati e applicate a dati personali, come la raccolta, registrazione, organizzazione, strutturazione, conservazione, memorizzazione, adattamento o modifica, consultazione, elaborazione, uso, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, diffusione, cancellazione, distruzione di dati anche se non registrati in una banca dati;

Art. 2
Ambito di applicazione e finalità

1. Il presente Regolamento stabilisce le misure organizzative, le procedure e le politiche di FISE per garantire che i dati personali:

a) siano acquisiti e trattati in forza di idonea e pertinente base giuridica per scopi determinati, espliciti e legittimi;
b) siano trattati solo per le finalità proprie di FISE e in maniera non eccedente le predette finalità;
c) siano trattati nel rispetto dei diritti e della dignità degli interessati;
d) siano protetti dal rischio, anche solo potenziale, di distruzione, perdita, modificazione, rivelazione non autorizzata, accesso non autorizzato, non esattezza e non adeguatezza rispetto alle finalità per cui sono trattati;
e) siano comunicati all'interno e all'esterno di FISE ovvero pubblicati in maniera non eccedente le finalità del trattamento per i quali furono acquisiti.

2. I dipendenti di FISE e quanti siano investiti di ruoli, anche dirigenziali, ovvero siano stati nominati quali membri degli organi della Federazione di cui all'art. 17 dello Statuto di FISE, nell'ambito delle mansioni cui sono preposti in via ordinaria applicano il presente Regolamento, facendo riferimento per ogni evenienza non espressamente prevista o nei casi dubbi al Data Protection Officer.

3. Ai sensi degli artt. 5, 10 e 15 dello Statuto di FISE, il presente Regolamento obbliga altresì, rispettivamente, gli Affiliati, i Tesserati e gli Aggregati, fermi restando:

a) per quanto riguarda i Tesserati che rivestano la qualità di Interessati i diritti ad essi attribuiti dal GDPR e i doveri di FISE, nella qualità di Titolare del trattamento, nei loro confronti;
b) per quanto attiene gli Affiliati e i Tesserati, la loro qualificazione di Titolari autonomi anche con riferimento ai Dati Personali eventualmente trasmessi a FISE nell'ambito delle attività di interesse pubblico da questi poste in essere.

Art. 3
Principi

1. Il Trattamento dei dati personali all'interno di FISE deve conformarsi ai seguenti principi:

a) Principio di correttezza: le modalità di raccolta e di utilizzo dei dati devono essere corrette, come lo stesso trattamento dei dati in tutti i suoi aspetti. Il principio di correttezza è legato anche alla chiarezza e trasparenza delle informative e alla necessità che l'informazione fornita all'interessato sia tale da far comprendere in modo adeguato non solo le modalità del trattamento ma anche le sue conseguenze.
b) Principio di esattezza dei dati: i dati devono essere esatti e, se necessario, aggiornati. Devono essere adottate tutte le misure ragionevoli al fine di verificare l'esattezza dei dati, rispetto alle finalità dichiarate, garantire il loro aggiornamento e completezza, e cancellare o rettificare tempestivamente i dati inesatti o le anomalie riscontrate.
c) Principio di liceità: ogni trattamento deve trovare fondamento su una delle basi giuridiche indicate all'art. 6 del Regolamento europeo 2016/679, vale a dire il: consenso,

adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il Titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del Titolare o di terzi cui i dati vengono comunicati. In caso di categorie particolari di dati, quali i dati idonei a rivelare lo stato di salute dell'interessato, il trattamento deve trovare fondamento in una delle basi giuridiche indicate dall'art. 9 del GDPR.

d) Principio della limitazione della conservazione: i dati devono essere conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono stati trattati. Unitamente al tempo di conservazione è di dirimente importanza l'individuazione di modalità di conservazione distinte in funzione delle diverse fasi del trattamento.
e) Principio di limitazione delle finalità: gli scopi del trattamento devono essere determinati, espliciti e legittimi. I trattamenti successivi a quelli iniziali non devono avere, salvo eccezioni, finalità incompatibili a quelle originarie.
f) Principio di non eccedenza o minimizzazione dell'uso dei dati: i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità. Possono essere utilizzati solo i dati sufficienti al perseguimento dei legittimi fini dichiarati, e non eccedenti i fini stessi. Il principio di minimizzazione ha una efficacia trasversale e implica una riduzione al minimo del numero dei dati, del tipo di trattamenti, dei soggetti coinvolti e del periodo di conservazione.
g) Principio di trasparenza: tracciabilità del dato da parte dell'interessato e modalità operative che tengano conto della possibilità di *disclosure* in ogni momento a richiesta dell'interessato.
h) Principio dell'integrità e della riservatezza: deve essere garantita una adeguata sicurezza del dato personale. L'adozione di misure tecniche e organizzative adeguate protegge il dato da trattamenti non autorizzati o illeciti e lo assicura da perdita, distruzione o danno accidentale.

Titolo II
Misure organizzative

Art. 4
Funzioni e processi

1. Ai sensi dell'art. 4, par. 1, n. 7, del GDPR, FISE, in quanto soggetto giuridico che determina le finalità e i mezzi del trattamento di Dati personali, agisce in qualità di Titolare del trattamento.
2. In particolare, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità dei trattamenti, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà degli Interessati, per mezzo del presente Regolamento FISE adotta misure organizzative e politiche generali in maniera da garantire ed essere in grado di dimostrare il rispetto delle regole e dei principi stabiliti dal GDPR e dalla normativa nazionale.
3. Le misure organizzative riguardano

a) la definizione di ruoli e responsabilità sia all'interno, sia all'esterno della Federazione.
b) la definizione di regole di condotta e procedure.

4. Internamente alla Federazione il presente Regolamento stabilisce il ruolo, gli obblighi e le responsabilità de:

a) gli Incaricati del trattamento;
b) il Data Manager o Responsabile privacy;
c) il Responsabile dei sistemi informativi;
d) i Referenti della protezione dei dati e i Subreferenti
e) il Responsabile della protezione dei dati (DPO).

La nomina a Data Manager e Responsabile dei sistemi informativi possono essere assegnati ad un'unica persona.

5. Esternamente alla Federazione, il presente Regolamento disciplina i casi e le modalità con le quali, nel rispetto del GDPR e della normativa vigente, devono essere disciplinati i rapporti con i Responsabili esterni del trattamento e i Contitolari.

6. La definizione di regole di condotta e delle procedure riguarda

a. la scelta più appropriata della base giuridica del trattamento;
b. le regole da osservare nell'acquisizione dei Dati personali, nella loro conservazione ed eventuale distruzione;
c. il corretto utilizzo degli strumenti informatici;
d. la tutela dei diritti degli Interessati e la gestione di loro eventuali istanze;
e. la valutazione dei rischi e dell'impatto per i diritti e le libertà degli interessati connessi ai trattamenti posti in essere da FISE;
f. la gestione di eventuali fenomeni di perdita, distruzione, accesso illegittimo e sottrazione di Dati personali.

7 Il presente Regolamento non sostituisce e non modifica gli altri Regolamenti e le vigenti deliberazioni adottate dagli organi della Federazione o i Principi emanati dal CONI tempo per tempo vigenti, ma li integra limitatamente alla corretta modalità di trattamento dei Dati Personali di modo che, nell'applicazione di detti Regolamenti, Deliberazioni e Principi i soggetti del comma 4 si conformano anche al presente Regolamento. In caso di contrasto del presente Regolamento con detti Regolamenti, Deliberazioni e Principi, i soggetti di cui al comma 4, prima di procedere con le attività di trattamento si consultano con il DPO, il quale rende sul punto il proprio parere circa il miglior modo di risolvere eventuali antinomie nel rispetto del GDPR, del Codice e gli indirizzi e le linee guida del Garante.

8. Del pari, fatta eccezione per il DPO, l'individuazione delle figure di cui al comma 4, non modifica l'organigramma della Federazione, ma avviene in coerenza con lo stesso e con le mansioni svolte da ciascuno dei dipendenti e membri degli organi della FISE i quali curano il rispetto del presente Regolamento, della normativa tempo per tempo vigente e delle Linee Guida dell'Autorità Garante per la protezione dei dati personali nell'ambito delle ordinarie procedure previste per la gestione delle funzioni e degli organi cui appartengono ovvero nell'adempimento ai contratti stipulati dalla Federazione.

9 Nel rispetto dell'indipendenza del DPO, il coordinamento delle funzioni di cui al comma 4 è affidato al Data Manager che le convoca in apposito Comitato con cadenza almeno annuale ovvero, secondo migliore convenienza, in coincidenza con le sedute del Consiglio dei Presidenti dei Comitati Regionali. Il Comitato è convocato ogni qualvolta se ne presenti la necessità ovvero qualora ne faccia richiesta il DPO. Al Comitato non partecipano i Responsabili esterni, i Subreferenti e gli Incaricati salvo che, in ragione dell'oggetto della seduta, il Data Manager, sentito il DPO, ne richieda la presenza.

Art. 5
Data Manager

1. Il Data Manager svolge la funzione di coordinamento e di punto di contatto fra le funzioni di cui all'art. 4 comma 4 al fine di assicurare, in stretto coordinamento con il DPO e con il Responsabile dei sistemi informativi, se nominato separatamente, il raggiungimento e il mantenimento di un livello di protezione adeguato in relazione allo specifico o agli specifici trattamenti di dati personali posti in essere dalla Federazione.

2. Il Data Manager coordina i soggetti di cui all'art. 4 comma 4 e supporta le funzioni operative della Federazione di volta in vota interessate, al fine di assicurare che:

a) tutti siano correttamente informati sull'evoluzione del contesto interno ed esterno relativo al trattamento dei dati personali e ricevano adeguate istruzioni e formazione sul modo di procedere;
b) i rapporti con terze parti (destinatari, responsabili e contitolari) siano correttamente formalizzati e che quanto così formalizzato sia correttamente adempiuto dai terzi;
c) la Federazione sia dotata di strumenti tecnici, anche informatici, con standard adeguati ad una corretta gestione e ad una adeguata protezione dei dati personali;
d) gli atti dai quali risulti la base giuridica del trattamento (contratti e consensi) e la corretta informazione agli interessati (informativa) siano archiviati e resi disponibili a tutte le funzioni della Federazione;
e) il Registro dei trattamenti è correttamente tenuto e implementato da parte dei Referenti, degli Incaricati, dei Responsabili esterni del trattamento e dei Contitolari;
f) vi sia correttezza, esattezza e completezza di dati personali oggetto di trattamento e non eccedenza degli stessi rispetto alle finalità del trattamento di volta in volta considerati;
g) non siano trasmessi e non sia consentito l'accesso ai dati personali a soggetti non incaricati del loro trattamento o privi delle necessarie attribuzioni per accedervi.

Art. 6
Responsabile dei Sistemi Informativi

1. Il Responsabile dei sistemi informativi ha la responsabilità complessiva di tutto il sistema informativo federale, incluso il coordinamento, lo sviluppo, il mantenimento e il monitoraggio del programma di sicurezza delle informazioni, nonché di garantire che le informazioni siano opportunamente protette, considerando sia gli aspetti di natura logica, sia organizzativa e

normativa. In particolare, il Responsabile dei Sistemi informativi, sentito il DPO e di concerto con il Data Manager, se nominato separatamente, dovrà:

a) definire e coordinare un piano operativo per garantire la sicurezza delle informazioni, definendo azioni e tempistiche che dovranno essere attuate congiuntamente ai singoli dipartimenti;
b) eseguire e aggiornare l'analisi dei rischi di sicurezza, identificando le principali criticità a livello organizzativo, di processo e tecnologico;
c) definire norme comportamentali, soluzioni procedurali e sistemi architetturali per garantire la riservatezza, l'integrità e la disponibilità delle informazioni (es. configurazione sicura dei sistemi, definizioni di norme per la gestione degli asset, gestione degli incidenti) secondo gli indirizzi di cui all'allegata Appendice;
d) monitoraggio del corretto funzionamento delle misure di protezione adottate.

Art. 7

Responsabile della protezione dei dati - *Data Protection Officer* (DPO).

1. Il DPO può essere scelto fra i dipendenti della Federazione ovvero mediante un contratto di prestazione di servizi.

2. In ogni caso, il DPO deve essere individuato tra persone che abbiano competenze specialistiche in materia di protezione dei dati personali e adeguata conoscenza del GDPR e delle prassi nazionali in materia di protezione dei dati personali.

3. Al DPO:

a) devono essere fornite le risorse necessarie per assolvere i propri compiti, per accedere ai dati personali e ai trattamenti e, a seconda del profilo professionale prescelto, per acquisire consulenze indipendenti nei settori della medicina, dell'informatica e giuridico legali.
b) deve essere assicurata la possibilità di riferire direttamente agli organismi di controllo e vigilanza della Federazione;

4. Qualora sia individuato in un soggetto esterno, nel contratto di prestazione di servizi deve essere espressamente previsto che non costituisce causa di risoluzione del rapporto la mancata esecuzione di istruzioni, ricevute dal titolare, inerenti i suoi poteri di controllo e vigilanza, anche se contenute in delibere degli Organi federali.

5. Analogamente, il contratto di lavoro del dipendente nominato DPO deve essere integrato con una pattuizione aggiuntiva che escluda la possibilità di applicare sanzioni disciplinari e non costituisce giusta causa di licenziamento qualunque atto compiuto dal dipendente nella veste di DPO. Ove nominato fra i dipendenti della Federazione, il DPO può svolgere altre mansioni purché non implichino, direttamente o sotto la sua diretta responsabilità, il trattamento di dati personali in maniera significativa e continuativa.

6. Il DPO deve essere coinvolto in tutte le questioni relative alla protezione dei dati personali e deve essere posto in condizioni di esercitare concretamente un'attività di vigilanza e controllo

sul rispetto del presente Regolamento da parte di Contitolari, Responsabili esterni, Referenti e Incaricati.

7. Il DPO deve, in particolare, intervenire:

a) nella definizione e nella gestione dei rapporti con i contitolari e i responsabili e in tutti i rapporti che comportino il trasferimento di dati personali;
b) nella definizione delle istruzioni date agli incaricati e nella definizione della necessità formative degli stessi;
c) nella definizione di nuovi trattamenti e nella valutazione preliminare dei trattamenti da sottoporre a valutazione di impatto (c.d. DPIA) e nell'esecuzione della stessa;
d) alla valutazione di conformità di ogni nuova finalità di trattamento dei dati personali ovvero di ogni variazione delle finalità e delle modalità dei trattamenti esistenti
e) in tutti i casi in cui sia richiesta una consulenza specialistica in merito agli obblighi derivanti dal GDPR;
f) nelle attività che comportino rapporti con il Garante per la protezione dei dati personali;
g) nella gestione delle istanze degli interessati a chiunque inoltrate e che possono rivolgersi direttamente a lui per l'esercizio dei propri diritti.

8. Il DPO supporta gli Uffici della federazione nel monitoraggio delle misure tecniche e organizzative adottate e nel loro costante aggiornamento:

a) all'evoluzione del contesto interno ed esterno e del quadro normativo in materia di protezione dei dati personali al fine di individuare tempestivamente i requisiti normativi applicabili al contesto;
b) all'evoluzione degli scenari di rischio in materia di protezione dei dati personali al fine di:
    i. individuare eventuali nuovi scenari di rischio;
    ii. individuare variazioni negli scenari di rischio già individuati in precedenza.
c) alla verifica dei singoli trattamenti, al fine di determinare se sono svolti in conformità ai requisiti stabiliti dal presente Regolamento e dalla normativa di settore;
d) al riesame, su base pianificata annuale o su base non pianificata, del presente Regolamento. Il riesame su base non pianificata avviene a fronte di:
    i. gravi o ripetute non conformità;
    ii. incidenti in materia di protezione dei dati personali;
    iii. significative variazioni del contesto di riferimento esterno, incluse variazioni del quadro normativo e giurisprudenziale, eventuali indirizzi emanati dal CONI, dalle organizzazioni sportive internazionali cui FISE aderisce ovvero a seguito di rilevanti provvedimenti del Garante ivi inclusi quelli di cui all'art. 2 *quinquiesdecies*, del Codice della privacy;
    iv. significative variazioni del contesto di riferimento interno, a seguito di riorganizzazioni o di significative variazioni nelle procedure operative, anche determinate dall'adozione di nuovi strumenti, anche informatici, di supporto all'attività.

9. Nell'attività di vigilanza, il DPO può coordinare la propria attività con l'Organismo di vigilanza nominato ai sensi del d.lgs. 8 giugno 2001, n. 231 condividendo l'inserimento di elementi di rilevanti ai fini della protezione dei dati nei flussi informativi destinati a detto organismo.
10. Il nominativo e i dati di contatto del DPO devono essere pubblicati sul sito web istituzionale della Federazione. Allo stesso deve essere assegnata una casella di posta elettronica dedicata (dpo@fise.it).

Art. 8
Referenti interni

1. In forza del presente Regolamento, in considerazione della complessità e della molteplicità delle funzioni istituzionali della Federazione e della quantità e qualità dei dati trattati, oltre che della necessità di garantire l'adozione di misure organizzative capillari sono designati quali Referenti per il trattamento dei dati

a) i Presidenti dei Comitati Regionali;
b) i Responsabili degli uffici centrali della Federazione.

2. I Referenti operano sotto la diretta responsabilità del Titolare e devono assicurare che gli Incaricati del trattamento e chiunque sia sottoposto alla propria direzione e coordinamento, osservino il presente Regolamento e la normativa vigente, ivi incluse le direttive del Garante.
3. I Referenti assicurano, altresì, il raggiungimento e il mantenimento di un livello di protezione adeguato in relazione allo specifico o agli specifici trattamenti di dati personali posti in essere dall' Ufficio cui sono preposti, coordinando trasversalmente i soggetti coinvolti.
4. In particolare, ogni Referente, deve assicurare:

a) l'adozione di idonee misure per assicurare, nell'organizzazione delle prestazioni e dei servizi che comportano il trattamento di dati personali e in relazione al predetto trattamento, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale;
b) la compilazione e il costante aggiornamento del Registro dei Trattamenti in occasione della definizione di nuovi trattamenti o della modifica delle finalità di quelli esistenti;
c) ove richiesta in base al presente Regolamento, e sentito il *Data Protection Officer,* l'esecuzione, in fase di progettazione di nuovi trattamenti, di una valutazione di impatto e di rischio;
d) la nomina, con atto formale da adottarsi sul modello allegato al presente Regolamento oppure attraverso idonea procedura informatica, delle persone incaricate del trattamento dei dati personali e che possono avere accesso agli stessi;
e) che non siano trasmesse e non sia consentito l'accesso ai dati personali a soggetti non incaricati del loro trattamento in conformità al presente Regolamento;
f) che siano trasmessi o sia consentito l'accesso ai dati personali trattati nell'ambito proprio Dipartimento solo previa adozione di misure tecniche di protezione eventualmente stabilite nel presente Regolamento (quali, a titolo esemplificativo, la pseudonimizzazione, la cifratura, l'anonimizzazione dei dati personali) e, salvo che la trasmissione o l'accesso

ai dati sia consentita senza adozione di misure di protezione dal presente Regolamento, da istruzioni specifiche della Federazione o da norme imperative di legge.

g) la costante collaborazione con il *Data Protection Officer* in relazione ai compiti ad esso affidati in base la presente Regolamento.

Art. 9
Nomina di SubReferenti interni

1. I singoli Referenti, nei limiti di quanto loro consentito dalla regolamentazione interna della Federazione, sono autorizzati in via generale a nominare all'interno degli Uffici o dei Comitati cui sono preposti ulteriori SubReferenti, da individuarsi fra il personale dipendente della Federazione, purché ne siano stabilite le deleghe e i compiti.

2. I Referenti interni possono essere nominati in relazione al trattamento di dati personali afferenti agli Uffici di appartenenza ovvero in relazione a singole attività, anche non ricorrenti, che comportino il trattamento di dati personali.

3. Della nomina dei SubReferenti deve essere informato il Titolare, nella persona del Segretario Generale. La nomina ha efficacia trascorsi 30 giorni dalla comunicazione senza che il Segretario Generale, sentito il DPO e il Data Manager, abbia fatto opposizione. In caso di opposizione la nomina non ha corso.

Art. 10
Incaricati del Trattamento

1. Ogni dipendente della Federazione, il personale non strutturato, a tempo indeterminato, definito o parziale, i tirocinanti, gli operatori di supporto preposti a mansioni che implichino il trattamento di dati personali, ovvero qualora sia assegnato ad una mansione non ricorrente che implichi il trattamento di dati personali deve ricevere un incarico dal Referente interno cui risponde. L'incarico è predisposto sulla base del modello allegato al presente Regolamento ovvero mediante sistemi informatici di supporto.

2. Qualora nella Federazione agiscano operatori non afferenti ad uno specifico Ufficio il Referente interno è individuato in forza del presente Regolamento nel Data Manager:

3. L'incarico deve individuare l'ambito del trattamento consentito in stretta relazione con le funzioni assegnate all'Ufficio di assegnazione, alla qualifica ricoperta e alle mansioni assegnate all'incaricato.

4. L'incarico deve essere aggiornato in occasione del mutamento delle mansioni o del profilo funzionale dell'incaricato anche a seguito di trasferimento all'interno del medesimo Ufficio.

5. L'atto di incarico è efficace fino a revoca ovvero fino alla cessazione del rapporto di collaborazione con la Federazione e deve essere reiterato dal Referente interno in presenza di ogni rinnovo o di un nuovo affidamento di mansioni all'interno della Federazione.

6. I Referenti devono verificare gli atti di incarico con cadenza annuale per eventuali adeguamenti riguardanti le fonti normative o regolamentari, le mutate esigenze, le modifiche procedurali, i mutamenti dei ruoli, le cessazioni dal servizio.

7. L'Incaricato, nello svolgimento delle operazioni strettamente connesse all'adempimento delle sue funzioni, deve attenersi al presente Regolamento e alle istruzioni impartite dal Referente interno da cui dipende.

8. Gli Incaricati devono comunque assicurare che i dati personali da ciascuno direttamente trattati:

a) siano raccolti e registrati per scopi determinati, espliciti e legittimi, conformemente all'eventuale consenso prestato dall'interessato o alle finalità coerenti con la diversa base giuridica del trattamento individuata dal presente Regolamento;
b) esatti e, se necessario, aggiornati, pertinenti, completi, non eccedenti rispetto al conseguimento delle finalità per le quali il dato viene raccolto e, ove si tratti di dati sensibili, indispensabili rispetto alle finalità per le quali sono raccolti o successivamente trattati;
c) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

Art. 11
Nomina di Funzioni esterne

1. In fase di definizione della documentazione di gara di cui al d.lgs. 50/2016, nella selezione dei fornitori di beni, lavori e servizi che comportino il trattamento di dati personali già in possesso della Federazione, i competenti Uffici della Federazione ovvero il Responsabile Unico del Procedimento – RUP - e di Direttore dell'Esecuzione del Contratto – DEC - se nominato, sentiti il Data Manager e il *Data Protection Officer,* devono determinare la tipologia di rapporto da instaurare con il relativo fornitore ai fini del trattamento dei dati personali.

2. Sono nominati:

a) Responsabili esterni del trattamento i fornitori, ed in particolar modo, i prestatori di servizi che trattano i dati nell'esclusivo interesse di FISE e quindi per le sole finalità determinate unilateralmente dalla Federazione ovvero che siano previste dalla legge ovvero dal CONI, dalla FEI, dal CIO o da altri Organismi nazionali o internazionali cui l'attività della Federazione deve conformarsi.
b) Contitolari del trattamento i fornitori che trattano i dati anche per finalità proprie determinate di concerto con Federazione.

3. Lo schema di contratto incluso nella documentazione di gara, ovvero il capitolato d'oneri, ovvero ancora quello tecnico, qualora gli aspetti relativi al trattamento dei dati siano sottoposti a valutazione in ragione del tipo di procedura prescelta, devono riportare gli obblighi e i doveri cui i Contitolari e i Responsabili dovranno conformarsi in sede di esecuzione del contratto.

4. A tal fine, le Funzioni di Federazione incaricate di predisporre la documentazione di gara utilizzano le clausole tipo allegate al presente Regolamento.

5. Qualora l'esecuzione del contratto comporti il trattamento di dati personali appartenenti alle categorie di cui agli artt. 9 e 10 del GDPR, la documentazione di gara dovrà prevedere l'obbligo dei partecipanti di dimostrare di aver adottato misure tecniche e organizzative idonee a proteggere i dati personali. Nei medesimi casi, la documentazione deve essere sottoposta al parere preventivo del DPO.
6. L'elenco dei Responsabili e dei Contitolari, i loro dati di contatto e l'indicazione della tipologia di dati trattati, sono pubblicati sul sito web della Federazione. In caso di Contitolarità deve essere pubblicato un estratto del contratto che dia evidenza delle attività riservate al Contitolare, del nominativo del DPO, e dei Responsabili esterni del Contitolare, oltre al punto di contatto unico cui si possono rivolgere gli interessati.
7. L'elenco dei Responsabili esterni e dei Contitolari deve essere pubblicato sul sito web istituzionale della Federazione.

Art. 12
Contratti con i Responsabili esterni del trattamento

1. In ogni caso, il contratto con i Responsabili deve indicare e stabilire:

a) la durata e le finalità del trattamento;
b) la natura del trattamento;
c) il tipo di dati personali e le categorie di interessati;
d) gli obblighi e i diritti della Federazione;
e) il divieto per il Responsabile di trattare i dati per finalità diverse da quelle oggetto del relativo contratto;
f) l'impegno del Responsabile:
    a) a trattare i dati personali, anche appartenenti alle speciali categorie di dati di cui agli artt. 9 e 10 del GDPR, nel rispetto del presente Regolamento e seguendo le istruzioni specifiche e particolari della Federazione;
    b) a trattare i dati personali esclusivamente per le finalità previste dal contratto o dalla convenzione;
    c) a compilare e tenere aggiornato il registro dei trattamenti della Federazione ovvero a tenerne uno proprio, purché conforme alle indicazioni del presente Regolamento, rendendolo accessibile alla Federazione;
    d) a nominare i soggetti incaricati del trattamento e garantire che i dati trattati siano portati a conoscenza soltanto del personale incaricato del trattamento, salvo che sia diversamente previsto da un obbligo inderogabile di legge;
    e) a garantire e documentare che le persone incaricate del trattamento dei dati personali si siano impegnate alla riservatezza, ovvero abbiano un obbligo legale o deontologico alla riservatezza;
    f) a garantire e documentare in coerenza con quanto previsto ex art. 32 del GDPR l'adozione di misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio connesso al trattamento quali, a titolo esemplificativo: la

pseudonimizzazione e la cifratura dei dati personali; la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;

g) a garantire i diritti degli interessati, ovvero a provvedere direttamente a soddisfare eventuali richieste degli stessi che siano manifestazione di un diritto loro attribuito dalla normativa vigente;
h) a cancellare o restituire alla Federazione tutti i dati personali alla scadenza del contratto, salvo che vi sia un obbligo stabilito da una diposizione inderogabile di legge che preveda la conservazione dei dati da parte del Responsabile esterno;
i) a consentire le attività di audit, comprese le ispezioni, da parte della Federazione o da un altro soggetto da questa incaricato.

Art. 13
Contratti con i Contitolari del trattamento

1. Nell'accordo con il Contitolare devono essere definite in maniera congiunta le finalità del trattamento e devono essere ripartiti i ruoli e determinate le responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR e dalla normativa vigente, con particolare riguardo all'esercizio dei diritti dell'interessato e agli obblighi di informazione verso ciascun interessato.

2. I contratti devono pertanto:

a) definire le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dalla normativa vigente;
b) dare evidenza dei flussi di dati personali tra le parti;
c) definire le rispettive funzioni relativamente alla comunicazione dell'informativa e al suo contenuto;
d) definire i rispettivi obblighi in merito all'esercizio dei diritti dell'interessato e indicare un punto di contatto unico per l'esercizio di tali diritti.

3. In ragione di quanto sopra, un accordo di contitolarità deve contenere almeno:

a) l'indicazione delle finalità e delle modalità del trattamento;
b) le modalità di esecuzione congiunta di una DPIA ove necessario;
c) i compiti e le responsabilità di entrambi i contitolari del trattamento dei dati personali nell'acquisizione dei dati personali;
d) la definizione dei rispettivi ambititi di copertura degli obblighi informativi;
e) i trattamenti e le relative finalità cui sono soggetti i dati personali con indicazione delle basi giuridiche degli stessi;

f) indicare le finalità ulteriori compatibili con quelle originariamente poste a base del trattamento che ciascun titolare persegue;
g) le categorie di soggetti, responsabili e destinatari, cui i dati possono essere trasmessi;
h) l'obbligo di entrambe le parti di consentire agli interessati l'esercizio dei propri diritti e l'obbligo di darsi reciproca assistenza nel riscontrare i diritti degli interessati;
i) i destinatari ai quali i dati personali possono essere comunicati;
j) il nominativo e i dati di contatto degli eventuali Responsabili e Sub Responsabili nominati da ciascuno dei contitolari o congiuntamente da entrambi.
k) l'obbligo reciproco di entrambi i contitolari di scambiarsi la documentazione atta a dimostrare la legittimità del trattamento e, ove questo sia basato sul consenso, la documentazione dalla quale risulta il consenso.

