

ATTO DI NOMINA A RESPONSABILE DEL TRATTAMENTO
in applicazione dell'art.28 del Regolamento Europeo 679/2016 (in seguito "GDPR")

PREMESSO CHE

- La Federazione Italiana Scherma (di seguito "FIS"), riveste la qualifica di Titolare del trattamento dei dati personali dei propri tesserati;
 - Il contratto di supporto nel marketing Federale stipulato con DIGITAL PA SRL prevede il trattamento da parte di quest'ultima, per conto del Titolare, dei dati personali meglio descritti nell'**allegato 3** del presente documento
- DIGITAL PA SRL, con la sottoscrizione del presente incarico, garantisce la veridicità di quanto dichiarato nella *check list* del Fornitore (**allegato 4** del presente documento) e dichiara di assicurare – nello svolgimento della richiamata attività – che il trattamento dei dati personali soddisferà i requisiti del GDPR e garantirà la tutela dei diritti degli interessati.

Tutto quanto premesso, la FIS, in qualità di Titolare del trattamento

NOMINA

La DIGITAL PA SRL con sede in Via S.T. D'Aquino, 18/A – 09134 Cagliari, quale Responsabile del trattamento dei dati, effettuato con strumenti elettronici o comunque automatizzati o con strumenti diversi, per quanto necessario alla corretta esecuzione del contratto indicato in premessa.

In qualità di Responsabile, la DIGITAL PA SRL ha il dovere di compiere tutto quanto necessario per il rispetto delle vigenti disposizioni in materia di trattamento dei dati personali.

In particolare, dovrete:

- Osservare le istruzioni impartite dal Titolare del trattamento, anche successivamente al presente incarico;
- Osservare il divieto di comunicazione e di diffusione dei dati personali trattati e garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- Garantire nell'ambito della Vostra organizzazione la corretta applicazione di adeguate misure tecniche e organizzative ai sensi dell'art. 32 Regolamento Europeo 679/2016, e impartire istruzioni ad eventuali incaricati, vigilandone l'operato affinché siano garantite le suddette misure;
- Richiedere specifica autorizzazione scritta a FIS laddove intendiate avvalervi di altro Responsabile del Trattamento; In caso affermativo, il relativo contratto o atto di nomina dovrà prevedere gli stessi obblighi in materia di protezione dei dati di cui al presente atto di nomina;
- consegnare tempestivamente a FIS e comunque non oltre le 24 ore successive al loro ricevimento, i reclami degli interessati e le eventuali istanze del Garante;

Ricordiamo inoltre che, ai sensi delle disposizioni di legge, il Responsabile è altresì tenuto a:

- assistere il Titolare del trattamento con misure tecnico organizzative adeguate al fine di soddisfare l'obbligo del Titolare di dare seguito alle richieste di esercizio dei diritti dell'interessato;

- assistere il Titolare del trattamento nel rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR, ovvero in materia di sicurezza dei dati personali, valutazione d'impatto sulla protezione dei dati e consultazione preventiva. Nel dettaglio, per quanto concerne la gestione dell'eventuale *data breach* avvenuto presso o sotto la gestione del Responsabile del trattamento, quest'ultimo deve darne comunicazione al Titolare senza ingiustificato ritardo e comunque entro un massimo di 12 (dodici) ore da quando si è verificata mediante una comunicazione da inviarsi all'indirizzo email privacy@federscherma.it. Entro le successive 20 (venti) ore il Responsabile del trattamento deve altresì, fornire al Titolare le informazioni di dettaglio utilizzando a tal fine il modello allegato (**allegato 5**).
- mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 GDPR consentendo e contribuendo all'attività di revisione, comprese le ispezioni realizzate dal Titolare del trattamento o da altro soggetto da questi incaricato;

Per quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.

Il Responsabile del trattamento sarà tenuto a risarcire e tenere indenne il Titolare da qualsiasi reclamo, perdita, responsabilità, valutazione, danno, costo, sanzione amministrativa e altra spesa (incluse le spese legali) derivante o risultante da qualsiasi rivendicazione, richiesta, istanza, azione o altre procedura di terzi (comprese le autorità di controllo) subite dal Titolare a seguito di violazioni della normativa applicabile in materia di protezione dei dati personali da parte Responsabile del trattamento, dai dipendenti, amministratori, dirigenti, agenti e altri suoi collaboratori, o da eventuali sub responsabili del trattamento.

La presente nomina è condizionata, per oggetto e durata, all'incarico richiamato in premessa, e si intenderà revocata di diritto alla cessazione dello stesso.

