



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Dipartimento federale di giustizia e polizia DFGP  
Ufficio federale di polizia fedpol

# **Sistema d'informazione**

# **HOOGAN**

# **Regolamento sul trattamento dei dati**

Berna, dicembre 2009

**INDICE**

<b>REGOLAMENTO SUL TRATTAMENTO DEI DATI.....</b>	<b>1</b>
SEZIONE 1 DISPOSIZIONI GENERALI .....	2
Art. 1    Contenuto.....	2
Art. 2    Nozioni .....	2
Art. 3    Scopo .....	3
Art. 4    Struttura di HOOGAN.....	4
SEZIONE 2 AUTORITÀ E SERVIZI .....	4
Art. 5    Organi di fedpol.....	4
Art. 6    CSI DFGP .....	4
Art. 7    SZH.....	4
Art. 8    Cgcf.....	5
Art. 9    Organi cantonali .....	5
SEZIONE 3 UTENTI E ACCESSO AI DATI .....	6
Art. 10   Utenti.....	6
Art. 11   Autorizzazione individuale d'accesso .....	6
Art. 12   Revoca dell'autorizzazione d'accesso .....	7
Art. 13   Formazione degli utenti .....	7
Art. 14   Accesso ai dati .....	7
Art. 15   Accesso ai dati sulle persone e sugli eventi .....	8
SEZIONE 4 TRATTAMENTO DEI DATI .....	8
Art. 16   Registrazione in HOOGAN.....	8
Art. 17   Misure .....	9
Art. 18   Divieto di recarsi in un Paese determinato .....	9
Art. 19   Registrazione e controllo dei dati .....	9
Art. 20   Registrazione dei dati.....	10
Art. 21   Durata di conservazione.....	10
Art. 22   Comunicazione dei dati.....	10
Art. 23   Stampa e ulteriore utilizzo dei dati.....	10
Art. 24   Informazione delle persone interessate.....	11
SEZIONE 5 CANCELLAZIONE E ARCHIVIO FEDERALE .....	11
Art. 25   Cancellazione dei dati e comunicazione ai Cantoni .....	11
Art. 26   Consegna dei dati e dei documenti all'Archivio federale .....	11
SEZIONE 6 SICUREZZA INFORMATICA .....	12
Art. 27   Sicurezza informatica .....	12
Art. 28   Sicurezza dei dati.....	12
Art. 29   Misure di protezione dei dati (riservatezza) nel settore dei terminali.....	12
Art. 30   Trasmissione sicura .....	12
Art. 31   Assistenza agli utenti e obbligo di notifica .....	12
Art. 32   Sviluppo del programma HOOGAN.....	13
Art. 33   Registrazione cronologica .....	13
Art. 34   Sorveglianza e responsabilità .....	13
Art. 35   Utilizzo abusivo di HOOGAN.....	13
Art. 36   Requisiti tecnici .....	14
Art. 37   Allegati al regolamento sul trattamento dei dati HOOGAN.....	14

---

SEZIONE 7 DISPOSIZIONI FINALI .....	14
Art. 38 Entrata in vigore e pubblicazione .....	14
ALLEGATO 1: ORDINANZA DEL 4 DICEMBRE 2009 SULLE MISURE DI POLIZIA AMMINISTRATIVA E I SISTEMI D'INFORMAZIONE DELL'UFFICIO FEDERALE DI POLIZIA .....	15
ALLEGATO 2: DIRETTIVA DEL DFGP DEL 30 SETTEMBRE 2004 SULL'INSTALLAZIONE DI COLLEGAMENTI ONLINE E IL RILASCIO DI AUTORIZZAZIONI D'ACCESSO AD APPLICAZIONI INFORMATICHE DEL DFGP (DIRETTIVA ONLINE DFGP).....	19
ALLEGATO 3: ISTRUZIONI DEL CIC DEL 27 SETTEMBRE 2004 SULLA SICUREZZA INFORMATICA NELL'AMMINISTRAZIONE FEDERALE (ISTRUZIONI CIC SULLA SICUREZZA INFORMATICA) .....	23
ALLEGATO 4: DIRETTIVA DEL 1° GENNAIO 2010 SULL'UTILIZZO E IL TRATTAMENTO DEI DATI DEL SISTEMA D'INFORMAZIONE HOOGAN DA PARTE DEGLI ORGANIZZATORI DI MANIFESTAZIONI SPORTIVE E DEI LORO RESPONSABILI DELLA SICUREZZA.....	26
ALLEGATO 5: CONCORDATO DEL 15 NOVEMBRE 2007 DELLA CONFERENZA DEI DIRETTORI CANTONALI DI GIUSTIZIA E POLIZIA SULLE MISURE CONTRO LA VIOLENZA IN OCCASIONE DI MANIFESTAZIONI SPORTIVE .....	29

---

**REGOLAMENTO SUL TRATTAMENTO DEI DATI****del sistema d'informazione HOOGAN dell'Ufficio federale di polizia fedpol**

(Regolamento sul trattamento dei dati HOOGAN del 1° gennaio 2010, sostituisce la versione del 1° gennaio 2007)

*L'Ufficio federale di polizia fedpol,*

visti gli articoli 24a e seguenti della legge federale del 21 marzo 1997<sup>1</sup> sulle misure per la salvaguardia della sicurezza interna (LMSI, stato 1° gennaio 2010);

visti gli articoli 4 e seguenti dell'ordinanza del 4 dicembre 2009<sup>2</sup> sulle misure di polizia amministrativa e i sistemi d'informazione dell'Ufficio federale di polizia;

visto l'articolo 21 dell'ordinanza del 14 giugno 1993<sup>3</sup> relativa alla legge federale sulla protezione dei dati (OLPD);

vista l'ordinanza del 4 luglio 2007<sup>4</sup> sulla protezione delle informazioni della Confederazione (ordinanza sulla protezione delle informazioni, Oprl, stato 1° agosto 2007);

vista la direttiva del DFGP del 30 settembre 2004 sull'installazione di collegamenti online e il rilascio di autorizzazioni d'accesso ad applicazioni informatiche del DFGP (direttiva online DFGP);

nel rispetto del concordato del 15 novembre 2007<sup>5</sup> della Conferenza dei direttori cantonali di giustizia e polizia sulle misure contro la violenza in occasione di manifestazioni sportive;

*emana le seguenti direttive:*

*Uso della forma maschile:*

*per ragioni di leggibilità, si è scelto di utilizzare la forma maschile per indicare persone di entrambi i sessi.*

---

1 RS 120

2 RS 120.52.

3 RS 235.11

4 RS 510.411

5 Secondo l'articolo 15 del concordato, quest'ultimo entra in vigore non appena almeno due Cantoni vi aderiscono, ma non prima del 1° gennaio 2010, cfr. allegato 5.

## SEZIONE 1 DISPOSIZIONI GENERALI

### Art. 1 Contenuto

Il regolamento sul trattamento dei dati descrive le procedure di trattamento dei dati e di controllo nonché la gestione del sistema d'informazione HOOGAN (HOOGAN). Esso contiene informazioni sull'organo responsabile della protezione e della sicurezza dei dati, sulla provenienza dei dati e lo scopo per cui essi sono resi noti regolarmente. Descrive infine la procedura per l'assegnazione dei diritti d'accesso a HOOGAN.

### Art. 2 Nozioni

Definizioni:

- a. *Dipartimento*: il Dipartimento federale di giustizia e polizia (DFGP);
- b. *fedpol*: l'Ufficio federale di polizia;
- c. *Detentore dei dati*: l'Ufficio federale responsabile di HOOGAN;
- d. *Responsabile HOOGAN*: il servizio di fedpol responsabile dell'intero sistema HOOGAN che presiede il comitato di progetto;
- e. *Responsabile dell'applicazione HOOGAN*: il servizio di fedpol responsabile dell'applicazione HOOGAN per quanto riguarda gli utenti. Il responsabile dell'applicazione HOOGAN è membro del comitato di progetto. Si occupa anche della pianificazione, dello sviluppo e della gestione del sistema. Funge inoltre da punto di contatto per gli utenti e da amministratore degli utenti HOOGAN. In qualità di responsabile della formazione HOOGAN, redige la documentazione per la formazione e i manuali per l'uso e organizza corsi di base e di ripetizione per i collaboratori autorizzati ad accedere al sistema della Confederazione, dei Cantoni, dei Comuni, del Servizio centrale svizzero in materia di tifoseria violenta e del Corpo delle guardie di confine (Cgcf);
- f. *Controllo qualità HOOGAN*: il servizio di fedpol responsabile della registrazione e del controllo dei dati nonché del rispetto delle basi legali. Il controllo qualità HOOGAN verifica l'esattezza dei dati registrati dai servizi competenti dei Cantoni e delle città e successivamente li trasferisce nel sistema di produzione oppure li rispedisce al servizio autore della registrazione, indicandone il motivo;
- g. *Specialista HOOGAN*: il servizio di fedpol responsabile dell'amministrazione dei dati di base non personali di HOOGAN (registrazione di manifestazioni, organizzazioni ecc.);
- h. *settore Tifoseria violenta*: il servizio di fedpol incaricato della gestione di HOOGAN. Ne fanno parte il responsabile dell'applicazione HOOGAN, il controllo qualità HOOGAN e gli specialisti HOOGAN;
- i. *Incaricato della protezione dei dati e della protezione delle informazioni di fedpol*: la sezione del Servizio giuridico di fedpol responsabile del rispetto delle prescrizioni in materia di protezione dei dati delle applicazioni di fedpol;