Art. 14
Rapporti con il CONI

1. Ai sensi dell'art. 26 del GDPR i trattamenti posti in essere per finalità stabilite dal CONI ovvero degli Organismi da questo istituiti, sono eseguiti, senza necessità di stipula di accordi giuridicamente vincolanti o di autorizzazioni specifiche, in base alle delibere del CONI, in quanto parte del diritto interno cui FISE è soggetta in forza di quanto previsto dal d.lgs. 23 luglio 1999 n. 242 e dallo Statuto del CONI.
2. In caso di emanazione di nuove delibere e indirizzi da parte del CONI, il Data Manager, previo parere del DPO e, se del caso, previa esecuzione di una valutazione di impatto e di rischio, emana istruzioni specifiche per il corretto trattamento dei dati personali in esecuzione delle predette delibere.
3. Gli atti adottati dalla Federazione e sottoposti all'approvazione del CONI, se comportano l'interscambio di dati personali con il CONI medesimo per le finalità da quest'ultimo perseguite devono prevedere quanto richiesto dall'art. 26 del GDPR senza necessità di stipula di un accordo di contitolarità.
4. Resta salva la facoltà dei competenti Organi federali, sentito il DPO, di stipulare accordi di contitolarità ovvero di diversamente regolamentare i rapporti con il CONI e con gli Organismi da questo istituiti.

Art. 15
Rapporti con le Organizzazioni internazionali e con gli Organismi sportivi appartenenti a giurisdizioni extraeuropee.

1. Nelle ipotesi di cui all'art. 19, commi 1 e 2, del presente Regolamento, il trasferimento di Dati personali verso Organizzazioni internazionali e altri Organismi sportivi appartenenti a giurisdizioni extraeuropee e in relazione ai quali non sia intervenuta una decisione di adeguatezza di cui all'art. 45 del GDPR, è eseguito in base all'art. 49, paragrafo 1, lett. d), del GDPR in accordo e nei limiti in cui detto trasferimento sia esplicitamente previsto o implicato dagli statuti

o dai regolamenti o altri atti interni, comunque denominati, adottati da dette Organizzazioni e Organismi e che FISE sia tenuta a rispettare.
2. Fuori dalle ipotesi del comma 1, i competenti Organismi federali, sentito il DPO, provvedono alla stipula con le Organizzazioni e con gli Organismi interessati di accordi contenenti le clausole tipo di protezione di cui all'art. 46, paragrafo 1, lett. c) e d) del GDPR secondo il modello allegato al presente Regolamento.
3. Ove non sia possibile procedere ai sensi del comma 2, il trasferimento dei Dati personali è subordinato al consenso esplicito dell'interessato, previo rilascio allo stesso delle informazioni di cui all'art. 49, paragrafo 1, lett. a) del GDPR.
4. Resta in ogni caso salva la facoltà della Federazione di procedere al trasferimento di Dati personali verso paesi extraeuropei al fine di accertare, esercitare o difendere un diritto di FISE in sede giudiziaria anche di fronte agli organi internazionali di giustizia sportiva.

Art. 16
Rapporti con gli Affiliati e gli Aggregati.

1. Gli Affiliati e gli Aggregati operano in qualità di titolari autonomi del trattamento e sono responsabili in via esclusiva dei trattamenti dei dati personali dei Tesserati da loro raccolti.
2. Ai fini del rispetto dell'art. 14 del GDPR, la trasmissione dagli Affiliati e Aggregati a FISE dei dati personali dei Tesserati o dei componenti degli organi sociali previsti nelle procedure di affiliazione e tesseramento e in ogni altra procedura in cui sia previsto la trasmissione di dati a FISE, deve avvenire previa compilazione da parte degli interessati personalmente dei moduli predisposti da FISE e recanti l'informativa sul trattamento dei dati da parte di FISE.
3. Gli Affiliati e gli Aggregati devono provvedere a far sottoscrivere agli interessati personalmente l'informativa per presa visione e, ove previsto, il trattamento al consenso trasmetterne copia a FISE unitamente al relativo modulo.

Titolo III
Condizioni per il legittimo trattamento dei dati personali

Art. 17
Acquisizione dei dati personali

1. Un dato personale è acquisito da FISE quando, nell'esercizio delle sue funzioni, viene ricevuto da un Incaricato del trattamento o da altro dipendente o collaboratore di FISE, ovvero da un Responsabile esterno del trattamento o da un Contitolare, in forma scritta (anche mediante mezzi informatici) o orale (anche mediante sistemi audio/video), ovvero quando viene acquisito in maniera automatica senza intervento umano e viene archiviato su qualunque supporto che ne consenta il successivo trattamento a qualunque fine.
2. I dati personali sono acquisiti direttamente dall'interessato quando è l'interessato medesimo, o chi ne abbia la rappresentanza, a trasmetterli a FISE con qualsiasi mezzo e in qualsiasi forma,

scritta o orale. I dati non sono acquisiti dall'interessato quando sono già in possesso di FISE ovvero quando vengono forniti da un terzo.

Art. 18
Registro informatico dei trattamenti

1. È istituito da FISE il Registro dei Trattamenti svolti in qualità di Titolare.
2. Il Registro è tenuto in formato elettronico mediante sistema che consenta di tenere traccia delle modifiche ad esso apportate.
3. I Referenti collaborano con il Data Manager al fine di assicurare che il Registro sia costantemente aggiornato in relazione ai trattamenti posti in essere sotto la loro responsabilità.
4. Il Registro deve indicare almeno:

a) il nome del Titolare del trattamento;
b) il nome e i dati di contatto del *Data Protection Officer*;
c) ove applicabile, il nome e i dati di contatto del Contitolare, dei Responsabili esterni del trattamento da questi nominati e del DPO del Contitolare;
d) le categorie di incaricati che eseguono il trattamento;
e) la base giuridica del trattamento;
f) le finalità del trattamento;
g) una descrizione delle categorie di interessati;
h) una descrizione delle categorie di dati personali;
i) le categorie di destinatari, a cui i dati personali sono stati o saranno comunicati.
j) i termini ultimi previsti per la cancellazione delle diverse categorie di dati, ovvero la specificazione dei casi in cui la conservazione avviene a tempo indeterminato;
k) gli applicativi informatici utilizzati nel trattamento;
l) ove applicabile, l'indicazione se è stata eseguita una DPIA con possibilità di accesso diretto agli esiti della stessa;

5. I trattamenti sono inseriti nel Registro per categorie corrispondenti alle diverse funzioni di FISE, purché abbiano ad oggetto attività ripetitive.

Art. 19
Basi giuridiche che legittimano il trattamento

1. La Federazione tratta i dati personali, anche sensibili, senza necessità di consenso dell'interessato, ma sulla base di quanto previsto dagli artt. 6, paragrafo 1, lett. e) e 9, paragrafo 1, lett. g) del GDPR qualora e nella misura in cui detti dati siano necessari per le seguenti finalità:

a) affiliazione, aggregazione e tesseramento e revoca, a qualsiasi titolo, e modificazione dei provvedimenti di ammissione, aggregazione e tesseramento;
b) amministrazione della giustizia sportiva;
c) controllo in ordine al regolare svolgimento delle competizioni e dei campionati sportivi;
d) attività connesse all'utilizzazione dei contributi e fondi pubblici;
e) prevenzione e repressione del doping umano e animale;

f) preparazione olimpica e all'alto livello;
g) formazione dei tecnici;
h) utilizzazione e gestione degli impianti sportivi pubblici.

2. Ove afferenti alle finalità di cui al comma 1, hanno la medesima base giuridica i trattamenti effettuati su dati, anche sensibili, per le seguenti finalità intermedie o comunque connesse:

a) accesso a documenti amministrativi e accesso pubblico;
b) rilascio di documenti di riconoscimento o di viaggio;
c) documentazione delle attività istituzionali della Federazione, con particolare riguardo alla redazione di verbali e resoconti dell'attività di assemblee, commissioni e di altri organi collegiali di cui all'art. 17 dello Statuto federale;
d) esercizio del mandato degli organi della Federazione di cui all'art. 17 dello Statuto federale, ivi compresa la loro sospensione o il loro scioglimento, nonché l'accertamento delle cause di ineleggibilità, incompatibilità o di decadenza;
e) accertamento dei requisiti di onorabilità e di professionalità;
f) concessione, liquidazione, modifica e revoca di benefici economici agevolazioni, elargizioni, altri emolumenti e abilitazioni;
g) conferimento di onorificenze e ricompense;
h) rilascio e revoca di autorizzazioni o abilitazioni;
i) concessione di patrocini, patronati e premi di rappresentanza;
j) attività sanzionatorie e di tutela in sede amministrativa o giudiziaria;
k) procedure ad evidenza pubblica e attività amministrative e contabili.

3. Il trattamento dei dati personali degli interessati assunti alle dipendenze della Federazione sono trattati, senza necessità di consenso, in base al relativo contratto di lavoro e nella misura in cui siano necessari all'esecuzione della prestazione lavorativa. I dati sensibili dei lavoratori ed in particolare quelli idonei a rivelare lo stato di salute, sono trattati per assolvere e esercitare i diritti della Federazione in materia di diritto del lavoro e della sicurezza e protezione sociale ovvero per finalità di medicina preventiva e del lavoro e per la misurazione della capacità lavorativa dei lavoratori.

4. Ai sensi degli artt. 85 del GDPR e 136, lett. c) e 137 comma 3, del Codice della privacy, sono trattati senza il consenso dell'interessato, anche mediante pubblicazione di articoli e notizie redatti con o senza l'ausilio di giornalisti o pubblicisti iscritti nel relativo Albo, i dati, anche sensibili, di interesse pubblico o relativi a circostanze o fatti resi noti direttamente dagli interessati tramite loro comportamenti in pubblico quali ad esempio, i risultati di manifestazioni sportive, gli eventi occorsi nelle stesse, i premi assegnati e i fatti concernenti gli sportivi.

5. Fuori dalle ipotesi previste dai commi precedenti i dati personali sono trattati sulla base del consenso degli interessati.

6. Resta ferma la possibilità della Federazione di trattare i dati, anche sensibili, in suo possesso o di acquisirne ulteriori ove ciò sia necessario per:

a) adempiere ad un obbligo di legge cui la Federazione sia sottoposta;
b) difendere in giudizio gli interessi e i diritti della Federazione.

8. In caso di progettazione di nuovi trattamenti, deve sempre essere preventivamente sentito il DPO al fine di verificare la base giuridica sul quale fondarlo e ogni aspetto connesso.

Art. 20
Informazione agli interessati

1. Il rilascio di una informativa agli interessati conforme al presente Regolamento è adempimento inderogabile qualunque sia la base giuridica utilizzata per il trattamento dei dati personali e, quindi, anche in assenza di consenso dell'interessato o di chi ne ha la rappresentanza.
2. Il rilascio dell'informativa all'interessato, o a chi ne ha la rappresentanza, può essere omesso solo nel caso in cui sia già stata resa in precedenza al medesimo interessato, sempre che alcuni elementi della stessa non siano cambiati in parallelo ad una corrispondente modifica del Registro dei trattamenti. In tale ultimo caso gli interessati devono essere informati dei soli cambiamenti intervenuti.
3. Gli Incaricati e, se del caso, quanti operino sotto l'autorità dei Responsabili esterni e dei Contitolari, devono assicurare che, prima dell'acquisizione dei dati personali o contestualmente all'acquisizione degli stessi, sia stata consegnata, o comunque messa a disposizione degli interessati o di chi li rappresenta, l'informativa sul trattamento dei dati personali.
4. L'informativa è redatta sulla base del modello allegato al presente Regolamento.
5. Informative specifiche possono essere predisposte, sentito il DPO, ove sorga la necessità di dare informazioni particolari agli interessati non contenute nel modello allegato. Le informative specifiche, possono essere redatte in forma sintetica ma devono comunque contenere:

a) l'indirizzo web dal quale è possibile reperire l'informativa generale;
b) l'identità del Titolare e i dati di contatto dei Responsabili del trattamento e del DPO;
c) le misure di sicurezza eventualmente utilizzate (es. anonimizzazione, pseudonimizzazione, cifratura ecc.).
d) le conseguenze derivanti dalla mancata prestazione del consenso o del conferimento dei dati;
e) la natura dei dati trattati;
f) l'elenco dei diritti spettanti all'interessato;
g) le categorie dei destinatari cui i dati possono essere trasmessi, le ragioni di tale trasmissione e l'eventuale possibilità di trasferimento dei dati in paesi extra UE;
h) i diritti dell'interessato.

6. Sono comunque fornite informative specifiche sulla base dei modelli allegati al presente Regolamento nelle seguenti ipotesi:

a) trattamenti per i quali e necessario il consenso dell'interessato;
b) procedimenti antidoping;
c) utilizzo dei cookie nel sito web;
d) trattamenti per i quali sussiste un rapporto di contitolarità.

7. L'informativa relativa all'utilizzo dei coolie deve essere contenuta in un banner. Il *banner*, oltre a dover presentare dimensioni sufficienti a ospitare l'informativa, seppur breve, deve essere parte

integrante dell'azione positiva nella quale si sostanzia la manifestazione del consenso dell'utente. Il superamento della presenza del banner al video deve essere possibile solo mediante un intervento attivo dell'utente, appunto attraverso la selezione di un elemento contenuto nella pagina sottostante il banner stesso. È necessario, in ogni caso, che dell'avvenuta prestazione del consenso dell'utente sia tenuta traccia mediante apposito cookie tecnico.

8. Il Data Manager, sentito il DPO, assicura che l'Informativa, ovvero le informative specifiche, abbiano la massima diffusione possibile mediante:

a) la pubblicazione sul sito web della Federazione o sui social network utilizzati dalla Federazione;
b) la riproduzione della stessa su tutta la modulistica utilizzata dalla Federazione;
c) l'affissione nei locali della Federazione ovvero in occasione di convegni, eventi, anche sportivi, workshop ecc. organizzati dalla Federazione;
d) nel materiale promozionale o pubblicitario prodotto dalla Federazione ovvero nelle pubblicazioni della Federazione.

9. L'informativa ovvero le informative specifiche sono aggiornate in occasione dell'avvio di nuovi trattamenti o di trattamenti aventi finalità diverse da quelli già in essere ovvero in occasione delle revisioni del presente Regolamento.

Art. 21

Modalità di rilascio dell'informativa e di eventuale raccolta del consenso

1. Gli Incaricati che, in ragione dell'organizzazione interna della Federazione, hanno il primo contatto con l'interessato, procedono secondo le seguenti modalità:

a) devono verificare l'identità dell'interessato chiedendogli di esibire un documento di riconoscimento in corso di validità e riscontrare la corrispondenza dei dati con quanto dichiarato nel modello;
b) prima di consegnare la modulistica allegata al presente Regolamento devono verificare che la stessa non risulti precompilata in nessuna sua parte;
c) nel caso gli interessati siano minori, gli Incaricati devono verificare che la modulistica sia stata debitamente compilata nella parte in cui chi presta il consenso dichiara di essere esercente la potestà genitoriale;
d) in ogni caso, gli Incaricati devono verificare che sia stata sottoscritta la dichiarazione di presa visione dell'informativa;
e) il consenso, ove richiesto ai sensi dell'art. 19, deve essere rilasciato in forma scritta utilizzando l'apposito modulo predisposto da FISE e deve riguardare in maniera separata e distinta da altre materie il trattamento dei dati personali;
f) l'incaricato del trattamento deve assicurare la conservazione del modulo e dell'informativa per tutta la durata del trattamento e deve assicurarsi che lo stesso sia a disposizione delle funzioni di FISE che eseguono i trattamenti per i quali il consenso è stato prestato.

2. Qualora i dati siano acquisiti presso gli Affiliati e gli Aggregati e da questi trasmessi alla Federazione, le attività di cui al comma 1, lett. da a) a e) sono compiute dagli Incaricati nominati dagli Affiliati e dagli Aggregati. Gli Incaricati della Federazione addetti agli uffici che ricevono la documentazione devono verificare che l'informativa e il consenso siano stati somministrata e raccolto sulla base della modulistica predisposta da FISE e che la stessa sia stata debitamente compilata in ogni parte necessaria. In caso di non conformità, l'Incaricato della Federazione non da corso al trattamento dei dati e ne informa l'Affiliato o l'Aggregato.

Art. 22
Informativa e consenso per via telematica

1. L'accesso ai servizi *on-line* della FISE è consentito solo a utenti registrati.

2. La registrazione deve poter avvenire solo a titolo personale mediante emissione di codici identificativi e chiavi di accesso univoche e deve essere confermata mediante procedura che preveda l'invio di una mail all'indirizzo dichiarato nel *form* di registrazione dell'interessato con indicazione di un link.

3. Qualora, per il tipo di servizio richiesto, sia necessario comunicare in sede di accesso ai servizi telematici i dati relativi ai minori, gli esercenti la potestà genitoriale, al momento della registrazione, devono spuntare la relativa casella. Al fine di assicurare una corretta acquisizione del consenso:

a) nessuna delle caselle deve essere preimpostata;
b) l'interessato deve aver selezionato la casella di presa visione dell'informativa che deve essere distinta da quella per la prestazione dell'eventuale consenso;
c) le caselle del consenso devono avere funzione esclusiva e devono essere distinte per ogni trattamento avente finalità diversa;

3. La mancata prestazione del consenso deve impedire l'accesso al servizio *on-line* esclusivamente se è omesso in relazione ai dati che sono necessari all'esecuzione del servizio medesimo.

Titolo IV
Politiche di protezione e trattamenti per impostazione predefinita

Art. 23
Protezione dei dati per impostazione predefinita

1. I Referenti, nell'organizzazione e nella gestione delle funzioni federali cui sono preposti, adottano le politiche generali per la tutela dei dati previste nel presente Titolo.

2. Qualora, per motivi di migliore organizzazione e gestione dei servizi cui sono preposti, sorga la necessità di discostarsi dalle seguenti politiche, i Referenti devono informarne il Data Manager e consultare il DPO e valutare congiuntamente con questi se, in ragione del rischio elevato per i diritti degli interessati, debba preventivamente procedersi con una valutazione di impatto e di rischio (DPIA).

Art. 24

Politiche generali per il trattamento di dati in forma cartacea

1. L'archiviazione e la catalogazione dei documenti deve essere organizzata in maniera da permettere la pronta reperibilità e l'identificazione dell'interessato, al fine di consentire l'esercizio dei propri diritti da parte di quest'ultimo.

2. Gli atti e i documenti contenenti dati personali, affidati agli Incaricati del trattamento per lo svolgimento dei relativi compiti, devono essere utilizzati assicurandosi che agli stessi non abbia accesso altro personale di FISE non coinvolto nel trattamento, ovvero a visitatori e terze parti.

3. Le singole fasi di lavoro e la condotta da osservare devono evitare che i dati siano soggetti a rischi di perdita o distruzione, che vi possano accedere persone non autorizzate, che vengano svolte operazioni di trattamento non consentite o non conformi ai fini per i quali i dati stessi sono stati raccolti.

4. Pertanto:

a) i documenti devono essere conservati in archivi chiusi, accessibili solo al personale incaricato di un trattamento che ne comporti l'utilizzo;
b) il prelievo e la restituzione di atti e documenti dall'archivio deve essere annotato in apposito registro ove vengano riportati i dati dell'Incaricato, la data del prelievo e quella della riconsegna;
c) i medesimi atti e documenti possono essere presi dall'archivio e detenuti presso le postazioni di lavoro degli incaricati a ciò legittimati, che devono provvedere alla loro custodia. Alla cessazione delle attività di trattamento devono essere restituiti all'archivio;
d) tutte le operazioni di trattamento devono essere effettuate considerando tutti i dati confidenziali e, di norma, soggetti al segreto d'ufficio;
e) i documenti contenenti dati personali non devono essere portati fuori dagli uffici della Federazione, salvo che l'asporto sia necessario per il perseguimento delle finalità connesse al trattamento per il quale sono stati raccolti. In tali casi dovrebbe portarsi all'esterno una copia dell'atto e non l'originale. Ove ciò non sia possibile deve lasciarsi in archivio una copia dell'atto o del documento, ovvero provvedere alla digitalizzazione dello stesso e alla sua archiviazione informatica;
f) in caso di allontanamento, anche temporaneo, dalla propria postazione di lavoro, si devono porre in essere tutte le misure necessarie affinché altri dipendenti non incaricati del medesimo trattamento, visitatori o terzi, non possano accedere ai dati personali;
g) la postazione di lavoro deve essere utilizzata in modo esclusivo da un solo utente e protetta, evitando che terzi possano accedere ai dati che si stanno trattando. Nella turnazione del personale può consentirsi l'avvicendamento di più persone nella stessa postazione, purché tutte incaricate del medesimo trattamento;
h) qualora si ricevano alla propria postazione di lavoro dipendenti di FISE non incaricati del trattamento, ovvero terze persone, e si tengano sulla propria scrivania cartelle e fascicoli, devono essere adottate misure di anonimizzazione mediante copertura, anche temporanea, dei dati identificativi dell'interessato riportati sul frontespizio dei

documenti, dei fascicoli e delle cartelle. Si deve quindi inserire, a seconda delle necessità operative e organizzative, informazioni che non permettano di percepire l'identità dei soggetti interessati dal trattamento. In caso di allontanamento non devono essere lasciati sulla scrivania documenti contenenti dati personali, a meno che non si chiuda a chiave la porta della stanza;

i) gli atti e i documenti dei quali esiste un unico esemplare dovrebbero essere digitalizzati;
j) salvo che si tratti di copie, la distruzione di documenti deve essere preceduta dalla verifica che sia spirato il termine di conservazione come riportato nel Registro del trattamento in relazione alla categoria di riferimento, avuto riguardo alla data di protocollo in entrata. Ove non si conosca la data di acquisizione del documento da parte di FISE, deve aversi riguardo alla data in cui il documento è pervenuto all'Interessato.
k) prima di gettare la documentazione nel cestino della carta si deve provvedere a renderne non comprensibile il contenuto, ovvero procedere alla separazione del dato identificativo dal resto delle informazioni mediante separazione fisica dei fogli e distruzione di quelli contenenti dati identificativi.

Art. 25
Politiche generali per l'utilizzo degli strumenti informatici

Il Responsabile dei sistemi informativi, di concerto con il DPO e, se nominato separatamente, il Data Manager, implementa progressivamente le procedure relative all'utilizzo, alla gestione, al mantenimento e allo smaltimento delle dotazioni informatiche della Federazione secondo le linee direttive allegate al presente Regolamento.

Art. 26
Trattamenti ulteriori e condivisione dei dati all'interno di FISE

1. Gli Incaricati non possono di regola condividere i Dati personali che trattano nell'adempimento delle proprie funzioni con altri dipendenti o collaboratori della Federazione che non siano incaricati del medesimo trattamento o di trattamenti che richiedano l'utilizzazione dei medesimi dati personali.

2. Gli incaricati non possono altresì utilizzare i dati personali per finalità diverse da quelle per i quali furono originariamente acquisiti, salve le ipotesi di cui all'art. 19, comma 7.

3. I commi 1 e 2 non si applicano qualora gli incaricati abbiano ricevuto diverse istruzioni dal proprio Referente o SubReferente e ricorra almeno una delle seguenti circostanze:

a) per il trattamento ulteriore senza applicazione delle misure di protezione è stato ottenuto il consenso da parte dell'interessato. Insieme ai dati deve essere sempre trasmesso internamente o reso accessibile, mediante sistemi informatici, il consenso prestato da tutti gli interessati cui i dati si riferiscono;
b) i dati vengono sottoposti a procedure di anonimizzazione o pseudonomizzazione;
c) il trattamento ulteriore è stato oggetto di DPIA, nel qual caso la trasmissione avviene nel rispetto delle prescrizioni della DPIA.

d) il dato deve essere trasferito per consentirle di svolgere un trattamento che ha una base giuridica diversa dal consenso, come risultante dal Registro dei Trattamenti.

4. I Referenti o i SubReferenti comunicano le istruzioni di cui al comma precedente al Data Manager.

Art. 27

Politiche generali relative alla comunicazione di dati personali a terzi

1. La trasmissione di dati personali a terzi può avvenire:

a) nelle ipotesi previste dal presente Regolamento e, in ogni caso, ove sia necessaria per perseguire le finalità per le quali i dati furono originariamente acquisiti;
b) ove sia necessario per adempiere ad un obbligo di legge o di regolamento ivi incluse le norme vincolati emanate dai soggetti dell'ordinamento sportivo, anche internazionale;
c) nelle ipotesi di cui all'art. 19, commi 1 e 2, qualora la comunicazione dei dati risponda ad un rilevante interesse pubblico stabilito dalla legge;
d) ove vi sia un ordine dell'Autorità giudiziaria o amministrativa competente ivi inclusi gli Organismi di giustizia sportiva, anche internazionali.

2. La trasmissione di dati è sempre fatta in maniera non eccedente le finalità stabilite dalle disposizioni che la consentono e, ove ciò non contrasti con le stesse o con le finalità da esse perseguite, previa applicazione delle misure di protezione di cui all'art. 28.

Art. 28

Conservazione dei dati

1. I dati personali sono conservati per un periodo di 10 anni decorrenti dalla cessazione del rapporto di tesseramento e, per quanto attiene agli altri rapporti, dalla cessazione degli stessi, fatti salvi gli effetti dell'inoltro di eventuali atti interruttivi della prescrizione.

2. Gli atti e i provvedimenti emessi nell'esercizio delle funzioni di cui all'art. 19, commi 1 e 2, ivi compresi i provvedimenti degli Organi di giustizia sportiva e gli atti del relativo processo, sono conservati a tempo indeterminato.

3. Il Data Manager cura la cancellazione e la distruzione degli atti per i quali sia spirato il termine di conservazione.

Art. 29

Diritto di accesso agli atti amministrativi e accesso civico generalizzato

1. Nei trattamenti aventi le finalità di cui all'art. 19, commi, 1 e 2, l'accesso agli atti amministrativi continua ad essere disciplinato dalla Legge 7 agosto 1990, n. 241 nel testo vigente, nonché, in materia di investigazioni difensive, dalla Legge 7 dicembre 2000, n. 397.

2. Qualora l'istante sia soggetto diverso dall'interessato o nei documenti richiesti vi sano dati riferiti a più di un interessato, l'accesso è sempre limitato alla sola visione dei dati personali la cui conoscenza sia necessaria per curare o difendere l'interesse giuridico dell'istante, nel rispetto dei

principi di pertinenza e di non eccedenza dei dati da visionare rispetto alle finalità per le quali è consentito l'accesso stesso.
3. Qualora l'istanza di accesso riguardi documenti contenenti categorie particolari di dati di cui all'art. 9 del GDPR, l'accesso è consentito a condizione che ciò si renda necessario per far valere o difendere in sede giudiziaria una situazione giuridicamente rilevante di rango almeno pari ai diritti del terzo, ovvero consista in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile, sempre che le informazioni richieste siano pertinenti e non eccedenti le finalità per cui è richiesto l'accesso stesso.
4. Nell'ipotesi di cui all'art. 3, prima di procedere all'ostensione degli atti, gli incaricati richiedono il parere del DPO, salvo che questi si sia già espresso in precedenza su questione analoga.

Art. 30
Accesso civico generalizzato

1. L'accesso civico ai dati, ai documenti e alle informazioni di cui dispone la Federazione continua ad essere disciplinato dal d.lgs. 14 marzo 2013 n. 33.
2. I documenti sono di regola trasmessi in forma integrale salvo quanto previsto dai commi 3, 4 e 5.
3. Ove i documenti contengano dati, ancorché non appartenenti a speciali categorie di cui all'art. 9 del GDPR, relativi, ad esempio, a provvedimenti sanzionatori o disciplinari, alle attività ispettive della Federazione o di altri Organismi, alla conduzione di indagini su reati e sul loro perseguimento, ai risultati di test antidoping sugli atleti ovvero in qualunque altro caso nei documenti richiesti vi siano informazioni che si possano ritenere, per qualunque ragione sottoposte a particolari regimi di riservatezza o segretezza, prima di procedere all'ostensione gli Incaricati, d'intesa con il proprio Referente, richiedono un parere del DPO.
4. L'istanza di accesso civico generalizzato relativa a documenti contenenti dati appartenenti alle particolari categorie di dati di cui all'art. 9 del GDPR è rigettata salvo che la stessa sia motivata o si possa comunque desumere dalla medesima l'esistenza di un diritto di rango almeno pari ai diritti dell'interessato alla riservatezza di tali dati, ovvero di un diritto della personalità o in un altro diritto o libertà fondamentale.
5. Ancorché non consentano una valutazione sull'esistenza di un diritto di pari rango, le domande di accesso civico generalizzato di cui al comma precedente sono riscontrate positivamente ove sia possibile applicare ai documenti le misure di protezione di cui all'art. 28 sempre che, in considerazione della quantità di documenti richiesti, l'applicazione di dette misure non rappresenti un onere sproporzionato per la Federazione.