Al termine del rapporto, sarà pertanto onere del Responsabile provvedere alla restituzione e, ove richiesta, cancellazione sicura dei dati personali trasmessi dal Titolare

Resta inteso che la presente designazione non comporta alcun diritto per il Responsabile del trattamento ad uno specifico compenso o indennità o rimborso per l'attività svolta, che deve intendersi già ricompreso all'interno di quanto previsto nel Contratto, ai sensi e per gli effetti del GDPR, né ad un incremento del compenso spettante allo stesso in virtù dei rapporti intercorrenti con il Titolare.

Luogo e data, _____,

Il Titolare del Trattamento
ASSOCIAZIONE ITALIANA SCHERMA
Via Tiziano, 74 - 00186 RM
Cod. Fisc. 06271310582
Part. IVA 01382901001

Firma del Responsabile (per ricevuta, presa visione ed accettazione)

ALLEGATO 3
SOGGETTI INTERESSATI E TIPOLOGIE DI DATI PERSONALI

Soggetti Interessati <i>(I dati personali trattati riguardano le seguenti categorie di soggetti interessati)</i>	FORNITORI BENI E SERVIZI, PROFESSIONISTI, CLIENTI, TESSERATI
Categorie di dati <i>(I dati personali trattati riguardano le seguenti categorie di dati)</i>	PERSONALI COMUNI, AZIENDALI GENERICI E SPECIFICI, FINANZIARI

Allegato 4
Check list del Fornitore

Nr.	Argomento	Risposta		Note
1	Principi generali relativi al trattamento dei dati personali (art. 5 GDPR). Le attività di trattamento dei dati personali rispettano i seguenti principi?	Si	No	
1.1.	Sono trattati secondo i principi di liceità, correttezza e trasparenza?			
1.2.	Sono raccolti per finalità esplicite, specifiche e legittime e non ulteriormente trattati per finalità incompatibili con quelle per cui sono stati raccolti?			
1.3.	Sono adeguati, pertinenti e limitati rispetto a quanto necessario al perseguimento delle predette finalità?			
1.4.	Sono esatti e se necessario aggiornati?			
1.5.	Sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al perseguimento delle finalità per cui sono trattati?			
1.6.	Sono trattati in modo da garantire una sicurezza adeguata mediante l'adozione di misure tecniche e organizzative che tutelino i dati da trattamenti illeciti, dalla perdita, dalla distruzione o da danni incidentali?			
1.7.	Il Fornitore è in grado di dare evidenza del rispetto di quanto sopra?			
Nr.	Argomento	Risposta		Note
2	Diritti degli interessati (art. 17 – 18- 20 GDPR)	Si	No	
2.1.	Il Fornitore ha una procedura che consenta la rettifica dei dati personali inesatti in caso di richiesta del Titolare?			
2.2.	Il Fornitore ha delle modalità o procedure in caso di richiesta di cancellazione di dati da parte del Titolare?			
2.3.	Il Fornitore è in grado di garantire la portabilità dei dati su richiesta del Titolare, fornendo i dati personali in un formato strutturato, comunemente usato e leggibile da dispositivo ed è in grado di trasmetterli ad altro Titolare?			
Nr.	Argomento	Risposta		Note
3	Accordi sul trattamento dei dati (art. 28)	Si	No	
3.1.	Il Fornitore informa il Titolare di eventuali subfornitori ed è in grado di garantire che vengano incaricati solo se forniscano sufficienti garanzie per attuare le misure tecniche e organizzative adeguate al trattamento dei dati personali?			
Nr.	Argomento	Risposta		Note
4	Autorità del Titolare o del Responsabile (art. 29 GDPR)	Si	No	
4.1.	I dipendenti e i collaboratori de fornitore sono adeguatamente formati in materia di protezione dei dati personali?			
4.2.	È stata definita, una “politica gestionale” riguardante la normativa in materia di protezione dei dati personali (data			