- j. *Corpo delle guardie di confine (Cgcf)*: il servizio che applica divieti d'entrata e divieti di recarsi in un Paese determinato;
- k. *Amministratore degli utenti Cgcf*: collaboratore del Cgcf incaricato del trattamento delle autorizzazioni d'accesso al sistema HOOGAN;
- l. *CSI DFGP*: il Centro servizi informatici del Dipartimento;
- m. *Servizio tifoseria violenta (SZH)*: il Servizio centrale svizzero in materia di tifoseria violenta (la sigla deriva dal tedesco Schweizerische Zentralstelle Hooliganismus);
- n. *Amministratore cantonale degli utenti*: registra e gestisce i dati sugli utenti delle polizie cantonali, cittadine e comunali e li comunica mediante richiesta d'accesso al responsabile dell'applicazione HOOGAN;
- o. *Organizzatore di manifestazioni sportive*: qualsiasi organizzatore di manifestazioni sportive autorizzato a ricevere dati provenienti da HOOGAN;
- p. *Autorità estera*: l'organo estero competente in materia di sicurezza, autorizzato a ricevere dati provenienti da HOOGAN;
- q. *RIPOL*: il sistema informatizzato di ricerca;
- r. *Manifestazioni sportive*: tutte le manifestazioni sportive nazionali e internazionali;
- s. *Rapporto sulla manifestazione sportiva*: rapporto contenente informazioni, non personali relative agli interventi di polizia durante le manifestazioni sportive;
- t. *Accesso integrale*: accesso a HOOGAN che consente di leggere, registrare, modificare o cancellare i dati;
- u. *Accesso limitato*: accesso a HOOGAN via RIPOL, che consente unicamente di leggere i dati attivi al momento della consultazione;
- v. *Portale SSO DFGP*: il portale elettronico Single Sign On (SSO) del Dipartimento che mette a disposizione un sistema di autenticazione unico per tutte le applicazioni specifiche come, ad esempio, per l'accesso integrale a HOOGAN.
- w. *Utente*: il collaboratore di un'autorità di polizia cantonale o cittadina all'interno di un cosiddetto servizio specializzato decentrato.

### **Art. 3    Scopo**

fedpol gestisce, conformemente all'articolo 24a capoverso 1 LMSI, il sistema d'informazione elettronico HOOGAN nel quale sono registrati dati relativi a persone che hanno avuto un comportamento violento in occasione di manifestazioni sportive in Svizzera o all'estero. Gli eventi e i rapporti registrati relativi alle manifestazioni sportive fungono da base per la redazione di rapporti di analisi e l'allestimento di statistiche.

**Art. 4      Struttura di HOOGAN**

In HOOGAN sono registrati sia i dati personali soggetti alla legge federale del 19 giugno 1992 sulla protezione dei dati (LPD)<sup>6</sup> sia i dati sulle manifestazioni sportive che, essendo di carattere non personale, non sono soggetti alla LPD.

**SEZIONE 2 AUTORITÀ E SERVIZI****Art. 5      Organi di fedpol**

<sup>1</sup> fedpol è l'organo federale responsabile di HOOGAN e detentore dei dati del sistema<sup>7</sup>. In seno a fedpol la competenza per HOOGAN è attribuita al settore Tifoseria violenta della divisione principale Servizi.

<sup>2</sup> Il responsabile dell'applicazione HOOGAN è responsabile dell'applicazione HOOGAN per quanto riguarda gli utenti. È inoltre membro del comitato di progetto. Si occupa anche della pianificazione, dello sviluppo e della gestione del sistema. Funge inoltre da punto di contatto per gli utenti e da amministratore degli utenti HOOGAN. In qualità di responsabile della formazione HOOGAN, redige la documentazione per la formazione e i manuali d'uso e organizza corsi di base e di ripetizione per i collaboratori autorizzati ad accedere al sistema della Confederazione, dei Cantoni, dei Comuni, del Servizio centrale svizzero in materia di tifoseria violenta e del Corpo delle guardie di confine (Cgcf).

<sup>3</sup> Il controllo qualità HOOGAN del settore Tifoseria violenta vigila sul rispetto, da parte degli utenti, delle basi legali, in particolare della LMSI, dell'ordinanza sulle misure di polizia amministrativa e i sistemi d'informazione dell'Ufficio federale di polizia, della LPD nonché del regolamento sul trattamento dei dati. È incaricato di verificare, correggere, accettare o respingere i dati registrati provvisoriamente.

<sup>4</sup> Lo specialista HOOGAN è responsabile dell'amministrazione dei dati di base non personali di HOOGAN.

**Art. 6      CSI DFGP**

Il CSI DFGP, in qualità di fornitore di servizi del sistema d'informazione HOOGAN, è responsabile della gestione e del rispetto delle prescrizioni tecniche in materia di sicurezza informatica.

**Art. 7      SZH**

L'SZH è incaricato di eseguire una prima valutazione delle comunicazioni pervenute in materia di divieti di accedere a stadi e dei rapporti sulle manifestazioni sportive redatti dagli organizzatori delle medesime. È competente inoltre per le richieste relative ai divieti di recarsi in un Paese determinato, le interdizioni di accedere a un'area e all'obbligo di presentarsi alla polizia. L'SZH verifica, corregge e accetta o respinge i dati registrati provvisoriamente.

---

6 RS 235.1

7 Art. 24a cpv. 1 LMSI

**Art. 8 Cgcf**

<sup>1</sup> Per verificare l'identità di una persona, il Cgcf può consultare i dati personali e le misure contenuti in HOOGAN. Alcuni collaboratori designati del Cgcf beneficiano di un accesso integrale a HOOGAN<sup>8</sup>.

<sup>2</sup> fedpol comunica al Cgcf ogni misura relativa a un divieto di recarsi in un Paese determinato.

**Art. 9 Organi cantonali**

<sup>1</sup> I collaboratori responsabili delle autorità di polizia dei Cantoni e delle città<sup>9</sup> immettono i propri dati in HOOGAN, li modificano e li trasmettono al controllo qualità HOOGAN per il trasferimento nel sistema di produzione oppure li cancellano senza indugio. Gli altri servizi possono accedere a HOOGAN esclusivamente per identificare le persone in caso di violenza in occasione di manifestazioni sportive.

<sup>2</sup> Ogni corpo di polizia designa le persone incaricate del buon funzionamento di HOOGAN. Designa in particolare:

- a. gli utenti che registrano provvisoriamente i dati in HOOGAN e trasmettono la relativa documentazione all'SZH o al settore Tifoseria violenta. Tali utenti garantiscono che i dati da essi trasmessi ai suddetti servizi o registrati direttamente in HOOGAN siano corretti e completi;
- b. almeno una persona nel ruolo di amministratore cantonale degli utenti, incaricata di prestare assistenza al corpo cantonale di polizia e alle polizie cittadine e comunali e collegate al sistema e di verificare che esse rispettino la LMSI, l'ordinanza sulle misure di polizia amministrativa e i sistemi d'informazione dell'Ufficio federale di polizia nonché il presente regolamento;
- c. un addetto alla formazione che funge da interlocutore cantonale per tutte le questioni relative alla formazione HOOGAN e si adopera affinché gli utenti cantonali di HOOGAN possano seguire i corsi di formazione necessari nel proprio Cantone o presso il settore Tifoseria violenta. L'addetto alla formazione riceve dal responsabile della formazione HOOGAN la consulenza, il sostegno e la documentazione necessari per organizzare i corsi in seno al proprio corpo di polizia. Trasmette inoltre alle polizie cittadine e comunali competenti le informazioni ricevute dal settore Tifoseria violenta.

<sup>3</sup> I Cantoni designano un organo di controllo incaricato di vigilare sull'osservanza della protezione dei dati di HOOGAN. L'organo di controllo garantisce l'osservanza delle disposizioni in materia di protezione dei dati e di sicurezza delle informazioni e funge da interlocutore di fedpol.

---

8 Art. 9 cpv. 1 lett. d dell'ordinanza sulle misure di polizia amministrativa e i sistemi d'informazione dell'Ufficio federale di polizia

9 Art. 24a cpv. 7 LMSI e art. 9 cpv. 1 dell'ordinanza sulle misure di polizia amministrativa e i sistemi d'informazione dell'Ufficio federale di polizia

## SEZIONE 3 UTENTI E ACCESSO AI DATI

### Art. 10 Utenti

<sup>1</sup> HOOGAN è a disposizione dei servizi di fedpol competenti, dei servizi specializzati decentrati delle autorità di polizia cantonali e cittadine, dell'SZH e delle autorità doganali, mediante una procedura di richiamo<sup>10</sup>.