Art. 31
Pubblicazione delle deliberazioni e dei provvedimenti

1. Fatto salvo quanto previsto dall'art. 33, in ottemperanza ai principi di necessità, pertinenza e non eccedenza dei dati, nelle deliberazioni, degli atti e dei provvedimenti degli Organismi della Federazione destinati alla pubblicazione sul sito istituzionale della stessa in ottemperanza ai

doveri di trasparenza connessi ai trattamenti di cui all'art. 19, commi 1 e 2, sono di regola inseriti i soli dati la cui inclusione negli atti medesimi siano strettamente necessari per il raggiungimento delle finalità proprie di ciascun provvedimento e per soddisfare gli obblighi di motivazione previsti dalla legge.

2. Allorché negli atti di cui al comma 1 debbano essere riportati dati sensibili e giudiziari e sia possibile isolarli dal contesto del provvedimento senza comprometterne la necessaria motivazione e l'intellegibilità, gli atti medesimi sono pubblicati mediante l'applicazione di misure di sicurezza di cui all'art. 28.

Art. 32

Trattamenti connessi ai procedimenti di giustizia sportiva.

1. Ai dati personali in possesso della Federazione possono sempre accedere ed estrarre copia senza applicazione di misure di protezione gli Organismi di giustizia sportiva e gli Uffici federali preposti alla gestione amministrativa delle relative attività.

2. I dati acquisiti dagli Organi di giustizia sportiva, ivi inclusi quelli contenuti negli atti difensivi ovvero trasmessi dalla Magistratura ordinaria, sono trattati in via esclusiva dai predetti Organi e dagli Uffici federali di supporto agli stessi, salvo che sia espressamente prevista da disposizioni cogenti di legge o di regolamento la trasmissione ad altri Uffici federali.

3. È comunque sempre consentito ai competenti Uffici federali accedere a detti documenti per attività finalizzata alla verifica dei requisiti di eleggibilità, di tesserabilità e di partecipazione a competizioni e manifestazioni sportive come previsto dalle norme e dai regolamenti sportivi vigenti.

4. Le copie e gli estratti di cui all'art. 32 comma 3 del Regolamento di giustizia della Federazione sono rilasciati di regola alle sole parti oggetto del procedimento, ai loro difensori e ai consulenti tecnici che siano stati a ciò autorizzati dall'Organismo giudicante. Ulteriori richieste di accesso sono trattate nel rispetto delle norme previste dal presente Regolamento e dalla normativa vigente.

Art. 33

Pubblicazione dei provvedimenti della giustizia sportiva

1. Ai sensi dell'art. 59 del Regolamento di giustizia della Federazione, le sentenze e le altre decisioni degli Organi di giustizia sportiva sono pubblicate e rese accessibili attraverso il sito istituzionale della Federazione.

2. Con istanza motivata depositata presso la segreteria dell'Organo avanti al quale si svolge il giudizio, l'interessato, prima che sia definito il relativo grado di giudizio, può chiedere che le sue generalità e ogni altro dato idoneo a identificarlo siano omessi mediante l'applicazione di misure di protezione di cui all'art. 28.

3. Sono legittimati ad inoltrare l'istanza le parti, i testimoni, i consulenti e chiunque sia reso identificabile nel provvedimento attraverso l'indicazione delle generalità o di altri dati identificativi.

4. Le misure di protezione possono essere disposte d'ufficio qualora nel processo vengano trattati dati sensibili.
5. Sulla istanza provvede l'autorità che pronuncia la sentenza o adotta il provvedimento mediante annotazione sullo stesso del divieto di diffusione senza l'omissione e delle generalità e degli altri dati identificativi dell'istante.
6. In caso di annotazione la sentenza è comunque pubblicata in forma integrale sul sito istituzionale della Federazione, ma l'accesso è ristretto è ristretto alle sole parti del giudizio.

Art. 34
Trattamenti connessi all'antidoping umano – Rinvio

1. Nelle attività connesse alla prevenzione e al contrasto dell'antidoping umano, per quanto non diversamente previsto dal presente Regolamento, dalle disposizioni del CONI e dai provvedimenti del Garante, la Federazione si conforma all'International Standard for Protection of Personal Information (ISPPI) adottati dalla World Anti-Doping Agency – WADA.
2. Il Data Manager provvede alla pubblicazione sul sito istituzionale della Federazione dell'ISPPI tempo per tempo vigente.
3. I Referenti, in caso di contrasto tra gli ISPPI e il presente Regolamento ricorrono alla consulenza del DPO prima di procedere con il trattamento.

Art. 35
Politiche generali relative al trattamento dei dati del personale

1. Ai dati personali dei lavoratori è consentito l'accesso solo al personale della Federazione specificamente incaricato del relativo trattamento.
2. Possono essere diffuse internamente ed esternamente alla Federazione, senza il consenso del lavoratore le informazioni relative al personale necessarie al coordinamento delle diverse attività di FISE e necessarie all'esecuzione del contratto di lavoro quali:
ordini di servizio;

a) turni lavorativi o feriali;
b) documenti riguardanti l'organizzazione del lavoro;
c) mansioni cui sono deputati i singoli dipendenti e relativi incarichi;
d) dati di contatto dell'ufficio ivi incluso il cellulare aziendale e la mail aziendale.

3. Informazioni di tipo personale e più in generale i curricula possono essere pubblicati in maniera non eccedente la necessità di far conoscere la competenza specifica di un lavoratore in una determinata materia o disciplina.
4. Fatti salvi gli obblighi di trasparenza stabiliti disposizioni inderogabili di legge in relazione alle attività svolte dai lavoratori nei settori di cui all'art. 19, commi 1 e 2, il consenso del lavoratore è invece necessario per la diffusione:

a) di informazioni relative ad emolumenti percepiti o che fanno riferimento a particolari condizioni personali attinenti al rapporto di lavoro;
b) sanzioni disciplinari irrogate o informazioni relative a controversie giudiziarie;

c) assenze dal lavoro per malattia;
d) iscrizione e/o adesione dei singoli lavoratori ad associazioni sindacali;
e) fotografie, informazioni anagrafiche e familiari.

5. I documenti, anche informatici, contenenti dati personali sensibili dei lavoratori devono essere conservati separatamente da ogni altro dato dei lavoratori medesimi e comunque in modo da non consentirne una indistinta consultazione nel corso delle ordinarie attività.

Titolo V
Disposizioni procedurali

Art. 36
Diritti degli interessati

1. Gli interessati, rispetto ai dati personali che li riguardano, hanno diritto di:
a) ottenere la conferma che sia in corso un trattamento di dati personali che li riguardano e, in tal caso, ottenere l'accesso ai dati personali e informazioni sui trattamenti;
b) ottenere la rettifica dei dati personali inesatti che lo riguardano ovvero, se pertinente rispetto al trattamento, l'integrazione dei dati personali incompleti;
c) ottenere la limitazione dei trattamenti;
d) ricevere copia elettronica dei dati personali che li riguardano e personalmente forniti;
e) opporsi in qualsiasi momento, per motivi connessi alla propria situazione particolare, al trattamento automatizzato di dati.

2 Al fine di agevolare l'invio delle richieste degli interessati è istituita una mail dedicata: privacy@fise.it, amministrata dal Data Manager. Resta salva la facoltà degli interessati di rivolgersi direttamente al DPO all'indirizzo dpo@fise.it.

I Referenti e gli Incaricati del trattamento che ricevano una richiesta di esercizio dei propri diritti da parte di un interessato ne danno immediata comunicazione al Data Manager.

Il Data Manager provvede sulle istanze degli Interessati sentito il Referente o i Referenti sotto la cui direzione i dati oggetto dell'istanza sono trattati e comunica a ciascuno dei destinatari, ivi inclusi i Contitolari e i Responsabili esterni, cui sono stati trasmessi i dati personali, le eventuali rettifiche, cancellazioni o limitazioni del trattamento effettuate su richiesta dell'interessato e i provvedimenti comunque assunti su istanza dell'interessato.

Il Data Manager, sentito il DPO, può respingere la richiesta dell'interessato qualora:
a) il trattamento sia necessario per adempiere ad un obbligo di Legge, di Regolamento o ad un ordine della Pubblica Autorità;
b) l'esercizio dei diritti dell'interessato sia in contrasto con gli impegni contrattuali assunti da FISE con terze parti;
c) l'esercizio dei diritti dell'interessato possa arrecare un pregiudizio anche economico a FISE;

Il Data Manager comunica all'interessato entro 30 giorni le misure adottate in riscontro alla sua richiesta e, nel caso di rifiuto, i motivi dello stesso.

Art. 37

Nuovi trattamenti e valutazione di impatto e di rischio (DPIA)

1. Prima di inserire nel Registro un nuovo trattamento, ovvero prima di registrare una modifica ad un trattamento esistente, il Referente interno ne dà comunicazione al DPO e al Data Manager, perché verifichino se il nuovo trattamento o la modifica a quello esistente comporti un rischio elevato per i diritti e le libertà degli interessati e sia, dunque, opportuno procedere con una valutazione di impatto e di rischio (DPIA).

2. Ove eseguita la DPIA contiene almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento e della relativa base giuridica;
b) una valutazione (assessment) della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione (assessment) dei rischi per i diritti e le libertà degli interessati;
d) l'identificazione delle soluzioni e misure per gestire e mitigare i rischi individuati, includendo misure di sicurezza e organizzative a garanzia della protezione dei dati personali e della conformità alla normativa vigente.

3. La valutazione deve riguardare i seguenti elementi:

a) descrizione del trattamento, che specifichi natura, oggetto, contesto e finalità del trattamento;
b) categorie di dati personali trattati;
c) natura dei dati personali trattati;
d) necessità e proporzionalità dei trattamenti in relazione alle finalità (con conseguente esame ad es.: della liceità del trattamento, della minimizzazione del trattamento e del rispetto delle finalità oggetto di informative);
e) rischio per la sicurezza dei dati;
f) rischi per i diritti e le libertà degli interessati;
g) misure organizzative in essere per mitigare i rischi;
h) misure tecniche in essere per mitigare i rischi;
i) rispetto del presente Regolamento.

4. Salvo diversa indicazione del Data Protection Officer, determinata da situazioni di particolare complessità, la DPIA è eseguita secondo la Procedura standard di esecuzione in allegato al presente Regolamento.

5. Nei trattamenti che siano preceduti da progettazione, la sicurezza delle informazioni deve essere integrata nella progettazione. In particolare, laddove applicabile, in ogni progetto si deve richiedere che:

a) gli obiettivi di sicurezza delle informazioni siano compresi negli obiettivi di progetto;
b) la sicurezza delle informazioni sia parte integrante di tutte le fasi del progetto;
c) una valutazione del rischio per la sicurezza delle informazioni dovrebbe essere condotta in una fase iniziale del progetto, per identificare i necessari controlli.

6. Gli esiti della valutazione devono essere formalizzati in un Report finale, finalizzato a riassumere il processo DPIA e le scelte compiute per mitigare il rischio e a consentire la tracciabilità e documentabilità del processo stesso. Al Report devono essere allegate le osservazioni del DPO.

7. Se a seguito del DPIA, il Referente interno ritenga che non sussista alcun rischio, ovvero che possano essere adottate misure adeguate a mitigarlo, ne informa il Titolare che autorizza il trattamento ovvero, quando non ritenga che i rischi siano stati sufficientemente mitigati, anche sulla scorta del parere del DPO, può procedere ad una consultazione preventiva con l'Autorità Garante.

Art. 36

Violazione dei dati (*data breach*)

1. Il Responsabile dei sistemi informativi, gli Incaricati e i Responsabili esterni del trattamento devono comunicare al Data Manager ogni evento che comporti in modo accidentale o illecito la distruzione, la perdita, la modifica, la divulgazione o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati da e per conto di FISE.

2. Il Data Manager esprime il suo parere sulla gravità della violazione, ovvero:

a) se questa sia inoffensiva per le misure di sicurezza presenti;

b) se può comportare rischi per gli interessati al trattamento ed il grado dei rischi;

c) le misure di sicurezza eventualmente da adottare per porre rimedio alla violazione

e le trasmette al DPO per le valutazioni di competenza.

3. In caso di violazione dei dati personali FISE, in qualità di Titolare del trattamento, è tenuta a informare l'Autorità di Garante per la protezione dei dati senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuta a conoscenza.

4. Il Titolare è "a conoscenza" di una violazione quando abbia ragionevole grado di certezza in merito alla verificazione di un incidente di sicurezza. Nei casi dubbi il Data manager effettua senza indugio un *audit* mediante:

a) somministrazione di questionari agli Incaricati in cui sia richiesta la descrizione dettagliata degli eventi sospetti, delle loro manifestazioni, della tempistica, della frequenza degli stessi e delle persone eventualmente coinvolte;
b) verifica tecnica sugli applicativi informatici di FISE;
c) verifica dell'integrità degli archivi cartacei;
d) verifica di integrità degli spazi fisici in cui gli archivi cartacei e informatici sono conservati;
e) ogni altra verifica che sia ritenuta possibile e opportuna al fine di accertare l'eventuale violazione.

5. La notifica all'Autorità può essere omessa nel caso sia improbabile che la violazione dei dati personali rappresenti un rischio per i diritti e le libertà delle persone fisiche. Al fine di compiere questa valutazione il Titolare, sentito il DPO, tiene in considerazione i seguenti elementi:

a) tipo di violazione;
b) la natura, la sensibilità, e il volume dei dati coinvolti nella violazione;
c) la effettiva possibilità che dai dati sottratti sia possibile risalire a persone determinate o determinabili;
d) le conseguenze che possono derivare agli interessati dalla violazione dei dati (i.e l'incidenza sui loro diritti e libertà);
e) eventuali condizioni particolari degli interessati;
f) il numero di interessati coinvolti.

6. La notifica al Garante deve indicare:

a) la natura della violazione dei dati personali e le possibili cause;
b) le categorie e il numero approssimativo di interessati e/o delle registrazioni dei dati personali in questione;
c) le probabili conseguenze della violazione dei dati personali;
d) le misure adottate, o di cui si propone l'adozione, per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi.

7. Qualora FISE non sia in possesso di tutte le informazioni relative alla violazione precedentemente elencate, comunica al Garante, entro il termine di cui sopra, la sola violazione subita e poi fornisce in un successivo momento tutte le informazioni, motivando le ragioni del ritardo.

8. Qualora dalle analisi compiute emerga un elevato rischio per i diritti e le libertà degli interessati, ovvero qualora lo richieda il Garante, la violazione dei dati deve essere notificata anche agli interessati coinvolti.

9. La notifica della violazione all'interessato deve almeno contenere:

- la comunicazione dei dati di contatto del Titolare del trattamento;
- la descrizione delle probabili conseguenze delle violazioni dei dati personali;
- la descrizione delle misure adottate per porre rimedio alla violazione dei dati e per attenuare i possibili effetti negativi.

10. La comunicazione è effettuata, a cura del Titolare del trattamento, con il mezzo che dia maggiore garanzia di ricezione da parte dell'interessato, quali e-mail, sms o contatto diretto. Deve essere evitato l'invio di informazioni solo nel contesto di *update* generali o *newsletter*.

11. Nel caso la segnalazione diretta richieda sforzi sproporzionati, in ragione del numero di destinatari coinvolti, questa può essere effettuata attraverso una comunicazione pubblica.

MODELLO

ACCORDO DI CONTITOLARITÀ NEL TRATTAMENTO DEI DATI PERSONALI

(può essere inserita come articolo in un accordo più ampio - Art [●] - utilizzato per predisporre la documentazione di gara o essere trasformato in un accordo separato)

(Art. [●])

1. In esecuzione del presente contratto,

F.I.S.E., con sede legale in _____

e la Società [●], con sede legale in _____

d'ora in poi anche congiuntamente denominate le 'Parti', convengono e si stipulano quanto segue:

2. L'oggetto del presente accordo è l'instaurazione di un rapporto di contitolarità tra le Parti per il trattamento dei dati acquisiti, gestiti e trattati per le finalità [indicate dalle Parti negli articoli precedenti – oppure: segue elenco, es. per F.I.S.E.: tutto quanto concerne l'organizzazione e la gestione delle competizioni e manifestazioni sportive e/o degli eventi sportivi regionali, nazionali, internazionali / dare esecuzione al rapporto instaurato con il tesseramento, ivi incluse le attività correlate o accessorie o la fornitura di servizi, ecc. …)], mediante consenso richiesto e reso dagli interessati, ove dovuto.

3. Le Parti tratteranno i dati personali esclusivamente per le finalità indicate, ponendo in essere i trattamenti strettamente necessari all'esecuzione del contratto medesimo.

4. Le Parti concordano che i dati saranno utilizzati per le seguenti finalità <u>ulteriori</u> da ritenersi compatibili ai sensi dell'art. 6, par. 4, del Regolamento (UE) 2016/679:

a. per F.I.S.E.
   [es. adempimento a specifici obblighi di legge …ecc.]
b. per La Società
   [es. adempimento a specifici obblighi di legge …ecc.]

5. Le Parti concordano che nell'ambito di tali finalità i dati potranno essere trasmessi:

a. da F.I.S.E.
   [possono indicarsi, a seconda dei casi - categorie di soggetti – es. P.A. – o soggetti indicati nominativamente – Società x.y.]

b. dalla Società

[possono indicarsi, a seconda dei casi - categorie di soggetti – es. P.A. – o soggetti indicati nominativamente – Società x.y.]

In tutti i casi nei quali la trasmissione dei dati ai soggetti sopra indicati non avvenga per obbligo di legge o per ordine dell'autorità giudiziaria, le Parti si danno reciprocamente atto di aver, ciascuna per quanto di competenza, tenuto ogni condotta prescritta dal Regolamento (UE) 2016/679 e da altre disposizioni di legge comunque applicabili al trattamento dei dati personali, in caso di trasmissione di dati a terzi soggetti, assumendo in proprio ogni onere, obbligo e responsabilità comunque derivante dalla trasmissione di dati eseguita da ciascuna delle Parti.

6. Le Parti si danno reciprocamente atto che, ai sensi degli artt. 6 e 9 del Regolamento (UE) 2016/679, i trattamenti di cui al punto 1. hanno la seguente base giuridica [es. consenso, obbligo di legge, interesse pubblico – la base giuridica può essere anche diversa per ogni tipologia di trattamento prevista dal contratto.]

7. Le Parti si danno reciprocamente atto, e garantiscono reciprocamente, di aver posto in essere misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al predetto Regolamento (UE) 2016/679 e che è garantito un livello di sicurezza, anche informatica, adeguato al rischio, 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.

Del pari, le Parti garantiscono reciprocamente che il personale di ciascuna, che avrà accesso ai dati personali, è stato formalmente incaricato ed è debitamente formato in ordine al trattamento dei dati in generale e in Particolare in ordine ai doveri nascenti dal presente accordo.

Ciascuna delle Parti dichiara di aver ricevuto prima d'ora le *policy* interne dell'altra, in relazione alla protezione dei dati personali, e di averle trovate conformi alle disposizioni del Regolamento (UE) 2016/679.

8. Ferme restando le suddette garanzie di carattere generale, F.I.S.E. e la Società [●] determinano congiuntamente le rispettive responsabilità e i rispettivi compiti in merito all'osservanza degli obblighi derivanti dal Regolamento, con Particolare riferimento ai diritti degli interessati e agli obblighi di fornire le informazioni previste al momento della raccolta.

In Particolare,

F.I.S.E., nell'ambito della sua specifica sfera di titolarità, si impegna a:

i. es. raccogliere il consenso degli interessati;

i. es. archiviare i dati;

ii. es. provvedere alla cancellazione alla fine del trattamento

iii. es. tenere il registro dei trattamenti

la Società [●], nell'ambito della sua specifica sfera di titolarità, si impegna a:

- [●];
- [●];

9. L'accesso ai dati oggetto del presente contratto avverrà attraverso [indicare il metodo; se si tratta di condivisione attraverso sistemi informatici, specificare chi gestisce il sistema].

10. Le Parti, ciascuna in relazione al trattamento o alla parte di trattamento dalla stessa posta in essere, provvederà a riscontrare, nel rispetto e nei limiti delle disposizioni di cui al Regolamento 2016/679, le richieste degli interessati.

Resta comunque inteso che ciascuna delle Parti, per quanto nella sua materiale possibilità, provvederà a riscontrare eventuali richieste degli interessati che le dovessero pervenire. È obbligo dell'altra parte prestare assistenza reciproca nel riscontro delle richieste degli interessati, provvedendo a dare esecuzione alle stesse su richiesta dell'altra parte nel minor tempo possibile e, comunque, nel rispetto dei termini previsti dal Regolamento 2016/679.

11. È compito di [una o l'altra Parte a seconda della ripartizione dei ruoli], prima dell'acquisizione dei dati dagli interessati, e in ogni caso prima di iniziare il trattamento, fornire a [una o l'altra Parte] l'informativa redatta secondo il modello allegato al presente contratto [può utilizzarsi il modello in uso presso F.I.S.E. o presso il Contitolare].

In ogni caso, entrambe le Parti pubblicano sul proprio sito istituzionale l'informativa relativa ai trattamenti oggetto del presente contratto.

12. Le Parti dichiarano che, nell'esecuzione del presente contratto, si avvarranno dei seguenti Responsabili del Trattamento:

Per F.I.S.E.

…….

…….

…….

Per la Società

…….

…….

…….

13. Le Parti, di comune accordo, individuano come punto unico di contatto su cui far confluire eventuali istanze degli interessati il seguente indirizzo e-mail……..

14. La Società si impegna a manlevare e tenere indenne F.I.S.E. per qualsiasi costo, spesa, onere in cui questa dovesse incorrere in ragione della violazione da parte della Società di uno degli obblighi previsti dal presente contratto, ovvero dall'esecuzione delle attività poste sotto la responsabilità della Società. Identico obbligo di manleva e indennizzo grava su F.I.S.E. in relazione agli adempimenti posti sotto la sua responsabilità.

15. Le Parti si danno reciproca e tempestiva informazione, in ogni caso senza ingiustificato ritardo dal momento dell'avvenuta conoscenza, di ogni violazione di dati personali (cd. *data breach*); tale notifica è accompagnata da ogni documentazione utile, ai sensi degli artt. 33 e 34 del Regolamento UE, per permettere all'altra parte, ove ritenuto necessario, di notificare la violazione all'Autorità Garante per la protezione dei dati personali, entro il termine di 72 ore da quando il Titolare ne è venuto a conoscenza.

16. Le Parti si danno reciproca assistenza nel caso di richieste formulate dall'Autorità Garante in merito al trattamento dei dati personali effettuate in ragione del presente contratto.

17. Le Parti devono darsi reciproca e tempestiva informazione in caso di ispezioni o richiesta di informazioni e di documentazione da parte dell'Autorità Garante per la protezione dei dati personali.

ATTO DI NOMINA
DATA MANAGER

Conformemente a quanto previsto dal Regolamento Ue, 27 aprile 2016, n. 2016/679 in tema di protezione dei dati personali,

Il Titolare del trattamento dei dati personali
Federazione Italiana Sport Equestri

CONSIDERATO

che ogni dipendente di F.I.S.E., gli Incaricati del trattamento, il personale non strutturato, a tempo indeterminato, definito o parziale, gli operatori in formazione o in aggiornamento, operatori di supporto preposti ad un determinato servizio o mansione anche non ricorrente che implichi il trattamento di dati personali, deve ricevere un incarico dal Titolare del Trattamento cui risponde

NOMINA

in qualità di *Data Manager* del trattamento dei dati personali, il Dr. _____

L'ambito del trattamento consentito al Dr. _____, in qualità di *Data Manager*, così come specificato nel presente atto di nomina, nel rispetto delle funzioni assegnate, della qualifica ricoperta e delle mansioni svolte, viene così individuato:

a) adozione di idonee misure per assicurare, nell'organizzazione delle prestazioni e dei servizi che comportano il trattamento di dati personali ed in relazione al predetto trattamento, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale;
b) compilazione e il costante aggiornamento del Registro dei trattamenti;
c) rispetto dei principi di correttezza, esattezza e completezza di dati personali oggetto di trattamento assunti sotto la sua responsabilità;
d) eventuale esecuzione, in fase di progettazione di nuovi trattamenti, di una valutazione di impatto e di rischio, conforme alle direttive stabilite nel presente Regolamento;

e) nomina con atto formale da adottarsi su specifico modello (atto di nomina) dei Responsabili del trattamento, degli Incaricati del trattamento dei dati e di ogni altra figura necessaria al trattamento dei dati personali e all'accesso agli stessi;
f) divieto di trasmissione e accesso ai dati personali a soggetti non incaricati del loro trattamento in conformità al presente Regolamento;
g) controllo sulla trasmissione e sull'accesso ai dati personali trattati solo previa adozione di misure tecniche e salvo che gli stessi siano consentiti senza adozione di misure di protezione dal presente Documento, da istruzioni specifiche di Titolare o da norme imperative di legge;
h) controllo circa l'adeguata formazione agli incaricati del trattamento in relazione alle funzioni che andranno a svolgere.
i) […]

Nell'ambito del predetto trattamento consentito, il Dr. _____, in qualità di *Data Manager* si impegna ad assicurare che i dati personali:

a) verranno raccolti e registrati per scopi determinati, espliciti e legittimi, conformemente al consenso prestato dall'interessato o alle finalità coerenti con la diversa base giuridica del trattamento individuata dal Regolamento di F.I.S.E., nonché negli Accordi di Contitolarità posti in essere, o a seguito di valutazione di impatto e di rischio (DPIA);
b) saranno esatti e, se necessario, aggiornati, pertinenti, completi, non eccedenti rispetto al conseguimento delle finalità per le quali il dato viene raccolto e, ove si tratti di categorie particolari di dati, indispensabili rispetto alle finalità per le quali sono raccolti o successivamente trattati;
c) saranno conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati, in osservanza del principio di minimizzazione.

Il Dr. _____, in qualità di *Data Manager* del trattamento dei dati, nello svolgimento delle operazioni strettamente connesse all'adempimento delle sue funzioni, deve attenersi al Regolamento adottato da F.I.S.E., nonché alle istruzioni impartite da questa impartite quale Titolare del Trattamento da cui dipende, nonché alle istruzioni previste negli Accordi di contitolarità.

Il *Data Manager* del Trattamento, nominato con il presente atto, dichiara di essere a

conoscenza di quanto previsto dal Regolamento Europeo n. 679/2016 in tema di protezione dei dati personali.

Il presente incarico deve essere aggiornato in occasione del mutamento delle mansioni o del profilo funzionale dell'incaricato.

Luogo e data_____

IL TITOLARE DEL
TRATTAMENTO

Federazione Italiana Sport Equestri

In persona del legale rappresentante *pro-tempore*

_____

Per accettazione
dell'incarico

IL DATA MANAGER DEL
TRATTAMENTO

_____

ATTO DI NOMINA AMMINISTRATORE DI SISTEMA

Il Titolare del trattamento dei dati

Federazione Italiana Sport Equestri

NOMINA

in qualità di Amministratore di sistema il Dr./la Dr.ssa ……

In relazione alle mansioni da Lei svolte alle nostre dipendenze, considerato che per preparazione ed esperienza Lei fornisce idonea garanzia del pieno rispetto delle vigenti diposizioni europee e nazionali in materia di trattamento di dati personali, con particolare riferimento al profilo relativo alla sicurezza nella custodia e nel trattamento dei dati personali, con la presente, Le conferiamo la nomina ad "Amministratore di sistema" per gestire il sistema informativo della Federazione consentendo la corretta utilizzazione avvalendosi di strumenti, attrezzature, componenti hardware e software a Lei messi a disposizione dal Titolare del trattamento.

In tale contesto sarà Suo compito:

- gestire il sistema informatico, nel quale risiedono le banche dati personali, in osservanza alla normativa vigente D.lgs. n. 196/2003 cosi modificato dal D.lgs. n. 101/2018 e Reg. UE 679/2016 (GDPR), attenendosi anche alle disposizioni del *Data Manager*:
- gestire il sistema di autenticazione informatica secondo le misure di sicurezza più idonee;
- adottare adeguati programmi antivirus, firewall ed altri strumenti software o hardware atti a garantire la massima misura di sicurezza, utilizzando le conoscenze acquisite in base al progresso tecnico software e hardware, verificandone l'installazione, l'aggiornamento ed il funzionamento degli stessi in conformità alla normativa vigente;
- adottare tutti i provvedimenti necessari ad evitare la perdita o la distruzione, anche solo accidentale, dei dati personali e provvedere al ricovero periodico degli stessi con copie di back-up, vigilando sulle procedure attivate in struttura. L'Amministratore di sistema dovrà anche assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro;
- indicare al personale competente o provvedere direttamente alla distruzione e smaltimento dei supporti informatici di memorizzazione logica o alla cancellazione dei dati per il loro reimpiego, alla luce del Provvedimento del Garante per la Protezione dei Dati personali del 13 ottobre 2008 in materia di smaltimento strumenti elettronici;
- vigilare sugli eventuali interventi informatici diretti al sistema informatico della Federazione effettuati da vari operatori esterni. In caso di anomalie sarà sua cura segnalarLe

direttamente alla Direzione;

- collaborare con il Titolare per l'attuazione delle prescrizioni impartite dal Garante;
- comunicare prontamente al Titolare qualsiasi situazione di cui sia venuta a conoscenza che possa compromettere il corretto trattamento informatico dei dati personali;
- adottare e gestire sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte di tutte le persone qualificate amministratori di sistema. Le registrazioni (*access log*) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i conferimenti allo *"username"* utilizzato, i riferimenti temporali e la descrizione dell'evento (*log-in e log-out*) che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

Per l'espletamento dell'incarico, vengono assegnate all'Amministratore di sistema le credenziali di autenticazione che gli permettono l'accessibilità al sistema per lo svolgimento delle stesse funzioni assegnate.