	privacy policy) che comprenda le istruzioni per l'utilizzo degli strumenti informatici?			
Nr.	Argomento	Risposta		Note
5	Registri delle attività di trattamento (art. 30 GDPR)	Si	No	
5.1.	Esiste un documento che fornisca una descrizione di tutti i processi aziendali e dei sistemi informatici utilizzati nel trattamento dei dati personali?			
Nr.	Argomento	Risposta		Note
6	Sicurezza del trattamento dei dati personali (artt. 24 e 32 GDPR)	Si	No	
6.1.	Sono in atto le seguenti misure tecniche e organizzative in relazione ai dati personali del Titolare?			
6.1.1.	- pseudonimizzazione			
6.1.2.	- cifratura			
6.1.3.	- capacità di assicurare su base permanente la riservatezza, l'integrità e la disponibilità e la resilienza dei sistemi e dei servizi			
6.1.4.	- la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico;			
6.1.5.	- la procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento			
6.2.	Sono in essere procedure di Valutazione e gestione del Rischio relativo alla sicurezza delle informazioni?			
6.3.	Per l'accesso ai dati è previsto l'utilizzo di un sistema di autenticazione informatica, cioè vengono attribuite agli incaricati utenti del sistema informativo le cosiddette credenziali di autenticazione?			
Nr.	Argomento	Risposta		Note
7	Violazioni di dati (Art. 33 GDPR)	Si	No	
7.1.	È stata definita, una "procedura per la gestione del data breach"?			
Nr.	Argomento	Risposta		Note
8	Responsabile della protezione dei dati (Art. 37 GDPR)	Si	No	
8.1.	E' stato nominato un responsabile della protezione dei dati del Fornitore?			
8.1.1.	- Se la risposta è si indicare nella casella sottostante il nome e i dati di contatto			
Nr.	Argomento	Si	No	Note
9	Sicurezza delle informazioni e cloud computing			

9.1.	I dati trattati in esecuzione dei rapporti contrattuali saranno oggetto di trattamento fuori dal territorio dello Stato?				
9.2.	In caso di risposta affermativa alla domanda precedente, dove trattati?				
	9.2.1.	All'interno dell'Unione Europea			
	9.2.2.	All'esterno dell'Unione Europea			
	9.2.3.	Negli Stati Uniti			
9.3.	Il fornitore prevede il pieno isolamento delle risorse di elaborazione dedicate allo svolgimento delle eventuali prestazioni che saranno svolte in favore del Titolare?				
Nr.	Argomento		Si	No	Note
10	Informativa e consenso (art. 7, 9 e 13 GDPR)				
10.1	Il fornitore rende l'informativa preventiva agli interessati e, qualora richiesto dalla legge acquisisce il loro consenso espresso documentato per iscritto?				
Nr.	Argomento		Risposta		Note
11	Certificazioni di Sicurezza delle Informazioni		Si	No	
11.1	Il Fornitore è in possesso di una certificazione di Sicurezza dei propri sistemi informativi?				
11.2	In caso di risposta affermativa alla domanda precedente, l'ambito della certificazione rilasciata comprende i servizi che dovrebbe essere svolti in favore del Titolare?				
11.3	In caso di risposta affermativa alla domanda sub. 1.1. di quale certificazione dispone il Fornitore.				
	11.3.1.	ISO/IEC 27001:2013			
	11.3.2.	PCI - DSS			
	11.3.3	CSA-STAR			
	Altro	Specificare			

ALLEGATO 5
MODELLO DI COMUNICAZIONE DEL *DATA BREACH* DAL RESPONSABILE AL TITOLARE TRATTAMENTO

Azienda	[Ragione sociale, sede, contatti]
Responsabile della protezione trattamento	[nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni]
Data dell'incidente	<input type="checkbox"/> Il ___/___/___ <input type="checkbox"/> Tra il ___/___/___ e il ___/___/___ <input type="checkbox"/> In un tempo non ancora determinato <input type="checkbox"/> E' possibile che sia ancora in corso
Luogo dell'incidente <i>(Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)</i>	
Classificazione dell'incidente	<input type="checkbox"/> violazione della riservatezza <input type="checkbox"/> violazione dell'integrità <input type="checkbox"/> violazione della disponibilità
Breve descrizione dell'incidente	
Categoria dei dati personali compromessi	<input type="checkbox"/> Dati anagrafici/codice fiscale <input type="checkbox"/> Dati di accesso e di identificazione (user name, password, customer ID, altro) <input type="checkbox"/> Dati relativi a minori <input type="checkbox"/> Dati personali idonei a rivelare 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 <input type="checkbox"/> Dati personali idonei a rivelare lo stato di salute e la vita sessuale <input type="checkbox"/> Dati giudiziari <input type="checkbox"/> Copia per immagine su supporto informatico di documenti analogici <input type="checkbox"/> Ancora sconosciuto <input type="checkbox"/> Altro :
Categorie e numero approssimativo degli interessati coinvolti nella violazione	
Descrizione delle probabili conseguenze del data breach	
Descrizione delle azioni già poste in essere o di cui si propone l'adozione per porre rimedio o attenuare gli effetti del <i>data breach</i>	