<sup>2</sup> Per l'attribuzione dei diritti d'accesso si applicano misure di sicurezza adeguate.

### Art. 11 Autorizzazione individuale d'accesso

<sup>1</sup> L'autorizzazione di accesso a HOOGAN è rilasciata a ogni utente a titolo personale (profilo d'accesso) e non può essere trasferita a terzi.

<sup>2</sup> Le richieste d'accesso vanno inoltrate al settore Tifoseria violenta mediante il modulo del DFGP disponibile su Internet, firmato dal superiore diretto. Il settore Tifoseria violenta verifica la completezza delle richieste e la loro conformità ai principi di cui alla sezione 4 della direttiva online DFGP e le trasmette al direttore di fedpol che decide in merito.

<sup>3</sup> Il responsabile dell'applicazione HOOGAN registra e gestisce ogni singolo utente.

<sup>4</sup> Le richieste d'accesso delle polizia cantonali o cittadine vanno trasmesse all'amministratore cantonale o cittadino degli utenti. Questi verifica la loro completezza e la loro conformità ai principi di cui alla sezione 4 della direttiva online DFGP e decide se accoglierle. L'amministratore cantonale o cittadino degli utenti registra e gestisce gli utenti delle polizie cantonali e cittadine.

<sup>5</sup> Le richieste d'accesso delle polizie comunali vanno trasmesse al competente amministratore cantonale degli utenti. Questi verifica la loro completezza e la loro conformità ai principi di cui alla sezione 4 della direttiva online DFGP e decide se accoglierle. L'amministratore cantonale degli utenti registra e gestisce gli utenti delle polizie comunali del proprio Cantone.

<sup>6</sup> Le richieste d'accesso delle autorità cantonali (escluse le polizie cantonali, cittadine e comunali) vanno trasmesse al settore Tifoseria violenta di fedpol. Questi verifica la loro completezza e la loro conformità ai principi di cui alla sezione 4 della direttiva online DFGP e decide se accoglierle. Il responsabile dell'applicazione HOOGAN registra e gestisce gli utenti delle autorità cantonali.

<sup>7</sup> Le richieste relative ad autorizzazioni individuali d'accesso per i collaboratori del CSI DFGP incaricati dello sviluppo e della manutenzione del sistema d'informazione HOOGAN vanno trasmesse al responsabile dell'applicazione HOOGAN. Questi verifica la loro completezza e la loro conformità ai principi di cui alla sezione 4 della direttiva online DFGP e le trasmette al direttore di fedpol. Il responsabile dell'applicazione HOOGAN registra e gestisce gli accessi dei collaboratori del CSI DFGP. Verifica inoltre periodicamente se gli accessi autorizzati sono ancora giustificati.

<sup>8</sup> Agli utenti in formazione possono essere concesse autorizzazioni d'accesso mediante una procedura semplificata. Tali utenti hanno accesso al sistema di formazione HOOGAN, completamente separato dal sistema di produzione. Se a uno di questi

---

10 Art. 24a cpv. 7 LMSI

utenti è concessa un'autorizzazione d'accesso al sistema di produzione, il responsabile dell'applicazione HOOGAN provvede a cancellare tale accesso senza preavviso.

<sup>9</sup> I diritti d'accesso sono attribuiti conformemente alle disposizioni della direttiva online DFGP, in particolare quelle contenute nella sezione 4, nonché all'ordinanza del 4 dicembre 2009 sulle misure di polizia amministrativa e i sistemi d'informazione dell'Ufficio federale di polizia<sup>11</sup>.

## **Art. 12 Revoca dell'autorizzazione d'accesso**

<sup>1</sup> L'autorizzazione individuale d'accesso a HOOGAN è revocata se non sono più soddisfatte le condizioni di cui all'articolo 14 del presente regolamento o se la persona non necessita più di un accesso a HOOGAN per svolgere la propria attività legale. I superiori comunicano senza indugio questi cambiamenti all'amministratore degli utenti competente (art.11).

<sup>2</sup> Se HOOGAN non è utilizzato per un periodo di 60 giorni, l'autorizzazione individuale d'accesso può essere provvisoriamente sospesa. La revoca della sospensione dev'essere richiesta all'amministratore degli utenti competente (art. 11).

<sup>3</sup> Se un utente autorizzato non utilizza il sistema per oltre un anno, il responsabile dell'applicazione HOOGAN può revocare la rispettiva autorizzazione d'accesso.

<sup>4</sup> In caso di abuso di un'autorizzazione d'accesso, fedpol informa il servizio interessato e revoca la rispettiva autorizzazione d'accesso.

## **Art. 13 Formazione degli utenti**

<sup>1</sup> Prima di ottenere un'autorizzazione d'accesso, ogni utente HOOGAN è tenuto a seguire una formazione conforme al proprio profilo d'accesso.

<sup>2</sup> Il responsabile dell'applicazione HOOGAN organizza i necessari corsi di base e di ripetizione in tedesco e in francese. Si occupa dell'istruzione dei formatori in ogni Cantone e all'interno del Cgcf. I formatori sono successivamente chiamati a istruire, a loro volta, gli utenti nel rispettivo settore di competenza.

<sup>3</sup> Il manuale d'applicazione offre supporto all'utente in tutte le aree del sistema. Il manuale è redatto in tre lingue (d/f/i).

## **Art. 14 Accesso ai dati**

Gli utenti delle diverse categorie dispongono soltanto delle autorizzazioni di cui hanno effettivamente bisogno. Le autorizzazioni d'accesso per ogni singola categoria d'utente sono disciplinate nell'ordinanza del 4 dicembre 2009 sulle misure di polizia amministrativa e i sistemi d'informazione dell'Ufficio federale di polizia. Il diritto di registrare dati e di modificarli è limitato alle persone che svolgono effettivamente queste attività. Le autorizzazioni d'accesso a HOOGAN (consultazione, registrazione e modifica) sono disciplinate nel modo seguente per ogni categoria d'utente. Le seguenti descrizioni si riferiscono tuttavia alla portata massima dell'accesso per ogni singola categoria:

---

<sup>11</sup> RS 120.52

- a. *utenti autorizzati alla consultazione*: gli utenti autorizzati alla consultazione beneficiano dell'accesso necessario per svolgere i propri compiti legali;
- b. *utenti autorizzati ad apportare modifiche legate a diffusioni attive all'interno di un Cantone*: in ogni polizia cantonale vi sono uno o più servizi di controllo che verificano le diffusioni attive registrate dai servizi esterni. Non è previsto alcun limite al numero di servizi esterni per ogni Cantone;
- c. *specialisti HOOGAN e controllo qualità HOOGAN*: gli specialisti e il controllo qualità HOOGAN beneficiano dell'accesso per il controllo delle registrazioni dei Cantoni e il loro trasferimento nel sistema di produzione;
- d. *l'incaricato della protezione dei dati e della protezione delle informazioni di fedpol*: beneficia di un accesso per controllare la registrazione cronologica relativa ai dati e rispondere alle richieste d'informazioni da parte di terzi;
- e. *CSI DFGP*: il personale addetto allo sviluppo del sistema, gli specialisti delle banche dati e dell'helpdesk dispongono dell'accesso necessario per poter svolgere la propria attività;
- f. il responsabile HOOGAN ai sensi dell'articolo 2 lett. d.

#### **Art. 15 Accesso ai dati sulle persone e sugli eventi**

<sup>1</sup> L'accesso per la registrazione in HOOGAN dei dati personali (fotografia, cognome, nome, data e luogo di nascita, luogo d'origine, indirizzo, tipo di misura e motivo della misura) e degli avvenimenti (rapporti sui fatti, rapporti sulle manifestazioni sportive, luogo, eventi, organizzazioni, registrazioni video) è limitato a un numero ristretto di utenti per Cantone.

<sup>2</sup> Le autorizzazioni d'accesso sono disciplinate dall'articolo 24a capoverso 7 LMSI e dall'articolo 9 dell'ordinanza del 4 dicembre 2009 sulle misure di polizia amministrativa e i sistemi d'informazione dell'Ufficio federale di polizia.

### **SEZIONE 4 TRATTAMENTO DEI DATI**

#### **Art. 16 Registrazione in HOOGAN**

Conformemente all'articolo 24a capoverso 2 LMSI, affinché nel sistema d'informazione possano essere registrati dati relativi a persone nei confronti delle quali sono state adottate misure quali il divieto d'accedere a stadi, l'interdizione di accedere a un'area, l'obbligo di presentarsi alla polizia e il fermo preventivo di polizia oppure il divieto di recarsi in un Paese determinato, è necessario che sia soddisfatta una delle seguenti condizioni:

- a. la misura è stata pronunciata o confermata da un'autorità giudiziaria;
- b. la misura è stata pronunciata in seguito a un reato denunciato alle autorità competenti;
- c. la misura è necessaria per la salvaguardia della sicurezza delle persone o della manifestazione sportiva e si può rendere verosimile che è giustificata.