Con il presente atto, vengono inoltre assegnati all' Amministratore di sistema i necessari poteri e supporti tecnici ed organizzativi per l'adeguamento di tutte le misure di sicurezza, come previsto dalle vigenti disposizioni in materia di sicurezza del trattamento dei dati.

Il Titolare provvederà, con cadenza almeno annuale, a svolgere le dovute verifiche sulle attività compiute dall'Amministratore di sistema. È obbligo di quest'ultimo prestare al Titolare la sua piena collaborazione per il compimento delle verifiche stesse; in ogni caso, è tenuto a predisporre, con cadenza trimestrale (*o altra cadenza*), una relazione scritta delle attività svolte in esecuzione delle incombenze affidatigli in forza del presente atto.

Della nomina ad Amministratore di sistema, così disposta con il presente atto, verrà data opportuna informazione nell'ambito dell'organizzazione della Federazione, nonché al personale interessato, con le modalità più opportune; specificatamente …..... *(ad esempio attraverso specifico ordine di servizio)*.

Con la sottoscrizione della presente, l'Amministratore di sistema accetta la nomina, conferma altresì la diretta ed approfondita conoscenza della normativa più volte citata nonché degli obblighi in essa prevista.

Data

.....

IL TITOLARE _____

Per accettazione e presa visione

L'amministratore di sistema

_____

Allegato 1: Amministratore di Sistema – ambiti di operatività

Il suo profilo di autorizzazione comprende le seguenti profili e piattaforme:

PROFILO	***TECNOLOGIA***	***AUTORIZZATO***

ATTO DI NOMINA AD INCARICATO DEL TRATTAMENTO

Conformemente a quanto previsto dal Regolamento Ue, 27 aprile 2016, n. 2016/679 in tema di protezione dei dati personali, e dal Regolamento adottato da F.I.S.E. in tema di protezione dei dati personali, il sottoscritto

_____

In qualità di Responsabile del trattamento dei dati personali

CONSIDERATO

che ogni dipendente di F.I.S.E. preposto ad un determinato servizio che implichi il trattamento di dati, ovvero assegnato ad una mansione anche non ricorrente che implichi il trattamento di dati personali, deve ricevere un incarico dal Responsabile del Trattamento cui risponde

NOMINA

in qualità di Incaricato del trattamento dei dati personali il/la Dr./Dr.ssa o /Sig./Sig.ra
NOME DIPENDENTE.

L'ambito del trattamento consentito al/alla Dr./Dr.ssa o Sig./Sig.ra
NOME DIPENDENTE
in qualità di Incaricato/, così come specificato nel presente atto di nomina, nel rispetto delle funzioni assegnate, della qualifica ricoperta e delle mansioni svolte, viene come di seguito individuato:
INDICARE AREA FUNZIONE (eventualmente anche più di una).

-
-
-

Nell'ambito del predetto trattamento consentito, il/la Dr./Dr.ssa o /Sig./Sig.ra
NOME DIPENDENTE
in qualità di Incaricato/a del trattamento dei dati, si impegna ad assicurare che i dati personali:

a) verranno raccolti e registrati per scopi determinati, espliciti e legittimi, conformemente al consenso prestato dall'interessato o alle finalità coerenti con la diversa base giuridica del trattamento individuata dalla Federazione;

b) saranno esatti e, se necessario, aggiornati, pertinenti, completi, non eccedenti rispetto al conseguimento delle finalità per le quali il dato viene raccolto e, ove si tratti di categorie particolari di dati, indispensabili rispetto alle finalità per le quali sono raccolti o successivamente trattati;
c) saranno conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati, in osservanza del principio di minimizzazione.

Il/la Dr. /Dr.ssa Sig./Sig.ra
NOME DIPENDENTE
in qualità di Incaricato/a del trattamento dei dati, nello svolgimento delle operazioni strettamente connesse all'adempimento delle sue funzioni, deve attenersi alle istruzioni impartite dal Responsabile del trattamento / Titolare del trattamento da cui dipende.

L'Incaricato/a del trattamento nominato con il presente atto dichiara di essere a conoscenza di quanto previsto dal Regolamento Europeo 679/2016 in tema di protezione dei dati personali.

Il presente incarico è efficace fino alla sua revoca ovvero fino alla cessazione del rapporto di collaborazione con F.I.S.E.

Il presente incarico deve essere aggiornato in occasione del mutamento delle mansioni o del profilo funzionale dell'Incaricato/a.

Luogo e data _____

IL RESPONSABILE DEL TRATTAMENTO

_____

NOMINA RESPONSABILE ESTERNO DEL TRATTAMENTO

(può essere utilizzato come clausola di un contratto più ampio, come parte della documentazione di gara o essere trasformato in un contratto autonomo)

1. In ragione dell'oggetto del presente contratto è nominata "Responsabile del trattamento"

la Società [●], con sede legale in _____

A tal fine, essa si impegna ad improntare il trattamento dei dati ai principi di correttezza, liceità e trasparenza.

2. La Società potrà eseguire i soli trattamenti funzionali, necessari e pertinenti all'esecuzione delle prestazioni contrattuali e, in ogni modo, non incompatibili con le finalità per cui i dati sono stati raccolti.

3. Le finalità del trattamento sono quelle stabilite dal contratto che di seguito si riassumono:

……

4. Il tipo di dati personali trattati in ragione delle attività oggetto del contratto sono:

……

5. Le categorie di interessati sono:

es. dipendenti e collaboratori,

es. utenti dei servizi

…

6. Nell'esercizio delle proprie funzioni, la Società si impegna a:

a) rispettare la normativa vigente in materia di trattamento dei dati personali, ivi comprese le norme che saranno emanate nel corso della durata del contratto;

b) trattare i dati personali per le sole finalità specificate e nei limiti dell'esecuzione delle prestazioni contrattuali;

c) trattare i dati conformemente alle istruzioni impartite dal Titolare, di seguito indicate, che la Società si impegna a far osservare anche alle persone da questi autorizzate ad effettuare il trattamento dei dati personali oggetto del presente contratto (d'ora in poi "persone autorizzate");

d) informare immediatamente il Titolare del trattamento nel caso in cui ritenga che un'istruzione costituisca una violazione del Regolamento UE sulla protezione dei dati o delle altre disposizioni di legge relative alla protezione dei dati personali;

e) garantire la riservatezza dei dati personali trattati nell'ambito del presente contratto e verificare che le persone autorizzate a trattare i dati personali in virtù del presente contratto:

   - si impegnino a rispettare la riservatezza o siano sottoposti ad un obbligo legale appropriato di segretezza;
   - ricevano la formazione necessaria in materia di protezione dei dati personali;
   - trattino i dati personali osservando le istruzioni impartite dal Titolare per il trattamento dei dati personali al Responsabile del trattamento;

f) adottare politiche interne e attuare misure che soddisfino i principi della protezione dei dati personali fin dalla progettazione di tali misure *(privacy by design),* nonché adottare misure tecniche e organizzative adeguate a garantire che i dati personali siano trattati, in ossequio al principio di necessità ovvero che siano trattati esclusivamente per le finalità previste e per il periodo strettamente necessario al raggiungimento delle stesse *(privacy by default);*

g) adottare tutte le misure tecniche e organizzative che soddisfino i requisiti del Regolamento UE, anche al fine di assicurare un adeguato livello di sicurezza dei trattamenti, in modo tale da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, modifica,

divulgazione non autorizzata, nonché di accesso non autorizzato, anche accidentale o illegale, o di trattamento non consentito o non conforme alle finalità della raccolta;

h) su eventuale richiesta del Titolare, assistere quest'ultimo nello svolgimento della valutazione d'impatto sulla protezione dei dati, conformemente all'articolo 35 del Regolamento UE e nella eventuale consultazione del Garante per la protezione dei dati personale, prevista dall'articolo 36 del medesimo Regolamento UE;

i) ai sensi dell'art. 30 del Regolamento UE, e nei limiti di quanto esso prescrive, tenere un Registro delle attività di trattamento effettuate sotto la propria responsabilità e cooperare con il Titolare e con l'Autorità Garante per la protezione dei dati personali, mettendo il predetto Registro a disposizione del Titolare e dell'Autorità, laddove ne venga fatta richiesta ai sensi dell'art. 30 comma 4 del Regolamento UE;

j) a fornire un piano di misure di sicurezza rimesse all'approvazione della F.I.S.E., che saranno concordate al fine di mettere in atto misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio e a garantire il rispetto degli obblighi di cui all'art. 32 del Regolamento UE. Tali misure comprendono, tra le altre:

   - la pseudonimizzazione e la cifratura dei dati personali;
   - la capacità di assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi che trattano i dati personali;
   - la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
   - una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

7. La Società deve mettere a disposizione di F.I.S.E. tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al Regolamento UE, oltre a contribuire e consentire al Titolare - anche

tramite soggetti terzi dal medesimo autorizzati, dandogli piena collaborazione - verifiche periodiche circa l'adeguatezza e l'efficacia delle misure di sicurezza adottate e il pieno e scrupoloso rispetto delle norme in materia di trattamento dei dati personali.

8. Nel caso in cui all'esito di tali verifiche periodiche, ispezioni e audit le misure di sicurezza dovessero risultare inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l'applicazione del Regolamento, la F.I.S.E. diffiderà la Società ad adottare tutte le misure più opportune entro un termine congruo che sarà all'occorrenza fissato. In caso di mancato adeguamento a seguito della diffida, resa anche ai sensi dell'art. 1454 c.c., la F.I.S.E. potrà risolvere il contratto ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.

9. La Società può ricorrere ad altro Responsabile (sub-Responsabile) del trattamento, previa autorizzazione scritta da parte di F.I.S.E..

10. Il sub-Responsabile del trattamento deve rispettare obblighi analoghi a quelli forniti dal Titolare al Responsabile Iniziale del trattamento, riportate in uno specifico contratto o atto di nomina. In caso di violazione da parte del sub-Responsabile del trattamento degli obblighi in materia di protezione dei dati, il Responsabile Iniziale del trattamento è interamente responsabile nei confronti del Titolare del trattamento di tali inadempimenti; la F.I.S.E. potrà in qualsiasi momento verificare le garanzie e le misure tecniche ed organizzative del sub-Responsabile tramite audit e ispezioni anche avvalendosi di soggetti terzi.

11. La Società manleverà e terrà indenne F.I.S.E. da ogni perdita, contestazione, responsabilità, spese sostenute, nonché dei costi subiti (anche in termini di danno reputazionale) in relazione anche ad una sola violazione della normativa in materia di Trattamento dei dati personali.

12. La Società Responsabile deve assistere F.I.S.E. al fine di dare seguito alle richieste per l'esercizio dei diritti degli interessati; qualora gli interessati esercitino tale diritto presso la Società, questa è tenuta ad inoltrare le istanze a F.I.S.E. tempestivamente, e comunque nel più breve tempo possibile, supportando quest'ultima al fine di fornire adeguato riscontro agli interessati nei termini prescritti;

13. La Società informa il Titolare tempestivamente e, in ogni caso senza ingiustificato ritardo dal momento dell'avvenuta conoscenza, di ogni violazione di dati personali (cd. *data breach*); tale notifica è accompagnata da ogni documentazione utile, ai sensi degli artt. 33 e 34 del Regolamento UE, per permettere a F.I.S.E., ove ritenuto necessario, di notificare questa violazione all'Autorità Garante per la protezione dei dati personali, entro il termine di 72 ore da quando il Titolare ne viene a conoscenza.

14. La Società deve avvisare tempestivamente, e senza ingiustificato ritardo, F.I.S.E. in caso di ispezioni, di richiesta di informazioni e di documentazione da parte dell'Autorità Garante per la protezione dei dati personali; inoltre, deve assistere F.I.S.E. nel caso di richieste formulate dall'Autorità Garante in merito al trattamento dei dati personali effettuate in ragione del presente contratto.

15. Al termine del contratto, la Società si impegna a:

i) restituire al Titolare del trattamento i supporti rimovibili eventualmente utilizzati su cui sono memorizzati i dati;

ii) distruggere tutte le informazioni registrate su supporto fisso, documentando per iscritto l'adempimento di tale operazione.

16. La Società non può trasferire i dati personali verso un Paese terzo o un'Organizzazione internazionale, salvo che non abbia preventivamente ottenuto l'autorizzazione scritta da parte di F.I.S.E..

INFORMATIVA PRIVACY

Gentile Signora/Egregio Signore,
La Federazione Italiana Sport Equestri – FISE Le fornisce le informazioni di seguito riportate relative al trattamento dei dati personali che La riguardano e di cui la Federazione entrerà in possesso.
Dato personale è qualunque informazione che possa essere associata alla Sua persona e che quindi La riguarda.

1. Perché leggere questa informativa?

FISE utilizzerà le informazioni che La riguardano e Lei ha il diritto di essere informato/a su quali siano queste informazioni, per quali scopi verranno utilizzate, a chi potranno essere comunicate etc. Dopo essere stato informato del mancato conferimento dei Suoi dati ovvero, ove il Suo consenso sia necessario, delle conseguenze relative al mancato consenso, sarà Lei, tramite un suo atto di volontà libero, a scegliere se darci i Suoi dati o meno e se autorizzare il trattamento dei Suoi dati.
FISE ha adottato uno specifico Regolamento sulla protezione dei dati personali che potrà consultare sul sito www.fise.it.

2. Chi è il Titolare del trattamento dei Suoi dati personali?

Il Titolare del trattamento dei Suoi dati è FISE con sede legale in, …….Tel. ……, Fax: …….., codice fiscale [●] e -mail……..
In alcuni casi, FISE utilizza i Suoi dati per seguire finalità determinate nell'ambito di rapporti con altri soggetti, pubblici e privati, denominati Contitolari. Se i Suoi dati vengono trattati nell'ambito di questi rapporti Lei dovrebbe aver ricevuto un'informativa specifica a riguardo. In ogni caso l'elenco dei contitolari, l'oggetto dei rapporti di questo con FISE e il modo di contattare questi contitolari sono disponibili sul sito www.fise.it

3. Chi è il Responsabile della protezione dei dati?

FISE ha nominato un Responsabile della protezione dei dati che ha funzioni di supporto e di vigilanza sull'applicazione delle regole sulla privacy e a cui Lei potrà rivolgersi in caso in cui ritenga siano state violati o negati i suoi diritti.
FISE ha nominato un Responsabile del trattamento dei dati. Il nominativo del Responsabile è pubblicato sul sito www.fise.it. Il Responsabile della protezione dei dati può essere contattato al seguente indirizzo e-mail dpo@fise.it

4. Chi è il Responsabile del trattamento?

Per prestare i suoi servizi, FISE si avvale spesso della collaborazione di fornitori o prestatori di servizi. In alcuni casi questi fornitori e prestatori di servizi trattano per conto di FISE i dati personali. L'elenco dei responsabili del trattamento è consultabile sul sito www.fise.it

5. **Come vengono trattati i dati che La Riguardano?**

I dati che La riguardano sono sottoposti a diverse operazioni, che si rendono necessarie per perseguire le finalità di seguito riportate. Tutte queste operazioni vengono effettuate da personale appositamente incaricato con strumenti informatici e mediante la lavorazione di documenti cartacei. I nostri archivi informatici sono protetti dalle intrusioni e sono accessibili solo a determinate persone incaricate di trattare i dati, in ragione delle attività lavorative che devono svolgere. Anche gli archivi cartacei sono accessibili solo a chi ha una valida ragione giuridica per trattare i dati.

6. Le informazioni acquisite per quali finalità verranno utilizzate?

FISE utilizzerà i Suoi dati per perseguire i propri fini istituzionali e quindi per:

- promuovere, organizzare, diffondere, coordinare e disciplinare lo sport e le attività equestri favorendo tutte le manifestazioni che tendono alla divulgazione della pratica e della cultura equestre e partecipando all'organizzazione delle stesse;
- promuovere e organizzare la formazione di cavalieri e tecnici;
- favorire e coordinare lo sviluppo dell'attività agonistica nazionale e internazionale;
- contribuire all'incremento e alla valorizzazione della produzione del cavallo sportivo in Italia;
- promuovere, sviluppare e organizzare tutte le attività connesse all'uso del cavallo comprese iniziative con finalità sociale o sanitaria;
- produrre, conservare e utilizzare filmati, fotografie, immagini, altri contenuti audiovisivi, registrazioni, notizie di risultati o avvenimenti sportivi e altri documenti di interesse pubblico o storico oppure di rilievo statistico;
- vigilare sulla regolarità di eventi ed attività sportive in ottemperanza ai propri regolamenti e a internazionali, anche per quanto attiene alla tutela della salute e all'utilizzo di sostanze proibite nell'attività sportiva (doping);
- cooperare con le autorità, anche comunicando dati personali precedentemente raccolti, come prescritto dalle leggi applicabili;
- organizzare e consentire il regolare svolgimento delle attività della giustizia sportiva, inclusa la pubblicazione delle relative decisioni;
- prevenire e contrastare l'uso di sostanze dopanti;
- adempiere ad obblighi di legge e per rispondere a richieste avanzate da autorità giudiziarie, nazionali o internazionali, che agiscano in base al diritto nazionale o dell'Unione Europea.

7. Cosa consente a FISE di trattare i dati che La riguardano?

Il trattamento dei Suoi dati ci viene consentito dalla Sua adesione al contratto associativo e per adempiere ai diritti e ai doveri da esso nascenti.
In altri casi il trattamento dei suoi dati è necessario per motivi di interesse pubblico, essendo FISE incaricata di svolgere funzioni pubbliche.

Per alcune attività particolari Le verrà invece chiesto il Suo consenso esplicito.

8. Cosa succede nel caso in cui Lei dovesse negare il conferimento dei dati o il consenso al loro trattamento?

Se Lei decidesse di non conferire i suoi dati, FISE non potrà procedere alla Sua associazione e al Suo tesseramento e Lei non potrà esercitare le facoltà e i diritti che ne derivano.

In tutti casi in cui Le viene richiesto il consenso significa che senza lo stesso FISE non può erogarLe il servizio richiesto o non può svolgere l'attività per la quale il consenso è richiesto. Il Suo mancato consenso determinerà, quindi, l'impossibilità per FISE di svolgere l'attività per la quale è richiesto il suo consenso.

9. Il consenso al trattamento dei dati può essere revocato?

Il suo consenso al trattamento dei dati può essere revocato ma questo non pregiudicherà i trattamenti già eseguiti e non impedirà i trattamenti ulteriori che siano obbligatori per legge o che siano necessari per tutelare un legittimo interesse di FISE.

10. A chi potranno essere comunicate le Sue informazioni?

All'interno della Federazione sono autorizzati ad effettuare operazioni di trattamento dei sui Suoi dati personali, secondo i principi di necessità, correttezza e liceità, solo soggetti espressamente incaricati. Questo significa che solo chi ha necessita dei Suoi dati per svolgere il suo lavoro potrà accedervi.

Dei Suoi dati personali possono venire a conoscenza i Responsabili del Trattamento e i Contitolari, ma anche loro sono soggetti agli obblighi di riservatezza e devono adottare tutte le misure tecniche e organizzative per proteggere i Suoi dati.

Ove previsto dalla legge, ovvero qualora ciò sia necessario a tutelare un legittimo interesse di FISE, i Suoi dati potrebbero essere comunicati a soggetti pubblici o privati che agiscono quali titolari autonomi. Se si tratta di privati sarà loro dovere informarLa sui trattamenti da loro posti in essere.

Nei casi previsti dalla legge, dai regolamenti e dalle norme statutarie i Suoi dati potrebbero essere soggetti a pubblicazione sul sito web www.fise.it o in altro materiale divulgativo. Ove possibile i dati verranno pubblicati in forma anonima.

Sempre in occasione di manifestazioni sportive saranno pubblicati sul sito web dei FISE i risultati sportivi e l'ammontare dei premi vinti.

Le ricordiamo che FISE, in quanto esercente pubbliche funzioni è soggetta alla disciplina dell'accesso agli atti e all'accesso civico generalizzato. Ove possibile, i documenti verranno forniti in forma anonima, ma potrebbero esserci casi in cui il prevalente interesse di un terzo gli consenta di accedere ai Suoi dati personali.

In occasione di manifestazioni internazionali i Suoi dati potrebbero essere trasferiti all'estero fuori dall'Unione europea o presso organizzazioni internazionali. Qualora i Paesi di destinazione non offrano garanzie adeguate per la tutela dei Suoi dati, Le chiederemo un consenso esplicito oppure chiederemo ai destinatari di prestare idonee garanzie per la sicurezza dei suoi dati.

Alcuni dati sono soggetti a pubblicazione come quelli relativi agli esiti delle manifestazioni sportive o le sentenze dei Giudici sportivi, ma in quest'ultimo caso, Lei può fare istanza al Giudice per evitare la pubblicazione del suo nominativo.

11. Le informazioni acquisite per quanto tempo verranno conservate?

In genere, i dati vengono conservati per un periodo di 10 anni dalla cessazione della Sua associazione a FISE o comunque fino allo spirare del termine di prescrizione relativo ai diritti connessi.

Ci sono casi in cui la conservazione si protrae per un periodo maggiore, o è ridotta ad un periodo minore, ma in questi casi Lei avrà ricevuto un'informativa specifica.

Ci sono infine dati che la legge ci obbliga a tenere per un periodo indeterminato come nel caso degli atti pubblici e dei provvedimenti amministrativi.

12. FISE utilizza processi decisionali automatizzati, compresa la profilazione?

FISE non utilizza nessun processo decisionale automatizzato, né tecniche di profilazione.

13. Quali sono i diritti che può esercitare

Rispetto ai dati che la riguardano Le sono riconosciuti diversi diritti.

I Suoi diritti sono:

<u>Diritto di revoca del consenso:</u>

Lei ha il diritto di revocare in qualsiasi momento il consenso prestato, senza pregiudicare la liceità del trattamento prima del Suo atto di revoca.

<u>Diritto di accesso:</u>

Lei ha il diritto di ottenere la conferma che sia o meno in corso un trattamento dei dati personali che La riguardano e in tal caso di ottenere le seguenti informazioni:

- finalità del trattamento;
- le categorie dei dati personali in questione;
- i destinatari o le categorie di destinatari a cui i dati personali sono comunicati o saranno comunicati;
- il periodo di conservazione dei dati personali presso FISE;
- qualora i dati non siano stati da Lei personalmente forniti, Lei ha diritto di sapere quale sia la fonte dei predetti dati e se i dati provengano da fonti accessibili al pubblico.

<u>Diritto alla cancellazione</u>:

Lei ha il diritto di chiederci la cancellazione dei dati che la riguardano nell'ipotesi in cui

- i dati non sono più necessari;
- Lei abbia revocato il consenso precedentemente prestato o si opponga ad un trattamento particolare;

– FISE abbia un obbligo di legge di cancellare i dati che La riguardano.

Diritto di rettifica e di integrazione:

Lei ha il diritto di ottenere dal Titolare del trattamento la rettifica senza giustificato ritardo dei Suoi dati personali inesatti. In relazione alle finalità del trattamento, Lei ha il diritto di ottenere l'integrazione dei Suoi dati personali incompleti, anche fornendo una dichiarazione integrativa.

Diritto alla portabilità dei dati personali:

Lei ha il diritto di ricevere i dati personali che La riguardano in un formato compatibile al comune uso e leggibile dai dispositivi comunemente in commercio. Lei ha il diritto di trasmettere suddetti dati ad altro titolare del trattamento e di chiedere a FISE la trasmissione diretta da un titolare all'altro. In quest'ultimo caso l'esercizio di questo Suo diritto è subordinato ad una verifica di fattibilità tecnica da parte della Società.

Diritto di opposizione al trattamento dei dati personali:

Lei ha il diritto di opporsi all'ulteriore trattamento dei Suoi dati, adducendo motivi legittimi connessi alla Sua situazione particolare. Tuttavia, quando il trattamento è necessario per l'esecuzione di un compito di interesse pubblico, per adempiere ad un obbligo imposto dalla legge oppure quando il trattamento è necessario per il perseguimento del legittimo interesse di FISE, quest'ultima sottoporrà a valutazione la Sua richiesta per verificare entro che limiti possa essere soddisfatta.

Diritto di limitazione di trattamento:

Lei ha diritto di chiedere a FISE la limitazione del trattamento dei dati nelle seguenti ipotesi:

a) quando ritiene che i dati che La riguardano non siano corretti e ne voglia verificare l'esattezza;

b) quando ritiene che il Suo consenso non sia stato validamente prestato e invece che chiedere la cancellazione dei dati da parte di FISE preferisca indicare entro che limiti possano essere utilizzati;

c) quando voglia impedirne la cancellazione perché deve esercitare un diritto in sede giudiziaria;

d) quando si è opposto al trattamento in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi di FISE per proseguire nel trattamento.

Diritto a proporre reclamo all'Autorità di controllo:

Lei può proporre reclamo al Garante per la protezione dei dati personali per lamentare una violazione della disciplina in materia di protezione dei dati personali e per richiedere una verifica dell'Autorità. Il reclamo potrà essere da Lei direttamente sottoscritto oppure dalle associazioni che La rappresentano. In quest'ultimo caso, è necessario conferire una delega scritta. La delega dovrà essere depositata presso il Garante per la protezione dei dati personali assieme a tutta la documentazione utile ai fini della valutazione del reclamo presentato. Lei potrà far pervenire l'atto utilizzando la modalità che ritiene più opportuna, consegnandolo a mano presso gli uffici del Garante (all'indirizzo di seguito indicato) o mediante l'inoltro di:

a) raccomandata A/R indirizzata a Garante per la protezione dei dati personali, Piazza di Monte Citorio, 121 00186 Roma;
b) e-mail all'indirizzo: garante@gpdp.it, oppure protocollo@pec.gpdp.it;
c) fax al numero: 06/69677.3785.

Per la presentazione del reclamo, è necessario provvedere preliminarmente al pagamento dei diritti di segreteria nella misura pari a euro 150, fatti salvi i casi eccezionali meritevoli di considerazione - in ragione delle condizioni economiche o di disagio del richiedente, della natura dell'attività svolta o delle finalità del trattamento - che giustifichino un esonero dal versamento.

INFORMATIVA PRIVACY

Gentile Signora/Egregio Signore,
La Federazione Italiana Sport Equestri – FISE Le fornisce le informazioni di seguito riportate relative al trattamento dei dati personali che La riguardano e di cui la Federazione entrerà in possesso.
FISE ha adottato uno specifico Regolamento sulla protezione dei dati personali consultabile sul sito www.fise.it.

1. Perché leggere questa informativa?

FISE utilizzerà le informazioni che La riguardano e Lei ha il diritto di essere informato/a su quali siano queste informazioni, per quali scopi verranno utilizzate, a chi potranno essere comunicate etc.

2. Chi è il Titolare del trattamento dei Suoi dati personali

Il Titolare del trattamento dei Suoi dati è FISE con sede legale in, …….Tel. ……, Fax: …….., codice fiscale [●] e -mail……..

3. Chi è il Responsabile della protezione dei dati

FISE ha nominato un Responsabile del trattamento dei dati. Il nominativo del Responsabile è pubblicato sul sito www.fise.it. Il Responsabile della protezione dei dati può essere contattato al seguente indirizzo e-mail: dpo@fise.it

4. Chi è il Responsabile del trattamento.

Per prestare i servizi FISE si avvale spesso della collaborazione di fornitori o prestatori di servizi. L'elenco dei responsabili del trattamento è consultabile sul sito www.fise.it

Come vengono trattati i dati che la Riguardano?

I dati che La riguardano sono sottoposti a diverse operazioni che si rendono necessarie per perseguire le finalità di seguito riportate con strumenti informatici e mediante la lavorazione di documenti cartacei.

5. Le informazioni acquisite per quali finalità verranno utilizzate?

FISE utilizzerà i Suoi dati per perseguire i propri fini istituzionali come risultanti dal proprio statuto e dai propri regolamenti, consultabili sul sito www.fise.it

6. Cosa consente a FISE di trattare i dati che La riguardano?

Il trattamento dei Suoi dati, ci viene consentito dalla Sua adesione al contratto associativo. In altri casi, il trattamento dei Suoi dati è necessario per motivi di interesse pubblico. Per alcune attività particolari, Le verrà invece chiesto il Suo consenso esplicito.

7. Cosa succede nel caso in cui Lei dovesse negare il conferimento dei dati o il consenso al loro trattamento.

Se Lei decidesse di non conferire i Suoi dati, FISE non potrà procedere alla Sua associazione e al Suo tesseramento e Lei non potrà esercitare le facoltà e i diritti che ne derivano. In tutti casi in cui Le viene richiesto il consenso significa che senza lo stesso FISE non può erogarLe il servizio richiesto o non può svolgere l'attività per la quale il consenso è richiesto.

8. Il consenso al trattamento dei dati può essere revocato?

Il Suo consenso al trattamento dei dati può essere revocato, ma questo non pregiudicherà i trattamenti già eseguiti e non impedirà i trattamenti ulteriori che siano obbligatori per legge o che siano necessari per tutelare un legittimo interesse di FISE.