## **Art. 17 Misure**

<sup>1</sup> Le misure<sup>12</sup> contro la violenza in occasione di manifestazioni sportive comprendono segnatamente:

- a. il divieto di accedere a stadi;
- b. l'interdizione di accedere a un'area;
- c. il divieto di recarsi in un Paese determinato;
- d. l'obbligo di presentarsi alla polizia;
- e. il fermo preventivo di polizia.

<sup>2</sup> Ad eccezione del divieto di recarsi in un Paese determinato e del divieto di accedere a stadi, le misure sono registrate provvisoriamente dai servizi competenti dei Cantoni e delle città. L'SZH effettua una prima selezione delle comunicazioni degli organizzatori di manifestazioni sportive (divieti di accedere a stadi) e delle polizie cantonali, a condizione che non si tratti di dati personali (rapporti sulle manifestazioni sportive). I servizi competenti dei Cantoni e delle città o gli organizzatori di manifestazioni sportive inviano all'SZH, attraverso HOOGAN, le comunicazioni corredate delle necessarie informazioni. I Cantoni inviano i dati personali di cui sono in possesso direttamente al settore Tifoseria violenta. L'SZH verifica la correttezza e la rilevanza delle informazioni e trasmette le informazioni su tali misure al settore Tifoseria violenta oppure le rispedisce al servizio cantonale unitamente a un messaggio d'errore.

## **Art. 18 Divieto di recarsi in un Paese determinato**

La decisione di un divieto di recarsi in un Paese determinato compete a fedpol. I Cantoni e l'SZH possono presentare richieste in tal senso. Oltre a essere registrato in RIPOL, ogni divieto pronunciato è comunicato al Cgcf e alle autorità doganali e di polizia estere.

## **Art. 19 Registrazione e controllo dei dati**

<sup>1</sup> Il servizio specializzato decentrato del Cantone registra in HOOGAN in un modulo di registrazione provvisorio i dati e le immagini in suo possesso. I dati personali sono verificati e registrati dal settore Tifoseria violenta, i dati relativi alle manifestazioni dall'SZH.

<sup>2</sup> Il settore Tifoseria violenta verifica se le informazioni che gli vengono trasmesse sono corrette e rilevanti ai sensi dell'articolo 24a capoverso 6 LMDI, e rispedisce al mittente, indicandone il motivo, le informazioni incomplete o irrilevanti, affinché siano completate o cancellate.

<sup>3</sup> Le comunicazioni provenienti dall'estero sono inviate direttamente al settore Tifoseria violenta. Il settore Tifoseria violenta esamina i dati, decide in merito alla loro registrazione e li immette in HOOGAN.

---

<sup>12</sup> L'interdizione di accedere a un'area, l'obbligo di presentarsi alla polizia e il fermo preventivo di polizia sono disciplinate dal 1° gennaio 2010 dal concordato sulle misure contro la violenza in occasione di manifestazioni sportive (cfr. allegato 5).

**Art. 20 Registrazione dei dati**

In HOOGAN i dati possono essere registrati in tedesco, francese o italiano. I dati immessi nei campi contenenti una lista di valori predefiniti sono tradotti automaticamente.

**Art. 21 Durata di conservazione**

La durata di conservazione dei dati personali è disciplinata dall'articolo 12 dell'ordinanza sulle misure di polizia amministrativa e i sistemi d'informazione dell'Ufficio federale di polizia, secondo cui i dati personali e le informazioni concernenti una singola misura sono cancellati trascorsi tre anni dalla scadenza della stessa. Se durante questi tre anni è registrata una nuova misura nei confronti della medesima persona, la durata di conservazione della prima registrazione è prorogata di tre anni a partire dalla data di registrazione della seconda misura; per la cancellazione di quest'ultima si applica lo stesso principio. Le singole misure sono tuttavia cancellate al più tardi dopo dieci anni.

**Art. 22 Comunicazione dei dati**

<sup>1</sup> La trasmissione dei dati registrati in HOOGAN è disciplinata dagli articoli 24a capoverso 8 e 9 BWIS e dagli articoli 10 e 11 dell'ordinanza sulle misure di polizia amministrativa e i sistemi d'informazione dell'Ufficio federale di polizia. Tali dati possono essere comunicati, per l'adempimento dei rispettivi compiti legali, agli organizzatori di manifestazioni sportive in Svizzera nonché alle autorità di polizia, di confine e agli organi di sicurezza all'estero. La trasmissione all'estero è disciplinata dall'articolo 17 capoversi 3-5 LMSI.

<sup>2</sup> Al termine della manifestazione sportiva, i responsabili della sicurezza o gli organizzatori della manifestazione in Svizzera cancellano immediatamente i dati loro forniti dal settore Tifoseria violenta. Entro 24 ore essi sono tenuti a notificare spontaneamente la cancellazione al settore Tifoseria violenta.

<sup>3</sup> Il settore Tifoseria violenta esegue dei controlli a campione per verificare che gli organizzatori delle manifestazioni sportive e i loro responsabili della sicurezza utilizzino i dati conformemente alla legge.

<sup>4</sup> La direttiva del 1° gennaio 2010 sull'utilizzo e il trattamento dei dati del sistema d'informazione HOOGAN da parte degli organizzatori di manifestazioni sportive e dei loro responsabili della sicurezza è direttamente applicabile (allegato 4).

**Art. 23 Stampa e ulteriore utilizzo dei dati**

<sup>1</sup> HOOGAN permette di stampare dati e di allestire elenchi.

<sup>2</sup> Da HOOGAN gli utenti possono trasferire sul PC dati su singoli eventi, con le relative entità principali, per allestire un rapporto di polizia o di consegna. In questi casi va rispettato l'articolo 13 dell'ordinanza sulle misure di polizia amministrativa e i sistemi d'informazione dell'Ufficio federale di polizia.

<sup>3</sup> Gli utenti possono allestire file di dati non elaborati, ossia, dopo aver effettuato una ricerca, possono scaricare sul PC il contenuto dei campi selezionati. I dati ottenuti,

utili per far luce sui reati, possono essere ulteriormente impiegati per eseguire analisi criminali.

<sup>4</sup> Gli amministratori degli utenti possono creare, a scopo di controllo, file di dati non elaborati a partire dalla gestione degli utenti.

<sup>5</sup> Tutti i dati e gli elenchi summenzionati registrati localmente e temporaneamente devono essere definitivamente cancellati immediatamente dopo l'uso.

<sup>6</sup> I dati e gli elenchi stampati sono soggetti alle stesse disposizioni sulla conservazione, il trattamento, la comunicazione e la distruzione dei dati applicabili ai dati trattati elettronicamente in HOOGAN. In caso di trasmissione di dati stampati che sono già stati registrati da un altro servizio in un'altra categoria, occorre prestare particolare attenzione alle loro possibilità di utilizzo.

#### **Art. 24    Informazione delle persone interessate**

I diritti delle persone interessate sono disciplinati dall'articolo 24a capoverso 10 LMSI. Chiunque può domandare all'incaricato della protezione dei dati e della protezione delle informazioni di fedpol se in HOOGAN sono trattati dati che lo concernono e chiedere la rettifica di dati inesatti.

### **SEZIONE 5 CANCELLAZIONE E ARCHIVIO FEDERALE**

#### **Art. 25    Cancellazione dei dati e comunicazione ai Cantoni**

<sup>1</sup> La durata massima di conservazione dei dati personali è disciplinata dall'articolo 12 dell'ordinanza sulle misure di polizia amministrativa e i sistemi d'informazione dell'Ufficio federale di polizia. Il settore Tifoseria violenta fissa un termine più breve, di tipo generico, alla cui scadenza si valuta se è necessario che la registrazione resti nel sistema. Ciò permette di constatare quando scade il termine di conservazione massimo dei singoli dati personali. Per quanto riguarda le comunicazioni, il servizio specializzato decentrato è tenuto a chiarire se una misura debba essere prolungata, eventualmente fino alla scadenza del termine massimo di conservazione. Se non è richiesta nessuna proroga, la misura è cancellata dal sistema.

<sup>2</sup> Le misure revocate sono cancellate automaticamente alla fine del mese.

#### **Art. 26    Consegna dei dati e dei documenti all'Archivio federale**

<sup>1</sup> I dati e i documenti cancellati da HOOGAN sono offerti all'Archivio federale per l'archiviazione. Non sono offerti per l'archiviazione i dati classificati provenienti direttamente da autorità di sicurezza estere e i dati trasferiti dall'estero.

<sup>2</sup> I dati cancellati da HOOGAN sono registrati nel modulo «BAR» (BAR = Bundesarchiv, ossia Archivio federale). Il responsabile dell'applicazione HOOGAN gestisce i dati registrati nel modulo «BAR» ed è responsabile degli aspetti organizzativi e tecnici del loro trasferimento all'Archivio federale svizzero e della loro successiva cancellazione.

<sup>3</sup> I documenti designati dall'Archivio come non degni di essere archiviati sono distrutti. Sono fatte salve le altre disposizioni legali in materia di distruzione dei dati.

## SEZIONE 6 SICUREZZA INFORMATICA

### **Art. 27    Sicurezza informatica**

<sup>1</sup> Alla sicurezza informatica si applicano le disposizioni delle istruzioni del CIC del 27 settembre 2004 sulla sicurezza informatica nell'Amministrazione federale (Istruzioni CIC sulla sicurezza informatica) nonché le seguenti disposizioni del presente regolamento.

<sup>2</sup> Prima di attivare per la prima volta un collegamento a HOOGAN, il servizio che lo ha richiesto deve dimostrare di adempiere i requisiti necessari<sup>13</sup>.

### **Art. 28    Sicurezza dei dati**

<sup>1</sup> Gli utenti immettono i propri dati in HOOGAN dove vengono registrati. I dati possono essere modificati dagli utenti autorizzati in virtù dell'articolo 14 del presente regolamento.

<sup>2</sup> Il CSI DFGP si occupa della sicurezza dei dati HOOGAN secondo le direttive vigenti nell'Amministrazione federale e ne allestisce regolarmente copie di sicurezza.

<sup>3</sup> In caso di perdita di dati o di interruzione di parte del sistema, è garantito il ripristino della consistenza e dell'integrità dei dati.

### **Art. 29    Misure di protezione dei dati (riservatezza) nel settore dei terminali**

<sup>1</sup> I terminali devono essere installati in zone protette, il cui accesso è sorvegliato.

<sup>2</sup> I dati stampati devono essere conservati in modo tale che terzi non li possano vedere e/o copiare. Una volta raggiunto lo scopo per cui erano stati allestiti, tali dati devono essere immediatamente distrutti.

### **Art. 30    Trasmissione sicura**

La trasmissione dei dati è eseguita direttamente in HOOGAN.

### **Art. 31    Assistenza agli utenti e obbligo di notifica**

<sup>1</sup> Gli utenti dei Cantoni ricevono assistenza tecnica in primo luogo dagli amministratori cantonali degli utenti. Se questi non sono in grado di risolvere il problema possono rivolgersi agli specialisti del settore Tifoseria violenta, i quali sono a disposizione degli utenti durante gli orari d'ufficio.

<sup>2</sup> L'assistenza tecnica per i terminali e la rete è assicurata in primo luogo dai responsabili IT. Se questi non sono in grado di risolvere il problema, si rivolgono al CSI DFGP disponibile durante gli orari d'ufficio dell'«IT Help Desk».

<sup>3</sup> Gli utenti sono informati sul livello di sicurezza di HOOGAN e sulle disposizioni relative all'uso del sistema e dei dati in esso contenuti. Essi sono a conoscenza delle

---

13 Art. 5 cpv. 1 della direttiva online del DFGP.

eventuali sanzioni in caso di violazione intenzionale o colposa della sicurezza informatica. Tutti gli utenti sono tenuti a segnalare al responsabile dell'applicazione HOOGAN le seguenti constatazioni:

- a. errori nei dati registrati, errori sull'identità delle persone registrate, errori nei dati di base o nelle loro strutture;
- b. punti deboli o difetti nella sicurezza del sistema, constatati o presunti;
- c. misure di sicurezza non applicate o non rispettate;
- d. eventi imprevisti che potrebbero ripercuotersi sulla sicurezza informatica.

### **Art. 32 Sviluppo del programma HOOGAN**

<sup>1</sup> Sviluppo, test, integrazione, formazione e produzione sono fasi nettamente distinte l'una dall'altra.

<sup>2</sup> Le richieste di ulteriore sviluppo del sistema sono raccolte e in seguito definite, annunciate, preventivate e realizzate come progetti di maggiore o minore portata.

<sup>3</sup> Con i programmi in fase di sviluppo e/o di test non è possibile accedere ai dati del sistema di produzione di HOOGAN.

<sup>4</sup> L'inserimento di programmi nel sistema di produzione è effettuato dal CSI DFGP tramite la procedura «change operativi».

### **Art. 33 Registrazione cronologica**

Ogni trattamento di dati in HOOGAN è registrato cronologicamente<sup>14</sup>. I dati registrati sono conservati per un anno.

### **Art. 34 Sorveglianza e responsabilità**

<sup>1</sup> fedpol è responsabile del sistema d'informazione HOOGAN.

<sup>2</sup> Il responsabile dell'applicazione HOOGAN vigila sul rispetto delle basi legali da parte degli utenti.

### **Art. 35 Utilizzo abusivo di HOOGAN**

<sup>1</sup> Se si sospetta o si accerta un utilizzo abusivo di HOOGAN da parte di un utente in seno all'Amministrazione federale, in particolare se si sospetta un accesso abusivo ai dati o una registrazione abusiva, l'incaricato della protezione dei dati e della protezione delle informazioni di fedpol deve esserne immediatamente informato. Per documentare i fatti, quest'ultimo può incaricare il controllo qualità HOOGAN di accertare i fatti e d'informarlo in via confidenziale. Egli informa successivamente il direttore di fedpol che, in caso di rilevanza penale, trasmette la comunicazione all'autorità competente.

---

<sup>14</sup> Art. 10 Ordinanza del 14 giugno 1993 relativa alla legge federale sulla protezione dei dati (OLPD).

<sup>2</sup> Se si sospetta o si accerta un utilizzo abusivo di HOOGAN da parte di un utente esterno all'Amministrazione federale, in particolare se si sospetta un accesso abusivo ai dati o una registrazione abusiva, l'autorità di perseguimento penale competente oppure l'incaricato della protezione dei dati e della protezione delle informazioni di fedpol devono esserne immediatamente informati. Quest'ultimo può incaricare il controllo qualità HOOGAN di accertare i fatti e d'informarlo in via confidenziale. Egli informa successivamente il direttore di fedpol che, in caso di rilevanza penale, a sua volta, ne informa l'autorità cantonale di perseguimento penale competente.

### **Art. 36 Requisiti tecnici**

<sup>1</sup> I terminali collegati al sistema presso l'Amministrazione federale, i corpi cantonali di polizia e il Cgcf devono soddisfare le prescrizioni tecniche della Confederazione.

<sup>2</sup> Tali requisiti sono stabiliti d'intesa con il CSI DFGP.

### **Art. 37 Allegati al regolamento sul trattamento dei dati HOOGAN**

<sup>1</sup> Gli allegati menzionati nel presente regolamento sul trattamento dei dati sono parte integrante del regolamento.

<sup>2</sup> Il responsabile dell'applicazione HOOGAN è responsabile del presente regolamento e del suo costante aggiornamento<sup>15</sup>.

## **SEZIONE 7 DISPOSIZIONI FINALI**

### **Art. 38 Entrata in vigore e pubblicazione**

Il presente regolamento sul trattamento dei dati sostituisce la versione del 1° gennaio 2007 ed entra in vigore il 1° gennaio 2010.

Berna, 31 dicembre 2009

### **UFFICIO FEDERALE DI POLIZIA fedpol**

del Dipartimento federale di giustizia e polizia

### **La Direttrice supplente**

Nicoletta della Valle

---

<sup>15</sup> Art. 11 Ordinanza del 14 giugno 1993 relativa alla legge federale sulla protezione dei dati (OLPD).

## ALLEGATO 1: ORDINANZA DEL 4 DICEMBRE 2009 SULLE MISURE DI POLIZIA AMMINISTRATIVA E I SISTEMI D'INFORMAZIONE DELL'UFFICIO FEDERALE DI POLIZIA

*Il Consiglio federale svizzero,*

visti gli articoli 5 capoverso 2, 11 capoverso 1, 15 capoversi 3 e 5, 24a capoversi 7 e 8, 26 capoverso 3 nonché 30 della legge federale del 21 marzo 1997 sulle misure per la salvaguardia della sicurezza interna (LMSI),

visti gli articoli 31c, 32a e 32b della legge del 20 giugno 19972 sulle armi (LArm),

ordina:

### **Sezione 1: Disposizioni generali**

#### **Art. 1 Oggetto**

La presente ordinanza disciplina:

- a. l'esecuzione di misure di polizia amministrativa, sulla base della LMSI, da parte dell'Ufficio federale di polizia (fedpol);
- b. il sistema d'informazione HOOGAN di fedpol;
- c. le banche dati dell'Ufficio centrale Armi e dell'Ufficio centrale Esplosivi e pirotecnica di fedpol.

#### **Art. 2 Collaborazione tecnico-scientifica**

<sup>1</sup> Fedpol può collaborare con servizi tecnico-scientifici, in particolare con il Servizio di ricerca scientifica di Zurigo (SRS). La collaborazione è disciplinata su base contrattuale.