9. A chi potranno essere comunicate le Sue informazioni?

All'interno della Federazione sono autorizzati ad effettuare operazioni di trattamento dei sui Suoi dati personali, secondo i principi di necessità, correttezza e liceità solo soggetti espressamente incaricati. Dei Suoi dati personali possono venire a conoscenza i Responsabili del Trattamento e i Contitolari. Ove previsto dalla legge, ovvero qualora ciò sia necessario a tutelare un legittimo interesse di FISE, i Suoi dati potrebbero essere comunicati a soggetti pubblici o privati. Nei casi previsti dalla legge, dai regolamenti e dalle norme statutarie i Suoi dati potrebbero essere soggetti a pubblicazione sul sito web www.fise.it, o in altro materiale divulgativo. Ove possibile i dati verranno pubblicati in forma anonima. Le ricordiamo che FISE, in quanto esercente pubbliche funzioni, è soggetta alla disciplina dell'accesso agli atti e all'accesso civico generalizzato. Potrebbero darsi casi in cui il prevalente interesse di un terzo gli consenta di accedere ai Suoi dati personali. In occasione di manifestazioni internazionali i Suoi dati potrebbero essere trasferiti all'estero. Qualora i Paesi di destinazione non offrano garanzie adeguate per la tutela dei Suoi dati, Le chiederemo un consenso esplicito oppure chiederemo ai destinatari di prestare idonee garanzie per la sicurezza dei Suoi dati.

10. Le informazioni acquisite per quanto tempo verranno conservate?

In genere i dati vengono conservati per un periodo di 10 anni dalla cessazione della Sua associazione a FISE, o comunque fino allo spirare del termine di prescrizione relativo ai diritti connessi. Ci sono, infine, dati che la legge ci obbliga a tenere per un periodo indeterminato.

11. Quali sono i diritti che può esercitare

Rispetto ai dati che La riguardano, Le sono riconosciuti diversi diritti. Diritto di accesso: Lei ha il diritto di ottenere informazioni circa i trattamenti che La riguardano; Diritto di rettifica e di integrazione: Lei ha il diritto di ottenere la rettifica dei dati personali inesatti. Diritto alla portabilità dei dati personali: Lei ha il diritto di ricevere i dati personali che La riguardano o di trasmettere suddetti dati ad altro titolare. Diritto alla limitazione: Lei ha diritto di chiederci la limitazione dei trattamenti in corso. Diritto a proporre reclamo all'Autorità di controllo: Lei può proporre reclamo al Garante per la protezione dei dati personali per lamentare una violazione della disciplina in materia di protezione dei dati personali.

12. Dove può reperire maggiori informazioni?

Maggiori informazioni sono reperibili sul sito internet www.fise.it

INFORMATIVA SUI COOKIES

Quando Lei utilizza il nostro sito, acconsente automaticamente all'utilizzo da parte di F.I.S.E. dei cookies sul Suo dispositivo. Tuttavia, è sempre possibile scegliere di evitare i cookies e di eliminarli seguendo le istruzioni riportate di seguito. Per qualunque dubbio relativo all'utilizzo dei cookies, può consultare il sito del Garante della Privacy.

Che cos'è un cookie?

Un cookie è un piccolo file dati che il browser Internet memorizza sul tuo dispositivo (computer, telefono cellulare, tablet) e che permette di informare il sito che l'utente (quindi Lei) è ritornato. Ogni cookie scade dopo un certo periodo di tempo, a seconda dello scopo per cui viene utilizzato.

Perché usiamo i cookies?

Utilizziamo i cookies per salvare le scelte dell'utente, per tenere attiva la sessione di navigazione, per generare statistiche di accesso al sito, o per mostrare inserzioni più pertinenti ai Suoi interessi.

Questo sito web utilizza cookies con il consenso preventivo dell'utente, a eccezione dei cookies strettamente necessari sul piano tecnico o statistici con dati aggregati, che analizzano la navigazione degli utenti per realizzare statistiche sulle visite o per migliorare l'offerta dei contenuti. Si prega di notare che i dati raccolti sono statistici e non personali.

In che modo questo Le è utile?

Alcuni cookies vengono utilizzati per raccogliere informazioni su come i visitatori utilizzano il sito web e sfruttiamo le informazioni per rilevare i problemi legati al sito, migliorare e perfezionare i servizi e le funzionalità. Ricordando le impostazioni, per esempio, è possibile memorizzare le proprie credenziali, così da non doverle reinserire ad ogni accesso al sito. Le impostazioni rilevate attraverso i cookies forniscono anche tipo di terminale utilizzato e in questo modo è possibile configurare il sito per fornire la migliore esperienza di navigazione possibile.

Generalmente, tali cookies raccolgono dati in forma anonima e consentono di determinare le informazioni, come il numero di visitatori della pagina internet, il modo in cui i visitatori hanno raggiunto il sito e le pagine da loro visitate. Per questo tipo di monitoraggio utilizziamo Google Analytics. Le informazioni generate dal cookie sull'utilizzo del sito web da parte dell'utente sono trasmesse e registrate sui server di Google e saranno gestite nel rispetto della privacy di Google.

Per ulteriori informazioni visitare: informativa sulla privacy di Google Analytics.

Come evitare e/o eliminare i cookies?

La maggior parte dei browser accetta i cookies di default, tuttavia è possibile modificare le impostazioni del browser per non accettare i cookies o cancellarli dal proprio sistema. A seconda del browser utilizzato, l'impostazione ha un nome diverso, ma la procedura è perlopiù simile e la configurazione predefinita può essere modificata dall'utente.

Un altro metodo è quello di cancellare (o eliminare) i cookies dal personal computer, partendo sempre da Strumenti/Opzioni, selezionando la voce "Opzioni Internet" ed infine nella scheda "Generale" cliccando sul pulsante "Elimina cookies".

Di seguito trova i browser più comuni e le rispettive modalità di navigazione "in incognito":

- Internet Explorer 8 e versioni successive; InPrivate Browsing;
- Firefox 3.5 e versioni successive; Private Browsing,
- Google Chrome 10 e versioni successive; Incognito Mode;
- Safari 2 e versioni successive; Private Browsing;
- Opera 10.5 e versioni successive; Private Browsing.

È consigliabile leggere la sezione di assistenza del proprio browser per ulteriori informazioni su come impostare la modalità "in incognito" o come eliminare i cookies. Come sopra precisato, disabilitare o cancellare dei cookies potrebbe precludere la fruizione ottimale di alcune aree del sito o compromettere l'utilizzo dei servizi.

Informativa sul trattamento dei dati personali
Art. 13 RGPD 679/2016
- Dipendenti o Collaboratori -

Gentile Signora / Egregio Signore,

ai sensi dell'art. 13 del RGPD 679/2016 *"Regolamento Generale sulla protezione dei dati",* recante disposizioni in materia di trattamento dei dati personali, La informiamo che, in relazione all'instaurazione ed all'esecuzione del rapporto di lavoro/di collaborazione con Lei in essere, la Federazione Italiana Sport Equestri (di segito F.I.S.E.), quale Titolare del trattamento dei dati, utilizzerà informazioni che La riguardano e da Lei forniti, qualificati come "Dati Personali". Tale norma prevede che chiunque effettui trattamenti di dati personali è tenuto ad informare il soggetto interessato su quali dati vengono trattati e su taluni elementi qualificanti il trattamento, che deve in ogni caso avvenire in maniera lecita, corretta e trasparente, tutelando la Sua riservatezza e garantendo i Suoi diritti.

A. Natura dei dati trattati:

Oltre ai Suoi dati identificativi (es. anagrafici), definiti dalla legge "dati personali" per il corretto svolgimento del rapporto di lavoro/di collaborazione, abbiamo la necessità di trattare alcuni dati considerati dalla legge "particolari". Si tratta dei dati personali dai quali si ricavano informazioni sul Suo stato di salute (es: infortunio, maternità) o sull'adesione ai sindacati (es. trattenuta in favore di un'organizzazione sindacale, richiesta di un permesso sindacale).
Precisiamo che nel trattare tali dati ci atterremo scrupolosamente ai limiti e alle condizioni imposte dal RGPD 679/2016.

B. Finalità e base giuridica del trattamento:

Il trattamento dei Suoi dati personali e/o particolari, è lecito perché ricorrono le seguenti basi giuridiche:

- esecuzione di un **contratto** di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso (art. 6, comma 1, lett. b);
- adempimento ad un **obbligo legale** al quale è soggetto il Titolare del trattamento (art. 6, comma 1, lett. c).

In alcuni casi la F.I.S.E. utilizzerà i Suoi dati per seguire finalità determinate nell'ambito di rapporti con altri soggetti, ad essa collegati, denominati Contitolari. Attraverso la sottoscrizione eventuale di un Accordo di Contitolarità, la F.I.S.E. e i Contitolari hanno infatti inteso implementare un sistema di gestione centralizzata dei Dati Personali di cui entreranno in possesso nell'ambito della propria attività, definendo così congiuntamente le finalità, le modalità relative ai trattamenti, e ripartendo le rispettive responsabilità nell'adempimento degli obblighi previsti sia contrattualmente che dalla normativa vigente.

Se i Suoi dati vengono trattati nell'ambito di questi rapporti l'elenco dei Contitolari, l'oggetto dei rapporti tra questi e la F.I.S.E. e il modo con cui poterli contattare è contenuto nell' Accordo di Contitolarità allegato al ……. o disponibile presso le sede della F.I.S.E. (eventuale).

In riferimento ai dati particolari, ai sensi dell'**all'art. 9 del Regolamento 679/2016**, saranno trattati esclusivamente per assolvere ad obblighi di legge o per consentire l'esercizio dei diritti dei Titolare o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale (art. 9, lett. b).
I Suoi dati sono trattati per la seguente **finalità: gestione del rapporto contrattuale con Lei in essere, in particolare:**

- provvedere alla gestione del Suo contratto di lavoro (consuntivazione presenze, assenze, elaborazione e gestione documenti di assunzione, consultazione e conservazione e archiviazione cedolini paga e certificazioni uniche);
- provvedere alla gestione degli infortuni sul lavoro e delle malattie professionali e non;
- provvedere ad assolvere agli obblighi nei confronti degli istituti di previdenza ed assistenza;
- provvedere ad assolvere agli obblighi nei confronti dell'amministrazione finanziaria;
- provvedere ad assolvere agli obblighi imposti dalla normativa in materia di sicurezza sul lavoro (d.lgs. n. 81/2008);

- provvedere agli obblighi formativi.

Inoltre, la F.I.S.E. potrà utilizzare i Suoi dati sulla base giuridica del legittimo interesse del Titolare del trattamento (art. 6, comma 1, lett. f) perseguiti con le seguenti finalità:

- definizione delle politiche aziendali per il personale (es. corsi di formazione, valutazione del personale, etc.) da parte dei Responsabili interni preposti;
- attività e adempimenti della Funzione Amministrazione Finanza e Controllo di Gestione.

Ulteriori dati (oltre quelli richiesti dalla legge o dal contratto), ove necessari, potranno essere acquisiti ed utilizzati, soltanto previo suo **consenso esplicito** (art. 6 comma 1, lett. a).
Una volta prestato, il consenso può essere sempre revocato in ogni momento, senza pregiudicare la liceità del trattamento basato sul consenso prestato prima della revoca.
Il rifiuto di prestarlo non ha nessuna conseguenza sul rapporto di lavoro né sulla sua prosecuzione.

C. Conservazione:

Tali dati verranno conservati per il tempo non superiore a quello strettamente necessario a perseguire le finalità per le quali gli stessi sono stati raccolti, per tutta la durata del rapporto di lavoro ed anche successivamente, nei limiti e nei tempi necessari per l'espletamento degli obblighi di legge e di contratto.
Le specifiche sui tempi di conservazione per ciascuna categoria di dato sono consultabili tramite apposita richiesta.

D. Obbligo o facoltà di conferire i dati e conseguenze di un eventuale rifiuto:

Il conferimento dei dati per le finalità di **gestione del rapporto contrattuale** è necessario.
La informiamo che, in loro mancanza, sarà impossibile per la F.I.S.E. adempiere agli obblighi di legge e di contratto con Lei in essere, pertanto, il loro mancato conferimento comporterà di fatto l'impossibilità di instaurare o proseguire il rapporto di lavoro, nei limiti in cui tali dati ci sono necessari per compiere correttamente gli adempimenti legati al Suo rapporto di lavoro.

E. Modalità di trattamento:

Il trattamento dei Suoi dati avverrà sia con strumenti cartacei che elettronici e con l'adozione di misure per prevenire la perdita dei dati, usi illeciti e non corretti, ed accessi non autorizzati, nel rispetto delle vigenti disposizioni in materia di tutela dei dati personali.
Tale trattamento è consentito:
1. ad addetti all'ufficio del personale, autorizzati al trattamento dei Suoi dati, previa nostra lettera di incarico che imponga loro il dovere di riservatezza e sicurezza del trattamento dei dati personali, con il compito di gestire il Suo rapporto contrattuale;
2. a soggetti nostri fornitori, nei limiti necessari per svolgere il loro incarico professionale per conto della nostra Azienda, nominati Responsabili del trattamento (*outsourcer*), previa nostra lettera di incarico che imponga loro il dovere di riservatezza e sicurezza del trattamento dei dati personali che si riferiscono al nostro personale.

F. Comunicazione dei dati:

E' prevista la sola comunicazione a soggetti che sono tenuti da norme di legge o di contratto quali:

- Istituzioni pubbliche es. INPS, INAIL, Direzione Provinciale del Lavoro, Agenzia delle Entrate).
- Fondi integrativi e/o Casse anche private di previdenza, assistenza e/o assicurazione.
- Istituti di credito per il pagamento delle retribuzioni.
- Studi Legali esterni e di contabilità, come contrattualmente previsto

La comunicazione dei dati è comunque limitata a quelli strettamente necessari ad effettuare gli adempimenti di competenza ed il trattamento avviene nel rispetto del principio di necessità ed indispensabilità.

G. Misure di sicurezza adottate dalla F.I.S.E. tutela dei dati acquisiti

I dati personali comunicati vengono protetti dalla F.I.S.E. mediante: una politica di gestione del materiale cartaceo che limita l'accesso ai dati e li protegge dalla loro, diffusione, perdita e distruzione;

a) politiche di utilizzo degli strumenti informatici.

H. Titolare del trattamento

Il titolare del Trattamento dei suoi dati personali è la F.I.S.E. **……** con sede legale in …….

Al fine di assicurare il raggiungimento ed il mantenimento di un adeguato livello di protezione dei dati, la F.I.S.E. e gli eventuali Contitolari ha/hanno provveduto alla nomina di un Responsabile del trattamento, contattabile al seguente indirizzo email…….

Troverà infine l'elenco aggiornato dei Responsabili del trattamento e dei singoli incaricati, ove richiesto, presso la sede del Titolare e presso quelle di ciascun Contitolare, o potrà richiedere tali informazioni direttamente al Responsabile del trattamento.

I. Diritti dell'Interessato:

All'interessato viene attribuita la facoltà di far valere i Suoi diritti, così come indicato dagli artt. 15 e ss. del RGPD del 2016/679.

Tra i diritti sono annoverati in particolare:
- il diritto di accesso alle informazioni sui trattamenti che la riguardano: le finalità del trattamento, le categorie dei dati personali in questione, i destinatari o le categorie di destinatari a cui i dati personali sono destinati o saranno comunicati, in particolare se destinatari di Paesi terzi o organizzazioni internazionali, quando è possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo, qualora i dati non siano raccolti presso l'interessato, diritto di avere tutte le informazioni disponibili sulla loro origine;

- il diritto di rettifica e di integrazione dei dati personali comunicati e inseriti;

- il diritto di limitazione al trattamento;

- il diritto di opposizione al loro trattamento;

- il diritto di revocare il trattamento basato sul consenso;

- il diritto alla portabilità dei dati;

- il diritto d cancellazione dei dati personali

- il diritto di proporre reclamo all'Autorità di controllo.

L'interessato può proporre reclamo al Garante per la protezione dei dati personali per lamentare una violazione della disciplina in materi di protezione dei dati personali e per richiedere una verifica da parte dell'Autorità mediante l'inoltro di:
- raccomandata A/R indirizzata al Garante per la protezione dei dati personali, presso la sede di Roma, Piazza di Monte Citorio, 121 – 00186 Roma;
- e-mail all'indirizzo: garante@gdpr.it; oppure protocollo@pec.gdpr.it ;
-fax al numero: 06 696773785

Per presa visione ed accettazione

Data_____

Firma _____

APPENDICE A

Linee guida per una corretta gestione dei sistemi, degli applicativi e delle dotazioni informatiche

1 Dispositivi portatili

Nel caso di utilizzo dei dispositivi mobili, si deve garantire che le informazioni ivi contenute non vengano compromesse. La politica dovrebbe prendere in considerazione:

a. la registrazione dei dispositivi mobili;
b. i requisiti per la protezione fisica;
c. la limitazione dell'installazione del software;
d. i requisiti per le versioni software per dispositivi mobili e per l'applicazione di patch;
e. la limitazione della connessione ai servizi di informazione;
f. tecniche di crittografia;
g. protezione da malware;
h. disabilitazione a distanza, cancellazione o blocco; non vi è alcun tool per poterlo fare (es. Intune con il wipe)
i. backup;
j. l'utilizzo di servizi web e applicazioni web.

I dispositivi mobili dovrebbero essere fisicamente protetti contro il furto.

I dispositivi che contengono informazioni sensibili non dovrebbero essere lasciati incustoditi e, ove possibile, dovrebbero essere fisicamente sotto chiave.

2 Inventario degli asset

Dovrebbero essere identificati gli asset rilevanti nel ciclo di vita delle informazioni, documentandone la loro importanza. Il ciclo di vita delle informazioni dovrebbe includere la creazione, la lavorazione, la conservazione, la trasmissione, la cancellazione. L'inventariazione delle risorse deve essere accurata, aggiornata, coerente e in linea con eventuali altri inventari. Per ciascuno degli asset identificati, deve essere anche identificato l'assegnatario del bene.

Nella fase di restituzione del bene, devono esser previste specifiche procedure per garantire che tutti i dati personali, eventualmente presenti sul bene, vengano gestite/cancellate in modo sicuro.

3 Gestione dei supporti rimovibili

Nella gestione di supporti rimovibili:

a) se non è più necessario, il contenuto di qualsiasi supporto riutilizzabile dovrebbe essere rimosso in modo irreversibile;

b) tutti i media devono essere conservati in un ambiente sicuro e protetto, in conformità con le specifiche dei produttori;
c) se la riservatezza e l'integrità dei dati contenuti nei supporti risultano essere importanti, dovrebbero essere utilizzate tecniche crittografiche per proteggere i dati sui supporti rimovibili;
d) copie multiple di dati importanti devono essere memorizzate su supporti separati per ridurre ulteriormente il rischio di perdita.

Procedure e livelli di autorizzazione devono essere documentati.

4 Dismissione dei supporti

Dovrebbero essere stabilite procedure formali per lo smaltimento sicuro dei media al fine di ridurre al minimo il rischio di perdite di informazioni.

Le procedure per lo smaltimento sicuro dei supporti contenenti informazioni riservate devono essere proporzionali alla sensibilità di tali informazioni. Devono essere considerati i seguenti elementi:

- supporti contenenti informazioni riservate devono essere conservati e smaltiti in modo sicuro, per esempio mediante incenerimento o triturazione;
- occorre prestare attenzione nella scelta di un soggetto esterno per lo smaltimento dei supporti, verificando che abbia esperienza adeguata;
- lo smaltimento di oggetti sensibili deve essere registrato.

5 Politica di controllo degli accessi

Dovrebbero essere stabilite politiche contenenti regole di controllo per l'accesso logico, i diritti di accesso e le restrizioni per specifici ruoli utente. La politica dovrebbe tener conto dei seguenti elementi:

- i requisiti di sicurezza delle applicazioni aziendali;
- la coerenza tra i diritti di accesso e la criticità delle informazioni dei sistemi e delle reti;
- la separazione dei ruoli per il controllo degli accessi, ad esempio richiesta di accesso e autorizzazione;
- i requisiti per l'autorizzazione formale delle richieste di accesso;
- i requisiti per la revisione periodica dei diritti di accesso;
- la rimozione dei diritti di accesso;
- i ruoli con accesso privilegiato.

6 Accesso alle reti e ai servizi di rete

Una politica per l'uso delle reti e dei servizi di rete dovrebbe contenere:

- le reti e i servizi di rete a cui si è autorizzati ad accedere;
- le procedure di autorizzazione per determinare chi ha il permesso di accesso alle reti e ai servizi di rete;

- i controlli e le procedure per proteggere l'accesso alle connessioni di rete e servizi di rete;
- i mezzi utilizzati per l'accesso alle reti e ai servizi di rete (ad esempio, l'uso di VPN o rete wireless);
- l'autenticazione degli utenti per l'accesso ai vari servizi di rete;
- il monitoraggio sull'utilizzo dei servizi di rete.

La politica di utilizzo dei servizi di rete deve essere coerente con la politica di controllo degli accessi logici dell'organizzazione.

7 Registrazione e de-registrazione degli utenti

Il processo di gestione degli utenti dovrebbe includere:

- ID utenti univoci per consentire agli utenti di collegarsi ai sistemi aziendali ed essere ritenuti responsabili delle loro azioni;
- la disattivazione immediata o la rimozione di ID utente per gli utenti che hanno lasciato l'organizzazione.

8 Provisioning degli accessi degli utenti

Il processo di provisioning per l'assegnazione o la revoca dei diritti di accesso dovrebbe:

- ottenere l'autorizzazione da parte del proprietario del sistema;
- verificare che il livello di accesso consentito sia in accordo con le policy per gli accessi e che sia coerente con gli altri requisiti, quali la separazione delle funzioni;
- garantire che i diritti di accesso non siano attivati (ad esempio per i fornitori) prima che le procedure di autorizzazione siano state completate;
- istituire e mantenere un registro centrale dei diritti di accesso concessi;
- tener conto dei diritti di accesso degli utenti che hanno cambiato ruoli o posti di lavoro e provvedere immediatamente alla rimozione o al blocco dei diritti di accesso degli utenti che hanno lasciato l'organizzazione;
- effettuare la revisione periodica dei diritti di accesso con i proprietari dei sistemi o dei servizi.

L'assegnazione dei diritti di accesso privilegiato dovrebbe essere controllata attraverso un processo formale di autorizzazione, considerando i seguenti aspetti:

- i diritti di accesso privilegiato, associati a ciascun sistema, devono essere associati a specifici utenti che operano sui sistemi stessi;
- i diritti di accesso privilegiati devono essere assegnati agli utenti in caso di necessità, cioè sulla base del requisito minimo per il loro ruolo/funzione;
- dovrebbe essere mantenuto un processo di autorizzazione e un record di tutti i privilegi assegnati. I diritti di accesso privilegiato non devono essere concessi fino a quando il processo di autorizzazione non è stato completato;

- dovrebbero essere definiti i requisiti per la scadenza dei diritti di accesso privilegiato;
- i diritti di accesso privilegiato dovrebbero essere assegnati a ID utente diversi da quelli utilizzati per le normali attività lavorative.
- le competenze degli utenti con diritti di accesso privilegiato devono essere riesaminate periodicamente, al fine di verificare se siano in linea con le loro funzioni.

9 Gestione delle informazioni segrete di autenticazione degli utenti

Il processo deve includere i seguenti requisiti:

- gli utenti devono essere costretti a cambiare le proprie credenziali di autenticazione al primo utilizzo;
- verificare l'identità di un utente prima di fornire nuove credenziali di autenticazione.

10 Riesame dei diritti di accesso degli utenti

La revisione dei diritti di accesso degli utenti dovrebbe considerare quanto segue:

- riesame a intervalli regolari dei diritti di accesso degli utenti e dopo ogni modifica, come la promozione, retrocessione o cessazione del rapporto di lavoro;
- riassegnazione dei diritti di accesso degli utenti quando avviene un cambiamento di ruolo all'interno della stessa organizzazione;
- le autorizzazioni per i diritti di accesso privilegiato devono essere riesaminate a intervalli più frequenti rispetto ai diritti di accesso normali;
- gli accessi privilegiati devono essere controllati ad intervalli regolari per garantire che non vi siano privilegi non autorizzati;
- modifiche agli account privilegiati devono essere registrate per la revisione periodica.

In caso di cessazione del rapporto di lavoro, i diritti di accesso di un utente devono essere rimossi o sospesi. I cambiamenti di occupazione dovrebbero riflettersi nella rimozione di tutti i diritti di accesso che non siano stati approvati per la nuova occupazione. I diritti di accesso che devono essere rimossi o modificati sono quelli di sia per l'accesso fisico che logico.

11 Utilizzo delle informazioni segrete di autenticazione

Tutti gli utenti dovrebbero:

- non condividere le informazioni di autenticazione, mantenendole riservate e assicurandosi che non siano divulgate a terze parti;
- evitare di mantenere un record (per esempio su carta, file o dispositivo portatile) delle informazioni di autenticazione;

- modificare le informazioni di autenticazione ogni qualvolta vi sia indicazione della loro possibile compromissione;
- le password utilizzate devono presentare le seguenti caratteristiche:
    - lunghezza minima 8 caratteri;
    - non essere banali o facilmente riconducibili a parole di uso comune presenti nel dizionario;
    - non basarsi su nulla che qualcun altro potrebbe facilmente indovinare o ottenere utilizzando le informazioni relative alla persona (ad esempio nomi, numeri di telefono, date di nascita, ecc.);
    - se provvisorie, cambiarle al primo log-on;
- non utilizzare le stesse informazioni di autenticazione per motivi di lavoro e non.

12 Procedure di log-on sicure

La procedura di registrazione ad un sistema o applicazione dovrebbe essere progettata per minimizzare la possibilità di accesso non autorizzato. La procedura di Log-on dovrebbe prevedere almeno:

- la convalida delle informazioni di log-on solo al termine di tutti i dati di input;
- il log dei tentativi falliti e di quelli corretti;
- qualora venga rilevata una violazione di accesso, il sistema deve prevedere un meccanismo di protezione (blocco dopo n tentativi falliti);
- lavisualizzare le seguenti informazioni al termine di un corretto log-on:
    - la data e l'ora del precedente log-on;
    - eventuali tentativi di log-on falliti dall'ultimo log-on corretto;
- non visualizzare la password che viene inserita;
- non trasmettere password in chiaro su una rete;
- terminare le sessioni dopo un determinato periodo di inattività, soprattutto in luoghi ad alto rischio come le aree pubbliche o esterne al di fuori della gestione della sicurezza dell'organizzazione oppure sui dispositivi mobili;
- limitare i tempi di connessione al fine di fornire un’ulteriore protezione per le applicazioni ad alto rischio e ridurre la finestra di opportunità per l'accesso non autorizzato.

13 Sistema di gestione delle password

Un sistema di gestione delle password dovrebbe:

- imporre l'utilizzo di ID utente e password individuali;
- consentire agli utenti di selezionare e modificare le proprie password e prevedere una procedura di conferma per ovviare ad errori di inserimento;
- applicare una scelta di password di qualità;
- modificare le password al primo log-on;
- modificare le password regolarmente;

- mantenere un record di password utilizzate in precedenza e prevenirne il riutilizzo;
- non visualizzare le password sullo schermo quando vengono inserite.

14 Controllo degli accessi al codice sorgente dei programmi

L'accesso al codice sorgente dei programmi e agli elementi associati (quali disegni, specifiche, programmi di verifica e piani di convalida) dovrebbe essere strettamente controllato al fine di evitare l'introduzione di funzionalità non autorizzate ed evitare modifiche involontarie, nonché per mantenere la riservatezza delle proprietà intellettuali. Le seguenti linee guida dovrebbero quindi essere considerate:

- il codice sorgente dei programmi e le librerie di origine dei programmi devono essere gestiti secondo le procedure stabilite;
- il personale di supporto non dovrebbe avere accesso illimitato alle biblioteche dei codici sorgente;
- l'aggiornamento delle librerie sorgente dei programmi e il rilascio dei codici sorgenti devono essere eseguiti solo dopo le autorizzazioni del caso;
- gli elenchi dei programmi dovrebbero essere tenuti in un ambiente sicuro;
- la manutenzione e la copia delle librerie dei codici sorgente dei programmi dovrebbero essere soggetti a rigide procedure di controllo per le modifiche.

15 Perimetro di sicurezza fisica

Il perimetro di sicurezza fisica, con particolare riferimento ai centri di elaborazione dati, dovrebbe considerare i seguenti aspetti:

- separazione fisica delle strutture per l'elaborazione dei dati dagli ambienti di lavoro;
- definizione del perimetro di sicurezza;
- apposizione di barriere fisiche per impedire l'accesso fisico non autorizzato ai locali;
- installazione di allarmi sulle porte antincendio posizionate sul perimetro di sicurezza, controllate e testate periodicamente;
- implementazione sistemi di rilevamento antintrusione;

16 Controlli di accesso fisico

Il controllo di accesso fisico, con particolare riferimento ai centri di elaborazione dati, dovrebbe considerare i seguenti aspetti:

- l'accesso alle aree in cui vi siano informazioni riservate deve essere limitato, ad esempio implementando un meccanismo di autenticazione;
- l'accesso del personale di servizio o di supporto dovrebbe essere limitato nelle aree protette.

17 Disposizione delle apparecchiature e loro protezione

Nella dislocazione delle apparecchiature dovrebbero essere tenuti in considerazione i seguenti aspetti:

- l'apparecchiatura dovrebbe essere situata in modo da ridurre al minimo l'accesso non necessario;
- i servizi di elaborazione delle informazioni che gestiscono dati sensibili dovrebbero essere posizionati con cura per ridurre il rischio che vengono visualizzate da persone non autorizzate durante il loro utilizzo;
- i controlli dovrebbero essere adottati per ridurre al minimo il rischio di potenziali minacce fisiche e ambientali, per esempio furto, incendio, esplosivi, fumo, acqua, polvere, vibrazioni, effetti chimici, interferenze di alimentazione elettrica, interferenze delle comunicazioni, radiazioni elettromagnetiche e vandalismo;
- le condizioni ambientali, come la temperatura e l'umidità, dovrebbero essere monitorati poiché potrebbero influenzare negativamente il funzionamento degli impianti di elaborazione delle informazioni.

18 Manutenzione delle apparecchiature

Dovrebbero essere seguite le seguenti linee guida per la manutenzione delle apparecchiature:

- le apparecchiature devono esser manutenute con intervalli di manutenzione raccomandati dal fornitore e dalle specifiche;
- il personale di manutenzione deve essere autorizzato per effettuare riparazioni;
- devono essere tenuti registri di tutti gli errori presunti o effettivi, e di tutta la manutenzione preventiva e correttiva.

Gli opportuni controlli dovrebbero essere attuati quando l'apparecchiatura è in programma per la manutenzione, tenendo conto del fatto che questa manutenzione viene eseguita da personale in loco o esterno all'organizzazione.

19 Sicurezza delle apparecchiature e degli asset all'esterno della sede della società

L'uso di qualsiasi apparecchiatura di memorizzazione delle informazioni al di fuori dei locali della Società di mutuo soccorso dovrebbe essere autorizzata dal responsabile della Società o dal Data Manager se nominato. Ciò si applica alle apparecchiature di proprietà della Società e per le attrezzature di proprietà privata ma utilizzate per conto della Società o contenente dati di cui la Società è titolare.

Le seguenti linee guida dovrebbero essere considerate per la protezione delle apparecchiature fuori sede:

- le attrezzature non devono essere lasciate incustodite in luoghi pubblici;
- se l'apparecchiatura è trasferita tra diversi individui o soggetti esterni, un registro deve essere mantenuto e che definisca la catena di custodia per

l'attrezzatura, comprendente almeno i nomi e le organizzazioni di coloro che sono responsabili per l'attrezzatura.

20 Dismissione sicura o riutilizzo delle apparecchiature

Le apparecchiature dovrebbero essere controllate al fine di garantire che non vi siano contenuti supporti di memorizzazione prima dello smaltimento o riutilizzo.

Supporti di memorizzazione contenenti informazioni riservate o protette da copyright dovrebbero essere distrutti fisicamente o le informazioni eliminate, cancellate o sovrascritte utilizzando tecniche per rendere le informazioni originali non recuperabili.

21 Apparecchiature incustodite degli utenti

Tutti gli utenti dovrebbero essere consapevoli dei requisiti di sicurezza e delle procedure per la protezione delle apparecchiature, così come le loro responsabilità per l'attuazione di tale protezione. Gli utenti dovrebbero essere avvisati di:

- terminare le sessioni attive una volta finito il lavoro, a meno che non ci siano meccanismi di bloccaggio come ad esempio uno screen saver protetto da password;
- log-off da applicazioni o servizi di rete quando non più necessari;
- i computer o dispositivi mobili devono essere protetti da un uso non autorizzato attraverso un blocco o un controllo equivalente, ad esempio password di accesso, quando non in uso.

22 Politiche di schermo e scrivania puliti

Dovrebbero essere considerate le seguenti linee guida:

- le informazioni aziendali sensibili o critiche devono essere chiuse a chiave (idealmente in un armadio o una cassa o altre forme di sicurezza) quando non sono necessarie, soprattutto quando l'ufficio è vuoto;
- computer e terminali, quando non in uso, dovrebbero essere lasciati disconnessi o protetti con un meccanismo di bloccaggio dello schermo con password o altri controlli;
- l'uso non autorizzato delle fotocopiatrici e altre tecnologie di riproduzione (ad esempio scanner, fotocamere digitali) deve essere evitata;
- supporti contenenti informazioni sensibili o riservate devono essere rimossi dalle stampanti immediatamente.

23 Procedure operative documentate

Procedure documentate devono essere predisposte per le attività operative sui sistemi di elaborazione delle informazioni e per i servizi di comunicazione. Le procedure operative dovrebbero specificare le istruzioni relativa a:

- l'installazione e configurazione di sistemi;
- il backup;

- i requisiti di programmazione, tra cui interdipendenze con altri sistemi;
- le istruzioni per la gestione degli errori che potrebbero verificarsi durante l'esecuzione del lavoro, comprese le restrizioni sull'uso di utilità di sistema;
- riavvio dei sistemi e procedure di ripristino in caso di guasto;
- la gestione di informazioni del registro di sistema;
- le procedure di monitoraggio.

Procedure operative per le attività di sistema dovrebbero essere trattate come documenti formali e le modifiche devono essere autorizzate dalla direzione. Ove tecnicamente possibile, i sistemi informativi devono essere gestiti in modo coerente, con le stesse modalità, strumenti e utilità.

24 Gestione dei cambiamenti

Nel processo di gestione dei cambiamenti dovrebbero essere considerati i seguenti elementi:

- l'identificazione e la registrazione dei cambiamenti significativi;
- la pianificazione e il test dei cambiamenti;
- la valutazione di potenziali impatti, compresi gli impatti di tali cambiamenti sulla sicurezza delle informazioni;
- procedura di approvazione formale per le modifiche proposte;
- la verifica che i requisiti di sicurezza delle informazioni siano state soddisfatte;
- la comunicazione dei dettagli di modifica a tutte le persone interessate;
- la redazione di un processo di cambiamento d'emergenza per consentire l'attuazione rapida e controllata di cambiamenti necessari per risolvere un incidente.

25 Controlli contro il malware

Una deguata politica di controllo dei malware dovrebbe:

- stabilire una politica formale che vieta l'uso di software non autorizzato;
- prevedere controlli che prevengono o rilevano l'uso di software non autorizzato (ad esempio applicazioni white list);
- prevedere l'implementazione dei controlli volti a rilevare l'uso di siti web malevoli noti o sospetti (per esempio lista nera);
- prevedere l'installazione e l'aggiornamento sistematico di software di rilevamento malware e software di riparazione per la scansione dei computer e dei media come un controllo preventivo.

26 Backup delle informazioni

Una politica di backup dovrebbe esser istituita per definire per il salvataggio delle informazioni, software e sistemi oltre ai requisiti di conservazione e protezione. Dovrebbero essere forniti servizi di backup adeguati volti a garantire che tutte le

informazioni essenziali e il software possano essere recuperati a seguito di un guasto o di un disastro.

I principali elementi di progettazione di un piano di backup sono:

- misura (ad esempio, completo o differenziale di backup) e frequenza dei backup devono riflettere le esigenze di business dell'organizzazione, i requisiti di sicurezza delle informazioni in questione e la criticità delle informazioni per il continuo funzionamento dell'organizzazione;
- i backup devono essere memorizzati in una posizione remota (con protezione ambientale e fisica), ad una distanza sufficiente per sfuggire ai danni eventualmente provocati da un disastro al luogo principale;
- supporti di backup devono essere testati regolarmente per garantire che possano essere effettivamente utilizzati in caso di emergenza.

Le procedure operative dovrebbero monitorare l'esecuzione dei backup e degli eventuali fallimenti al fine di garantire la completezza dei backup. Nel caso di sistemi e servizi critici, le modalità di backup devono coprire tutti i sistemi informativi, applicazioni e dati necessari per ripristinare il sistema completo in caso di disastro. Il periodo di conservazione deve essere determinato, tenendo conto di ogni esigenza dell'organizzazione.

27 Raccolta dei log degli eventi

Le registrazioni di eventi (LOG) devono includere, ove necessario:

- ID utente;
- attività del sistema;
- date, orari e dettagli di eventi chiave, per esempio log-on e log-off;
- l'identità del dispositivo o posizione, se possibile, e il sistema di identificazione;
- registrazioni di tentativi di accesso al sistema;
- modifiche alla configurazione del sistema;
- l'uso di utility e applicazioni di sistema;
- i file accessibili e il tipo di accesso;
- indirizzi IP e protocolli di rete;
- gli allarmi sollevati dal sistema di controllo accessi;
- l'attivazione e la disattivazione dei sistemi di protezione, come i sistemi antivirus e sistemi di rilevamento delle intrusioni;
- le registrazioni delle operazioni eseguite dagli utenti nelle applicazioni.

I LOG devono esser protetti da visualizzazioni e modifiche non autorizzate.

28 Limitazioni all'installazione del software

Si dovrebbero definire e applicare una politica sui software in dotazione agli utenti.

Dovrebbe essere applicato il principio del privilegio minimo. Si dovrebbero identificare quali siano le installazioni di software autorizzate (ad esempio, gli aggiornamenti, patch di sicurezza, etc.) e quali vietati (ad esempio, software ad uso personale, etc.).

29 Controlli di rete

Dovrebbero essere implementati degli specifici controlli per garantire la sicurezza delle informazioni nelle reti. In particolare, dovrebbero essere considerati i seguenti elementi:

- dovrebbero essere stabilite le responsabilità e le procedure per la gestione delle apparecchiature di rete;
- dovrebbero essere stabiliti specifichi controlli, al fine di salvaguardare la riservatezza e l'integrità dei dati che passano nelle reti pubbliche o su reti wireless;
- i sistemi sulla rete devono essere autenticati;
- i sistemi di connessione alla rete devono essere limitati.

30 Messaggistica elettronica

La sicurezza delle informazioni per la messaggistica elettronica dovrebbe includere le seguenti misure:

- proteggere i messaggi da accesso non autorizzato;
- assicurare il corretto indirizzamento e il trasporto del messaggio;
- l'affidabilità e la disponibilità del servizio;
- considerazioni di ordine giuridico, ad esempio i requisiti per le firme elettroniche;
- ottenere l'approvazione prima di utilizzare i servizi pubblici esterni come l'instant messaging, social networking o la condivisione di file

31 Procedure per il controllo dei cambiamenti di sistema

Le procedure di controllo delle modifiche dovrebbero essere documentate e applicate per garantire l'integrità dei sistemi, applicazioni e prodotti, dalle fasi iniziali della progettazione fino alle manutenzioni successive. Tali procedure di controllo dovrebbero includere:

- il mantenimento di un registro dei livelli di autorizzazione concordati;
- identificazione di tutti i software, le informazioni, le entità di database e hardware che richiedano modifica;
- garantire che la documentazione di sistema venga aggiornata e che la vecchia documentazione sia archiviata o smaltita;
- il mantenimento di un controllo della versione per tutti gli aggiornamenti software;
- garantire che la documentazione operativa e le procedure utente vengano modificate se necessario al fine di essere sempre aggiornate;

- garantire che l'attuazione delle modifiche avvenga al momento giusto e non disturbi i processi aziendali coinvolti.

32 Limitazioni ai cambiamenti dei pacchetti software

Per quanto possibile e praticabile, i pacchetti software forniti dal produttore dovrebbero essere utilizzati senza alcuna modifica. Quando un pacchetto software deve essere modificato, dovrebbero essere considerati i seguenti punti:

- consenso del venditore;
- la possibilità di ottenere le modifiche necessarie dal fornitore stesso, come gli aggiornamenti del programma standard;
- l'impatto qualora l'organizzazione diventi responsabile della futura manutenzione del software;
- la compatibilità con altri software in uso.

33 Sviluppo affidato all'esterno

Qualora lo sviluppo software sia in outsourcing, dovrebbero essere considerati i seguenti aspetti:

- accordi di licenza, proprietà del codice e diritti di proprietà intellettuale;
- requisiti contrattuali per la progettazione sicura, sviluppo e test;
- test di accettazione;
- fornitura casi di test;
- diritto contrattuale di controllare i processi di sviluppo e dei controlli.

34 Gestione degli incidenti relativi alla sicurezza delle informazioni

Si deve prevedere un processo di gestione degli incidenti di sicurezza delle informazioni con le seguenti caratteristiche:

- chiara definizione delle responsabilità di gestione degli incidenti;
- stabilire un processo formale dalla rilevazione dell'incidente fino alla risoluzione dello stesso;
- prevedere una tracciatura sistematica degli incidenti.

35 Aspetti relativi alla sicurezza delle informazioni nella gestione della continuità operativa

Dovrebbero essere definiti e implementati:

- una struttura di gestione adeguata al fine di mitigare e rispondere ad un evento dirompente;
- procedure documentate di piani di risposta e di recupero, in cui è specificato in che modo l'organizzazione gestirà un evento dirompente e manterrà la sicurezza delle informazioni a un livello predeterminato.

Secondo le esigenze di continuità di sicurezza delle informazioni, l'organizzazione deve stabilire, documentare, attuare e mantenere:

- i controlli di sicurezza delle informazioni all'interno di business continuity o di disaster recovery;
- i processi, le procedure e i controlli di sicurezza delle informazioni esistenti durante una situazione avversa;
- prove periodiche circa l'efficienza del sistema di business continuity o di disaster recovery implementato.

MODULO DI ESERCIZIO DEI DIRITTI DEGLI INTERESSATI

(ai sensi degli artt. 15-22 del GDPR 2016/679)

Spett.le

Federazione Italiana Sport Equestri

OGGETTO: ESERCIZIO DI DIRITTI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI (artt. 15-22 del Regolamento UE 2016/679)

Il/La Sottoscritto/a .....
nato/a ..... il .....
residente a .....
in Via/Piazza ..... n. ..... cap ..... prov …….....,
in qualità di (barrare solo la casella di interesse)

- □ soggetto interessato .....
- □ genitore del minore (inserire nominativo) .....

con la presente richiesta esercita i suoi diritti di cui agli artt. 15-22 del Reg. UE 2016/679 in materia di protezione dei dati personali (di seguito GDPR).

Tipologia di interessato (barrare solo le caselle di interesse):

- □ tesserato
- □ dipendente
- □ fornitore
- □ utente

Richiesta di accesso ai dati personali (art. 15 del GDPR)
Il/La Sottoscritto/a intende accedere ai dati che lo/la riguardano e, precisamente, chiede di avere:

- □ la conferma che sia o meno in corso un trattamento di dati personali che lo/la riguardino;
- □ l'accesso ai dati propri dati personali trattati;
- □ le informazioni relative a:
  - □ le finalità e le modalità del trattamento;
  - □ le categorie di dati personali in questione;
  - □ i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, nonché gli estremi identificativi di chi tratta i dati;
  - □ il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

□ l’origine dei dati qualora gli stessi non siano stati raccolti presso l'interessato; o l'esistenza di un processo decisionale automatizzato, ivi compresa la profilazione.

La presente richiesta riguarda (indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento): .....
.....
.....

Richiesta di intervento sui dati (artt. 16-21 del GDPR)

Il/La sottoscritto/a richiede di effettuare le seguenti operazioni (barrare solo le caselle di interesse):

□ rettificazione/integrazione dei dati;
□ cancellazione dei dati personali soggetti al trattamento;
□ limitazione del trattamento;
□ trasferimento dei dati personali (portabilità), ovvero:
  □ ottenere la restituzione dei propri dati forniti su un formato strutturato
  □ ottenere la trasmissione diretta dei dati ad un altro Titolare del trattamento (indicare nominativo del Titolare destinatario.....).

La presente richiesta riguarda (indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento):

.....
.....
.....

Richiesta di opposizione al trattamento (artt. 21-22 del GDPR)
Il/La sottoscritto/a si oppone al trattamento dei dati (barrare solo le caselle di interesse):

- □ che comporti delle decisioni basate unicamente sul trattamento automatizzato, compresa la profilazione, la quale produce effetti giuridici che mi riguardino e che incidono in maniera analoga significativamente sulla mia persona;
- □ effettuato per ricerca scientifica o storica o a fini statistici a norma dell’art. 89 par.1 GDPR ed in particolare al seguente settore della ricerca_____;
- □ effettuato per il perseguimento di un interesse pubblico o per il perseguimento del legittimo interesse del Titolare ai sensi dell’art. 6 par. 1 lett. e) e f) GDPR.

La presente richiesta riguarda (indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento):

….....
.....
.....

Il/La sottoscritto/a si riserva il diritto di proporre reclamo a un'Autorità di controllo, nonché di proporre qualsiasi altro ricorso giurisdizionale e amministrativo innanzi all'Autorità giudiziaria competente (artt. 77-80 GDPR).

Recapito per la risposta:

- Indirizzo postale: Via/Piazza.....n. .....
Comune..... CAP..... Provincia.....

oppure

- e-mail/PEC: .....

Eventuali precisazioni:

Il/La sottoscritto/a precisa (fornire eventuali spiegazioni utili o indicare eventuali documenti allegati):
.....
.....
.....
.....

Estremi di un documento d'identità in corso di validità (allegare copia fronte e retro del documento):

tipologia di documento ..... n. .....

Luogo e data

Firma leggibile

INFORMATIVA TESSERAMENTO

Gentile Signora/Egregio Signore,

La Federazione Italiana Sport Equestri – FISE - Le fornisce, ai sensi del Regolamento UE 2016/679 (di seguito, GDPR) e del D.Lgs 196/2003 nel testo vigente (Codice Privacy), le informazioni di seguito riportate relative al trattamento dei dati personali che La riguardano e di cui la Federazione entrerà in possesso all'atto del Suo tesseramento.
I dati personali da Lei forniti formeranno oggetto di trattamento nel rispetto della menzionata normativa.
Dato personale è qualunque informazione che possa essere associata alla Sua persona e che quindi La riguarda.

1. Chi è il Titolare del trattamento dei Suoi dati personali?

Il Titolare del trattamento dei Suoi dati è FISE con sede legale in, ……Tel. ……., Fax: …….., codice fiscale …….. e-mail…….

2. Perché leggere questa informativa?

L'informativa è una comunicazione rivolta all'interessato che ha lo scopo di informarlo sulle finalità e le modalità dei trattamenti operati dal Titolare del trattamento.
Nei casi in cui il trattamento dei Suoi dati personali si renda necessario per adempiere un obbligo legale al quale è soggetto il Titolare del trattamento, o per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, il Titolare rilascia comunque l'informativa ai sensi degli artt. 13 ss. del GDPR al fine di assicurarne la trasparenza e correttezza dei trattamenti. Nei casi invece in cui il trattamento dei dati personali che La riguardano sia lecito solo previo consenso, il rilascio dell'informativa è requisito indispensabile per l'acquisizione del relativo consenso.
Maggiori informazioni possono essere comunque reperite sul sito www.fise.it.

3. Le informazioni acquisite per quali finalità verranno utilizzate?

All'atto del Suo tesseramento Lei entra a far parte dell'Ordinamento Sportivo, e più precisamente di una specifica Federazione Sportiva Nazionale (FISE) dallo stesso riconosciuta, divenendo soggetto di tutti i diritti e gli obblighi previsti dai Regolamenti federali, nazionali e internazionali.
Il vincolo instaurato con FISE all'atto del Suo tesseramento comporta, fra gli altri, l'obbligo di una condotta conforme ai principi di lealtà e probità sportiva e l'obbligo dell'osservanza delle norme regolamentari interne e internazionali in materia di doping.
FISE utilizzerà i Suoi dati per perseguire i propri fini istituzionali o ad esse strumentali, e quindi:

A. per verificare l'esistenza delle condizioni per il suo tesseramento e per la gestione del rapporto instaurato con il tesseramento, l'erogazione dei servizi previsti, l'esecuzione delle attività correlate o accessorie alla fornitura dei servizi richiesti dal tesserato e, in generale, per dare adempimento a tutti gli obblighi previsti dall'ordinamento sportivo e inerenti il nuovo o rinnovato rapporto di tesseramento;
B. vigilare sulla regolarità di eventi e attività sportive in ottemperanza ai Regolamenti federali comunitari e internazionali, anche per quanto attiene alla tutela della salute e all'utilizzo di sostanze che alterino le naturali prestazioni fisiche degli atleti nelle attività sportive, anche in cooperazione e d'intesa con le Autorità o gli Organismi nazionali comunitari e internazionali competenti, comunicando i dati personali raccolti come prescritto dalle disposizioni vigenti in materia di doping;
C. per tutto quanto concerne l'organizzazione e la gestione delle competizioni e manifestazioni sportive e/o degli eventi sportivi regionali, nazionali e internazionali e per l'adempimento di ogni connesso obbligo o attività (es. produzione, conservazione e utilizzazione di filmati, fotografie e immagini, notizie di risultati, collocamenti e/o premi);
D. per la gestione dei processi della Giustizia sportiva;
E. per mantenere i rapporti con confederazioni e federazioni di appartenenza (Comitato Italiano Nazionale Olimpico – CONI - Federation Equestre Internazionale – FEI – Comitato Olimpico Internazionale - CIO), nonché con ogni altra Autorità o ente, nazionale o internazionale, deputato al controllo della regolarità delle competizioni e delle posizioni dei tesserati e della loro salute, inclusi i controlli antidoping (*National Antidoping Organization* – NADO - *World Anti-Doping Agency* - WADA);
F. l'invio di comunicazioni e informative istituzionali.

4. Cosa consente a FISE di trattare i dati che La riguardano?

Lo sport è una attività di interesse pubblico e FISE nelle attività comunque connesse con il Suo tesseramento opera nel perseguomento dell'interesse pubblico. Questo, ai sensi artt. 6, paragrafo 1, lett. e) e 9, paragrafo 1, lett. g) del GDPR consente di trattare i Suoi dati anche appartenenti a particolari categorie come quelli idonei a rivelare il Suo stato di salute di cui FISE potrebbe entrare in possesso ad esempio quando valuta la Sua idoneità all'attività agonistica ovvero qualora Lei ci fornisca tali dati in adempimento alle procedure antidoping.

In alcuni casi, nel corso del rapporto di tesseramento e per determinate finalità potrebbe essere richiesto il suo consenso al trattamento, ma in quel caso riceverà una informativa specifica relativa a quel singolo trattamento.

5. Cosa succede nel caso in cui Lei dovesse negare il conferimento dei Suoi dati?

Il conferimento delle informazioni di cui sopra ha carattere obbligatorio ai fini della Sua partecipazione all'attività sportiva. Se Lei decidesse di non conferire i necessari dati che La riguardano, FISE non potrà procedere al Suo tesseramento e Lei non potrà esercitare le facoltà e i diritti che ne derivano.

6. Come vengono trattati i dati che La riguardano?

I dati che La riguardano sono sottoposti a diverse operazioni, che si rendono necessarie per perseguire le finalità istituzionali esposte in precedenza. Tutte queste operazioni vengono effettuate da personale appositamente incaricato, con strumenti informatici e mediante la lavorazione di documenti cartacei. I nostri archivi informatici sono protetti dalle intrusioni e sono accessibili solo a determinate persone incaricate di trattare i dati, in ragione delle attività lavorative che competono loro. Anche gli archivi cartacei sono accessibili solo a chi ha una valida ragione giuridica per trattare i Suoi dati. In alcuni casi, quando per le finalità perseguite da FISE non è necessario che lei sia identificato o identificabile i suoi dati vengono sottoposti a procedure di anonimizzazione e psedonimizzazione.

FISE ha adottato un proprio regolamento interno in materia di protezione dei dati reperibile sul sito www.fise.it

Per quanto riguarda le attività connesse al contrasto e alla repressione del doping umano FISE adotta, per quanto compatibili, anche gli Satndard Internazionali elaborati dalla World AntDoping Agency reperibili sul sito www.fise.it.

7. A chi potranno essere comunicate le Sue informazioni?

All'interno e all'esterno di FISE sono autorizzati ad effettuare operazioni di trattamento dei sui Suoi dati personali, secondo i principi di necessità, correttezza e liceità, solo soggetti espressamente incaricati. Questo significa che solo chi ha necessita dei Suoi dati per svolgere il suo lavoro potrà accedervi.

Oltre che da personale della Federazione appositamente autorizzato al trattamento, i Suoi dati acquisiti potranno essere trattati, conosciuti e comunicati, per le finalità sopra esposte, anche a Responsabili del trattamento eventualmente designati ai sensi dell'art. 28 del GDPR, il cui elenco è disponibile sul sito www.fise.it.

I suoi dati possono essere comunicati anche soggetti esterni alla Federazione operanti quali Titolari autonomi (es. Comitato Italiano Nazionale Olimpico – CONI) qualora questi abbiano titolo e responsabilità a riceverli in base alle regole proprie dell'ordinamento sportivo.

Relativamente alla finalità di controllo della regolarità sanitaria della posizione dei tesserati i Suoi dati sono trasferiti agli enti nazionali e internazionali a ciò deputati dalla normativa vigente (CONI, NADO, WADA)

I Suoi dati possono essere trasferiti all'estero, in occasione di manifestazioni europee o internazionali o per l'esecuzione dei rapporti con la Federazione internazionale di riferimento (Federation Equestre Internazionale – FEI) o con altre Federazioni sportive straniere.

Le ricordiamo che il trasferimento dei dati verso organizzazioni internazionali e verso paesi extraeuropei sebbene sia consentito a FISE nel perseguimento dell'interesse pubblico (art. 49, paragrafo 1, lett. d), del GDPR) può sottoporre i suoi diritti e le sue libertà connesse ai dati trasferiti ad un rischio elevato.

Le ricordiamo poi che FISE, in quanto esercente pubbliche funzioni è soggetta alla disciplina dell'accesso agli atti e all'accesso civico generalizzato. Ove possibile, i documenti verranno forniti in forma anonima, ma potrebbero esserci casi in cui il prevalente interesse di un terzo gli consenta di accedere ai Suoi dati personali.

Le ricordiamo infine che le sentenze emesse dagli organi di Giustizia sportiva sono soggetti a pubblicazione sul sito www.fise.it e sono accessibili a chiunque. Lei può però fare tuttavia istanza all'Organismo giudicante perché vengano emanate particolari misure di protezione dei suoi dati.

Nei casi previsti dalla legge, dai regolamenti e dalle norme statutarie, i Suoi dati potrebbero essere soggetti a pubblicazione sul sito web www.fise.it o in altro materiale illustrativo e divulgativo. Ove possibile i dati verranno pubblicati in modalità aggregata o in altra forma anonima. In occasione di manifestazioni sportive possono essere pubblicati sul sito web di FISE anche i risultati sportivi e l'ammontare dei premi vinti.

8. Le informazioni acquisite per quanto tempo verranno conservate?

I Suoi dati vengono conservati per un periodo di 10 anni dalla cessazione del Suo tesseramento a FISE o comunque fino allo spirare del termine di prescrizione relativo ai diritti connessi.
Ci sono dati che la legge ci obbliga a tenere per un periodo indeterminato come nel caso degli atti pubblici e dei provvedimenti amministrativi.

9. Quali sono i diritti che può esercitare?

Rispetto ai dati che La riguardano, Le sono riconosciuti diversi diritti.
Diritto di accesso: Lei ha il diritto di ottenere informazioni circa i trattamenti che La riguardano; Diritto di rettifica e di integrazione: Lei ha il diritto di ottenere la rettifica dei dati personali inesatti. Diritto alla portabilità dei dati personali: Lei ha il diritto di ricevere i dati personali che La riguardano o di trasmettere suddetti dati ad altro titolare. Diritto alla limitazione: Lei ha diritto di chiederci la limitazione dei trattamenti in corso. Diritto a proporre reclamo all'Autorità di controllo: Lei può proporre reclamo al Garante per la protezione dei dati personali per lamentare una violazione della disciplina in materia di protezione dei dati personali.

10. Chi è il Responsabile della protezione dei dati?

FISE ha nominato un Responsabile della protezione dei dati che ha funzioni di supporto e di vigilanza sull'applicazione delle regole sulla privacy e a cui Lei potrà rivolgersi in caso in cui ritenga siano state violati o negati i suoi diritti.
Il Responsabile della protezione dei dati può essere contattato al seguente indirizzo e-mail dpo@fise.it

11. Dove può reperire maggiori informazioni?

Maggiori informazioni sono reperibili sul sito internet www.fise.it

APPENDICE B
Procedura ordinaria di esecuzione di una valutazione di impatto e di rischio – DPIA

La DPIA è un processo dinamico e continuo, finalizzato ad identificare e minimizzare i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei dati personali degli individui interessati dal rilascio di un nuovo progetto, soluzione o regola (i.e. di processo/procedura), assicurando che le criticità potenziali siano identificate, già in fase iniziale.
La DPIA è strutturata in fasi che hanno un ciclo ricorsivo, come di seguito descritto nel presente documento, dalla valutazione preliminare della necessità od opportunità per una DPIA, con definizione della proporzionalità di intervento e dimensionamento di strumenti e risorse necessari, alla identificazione dei rischi e individuazione delle soluzioni e misure per gestire i rischi stessi (*risk assessment* e *risk management*) al fine di ridurre l'impatto ad un livello accettabile.
La metodologia della DPIA permette a ogni Titolare del trattamento di individuare e gestire i rischi e le problematiche in tema di trattamento dati, adottare le misure tecniche ed organizzative adeguate, nonché tracciare e documentare il processo decisionale attraverso la registrazione dei risultati, anche per il tramite di un *report* finale.