<sup>2</sup> Nel caso di mandati conferiti a servizi tecnico-scientifici si applicano le disposizioni del diritto federale sulla protezione dei dati. I servizi incaricati devono salvaguardare il segreto d'ufficio.

### **Sezione 2:**

#### **Misure di polizia amministrativa contro il materiale di propaganda**

##### **Art. 3**

<sup>1</sup> Fedpol decide in merito al sequestro e alla confisca di materiale di propaganda ai sensi dell'articolo 13a LMSI dopo aver consultato il Servizio delle attività informative della Confederazione (SIC).

<sup>2</sup> L'autorità che mette al sicuro il materiale di propaganda lo trasmette senza indugio al SIC e informa quest'ultimo sulle circostanze della messa al sicuro e sulle persone e le società coinvolte.

<sup>3</sup> Fedpol confisca il materiale se l'incitamento alla violenza è concreto e serio.

<sup>4</sup> Fedpol distrugge il materiale confiscato, salvo che possa essere impiegato a scopi d'istruzione.

### **Sezione 3:**

#### **Misure di polizia amministrativa contro la violenza in occasione di manifestazioni sportive**

##### **Art. 4 Comportamento violento**

<sup>1</sup> Un comportamento violento è considerato tale segnatamente se una persona ha commesso o incitato a commettere:

- a. reati contro la vita e l'integrità della persona ai sensi degli articoli 111–113, 117, 122, 123, 125 capoverso 2, 129, 133 e 134 del Codice penale (CP);
- b. danneggiamenti ai sensi dell'articolo 144 CP;
- c. coazione ai sensi dell'articolo 181 CP;
- d. incendio intenzionale ai sensi dell'articolo 221 CP;
- e. esplosione ai sensi dell'articolo 223 CP;
- f. pubblica istigazione a un crimine o alla violenza ai sensi dell'articolo 259 CP;
- g. sommossa ai sensi dell'articolo 260 CP;
- h. violenza o minaccia contro le autorità e i funzionari ai sensi dell'articolo 285 CP.

<sup>2</sup> È inoltre considerato comportamento violento minacciare la sicurezza pubblica trasportando o utilizzando armi, esplosivi, polvere da sparo o pezzi pirotecnici in impianti sportivi, in loro prossimità o nel viaggio di andata e ritorno verso e da impianti sportivi.

**Art. 5 Prova del comportamento violento**

<sup>1</sup> Sono considerate prove di un comportamento violento:

- a. sentenze giudiziarie o denunce della polizia pertinenti;
- b. dichiarazioni attendibili o registrazioni visive della polizia, dell'Amministrazione delle dogane, del personale addetto alla sicurezza o delle federazioni e delle società sportive;
- c. divieti di accedere a stadi pronunciati dalle federazioni o dalle società sportive;
- d. comunicazioni di un'autorità straniera competente in materia.

<sup>2</sup> Le dichiarazioni ai sensi del capoverso 1 lettera b sono messe per scritto e firmate.

**Art. 6 Competenza e obbligo di comunicazione**

<sup>1</sup> I Cantoni nonché le autorità e gli uffici di cui all'articolo 13 LMSI sono tenuti a comunicare spontaneamente a fedpol informazioni e conoscenze relative ad atti di violenza commessi in occasione di manifestazioni sportive.

<sup>2</sup> Inoltre i Cantoni comunicano a fedpol:

- a. le decisioni, le revoche e le modifiche delle misure seguenti:
  1. il divieto di accedere a stadi,
  2. l'interdizione di accedere a un'area,
  3. l'obbligo di presentarsi alla polizia,
  4. il fermo preventivo di polizia;
- b. le violazioni delle misure di cui alla lettera a;
- c. le aree da loro interdette, allegando le relative piantine.

<sup>3</sup> Fedpol stabilisce la scala delle piantine di cui al capoverso 1 lettera c.

**Art. 7 Divieto limitato di lasciare la Svizzera**

<sup>1</sup> A fedpol compete la decisione di un divieto limitato di lasciare la Svizzera.

<sup>2</sup> La decisione definisce esattamente la durata del divieto e i Paesi di destinazione interessati.

<sup>3</sup> Una manifestazione sportiva inizia con il primo e termina con l'ultimo evento ufficiale che ne fanno parte.

<sup>4</sup> Si deve presumere che una persona parteciperà ad atti violenti in occasione di manifestazioni sportive in un determinato Paese, segnatamente se:

- a. ha partecipato ad atti violenti in Svizzera;
- b. è già nota in base alle informazioni fornite dai servizi di polizia stranieri sulla sua partecipazione ad atti violenti all'estero; oppure
- c. è membro di un gruppo che ha già partecipato ad atti violenti in Svizzera o all'estero.

<sup>5</sup> Per decidere un divieto limitato di lasciare la Svizzera devono inoltre sussistere indizi sull'intenzione della persona o del gruppo in questione di recarsi all'estero per seguire la manifestazione sportiva.

<sup>6</sup> Elementi concreti e attuali tali da giustificare un divieto limitato di lasciare la Svizzera, non preceduto da un'interdizione di accedere a un'area per aver commesso atti di violenza in occasione di manifestazioni sportive, sussistono se una persona:

- a. secondo le informazioni fornite da servizi di polizia stranieri ha commesso atti violenti all'estero;
- b. è membro di un gruppo che ha già più volte partecipato ad atti violenti in Svizzera o all'estero; e
- c. risulta certo che essa o il gruppo sono intenzionati a recarsi all'estero per seguire una determinata manifestazione sportiva.

<sup>7</sup> Il divieto limitato di lasciare la Svizzera, oltre a essere registrato nel sistema di ricerca informatizzato di polizia (RIPOL), è comunicato alle autorità di confine nonché alle competenti autorità doganali e di polizia straniere.

**Sezione 4: Sistema d'informazione HOOGAN****Art. 8 Dati**

<sup>1</sup> Nel sistema d'informazione elettronico HOOGAN sono registrati i dati delle persone che hanno avuto un comportamento violento in occasione di manifestazioni sportive in Svizzera e all'estero e contro cui è stata pronunciata una misura di cui all'articolo 6 capoverso 2 lettera a.

<sup>2</sup> In HOOGAN sono inoltre registrate le manifestazioni sportive, come pure gli avvenimenti a esse collegati e le aree interdette dai Cantoni.

**Art. 9 Diritti d'accesso**

<sup>1</sup> Le seguenti autorità possono accedere a HOOGAN esclusivamente per gli scopi seguenti:

- a. i servizi seguenti di fedpol:

1. il settore Tifoseria violenta: per gestire HOOGAN, per pronunciare divieti limitati di lasciare la Svizzera, per scambiare informazioni come previsto dalla legge nonché per analizzare e valutare la situazione,
  2. la Centrale operativa di fedpol: per identificare le persone in relazione alla violenza in occasione di manifestazioni sportive,
  3. l'Incaricato della protezione dei dati e della protezione delle informazioni di fedpol: per trattare le richieste d'informazione e di cancellazione dei dati registrati in HOOGAN;
- b. i collaboratori delle autorità di polizia dei Cantoni responsabili di prevenire la violenza in occasione di manifestazioni sportive: per pronunciare interdizioni di accedere a un'area, obblighi di presentarsi alla polizia e fermi preventivi di polizia, per analizzare e valutare la situazione e per trasmettere dati personali agli organizzatori di manifestazioni sportive in Svizzera;
  - c. i servizi delle autorità di polizia dei Cantoni: per identificare le persone in relazione alla violenza in occasione di manifestazioni sportive;
  - d. i servizi del Corpo delle guardie di confine (Cgcf) dell'Amministrazione federale delle dogane (AFD): per applicare i divieti limitati di lasciare la Svizzera e i divieti di entrata;
  - e. le unità del Servizio centrale svizzero in materia di tifoseria violenta (Servizio centrale): per eseguire una prima valutazione delle comunicazioni pervenute in materia di divieti di accedere a stadi e dei rapporti sulle manifestazioni sportive redatti dagli organizzatori delle medesime, nonché per richiedere di pronunciare divieti limitati di lasciare la Svizzera, interdizioni di accedere a un'area e obblighi di presentarsi alla polizia.
- <sup>2</sup> Per accedere a HOOGAN può essere concesso un diritto d'accesso integrale o limitato. L'accesso integrale consente di leggere, inserire, modificare e cancellare i dati. L'accesso limitato consente unicamente di leggere i dati attivi al momento della consultazione.
- <sup>3</sup> Beneficiano dell'accesso integrale:
- a. il settore Tifoseria violenta;
  - b. il Servizio centrale;
  - c. i collaboratori delle autorità di polizia dei Cantoni e del Cgcf responsabili di prevenire la violenza in occasione di manifestazioni sportive.
- <sup>4</sup> Beneficiano dell'accesso limitato:
- a. la Centrale operativa di fedpol;
  - b. l'Incaricato della protezione dei dati e della protezione delle informazioni di fedpol;
  - c. le autorità di polizia dei Cantoni;
  - d. il Cgcf.
- <sup>5</sup> L'accesso limitato delle autorità di polizia dei Cantoni e del Cgcf funziona per mezzo di un'interfaccia nel sistema d'informazione RIPOL.
- <sup>6</sup> Il Dipartimento federale di giustizia e polizia (DFGP) disciplina i dettagli dei diritti d'accesso e le premesse per il collegamento delle autorità a HOOGAN.
- <sup>7</sup> Il direttore di fedpol o il suo supplente decidono in merito alle richieste d'accesso individuali.
- <sup>8</sup> In seno a fedpol la responsabilità per HOOGAN è assunta dal settore Tifoseria violenta.