1. Valutazione preliminare

In linea con l'approccio basato sul rischio, il *Data Manager*, se nominato, ovvero l'Incaricato che governa il Dipartimento o l'Ufficio che esegue in maniera prevalente le attività di trattamento, deve consultarsi, fin dalle fasi iniziali della progettazione, con il DPO per verificare se questo *"può presentare un rischio elevato per i diritti e le libertà delle persone fisiche"* e deve essere, quindi, sottoposto a DPIA.
Ciò può avvenire, ad esempio, nei seguenti casi:

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione;
b) il trattamento, su larga scala, di categorie particolari e sensibili;
c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico;
d) monitoraggio sistematico;

e) *match* o combinazione di *database* e/o di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale;
f) dati relativi a persone vulnerabili (es. minori);
g) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;
h) trattamenti valutativi o di scoring;
i) trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

2. La valutazione del contesto

L'analisi preliminare implica una valutazione del contesto interno ed esterno al Titolare.

3. Valutare il contesto esterno

La valutazione del contesto esterno della F.I.S.E. prende in considerazione i seguenti fattori:

1. contesto settoriale;
2. contesto normativo;
3. contesto tecnologico;
4. contesto socioeconomico
5. contesto territoriale;

TABELLA DEI FATTORI DI VALUTAZIONE DEL CONTESTO ESTERNO	
Contesto settoriale	Valutazione degli aspetti inerenti siano essi clienti, soci, fornitori o *competitor*.
Contesto normativo	Valutazione dell'applicabilità di normative, incluse specifiche normative di settore, applicabili alla F.I.S.E. in materia di protezione dei dati personali.
Contesto tecnologico	Valutazione dell'andamento di minacce e vulnerabilità inerenti all'utilizzo dei sistemi informatici per il trattamento dei Dati personali
Contesto socioeconomico	Valutazione del valore intrinseco dei dati personali trattati dalla F.I.S.E. e potenziali minacce.
Contesto territoriale	Valutazione delle caratteristiche del contesto territoriale esterno alla sede della F.I.S.E. e del relativo impatto sulla protezione dei dati personali.

4. Valutare il contesto interno

La valutazione del contesto interno della F.I.S.E. prende in considerazione i seguenti fattori:

1. Contesto legale;
2. Contesto organizzativo e delle risorse umane;
3. Contesto IT;
4. Contesto Fisico e Ambientale

TABELLA DEI FATTORI DI VALUTAZIONE DEL CONTESTO INTERNO	
Contesto Legale	Valutazione profili giuridici e di responsabilità della F.I.S.E.
Contesto Organizzativo e delle Risorse Umane	Valutazione del modello organizzativo e delle risorse umane mediante cui è effettuato il trattamento dei dati personali
Contesto IT	Valutazione dei servizi IT, della relativa infrastruttura e dei sistemi mediante cui è effettuato il trattamento dei dati personali e relative misure di sicurezza
Contesto Fisico e Ambientale	Valutazione dei siti fisici (sedi, centrali) e delle caratteristiche ambientali

5. Report preliminare

La valutazione del contesto di riferimento per la protezione dei dati personali è riportata nel documento "Valutazione preliminare del Contesto di Rischio". Qualora da questa valutazione preliminare emerga la necessità di eseguire una DPIA dovrà essere eseguito secondo la presente procedura, salvo che la tipologia del trattamento, su indicazione del DPO, non richieda un approccio diverso.

6. Chi è coinvolto nel processo di DPIA

Per permettere una corretta applicazione della metodologia del *risk* e *privacy assessment* e *risk management*, l'attività di DPIA deve essere effettuata da parte del *Data manager* o, in mancanza, dell'Incaricato apicale dell'Ufficio della F.I.S.E. che, in maniera prevalente, gestisce le attività di trattamento nell'ambito della Federazione.

Il processo di DPIA deve coinvolgere, oltre al DPO, tutti i soggetti, anche esterni (Responsabile e Contitolari), che compiono operazioni di trattamento nell'ambito del trattamento soggetto a valutazione. Sono di regola coinvolte anche le funzioni trasversali, come il Responsabile di sistema IT ed, eventualmente, l'*Internal audit* e ogni altra funzione che subisca un impatto dal trattamento, anche se non partecipa materialmente alle attività di trattamento.

Le informazioni complessive relative al trattamento e alla sua finalità devono essere messe a disposizione di tutti i soggetti coinvolti fin dal principio, in modo da fargli acquisire tutti gli elementi necessari per una prima comprensione degli impatti potenziali e dei passi che potrebbero essere richiesti per procedere con le attività di *assessment*.

7. Come condurre una DPIA e la relativa reportistica

Il processo di DPIA deve essere condotto al fine di effettuare una valutazione approfondita dei rischi e dei relativi impatti di ogni trattamento dati. In particolare, la valutazione deve riguardare i seguenti elementi:

i. Descrizione del trattamento, che specifichi natura, oggetto, contesto, finalità del trattamento;
ii. Categorie di dati personali trattati;
iii. Natura dei dati personali trattati;
iv. Necessità e proporzionalità dei trattamenti in relazione alle finalità (con conseguente esame ad es. della liceità del trattamento, della minimizzazione del trattamento e del rispetto delle finalità oggetto di informative);
v. Rischio per la sicurezza dei dati;
vi. Rischi per i diritti e le libertà degli interessati;
vii. Misure organizzative in essere per mitigare i rischi;
viii. Misure tecniche in essere per mitigare i rischi.

8. Valutazione del rischio

Il rischio misura la probabilità di accadimento di un evento avverso che comporti in modo accidentale o illecito la distruzione, la perdita, la modifica, la divulgazione o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati da e per conto della Federazione.
La verifica del rischio può essere effettuata con diverse indagini:

a) somministrazione di questionari ai soggetti coinvolti nel trattamento o che subiscono un impatto dal trattamento;
b) valutazione di eventi pregressi verificati nell'ambito di trattamenti similari o che comportano in tutto o in parte le medesime attività di trattamento;
c) valutazioni compiute in letteratura o da studi indipendenti su attività implicate nel trattamento;

d) valutazioni di rischiosità dell'attività compiuta dalla normativa e valutazione generale del contesto normativo;
e) valutazione tecnica sugli applicativi informatici;
f) valutazione dell'integrità degli archivi cartacei;
g) valutazione dei valori economici coinvolti nel trattamento sia per la F.I.S.E. sia per terze parti;
h) valutazione della quantità dei dati trasferiti a terze parti e numero delle terze parti destinatarie;
i) trasferimento dei dati verso paesi che non diano adeguate garanzie sulla protezione dei dati;
j) ogni altra verifica che sia ritenuta possibile e opportuna al fine di accertare la probabilità di un evento.

La ponderazione di questi elementi deve restituire una valutazione oggettiva - in termini possibilmente numerici - che consentano di porli con criteri oggettivi e riscontrabili in una matrice di rischio costruita su 4 livelli:

1. MOLTO ALTO;
2. ALTO;
3. MEDIO;
4. BASSO.

8. Valutazione di impatto

Per ciascun trattamento soggetto a DPIA deve essere effettuata la valutazione di impatto sui diritti e le libertà individuali quali:

- furto o usurpazione identità;
- perdita economica;
- pregiudizio alla reputazione;
- danno morale (anche mediante scoperta di notizie non richieste);
- danno esistenziale;
- danno alla salute (compreso equilibrio psicologico);
- violazione, anche indiretta, del segreto professionale;
- privazione dei diritti di libertà (di associazione, di manifestazione del pensiero, di religione ecc.);
- impedimento all'esercizio del controllo sui propri dati.

Sulla base del numero o della qualità dei diritti limitati o compromessi la valutazione di impatto deve restituire una valutazione oggettiva - in termini possibilmente numerici - che consentano di porli con criteri oggettivi e riscontrabili in una matrice di impatto costruita su 4 livelli:

1. MOLTO ALTO;
2. ALTO;
3. MEDIO;
4. BASSO.

9 Valutazione di impatto e di rischio

Le matrici di rischio e di impatto vanno combinate secondo una matrice di rischio finale definita, secondo la quale per ogni scenario di rischio e impatto analizzato è stato determinato il Livello di Rischio Finale sulla sicurezza dei dati e d'Impatto sulle libertà individuali sulla base del seguente algoritmo:

LIVELLO DI RISCHIO DI UNO SCENARIO = LIVELLO DI VEROSIMIGLIANZA * LIVELLO DI IMPATTO

TABELLA DI ANALISI DEL LIVELLO DI RISCHIO FINALE						
LIVELLO DI VEROSIMIGLIANZA			LIVELLO DI IMPATTO			
			Basso	Medio	Alto	Molto Alto
			1	2	3	4
Basso		1	1	2	3	4
Medio		2	2	4	6	8
Alto		3	3	6	9	12
Molto Alto		4	4	8	12	16

I rischi potenziali di valore superiore 6 non sono accettabili e devono essere mitigati.

10. Mitigazione del rischio

A seguito della valutazione di rischio potenziale, devono essere identificate le misure idonee per ridurre probabilità e impatti individuando:

a) le attività e le soluzioni per la sicurezza dei dati;
b) le attività e le soluzioni per la protezione dei dati.

Queste devono comprendere:

A] Misure e controlli di tipo organizzativo, quali ad esempio:

a) Organizzazione e *governance*: specifici ruoli e responsabilità all'interno dell'organizzazione, controlli interni di supervisione, *governance* dei progetti, regole di interazione e le rispettive responsabilità in caso di contitolarità di un trattamento;
b) Processi: procedure e policy interne per la gestione dei rischi, degli incidenti, delle modifiche;
c) Garanzie: assunzione di garanzie e impegni ad azioni determinate da terze parti mediante atti giuridicamente vincolanti;
d) Formazione e consapevolezza: formazione adeguata del personale e consapevolezza dei potenziali rischi, selezione degli incaricati in base a qualifiche e competenze dimostrabili, guide operative per il personale su come usare i nuovi sistemi e su come condividere i dati quando necessario, materiale informativo per gli utenti, misure che consentano agli interessati di accedere alle proprie informazioni e al tempo stesso che rendano gli interessati consapevoli di come sono protette le proprie informazioni, di prevedere canali con cui gli utenti possano contattare l'organizzazione in caso di necessità di assistenza e con cui le organizzazioni possano rispondere alle richieste di accesso da parte degli interessati.

B] Misure e controlli di tipo tecnologico, come, ad esempio:

a) tenere aggiornato il software, la configurazione delle reti e dei sistemi informatici;
b) assicurare l'efficienza degli impianti e dei dispositivi;
c) disattivare i servizi di sistema non necessari;
d) dismettere i servizi o il software non usati o comunque obsoleti;
e) memorizzare le password in registri di sistema protetti e non accessibili dagli utenti;
f) prevedere meccanismi di autenticazione robusta;
g) accertare l'appropriatezza dei siti in base al trattamento previsto dei dati
h) modificare i settaggi e le credenziali di default;
i) eseguire test di vulnerabilità o di stress dei sistemi;
j) neutralizzare vulnerabilità note;
k) configurare servizi di trasmissione o di comunicazione protetti;

C] Misure e controlli sui dati e sugli archivi, come, ad esempio:

a) decidere di non raccogliere o memorizzare specifici tipi di informazioni se non necessarie;
b) definire periodi di conservazione mirati allo stretto tempo necessario per poi prevedere la distruzione;
c) dare garanzia della qualità dei dati;
d) eseguire i backup, partizionare gli archivi dei dati;
e) controllare gli accessi logici;
f) assicurare la possibilità di de-indicizzazione dei dati quando richiesto;

D] Misure di protezione - Azioni dirette sui dati

a) Anonimizzazione: rimozione o mascheratura delle informazioni personali quando non necessarie;
b) Pseudonimizzazione: sostituzione dei riferimenti personali con identificatori finti e garanzia che le informazioni aggiuntive per l'attribuzione dei dati personali ad uno specifico Interessato siano conservate in metadati separati
c) Cifratura dei dati, dei messaggi o degli archivi: soluzioni atte a rendere incomprensibili i dati acceduti tranne ai soli autorizzati che possiedono la chiave di decifratura.
d) Misure e controlli di sicurezza fisica, come, ad esempio sui supporti cartacei, sugli accessi fisici, sulla sicurezza degli impianti, dell'hardware e dei macchinari, protezione da fonti di rischio non umane etc.

E] Reintrodurre misure di protezione "*by default*"

11. Esiti della DPIA

Gli esiti della valutazione devono essere formalizzati in un report finale *"Risk & Privacy Impact Assessment",* secondo quanto previsto dalle *Policies* interne della F.I.S.E..

DECISIONE DELLA COMISSIONE

del 27 dicembre 2004

che modifica la decisione 2001/497/CE per quanto riguarda l'introduzione di un insieme alternativo di clausole contrattuali tipo per il trasferimento di dati personali a paesi terzi

[notificata con il numero C(2004) 5271]

(Testo rilevante ai fini del SEE)

(2004/915/CE)

LA COMMISSIONE DELLE COMUNITÀ EUROPEE,

visto il trattato che istituisce la Comunità europea,

vista la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati [1], e in particolare l'articolo 26, paragrafo 4,

considerando quanto segue:

(1) Al fine di facilitare i flussi di dati provenienti dalla Comunità, è opportuno che i responsabili del trattamento di dati siano in grado di realizzare trasferimenti di dati su scala mondiale attenendosi a un unico insieme di norme di protezione dei dati. In mancanza di una normativa internazionale in materia, le clausole contrattuali tipo costituiscono uno strumento estremamente utile, dal momento che consentono di trasferire dati personali provenienti da tutti gli Stati membri facendo riferimento ad un insieme comune di norme. La decisione 2001/497/CE della Commissione, del 15 giugno 2001, relativa alle clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi a norma della direttiva 95/46/CE [2] stabilisce un insieme modello di clausole contrattuali tipo che prevede garanzie adeguate per il trasferimento di dati verso paesi terzi.

(2) Dal momento dell'adozione di questa decisione si è acquisita una ricca esperienza. Inoltre, un consorzio di associazioni imprenditoriali [3] ha presentato un insieme alternativo di clausole contrattuali, destinato ad offrire un livello di protezione di dati comparabile a quello offerto dall'insieme di clausole adottato nella decisione 2001/497/CE, pur utilizzando meccanismi diversi.

(3) Considerando che l'uso di clausole contrattuali tipo nei trasferimenti internazionali ha carattere volontario (questo tipo di clausole è solo una delle varie possibilità previste dalla direttiva 95/46/CE per il trasferimento legittimo di dati personali verso paesi terzi), gli esportatori di dati nella Comunità e gli importatori di dati in paesi terzi dovrebbero poter optare per uno degli insiemi di clausole contrattuali tipo o scegliere un altro fondamento giuridico per il trasferimento di dati. Tuttavia, dal momento che ciascun gruppo costituisce un insieme coerente, non deve essere riconosciuta agli esportatori la possibilità di modificare totalmente o parzialmente tali insiemi né di combinarli in alcun modo.

(4) Le clausole contrattuali tipo proposte dalle associazioni imprenditoriali hanno lo scopo di rafforzare l'uso di clausole contrattuali tra gli operatori, ad esempio rendendo flessibili i requisiti in materia di verifica o precisando le norme che disciplinano il diritto di accesso.

(5) D'altro canto, l'insieme che qui si presenta contiene, come alternativa al sistema di responsabilità solidale previsto dalla decisione 2001/497/CE, un regime di responsabilità basato sugli obblighi di normale diligenza, in virtù del quale l'esportatore e l'importatore di dati dovrebbero rispondere dinnanzi agli interessati per la violazione degli obblighi contrattuali. L'esportatore è inoltre responsabile se non compie sforzi ragionevoli al fine di determinare se l'importatore è in grado di rispettare i suoi obblighi giuridici derivati dalle clausole (culpa in eligendo), avendo l'interessato la possibilità a questo titolo di avviare azioni contro l'esportatore di dati. L'applicazione della lettera b) della clausola I del nuovo insieme di clausole contrattuali tipo riveste particolare importanza al riguardo, soprattutto considerando la possibilità riconosciuta all'esportatore di dati di effettuare verifiche degli impianti dell'importatore di dati o di esigere prove che dimostrino la disponibilità di risorse finanziarie sufficienti per far fronte alle sue responsabilità.

[1] GU L 281 del 23.11.95, pag. 31. Direttiva modificata dal regolamento (CE) n. 1883/2003 (GU L 284 del 31.10.2003, pag. 1).

[2] GU L 181 del 4.7.2001, pag. 19.

[3] Camera di commercio internazionale (ICC), Japan Business Council in Europe (JBCE), European Information and Communications Technology Association (EICTA), EU Committee of the American Chamber of Commerce in Belgium (Amcham), Confederation of British Industry (CBI), International Communication Round Table (ICRT) e Federation of European Direct Marketing Associations (FEDMA).

(6) Quanto all'esercizio dei diritti del terzo beneficiario da parte degli interessati, si prevede un maggior coinvolgimento dell'esportatore di dati nella risoluzione dei reclami degli interessati, essendo l'esportatore di dati obbligato a mettersi in contatto con l'importatore di dati se necessario ad eseguire il contratto entro il termine normale di un mese. Se l'esportatore di dati rifiuta di eseguire il contratto e persiste il mancato rispetto degli obblighi da parte dell'importatore, l'interessato potrà invocare le clausole contro l'importatore di dati ed infine avviare un'azione dinnanzi ai tribunali di uno Stato membro. Questa accettazione della giurisdizione e l'accordo di conformarsi alla decisione di un tribunale o di un'autorità di protezione di dati competenti non reca pregiudizio agli eventuali diritti processuali degli importatori di dati stabiliti in paesi terzi, ad esempio in materia di appello.

(7) Al fine tuttavia di evitare gli abusi cui potrebbe dare luogo questo regime più flessibile, è opportuno riconoscere alle autorità competenti per la protezione dei dati la facoltà di vietare o sospendere più facilmente i trasferimenti di dati basati sul nuovo insieme di clausole contrattuali tipo quando l'esportatore di dati rifiuti di adottare misure adeguate contro l'importatore di dati per fargli rispettare gli obblighi contrattuali o quest'ultimo rifiuti di collaborare in buona fede con le autorità di controllo competenti in materia di protezione dei dati.

(8) L'uso di clausole contrattuali tipo sarà fatto mantenendo salva l'applicazione delle disposizioni nazionali adottate in conformità con la direttiva 95/46/CE o con la direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) [1], in particolare per quanto riguarda l'invio di comunicazioni commerciali ai cittadini dell'UE.

(9) Su questa base, le garanzie contenute nelle clausole contrattuali tipo presentate possono essere considerate sufficienti nel senso dell'articolo 26, paragrafo 2, della direttiva 95/46/CE.

(10) Il gruppo per la tutela delle persone con riguardo al trattamento di dati personali, creato dall'articolo 29 della direttiva 95/46/CE, ha emesso un parere [2] sul livello di tutela che offrono le clausole contrattuali tipo qui presentate. Di tale parere si è tenuto debito conto.

(11) Al fine di valutare le modalità di applicazione degli emendamenti alla decisione 2001/497/CE, è opportuno che la Commissione effettui una valutazione tre anni dopo la loro notifica agli Stati membri.

(12) La decisione 2001/497/CE deve essere modificata in modo conforme.

(13) Le misure previste nella presente decisione sono conformi al parere del comitato creato dall'articolo 31 della direttiva 95/46/CE,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

La decisione 2001/497/CE è modificata come segue:

1) All'articolo 1 è aggiunto il seguente paragrafo:

«I responsabili del trattamento potranno optare per uno degli insiemi – I o II – contenuti nell'allegato. Tuttavia, non potranno modificare le clausole né combinare singole clausole, né gli insiemi.»

2) I paragrafi 2 e 3 dell'articolo 4 sono sostituiti dal testo seguente:

«2. Agli effetti del paragrafo 1, quando il responsabile del trattamento affermi l'esistenza di garanzie sufficienti derivate dalle clausole contrattuali tipo contenute nell'insieme II dell'allegato, le autorità competenti in materia di protezione dei dati potranno esercitare i poteri di cui dispongono per proibire o sospendere i flussi di dati in entrambi i seguenti casi:

a) se l'importatore di dati rifiuta di collaborare in buona fede con le autorità competenti in materia di protezione dei dati o di rispettare gli obblighi che gli incombono chiaramente in virtù del contratto;

b) se l'esportatore di dati, dopo aver ricevuto una notifica delle autorità competenti in materia di protezione dei dati, rifiuta di adottare misure adeguate contro l'importatore di dati per far rispettare il contratto entro il termine normale di un mese.

[1] GU L 201 del 31.7.2002, pag. 37.
[2] Parere 8/2003, disponibile al seguente indirizzo: http://europa.eu.int/comm/privacy.

Agli effetti del precedente paragrafo, il rifiuto di cooperazione in buona fede o di esecuzione del contratto da parte dell'importatore non comprende i casi in cui tale cooperazione o esecuzione confligga con gli obblighi imposti dalla legislazione nazionale applicabile all'importatore di dati che non vadano al di là dei limiti necessari in una società democratica per la salvaguardia degli interessi elencati al paragrafo 1 dell'articolo 13 della direttiva 95/46/CE, in particolare le sanzioni previste in strumenti nazionali e/o internazionali, gli obblighi di dichiarazione in materia fiscale o in materia di lotta contro il riciclaggio di denaro.

Agli effetti della lettera a) del primo paragrafo, la cooperazione potrà comprendere, in particolare, la messa a disposizione da parte dell'importatore delle sue installazioni per il trattamento di dati a fini di verifica o l'obbligo di conformarsi ai pareri dell'autorità di controllo della protezione di dati nella Comunità.

3. Il divieto o la sospensione ai sensi dei paragrafi 1 e 2 saranno soppressi non appena cesseranno di esistere i motivi del divieto o della sospensione.

4. Quando gli Stati membri adottano misure in conformità con i paragrafi 1, 2 e 3, ne informano immediatamente la Commissione, che trasmette l'informazione agli altri Stati membri.»

3) All'articolo 5 la prima frase è sostituita dalla seguente:

«La Commissione valuterà le modalità di applicazione della presente decisione sulla base delle informazioni disponibili tre anni dopo la sua notifica e dopo la notifica degli eventuali emendamenti agli Stati membri.»

4) L'allegato è modificato come segue:

1. dopo il titolo, viene inserita l'espressione «INSIEME I»;

2. è inserito il testo contenuto nell'allegato alla presente decisione.

Articolo 2

La presente decisione è applicabile a decorrere dal 1° aprile 2005.

Articolo 3

Gli Stati membri sono destinatari della presente decisione.

Fatto a Bruxelles, il 27 dicembre 2004.

Per la Commissione
Charlie McCREEVY
Membro della Commissione

ALLEGATO

«INSIEME II

Clausole contrattuali tipo per il trasferimento di dati personali dalla Comunità verso paesi terzi (trasferimento da responsabile a responsabile del trattamento)

Accordo di trasferimento di dati

tra

_____ (nome)

_____ (indirizzo e paese di stabilimento)

(d'ora in poi "l'esportatore di dati")

e

_____ (nome)

_____ (indirizzo e paese di stabilimento)

(d'ora in poi "l'importatore di dati"),

ciascuno denominato una "parte", insieme "le parti".

Definizioni

Ai fini delle presenti clausole:

a) "dati personali", "speciali categorie di dati/dati sensibili", "trattamento", "responsabile del trattamento", "incaricato del trattamento", "interessato" e "autorità di controllo/autorità" avranno lo stesso significato indicato nella direttiva 95/46/CE (di conseguenza, si intenderà per "autorità" l'autorità competente in materia di protezione dei dati nel territorio di stabilimento dell'esportatore di dati);

b) per "esportatore di dati" si intende il responsabile del trattamento che trasferisce i dati personali;

c) per "importatore di dati" si intende il responsabile del trattamento che accetta di ricevere dall'esportatore dati personali per un ulteriore trattamento in conformità con i termini delle presenti clausole e che non è soggetto al sistema di un paese terzo in grado di garantire un'adeguata protezione;

d) per "clausole" si intendono le presenti clausole contrattuali, che costituiscono un documento indipendente che non integra condizioni commerciali stabilite dalle parti in virtù di altri accordi commerciali.

I dettagli del trasferimento (così come i dati personali trasferiti) sono specificati nell'allegato B, che costituisce parte integrante delle presenti clausole.

I. Obblighi dell'esportatore di dati

L'esportatore di dati garantisce e si impegna rispetto a quanto segue:

a) i dati personali sono stati raccolti, trattati e trasferiti in conformità con la legislazione applicabile all'esportatore di dati;

b) l'esportatore ha compiuto ragionevoli sforzi per determinare che l'importatore di dati sia in grado di rispettare gli obblighi giuridici ai quali è tenuto in virtù delle presenti clausole;

c) l'esportatore fornirà all'importatore di dati, se richiesto, copie della legislazione relativa alla protezione di dati del paese in cui è stabilito l'esportatore di dati o i riferimenti a tale legislazione (ove opportuno, ed escludendo la consulenza giuridica);

d) l'esportatore risponderà alle richieste degli interessati e delle autorità relative al trattamento dei dati personali da parte dell'importatore di dati, a meno che le parti non abbiano concordato che sia l'importatore a rispondere a tali richieste. Anche in questo caso, sarà l'esportatore a rispondere, secondo quanto ragionevolmente possibile e a partire dalle informazioni di cui possa ragionevolmente disporre, se l'importatore di dati non è in grado di rispondere o non è disposto a farlo. Le risposte dovranno essere fornite entro un termine ragionevole;

e) l'esportatore metterà a disposizione degli interessati che siano terzi beneficiari ai sensi della clausola III, previa loro richiesta, una copia delle presenti clausole, a meno che esse contengano informazioni confidenziali, nel qual caso è autorizzato a espungere tali informazioni. Nel caso in cui alcune informazioni siano espunte, l'esportatore di dati informerà per iscritto gli interessati del motivo dell'espunzione e del loro diritto di portare tale espunzione a conoscenza delle autorità. L'esportatore di dati dovrà tuttavia accettare qualunque decisione dell'autorità relativa all'accesso al testo completo delle clausole da parte degli interessati, purché questi ultimi abbiano accettato di rispettare la confidenzialità delle informazioni confidenziali espunte. L'esportatore di dati fornirà all'autorità, previa sua richiesta, una copia delle presenti clausole.

II. Obblighi dell'importatore di dati

L'importatore di dati garantisce e si impegna rispetto a quanto segue:

a) l'importatore attuerà le misure tecniche e organizzative necessarie a proteggere i dati personali contro una distruzione accidentale o illecita o la perdita accidentale, l'alterazione, la divulgazione o l'accesso di soggetti non autorizzati, e a garantire il livello di sicurezza adeguato ai rischi che comportano il trattamento e alla natura dei dati che devono essere protetti;

b) l'importatore avrà messo a punto procedure atte a garantire che qualsiasi terzo cui consenta di accedere ai dati personali, compresi gli incaricati del trattamento, rispetti e mantenga la confidenzialità e la sicurezza dei dati personali. Nessuna persona che operi sotto l'autorità dell'importatore di dati, compresi gli incaricati del trattamento, potrà trattare i dati personali a meno che non abbia ricevuto istruzioni dall'importatore di dati. Questa disposizione non si applica alle persone autorizzate o tenute ad accedere ai dati personali in base alle leggi o ai regolamenti;

c) l'importatore non ha motivo di ritenere, al momento di sottoscrivere le presenti clausole, che esistano atti normativi a carattere locale che possano avere un effetto negativo importante sulle garanzie previste dalle presenti clausole; l'importatore di dati informerà l'esportatore di dati (il quale, quando ne sia richiesto, trasmetterà tale notifica all'autorità) se verrà a conoscenza di un qualunque atto normativo avente tale carattere;

d) l'importatore tratterà i dati personali ai fini descritti nell'allegato B, ed è giuridicamente abilitato ad offrire le garanzie e a rispettare gli impegni indicati nelle presenti clausole;

e) comunicherà all'esportatore di dati un punto di contatto all'interno della sua organizzazione autorizzato a rispondere alle richieste riguardanti il trattamento dei dati personali e collaborerà in buona fede con l'esportatore di dati, l'interessato e l'autorità nell'ambito di tali inchieste entro un periodo di tempo ragionevole. Nel caso in cui l'esportatore di dati abbia cessato di esistere in diritto, o se così avranno concordato le parti, l'importatore di dati assumerà la responsabilità per quanto riguarda il rispetto delle disposizioni della lettera e) della clausola I;

f) fornirà all'esportatore di dati, su sua richiesta, prove che dimostrino la disponibilità di risorse finanziarie sufficienti a far fronte alle responsabilità cui è tenuto in virtù della clausola III (ad esempio, una copertura assicurativa);

g) metterà a disposizione dietro richiesta ragionevole dell'esportatore di dati, i suoi impianti di trattamento di dati, i suoi archivi e tutta la documentazione necessaria per il trattamento a fini di verifica, audit e/o certificazione. Queste attività saranno realizzate dall'esportatore di dati (o da un ispettore o revisore imparziale e indipendente designato dall'esportatore di dati e contro il quale non siano state opposte ragionevoli obiezioni dall'importatore di dati) al fine di determinare la conformità con le garanzie previste e gli impegni assunti nelle presenti clausole, con ragionevole preavviso e durante le normali ore lavorative. La richiesta sarà soggetta al consenso o all'approvazione, se necessari, delle autorità di regolamentazione o di vigilanza nel paese dell'importatore. L'importatore farà tutto il possibile per ottenere tale consenso o tale approvazione con tempestività;

h) tratterà i dati personali, a sua discrezione, in conformità con:

i) la legislazione in materia di tutela dei dati del paese nel quale è stabilito l'esportatore di dati;

ii) le disposizioni pertinenti [1] di qualsiasi decisione della Commissione adottata in conformità con il paragrafo 6 dell'articolo 25 della direttiva 95/46/CE, nelle quali si dimostri che l'importatore di dati rispetta le disposizioni pertinenti di tale autorizzazione o decisione ed è stabilito in un paese nel quale sono applicabili, ma non è coperto dall'autorizzazione o decisione ai fini del trasferimento o dei trasferimenti di dati personali [2]; o

iii) i principi relativi al trattamento di dati previsti nell'allegato A.