#### **Art. 10 Utilizzazione e trasmissione dei dati da parte di organizzatori**

- <sup>1</sup> Gli organizzatori di manifestazioni sportive sono autorizzati a trasmettere i dati registrati in HOOGAN ai responsabili della sicurezza di tali manifestazioni unicamente con il consenso dell'autorità che ha fornito i dati e soltanto per eseguire misure contro la violenza in occasione di manifestazioni sportive.
- <sup>2</sup> I responsabili della sicurezza sono autorizzati a trattare i dati unicamente in relazione alla manifestazione sportiva designata dall'autorità. A questo scopo sono autorizzati a trattare i dati in sistemi elettronici d'identificazione delle persone.
- <sup>3</sup> Dopo la manifestazione sportiva i responsabili della sicurezza e, se del caso, gli organizzatori della manifestazione cancellano immediatamente i dati. L'autorità che ha fornito i dati è informata entro 24 ore della cancellazione.
- <sup>4</sup> Fedpol disciplina nel regolamento sul trattamento dei dati l'utilizzazione e il trattamento dei dati da parte degli organizzatori di manifestazioni sportive e dei responsabili della sicurezza.

#### **Art. 11 Trasmissione dei dati ad autorità straniera**

- <sup>1</sup> Fedpol è autorizzato a trasmettere dati personali alle autorità di polizia e agli organi di sicurezza stranieri responsabili della sicurezza durante manifestazioni sportive.
- <sup>2</sup> Fedpol registra la trasmissione ad autorità straniera.
- <sup>3</sup> Quando trasmette informazioni e dati personali fedpol informa il destinatario sull'attendibilità e l'attualità dei dati.
- <sup>4</sup> Fedpol avverte il destinatario che:

- a. le informazioni e i dati personali possono essere utilizzati soltanto per lo scopo per cui sono stati trasmessi;
- b. si riserva il diritto di esigere informazioni sull'uso che ne è stato fatto.

**Art. 12 Durata di conservazione e cancellazione dei dati**

<sup>1</sup> I dati personali e le informazioni concernenti una singola misura sono cancellati trascorsi tre anni dalla scadenza della misura.

<sup>2</sup> Se durante questi tre anni è registrata una nuova misura contro la medesima persona, la durata di conservazione della prima registrazione è prorogata di tre anni a partire dalla data di registrazione della seconda misura.

<sup>3</sup> I dati concernenti una singola misura sono tuttavia cancellati al più tardi dopo dieci anni.

**Art. 13 Disposizioni organizzative**

<sup>1</sup> La sicurezza dei dati è retta:

- a. dall'articolo 20 dell'ordinanza del 14 giugno 19934 relativa alla legge federale sulla protezione dei dati (OLPD);
- b. dall'ordinanza del 26 settembre 20035 sull'informatica nell'Amministrazione federale (OIAF).

<sup>2</sup> Fedpol disciplina in un regolamento sul trattamento dei dati:

- a. le misure organizzative e tecniche intese a evitare il trattamento non autorizzato dei dati;
- b. la verbalizzazione automatica dei dati introdotti;
- c. le esigenze tecniche che devono essere soddisfatte dai terminali degli utenti.

**Art. 29**

La presente ordinanza entra in vigore il 1 gennaio 2010.

## ALLEGATO 2: DIRETTIVA DEL DFGP DEL 30 SETTEMBRE 2004 SULL'INSTALLAZIONE DI COLLEGAMENTI ONLINE E IL RILASCIO DI AUTORIZZAZIONI D'ACCESSO AD APPLICAZIONI INFORMATICHE DEL DFGP (DIRETTIVA ONLINE DFGP)

*Il Dipartimento federale di giustizia e polizia,*

visto l'articolo 38 della legge federale del 21 marzo 19971 sull'organizzazione del Governo e dell'Amministrazione (LOGA), ordina:

### **Sezione 1: Generalità**

#### **Art. 1 Scopo**

<sup>1</sup> La presente direttiva armonizza la procedura applicabile all'installazione di collegamenti online nel Dipartimento federale di giustizia e polizia (DFGP).

<sup>2</sup> Essa regola:

- a. la procedura e le condizioni per l'installazione di un collegamento online tra il DFGP e gli organi della Confederazione e dei Cantoni con il quale gli impiegati di questi organi (utenti) ottengono l'accesso a un'applicazione informatica del DFGP attraverso una procedura di richiamo;
- b. la procedura e le condizioni per il rilascio a questi utenti di autorizzazioni d'accesso individuali o collettive quando sono resi loro accessibili dati personali mediante il collegamento online.

#### **Art. 2 Condizioni**

Le condizioni per installare un collegamento online tra un'applicazione informatica del DFGP e gli utenti sono:

- a. l'esistenza di una base legale sufficiente ai sensi dell'articolo 19 capoverso 3 della legge federale del 19 giugno 1992 sulla protezione dei dati (LDP), che definisce concretamente le autorizzazioni per l'accesso e le condizioni quadro indispensabili (art. 3);
- b. l'utilizzazione vincolata (art. 4);
- c. la sicurezza del collegamento online (art. 5);
- d. una domanda della competente autorità cantonale quando l'installazione di un collegamento online riguarda un servizio cantonale (art. 16).

### **Sezione 2: Principi applicabili all'installazione di un collegamento online**

#### **Art. 3 Base legale**

Un collegamento online necessita di una base legale esplicita. Se il collegamento online permette di accedere a dati personali degni di particolare protezione o a profili della personalità, è necessaria una legge formale.

#### **Art. 4 Utilizzazione vincolata**

<sup>1</sup> Un collegamento online può essere installato soltanto se utilizzato per gli scopi previsti dalla base legale.

<sup>2</sup> Se nella base legale lo scopo è descritto soltanto in termini generali, occorre precisarlo nella domanda d'installazione di un collegamento online.

#### **Art. 5 Sicurezza**

<sup>1</sup> Un collegamento online non può essere installato finché non sono stati garantiti il corretto trattamento dei dati e la loro sicurezza, vale a dire se sono adempiute le misure tecniche e organizzative di cui alla sezione 3.

<sup>2</sup> Un'infrastruttura di sicurezza centralizzata (SSO Portale DFGP<sup>16</sup>) controlla l'accesso a tutte le informazioni e applicazioni informatiche del DFGP. L'SSO Portale DFGP garantisce una gestione standardizzata e un'efficace autenticazione degli utenti.

---

<sup>16</sup> Single-Sign-on Portale DFGP

### **Sezione 3: Misure tecniche e organizzative**

#### **Art. 6 Valutazione dei rischi**

Prima della messa in esercizio di un'applicazione informatica con un collegamento online, l'ufficio federale responsabile dell'applicazione informatica effettua una valutazione dei rischi conformemente alle pertinenti direttive del Consiglio informatico della Confederazione (CIC) nonché dell'Organo strategia informatica della Confederazione (OSIC) e attua le misure che ne derivano.

#### **Art. 7 Concetto di sicurezza dell'applicazione informatica**

<sup>1</sup> Sulla base della valutazione dei rischi, l'ufficio federale responsabile dell'applicazione informatica allestisce un concetto di sicurezza informatica che preveda sufficienti misure tecniche e organizzative di protezione e sicurezza ai sensi dell'articolo 20 dell'ordinanza del 14 giugno 1993 relativa alla legge federale sulla protezione dei dati (OLPD).

<sup>2</sup> Il concetto di sicurezza dell'applicazione informatica definisce segnatamente:

- a. i responsabili dell'applicazione;
- b. i responsabili della protezione dei dati;
- c. i responsabili della sicurezza informatica;
- d. l'organo di vigilanza;
- e. le regole applicabili alla verbalizzazione;
- f. la procedura d'identificazione e di autenticazione degli utenti;
- g. la codificazione dei dati;
- h. la procedura di rilascio delle autorizzazioni d'accesso;
- i. le regole e la procedura applicabili all'interruzione di collegamenti inattivi e al blocco di autorizzazioni d'accesso non sfruttati;
- k. la procedura di controllo ai sensi dell'articolo 9 capoverso 1 OLPD

<sup>3</sup> Il concetto di sicurezza dell'applicazione informatica è aggiornato periodicamente dall'ufficio federale responsabile.