Opzione scelta dall'importatore di dati: _____

Iniziali dell'importatore di dati: _____;

i) non rivelerà né trasferirà dati personali a terzi responsabili del trattamento stabiliti al di fuori dello Spazio economico europeo (SEE), a meno che notifichi all'esportatore di dati il trasferimento e

i) il terzo responsabile del trattamento sottoponga i dati a trattamento di conformità con una decisione della Commissione nella quale si dichiari che il paese terzo in questione offre la protezione adeguata, o

ii) il terzo responsabile del trattamento sottoscriva queste clausole o qualsiasi altro accordo di trasferimento di dati approvato da un'autorità competente nell'UE, o

iii) gli interessati abbiano avuto la possibilità di opporsi, dopo essere stati informati in merito alle finalità del trasferimento, alle categorie di destinatari e al fatto che i paesi verso i quali i dati vengono esportati potrebbero avere una normativa differente in materia di protezione di dati, o

iv) per quanto riguarda i trasferimenti ulteriori di dati sensibili, gli interessati abbiano dato il loro inequivocabile consenso a tali trasferimenti.

III. Responsabilità e diritti di terzi

a) Ciascuna delle parti sarà responsabile dinnanzi all'altra per i danni provocati dall'inadempimento delle presenti clausole. La responsabilità tra le parti si limiterà al danno realmente sofferto. È specificamente escluso il risarcimento punitivo (vale a dire il risarcimento finalizzato a punire una delle parti per la sua condotta inopportuna o colpevole). Ciascuna delle parti dovrà rispondere dinnanzi agli interessati per i danni provocati da eventuali violazioni dei diritti di terzi nell'ambito delle presenti clausole. Quanto precede fa salva la responsabilità dell'esportatore in base alla legislazione a lui applicabile in materia di protezione di dati.

b) Le parti concordano che gli interessati, in qualità di terzi beneficiari, potranno invocare di fronte all'importatore o all'esportatore di dati la presente clausola, le lettere b), d) ed e) della clausola I, le lettere a), c), d), e), h) ed i) della clausola II, la lettera a) della clausola III, la clausola V, la lettera d) della clausola VI e la clausola VII per le rispettive violazioni dei loro obblighi contrattuali in rapporto ai loro dati personali; a tal fine, si sottomettono alla giurisdizione del paese di stabilimento dell'esportatore. Nei casi in cui sostenga l'inadempienza da parte dell'importatore di dati, l'interessato dovrà richiedere in primo luogo all'esportatore di avviare azioni adeguate per far valere i suoi diritti nei confronti dell'importatore di dati; se l'esportatore non compie tali azioni entro un termine ragionevole (che nelle normali circostanze sarebbe di un mese), l'interessato potrà far valere i suoi diritti direttamente contro l'importatore di dati. Gli interessati potranno procedere direttamente contro l'esportatore di dati quando questi non abbia compiuto sforzi ragionevoli per determinare se l'importatore di dati sia in grado di rispettare gli obblighi giuridici ai quali è tenuto in virtù delle presenti clausole (ricadrà sull'esportatore di dati l'onere di provare l'effettivo compimento di sforzi ragionevoli).

[1] Per "disposizioni pertinenti" si intendono le disposizioni di un'autorizzazione o decisione che non siano esecutive (le quali sono disciplinate dalle presenti clausole).

[2] Nel caso in cui, tuttavia, si scelga questa opzione, dovranno applicarsi le disposizioni del punto 5 dell'allegato A, relativo ai diritti di accesso, rettifica, cancellazione e obiezione, che prevarranno su qualsiasi disposizione comparabile della decisione della Commissione in questione.

IV. Legislazione applicabile alle clausole

Le presenti clausole sono soggette alla legislazione del paese nel quale è stabilito l'esportatore di dati, ad eccezione delle disposizioni legali e regolamentari relative al trattamento dei dati personali da parte dell'importatore di dati ai sensi della lettera h) della clausola II, che saranno applicabili solo se l'importatore avrà scelto tale opzione nell'ambito della clausola.

V. Risoluzione di controversie con gli interessati o con l'autorità

a) In caso di controversia o di reclamo presentato contro una o entrambe le parti da un interessato o dall'autorità in merito al trattamento dei dati personali, le parti si informeranno reciprocamente di tali controversie o reclami e collaboreranno al fine di risolverli in modo amichevole quanto prima possibile.

b) Le parti concordano di rispondere a qualsiasi procedura di mediazione non vincolante e generalmente accessibile che sia stata avviata da un interessato o dall'autorità. Se decidono di partecipare alla procedura, possono farlo a distanza (ad es. per telefono o attraverso altri mezzi elettronici). Le parti concordano inoltre di valutare la possibilità di partecipare a qualsiasi altro procedimento di arbitrato, mediazione o, comunque, di risoluzione delle controversie messo a punto in materia di protezione dei dati.

c) Ciascuna delle parti si impegna ad accettare qualsiasi decisione dei tribunali competenti o dell'autorità del paese di stabilimento dell'esportatore di dati le cui decisioni siano definitive e contro le quali non sia possibile alcun ulteriore appello.

VI. Risoluzione delle clausole

a) Nel caso in cui l'importatore di dati violi gli obblighi ai quali è tenuto in virtù delle presenti clausole, l'esportatore di dati potrà sospendere temporaneamente il trasferimento dei dati personali all'importatore di dati sino a che non venga posto rimedio alla violazione o si concluda il contratto.

b) Nel caso in cui:

i) il trasferimento di dati personali all'importatore di dati sia stato sospeso temporaneamente dall'esportatore di dati per più di un mese in base a quanto previsto dalla lettera a);

ii) il rispetto delle presenti clausole da parte dell'importatore di dati abbia come conseguenza la violazione dei suoi obblighi legali o regolamentari nel paese di importazione;

iii) l'importatore di dati violi in modo sostanziale o persistente una qualche garanzia prevista o un qualche impegno assunto in virtù delle presenti clausole;

iv) una decisione definitiva contro la quale non sia possibile interporre appello dinnanzi a un tribunale competente del paese di stabilimento dell'esportatore di dati o dell'autorità stabilisca che l'importatore o l'esportatore di dati hanno violato le clausole; o

v) sia stata richiesta l'amministrazione giudiziaria o la liquidazione dell'importatore di dati, sia a titolo personale che in qualità di imprenditore, e tale richiesta non sia stata respinta entro il termine previsto dalla legislazione applicabile; si designi un liquidatore per alcuni dei suoi attivi; si nomini un curatore fallimentare, nel caso in cui l'importatore sia un privato; quest'ultimo abbia richiesto l'avvio di una procedura di concordato; ovvero si trovi in una situazione analoga dinnanzi ad una qualsiasi giurisdizione;

l'esportatore di dati, fatto salvo l'esercizio di qualsiasi altro diritto che possa vantare nei confronti dell'importatore di dati, è autorizzato a risolvere le presenti clausole, nel qual caso informerà l'autorità, se richiesto. Nei casi contemplati ai punti i), ii) o iv), anche l'importatore di dati potrà procedere alla risoluzione.

c) Ciascuna parte può risolvere le presenti clausole se i) la Commissione dichiara che il paese (o parte del suo territorio) verso il quale si trasferiscono i dati e nel quale essi sono trattati dall'importatore di dati garantisce un livello di protezione adeguato in conformità con il paragrafo 6 dell'articolo 25 della direttiva 95/46/CE (o qualsiasi testo che la sostituisca), ovvero ii) la direttiva 95/46/CE (o qualsiasi testo che la sostituisca) divenga direttamente applicabile in tale paese.

d) Le parti concordano che la risoluzione delle presenti clausole in qualsiasi momento, in qualsiasi circostanza e per qualsiasi motivo – ad eccezione della risoluzione in virtù della lettera c) della clausola VI) – non le esime dal rispetto degli obblighi e delle condizioni stabilite nelle presenti clausole per quanto riguarda il trattamento dei dati personali trasferiti.

VII. Modifica delle clausole

Le parti si impegnano a non modificare le presenti clausole se non per aggiornare alcune delle informazioni contenute nell'allegato B, nel qual caso informano l'autorità, dietro sua richiesta. Ciò non impedirà alle parti di aggiungere clausole commerciali aggiuntive ove lo ritengano opportuno.

VIII. Descrizione del trasferimento

I particolari del trasferimento e dei dati personali sono specificati all'allegato B. Le parti concordano che l'allegato B può contenere informazioni commerciali confidenziali che esse non riveleranno a terzi, a meno che non lo esiga la legislazione, ovvero in risposta a un ente regolatore o governativo competente, o quando ciò sia necessario in virtù della lettera e) della clausola I. Le parti potranno introdurre allegati aggiuntivi per regolare trasferimenti aggiuntivi, i quali saranno presentati all'autorità dietro sua richiesta. Come alternativa, la redazione dell'allegato B potrà essere effettuata in forma tale da coprire trasferimenti multipli.

Data: _____

PER L'IMPORTATORE DI DATI	PER L'ESPORTATORE DI DATI
.....	.....
.....	.....
.....	.....

ALLEGATO A

PRINCIPI RELATIVI AL TRATTAMENTO DEI DATI

1. Limitazione dei trasferimenti a una finalità specifica: I dati personali possono essere trattati e successivamente utilizzati o ulteriormente comunicati solo per i fini descritti all'allegato B o autorizzati successivamente dall'interessato.

2. Qualità e proporzionalità dei dati: I dati personali devono essere accurati e, ove necessario, aggiornati. I dati personali devono essere adeguati, pertinenti e non eccedenti in rapporto agli scopi per i quali sono trasferiti e successivamente trattati.

3. Trasparenza: Devono essere fornite agli interessati tutte le informazioni necessarie a garantire il trattamento leale dei dati (così come le informazioni sulla finalità del trattamento e sul possibile trasferimento), a meno che tali informazioni non siano già state fornite dall'esportatore di dati.

4. Sicurezza e confidenzialità: il responsabile del trattamento deve adottare misure tecniche e organizzative volte a garantire il livello di sicurezza adeguato ai rischi che comporta il trattamento dei dati, ad esempio contro la distruzione accidentale o illecita o la perdita accidentale, alterazione, divulgazione o accesso non autorizzati. Le persone che operano sotto l'autorità del responsabile del trattamento, compreso l'incaricato del trattamento, non devono trattare i dati a meno che non ricevano istruzioni del responsabile.

5. Diritti di accesso, rettifica, cancellazione e opposizione: Secondo quanto prevede l'articolo 12 della direttiva 95/46/CE, gli interessati hanno il diritto di conoscere, sia direttamente che attraverso un terzo, i dati personali che su di loro possiede un'organizzazione, ad eccezione delle richieste che configurino chiaramente un abuso di tale diritto, o per il fatto di essere state poste ad intervalli irragionevoli, o a causa del loro numero, o perché hanno natura ripetitiva o sistematica, o ad eccezione dei casi nei quali non è necessario concedere l'accesso all'interessato secondo la legislazione del paese dell'esportatore di dati. A condizione che l'autorità abbia dato la sua previa approvazione, l'accesso può inoltre non essere concesso quando il farlo avrebbe il probabile effetto di danneggiare gravemente gli interessi dell'importatore di dati o di altre organizzazioni che hanno rapporti con l'importatore di dati, e quando tali interessi prevalgono sugli interessi in materia di diritti e di libertà fondamentali dell'interessato. Non sarà necessario determinare l'origine dei dati personali quando ciò non sia possibile mediante sforzi ragionevoli, o se ciò comporterebbe la violazione dei diritti di persone diverse dall'interessato. L'interessato avrà il diritto di far rettificare, modificare o cancellare i dati personali quando essi non siano accurati o il loro trattamento non rispetti i principi stabiliti nel presente allegato. Se vi sono seri motivi di dubitare della legittimità della richiesta, l'organizzazione può richiedere ulteriori giustificazioni prima di procedere alla rettifica, alla modifica o alla cancellazione dei dati. Non sarà necessario notificare la rettifica, la modifica o la cancellazione dei dati ai terzi ai quali essi siano stati rivelati quando ciò richieda uno sforzo sproporzionato. Gli interessati devono inoltre potersi opporre al trattamento dei dati personali che li riguardano quando esistano motivi seri e legittimi relativi alla loro particolare situazione. L'onere della prova per qualunque rifiuto ricade sull'importatore di dati. L'interessato potrà ricorrere contro un rifiuto dinnanzi all'autorità.

6. Dati sensibili: L'importatore di dati adotta le misure aggiuntive (ad esempio in materia di sicurezza) che risultino necessarie a proteggere i dati sensibili in conformità con gli obblighi ai quali è tenuto in virtù della clausola II.

7. Dati utilizzati a fini di marketing: Quando il trattamento dei dati sia realizzato a fini di marketing diretto, dovranno esistere procedimenti efficaci tali da consentire all'interessato di opporsi in qualsiasi momento a che i suoi dati personali siano utilizzati per gli scopi suddetti.

8. Decisioni automatizzate: Agli effetti del presente allegato, per «decisione automatizzata» si intende una decisione dell'esportatore o dell'importatore di dati che abbia effetti giuridici sull'interessato o che lo interessi in modo significativo e che si basi unicamente su un trattamento automatizzato di dati personali destinato a valutare determinati aspetti della sua personalità, come il suo rendimento lavorativo, la sua solvibilità, l'affidabilità, la condotta, ecc. L'importatore di dati non adotta nessuna decisione automatizzata relativa agli interessati, eccettuati i casi in cui:

   a. i) tali decisioni siano state adottate dall'importatore di dati al momento di stipulare o eseguire un contratto con l'interessato, e

      ii) si offra all'interessato l'opportunità di discutere i risultati di una decisione automatizzata che lo riguarda con un rappresentante della parte che abbia adottato la decisione ovvero la possibilità di presentare osservazioni a questa parte;

   o

   b. la legislazione applicabile all'esportatore di dati stabilisca altrimenti.

ALLEGATO B

DESCRIZIONE DEL TRASFERIMENTO

(Dovrà essere riempito dalle parti)

Interessati

I dati personali trasferiti si riferiscono alle seguenti categorie di interessati:

.....

.....

.....

.....

Finalità del trasferimento o dei trasferimenti

Il trasferimento viene effettuato per le seguenti finalità:

.....

.....

.....

.....

Categorie di dati

I dati personali trasferiti riguardano le seguenti categorie di dati:

.....

.....

.....

.....

Destinatari

I dati personali trasferiti potranno essere forniti unicamente ai seguenti destinatari o categorie di destinatari:

.....

.....

.....

Dati sensibili (se del caso)

I dati personali trasferiti rientrano nelle seguenti categorie di dati sensibili:

.....

.....

.....

.....

Informazioni sulla notificazione presentata dall'esportatore di dati (se applicabile)

.....

.....

Altre informazioni utili (periodo massimo di conservazione e qualsiasi altra informazione pertinente)

.....

.....

Punti di contatto per consultazioni in materia di protezione di dati

Importatore di dati	**Esportatore di dati**
.....	.....
.....	.....
.....	.....

CLAUSOLE COMMERCIALI ILLUSTRATIVE (OPZIONALI)

Risarcimento tra l'esportatore e l'importatore di dati:

"Ciascuna delle parti risarcisce e manleva l'altra per qualunque costo, onere, danno, spesa o perdita causati all'altra parte in seguito alla violazione di una qualsiasi delle disposizioni delle presenti clausole. L'indennizzo dipenderà dai seguenti elementi: a) la parte o le parti che devono ricevere l'indennizzo (la 'parte indennizzata') notifica immediatamente il reclamo all'altra parte/alle altre parti; b) la parte/le parti che deve/devono provvedere all'indennizzo abbia/abbiano il controllo esclusivo della difesa e della risoluzione di una controversia di questo tipo; e c) la parte indennizzata cooperi ed assista in misura ragionevole la parte indennizzatrice nella difesa del reclamo."

Soluzione delle controversie tra l'esportatore e l'importatore di dati (le parti potranno convenire di sostituire questa clausola con qualsiasi altra clausola di giurisdizione o di soluzione alternativa di conflitti):

"Qualunque controversia tra l'importatore e l'esportatore di dati in rapporto con una supposta violazione di una qualsiasi delle disposizioni delle presenti clausole sarà risolta in via definitiva con riferimento alle norme di arbitrato della Camera di commercio internazionale, da uno o più arbitri designati in conformità con tali norme. La sede dell'arbitrato sarà [ ]. Il numero di arbitri sarà di [ ]."

Attribuzione dei costi:

"Ciascuna parte osserverà gli obblighi ai quali è tenuta in virtù delle presenti clausole a proprie spese."

Clausola aggiuntiva di risoluzione

"In caso di risoluzione delle presenti clausole, l'importatore di dati deve, a discrezione dell'esportatore, restituire immediatamente tutti i dati personali soggetti alle presenti clausole e le copie in suo possesso, ovvero distruggerli completamente e certificare tale circostanza all'esportatore, a meno che la legislazione nazionale o la regolamentazione locale applicabile all'importatore gli impedisca la restituzione o la distruzione totale o parziale di tali dati, nel qual caso l'importatore si impegna a mantenere il segreto sui dati personali e a non sottoporli a ulteriore trattamento per qualsivoglia finalità. L'importatore di dati accetta, su richiesta dell'esportatore di dati, di mettere a disposizione di quest'ultimo o di un ispettore da questi designato e al quale l'importatore di dati non opponga ragionevoli obiezioni, i suoi impianti di trattamento per verificare che ciò sia stato fatto, con ragionevole preavviso e durante l'orario di lavoro.".»

INFORMATIVA APPALTI

Gentile Signora/Egregio Signore,

La Federazione Italiana Sport Equestri – FISE - Le fornisce, ai sensi del Regolamento UE 2016/679 (di seguito, GDPR) e del D.lgs. 196/2003 nel testo vigente (Codice Privacy), le informazioni di seguito riportate relative al trattamento dei Suoi dati personali. Il trattamento dei Suoi dati si rende necessario in relazione alla domanda di partecipazione, alla procedura di gara indetta dalla Federazione, Sua o della Società/Ente di cui Lei è legale rappresentante o comunque ivi incaricato di funzioni rilevanti ai fini della partecipazione stessa.
I dati personali da Lei forniti formeranno oggetto di trattamento nel rispetto della menzionata normativa.

1. Chi è il Titolare del trattamento dei Suoi dati personali?

Il Titolare del trattamento dei Suoi dati è FISE con sede legale in, ……Tel. ……..……..……, Fax: …….., codice fiscale ……..…….. e-mail…….

2. Perché leggere questa informativa?

L'informativa è una comunicazione rivolta all'interessato che ha lo scopo di informarlo sulle finalità e le modalità dei trattamenti operati dal Titolare del trattamento.
Nei casi in cui il trattamento dei Suoi dati personali si renda necessario per adempiere un obbligo legale al quale è soggetto il Titolare del trattamento, o per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, il Titolare rilascia comunque l'informativa ai sensi degli artt. 13 ss. del GDPR al fine di assicurarne la trasparenza e correttezza dei trattamenti. Nei casi invece in cui il trattamento dei dati personali che La riguardano sia lecito solo previo consenso, il rilascio dell'informativa è requisito indispensabile per l'acquisizione del relativo consenso.
Maggiori informazioni possono essere comunque reperite sul sito www.fise.it.

3. Le informazioni acquisite per quali finalità verranno utilizzate?

FISE utilizzerà i Suoi dati per perseguire i propri fini istituzionali o ad essi strumentali, e quindi:

A. per effettuare i controlli necessari alla partecipazione alle procedure di gara, ai sensi della normativa vigente (*lex generalis*) e delle prescrizioni riportate nella documentazione di gara (*lex specialis*);
B. per dare adempimento a tutti gli obblighi previsti dalla legge o dalle Autorità preposte, relativamente all'intero svolgimento della gara;
C. per tutto quanto concerne l'organizzazione e la gestione dei rapporti con tutti i partecipanti alla gara, ivi inclusa l'effettuazione delle comunicazioni -anche con l'uso di mezzi elettronici- inerenti tutte le fasi di gara, comprese eventuali interlocuzioni, ove previste dalla normativa;
D. per l'adempimento di ogni connesso obbligo o attività, anche susseguente alla gara, come la gestione di ogni eventuale contenzioso civile, penale o amministrativo e la gestione degli obblighi conseguenti alla stipulazione del contratto;
E. per mantenere i rapporti con ogni Autorità o Ente, nazionale o internazionale, deputato al controllo della regolarità delle gare ed appalti, nonché per la gestione di obblighi di natura tributaria o contabile;
F. per l'invio di comunicazioni e informative istituzionali;
G. per l'inserimento nelle anagrafiche e nei database informatici comunali;
H. per la rendicontazione nei confronti delle Autorità e degli Enti la cui normativa riconosce poteri di vigilanza e controllo nei confronti della FISE.

4. Cosa consente a FISE di trattare i dati che La riguardano?

Le procedure di gara e di appalto sono organicamente disciplinate dalla legge per motivi di interesse pubblico. Ai sensi di tale normativa, il trattamento è necessario per adempiere agli obblighi di legge al quale è soggetto il Titolare del trattamento. In particolare, il trattamento è necessario ai fini della stipula e dell'esecuzione del contratto (art. 6 par. 1 lett. b) GDPR), nonché per adempiere ad obblighi giuridici a cui è soggetto il Titolare del trattamento (art. 6 par.1 lett. c) GDPR) o per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento; in particolare, per la gestione della procedura ad evidenza pubblica finalizzata alla selezione del contraente (art. 6 par. 1 lett. e) GDPR).
Il D.lgs. n. 50/2016 dispone l'obbligo, per la stazione appaltante, di acquisire insieme ai dati inerenti la partecipazione alle procedure di gara, gli eventuali atti conseguenti quali – fra gli altri – l'ammissione, l'esclusione, l'aggiudicazione, la stipulazione. Ciò consente di trattare anche dati appartenenti a particolari

categorie, come quelli giudiziari, di cui FISE potrebbe entrare in possesso ad esempio all'atto del controllo dei requisiti di partecipazione alla gara, ai fini della verifica dell'assenza di cause di esclusione ex art. 80 D.lgs. n. 50/2016.
Qualora, nel corso delle procedure di gara e per determinate finalità, dovesse essere richiesto il Suo consenso al trattamento, riceverà una informativa relativa a quel singolo trattamento.

5. Cosa succede nel caso in cui Lei dovesse negare il conferimento dei Suoi dati?

Il conferimento delle informazioni di cui sopra ha carattere obbligatorio ai fini della partecipazione alle procedure di gara. Se Lei decidesse di non conferire i necessari dati che La riguardano, ne deriverebbe l'impossibilità di ammissione alla gara o la sua esclusione o la decadenza dall'aggiudicazione, nonché, in ogni caso, l'impossibilità di stipulare il contratto.

6. Come vengono trattati i dati che La riguardano?

I dati che La riguardano sono sottoposti a diverse operazioni, che si rendono necessarie per perseguire le finalità esposte in precedenza. Tutte queste operazioni vengono effettuate da personale appositamente incaricato, con strumenti informatici e mediante la lavorazione di documenti cartacei. I nostri archivi informatici sono protetti dalle intrusioni e sono accessibili solo a determinate persone incaricate di trattare i dati, in ragione delle attività lavorative che competono loro. Anche gli archivi cartacei sono accessibili solo a chi ha una valida ragione giuridica per trattare i Suoi dati. In alcuni casi, quando per le finalità perseguite da FISE non è necessario che lei sia identificato o identificabile i suoi dati vengono sottoposti a procedure di anonimizzazione e psedonimizzazione.
La FISE si impegna al rispetto delle disposizioni che, anche al di fuori della disciplina sulla tutela dei dati e sugli appalti, tutelano i diritti delle Società e degli offerenti e che prescrivono, fra l'altro, non solo di chiedere le informazioni non eccedenti l'oggetto dell'appalto (ad esempio: necessità effettiva di acquisire copie di fatture in luogo di altra documentazione equipollente), ma anche di tenere in debita considerazione *"l'esigenza di protezione dei segreti tecnici e commerciali"* (art. 42 D.lgs. 12 aprile 2006, n. 163 co. 3 D.lgs. n. 358/1992; art. 14 co. 3, D.lgs. n. 157/1995), nel rispetto di quanto previsto dal Garante (16 febbraio 1999, in Bollettino n. 7, pag. 7) già nel vigore della previgente normativa in materia di appalti.

7. A chi potranno essere comunicate le Sue informazioni?

All'interno e all'esterno di FISE sono autorizzati ad effettuare operazioni di trattamento dei sui Suoi dati personali, secondo i principi di necessità, correttezza e liceità, solo soggetti espressamente incaricati. Questo significa che solo chi ha necessita dei Suoi dati per svolgere il suo lavoro potrà accedervi.
Oltre che da personale della Federazione appositamente autorizzato al trattamento, i Suoi dati acquisiti potranno essere trattati, conosciuti e comunicati, per le finalità sopra esposte, anche a Responsabili del trattamento eventualmente designati ai sensi dell'art. 28 del GDPR, il cui elenco è disponibile sul sito www.fise.it.
I suoi dati possono essere comunicati, oltre al personale di FISE che cura il procedimento di gara o attività ad esso attinenti:
- alle Autorità o Enti pubblici competenti in materia di procedure di gara ed appalto o coinvolte nelle attività in oggetto, ivi incluse le attività conseguenti ai sensi di legge, quali, con elenco non esaustivo: ANAC, INPS, INAIL, Autorità giudiziaria, Ministero delle Infrastrutture e dei Trasporti;
- alle Società, anche bancarie, per tutto quanto necessario alla fase esecutiva dell'appalto, compresi i pagamenti e ogni altro adempimento che sia previsto come obbligatorio per FISE;
- eventualmente ad altri soggetti esterni alla Federazione operanti quali Titolari autonomi aventi titolo alla trasmissione dei dati ai sensi di legge;
- agli uffici postali, alle imprese di consegna e trasporto per l'invio di documenti;
- ai titolari di situazioni soggettive tutelate dalla legge, correlate alla partecipazione alla gara come, fra gli altri, eventuali controinteressati, in particolare in caso di richiesta di accesso ai documenti amministrativi.
Le ricordiamo che FISE, in quanto esercente pubbliche funzioni è soggetta alla disciplina dell'accesso agli atti e all'accesso civico generalizzato. Ove possibile, i documenti verranno forniti in forma anonima, ma potrebbero esserci casi in cui il prevalente interesse di un terzo gli consenta di accedere ai Suoi dati personali. Nei casi previsti dalla legge, dai regolamenti e dalle norme statutarie, i Suoi dati potrebbero essere soggetti a pubblicazione sul sito web www.fise.it.

8. Le informazioni acquisite per quanto tempo verranno conservate?

I Suoi dati vengono conservati per finalità di archiviazione per un periodo indeterminato, secondo quanto previsto dalla legge per gli atti pubblici e i provvedimenti amministrativi.

9. Quali sono i diritti che può esercitare?

Rispetto ai dati che La riguardano, Le sono riconosciuti diversi diritti.
Diritto di accesso: Lei ha il diritto di ottenere informazioni circa i trattamenti che La riguardano; Diritto di rettifica e di integrazione: Lei ha il diritto di ottenere la rettifica dei dati personali inesatti. Diritto alla portabilità dei dati personali: Lei ha il diritto di ricevere i dati personali che La riguardano o di trasmettere suddetti dati ad altro titolare. Diritto alla limitazione: Lei ha diritto di chiederci la limitazione dei trattamenti in corso. Diritto a proporre reclamo all'Autorità di controllo: Lei può proporre reclamo al Garante per la protezione dei dati personali per lamentare una violazione della disciplina in materia di protezione dei dati personali.

10. Chi è il Responsabile della protezione dei dati?

FISE ha nominato un Responsabile della protezione dei dati che ha funzioni di supporto e di vigilanza sull'applicazione delle regole sulla privacy e a cui Lei potrà rivolgersi in caso in cui ritenga siano state violati o negati i suoi diritti.
Il Responsabile della protezione dei dati può essere contattato al seguente indirizzo e-mail dpo@fise.it

11. Dove può reperire maggiori informazioni?

Maggiori informazioni sono reperibili sul sito internet www.fise.it