<sup>4</sup> Il rapporto finale dell'incaricato della sicurezza informatica del Dipartimento (ISID) e dell'Organo strategia informatica della Confederazione (OSIC) può sostituire il concetto di sicurezza dell'applicazione informatica se il regolamento per il trattamento menziona i punti di cui al capoverso 2.

#### **Art. 8 Regolamento per il trattamento**

Conformemente all'articolo 21 OLPD, gli uffici federali responsabili delle applicazioni informatiche emanano un regolamento per il trattamento delle loro applicazioni informatiche.

### **Sezione 4: Condizioni per il rilascio di autorizzazioni d'accesso individuali**

#### **Art. 9 Idoneità**

L'accesso online deve permettere di raggiungere gli obiettivi perseguiti.

#### **Art. 10 Necessità**

<sup>1</sup> L'accesso online deve essere necessario all'adempimento di un compito stabilito dalla legge.

<sup>2</sup> L'autorizzazione d'accesso è ritenuta necessaria se l'adempimento di un compito senza il collegamento online richiederebbe un onere supplementare sproporzionato.

#### **Art. 11 Proporzionalità**

<sup>1</sup> L'accesso online deve essere proporzionale.

<sup>2</sup> È proporzionale se vi è un rapporto ragionevole tra l'ingerenza nella sfera personale della persona interessata e l'utilità auspicata di tale trattamento di dati.

<sup>3</sup> L'autorizzazione d'accesso va limitata ai dati e alle funzioni necessari all'utente per l'adempimento dei compiti.

#### **Art. 12 Criteri d'esame**

All'atto della valutazione dei principi giusta gli articoli 9-11 sono determinanti segnatamente i seguenti criteri d'esame:

- a. la frequenza prevedibile dell'utilizzazione del singolo accesso;
- b. l'attuale frequenza di utilizzazione da parte dell'organo interessato;
- c. il numero di collaboratori dell'organo interessato che dispongono già di un diritto d'accesso;
- d. la portata dell'accesso accordato all'organo interessato;
- e. la necessità di agire in modo indipendente e rapido (ad es. al di fuori dei normali orari d'ufficio);

- f. la portata dell'accesso richiesto (criteri di ricerca, entità dei dati visualizzabili);
- g. le funzioni richieste (interrogazione, registrazione, mutazione, cancellazione).

## **Sezione 5: Organizzazione**

### **Art. 13 Organo centrale di autenticazione**

<sup>1</sup> L'organo centrale di autenticazione (servizio di autenticazione DFGP) è responsabile dell'autenticazione degli utenti che richiedono un accesso online ad applicazioni informatiche del DFGP. Gestisce l'SSO Portale DFGP.

<sup>2</sup> Riceve le domande d'accesso, procede all'autenticazione degli utenti e trasmette le domande all'ufficio federale responsabile dell'applicazione informatica.

<sup>3</sup> Coordina la procedura per il rilascio di autorizzazioni d'accesso individuali.

### **Art. 14 Competenze in seno agli uffici federali**

<sup>1</sup> Il consulente per la protezione dei dati dell'ufficio federale responsabile dell'applicazione informatica (CPDU) vigila sulla pianificazione e sull'installazione dei collegamenti online e provvede affinché siano rispettate le regole relative al rilascio delle autorizzazioni d'accesso individuali.

<sup>2</sup> Esamina la prima domanda d'autorizzazione d'accesso individuale presentata da ogni organo della Confederazione o dei Cantoni e controlla il rispetto dei principi di cui alla sezione 4. Vigila, mediante sondaggio, affinché le successive autorizzazioni d'accesso individuali vengano rilasciate conformemente ai numeri 9-12.

<sup>3</sup> Esamina l'esattezza e la completezza del regolamento per il trattamento.

<sup>4</sup> L'incaricato per la sicurezza informatica dell'unità amministrativa è responsabile dell'esame degli aspetti legati alla sicurezza informatica. Controlla segnatamente se le misure di sicurezza sono conformi alle condizioni di cui agli articoli 6 e 7.

### **Art. 15 Fornitore di prestazioni dell'applicazione informatica**

Il fornitore di prestazioni di ogni applicazione informatica è competente per la realizzazione tecnica dei collegamenti online se le autorizzazioni d'accesso individuali sono state rilasciate.

## **Sezione 6: Procedura per l'installazione di un collegamento online**

### **Art. 16 Domanda della competente autorità cantonale**

La competente autorità cantonale inoltra la domanda per l'installazione di un collegamento online all'ufficio federale responsabile dell'applicazione informatica. La domanda deve contenere:

- a. il nome degli organi per i quali chiede l'installazione di un collegamento online;
- b. il nome dell'applicazione informatica per la quale questi organi necessitano un collegamento online;
- c. lo scopo per il quale il collegamento va installato purché nella base legale esso sia descritto soltanto in termini generali.

### **Art. 17 Esame della domanda per l'installazione di un collegamento online**

<sup>1</sup> Il CPDU esamina la domanda segnatamente per quanto concerne:

- a. la presenza di una base legale sufficiente;
- b. l'utilizzazione vincolata;
- c. le domande d'autorizzazione d'accesso collettive.

<sup>2</sup> Una volta accettata la domanda, trasmette il regolamento per il trattamento dell'applicazione informatica all'autorità cantonale richiedente.

## **Sezione 7: Procedura per il rilascio di autorizzazioni d'accesso online individuali**

### **Art. 18 Domanda d'accesso**

<sup>1</sup> La domanda di rilascio per un accesso individuale va inoltrata con un modulo DFGP disponibile su Internet o Intranet.

<sup>2</sup> La domanda va inviata elettronicamente al servizio di autenticazione DFGP.

### **Art. 19 Esame delle domande di rilascio di un'autorizzazione d'accesso online**

<sup>1</sup> L'ufficio federale responsabile dell'applicazione informatica esamina le domande d'autorizzazione d'accesso online individuali secondo i principi di cui alla sezione 4.

<sup>2</sup> Il CPDU esamina la prima domanda individuale presentata da un organo della Confederazione o dei Cantoni. Controlla, mediante sondaggio, le autorizzazioni d'accesso individuali rilasciate successivamente a un'utente appartenente al medesimo organo.

<sup>3</sup> L'ufficio federale responsabile dell'applicazione informatica designa le persone abilitate a esaminare le successive domande d'autorizzazione. Può delegare l'esame a organi cantonali.

#### **Art. 20 Autorizzazioni d'accesso collettive**

<sup>1</sup> Un'autorizzazione d'accesso collettiva permette a tutti gli utenti appartenenti al medesimo gruppo di utilizzare gli stessi parametri d'identificazione (login di gruppo) quando si annunciano all'SSO Portale EJPD e alle applicazioni informatiche del DFGP.

<sup>2</sup> Un'autorizzazione d'accesso collettiva può essere rilasciata a una determinata categoria di utenti se sono adempiute le condizioni di cui alla sezione 4. Inoltre devono essere adempiute le condizioni seguenti:

- a. la stazione di lavoro è utilizzata in continuazione;
- b. il collegamento con un'applicazione deve essere stabilito molto rapidamente poiché l'accesso è urgente;
- c. la stazione di lavoro può essere utilizzata da tutti i componenti del gruppo di utenti menzionato nella domanda d'accesso;
- d. i titolari di autorizzazioni collettive possono soltanto consultare i dati nel rispettivo sistema informatico;
- e. i piani dei turni del gruppo di utenti sono conservati durante un anno;
- f. l'elenco dei componenti del gruppo di utenti è consegnato al responsabile dell'applicazione; e
- g. le mutazioni nel gruppo di utenti sono annunciati due volte l'anno al responsabile dell'applicazione;

#### **Art. 21 Vigilanza**

Il CPDU esamina periodicamente se gli accessi accordati sono conformi ai principi di cui alla sezione 4.

### **Sezione 8: Disposizioni finali**

#### **Art. 22 Disposizioni esecutive**

La presente direttiva figura in allegato ed è parte integrante dei regolamenti per il trattamento di ogni applicazione informatica del DFGP con collegamenti online.

#### **Art. 23 Disposizioni transitorie**

<sup>1</sup> Le autorizzazioni d'accesso individuali esistenti al momento dell'entrata in vigore della presente direttiva restano valide fino all'introduzione di un'efficace autenticazione degli utenti. A tale momento saranno esaminate le autorizzazioni d'accesso individuali conformemente all'articolo 19.

<sup>2</sup> Quando un'applicazione informatica esistente è sostituita con una nuova, le autorizzazioni per l'installazione di un collegamento online (art. 17) conservano la loro validità.

<sup>3</sup> Fino all'introduzione della firma elettronica nel DFGP è imperativo inviare per posta o fax al Servizio di autenticazione DFGP una copia firmata della domanda d'accesso (art. 18 cpv. 1).

<sup>4</sup> Il DFGP trasmette entro il 31 dicembre 2004 i regolamenti per il trattamento delle applicazioni informatiche accessibili online il 31 agosto 2004 alle autorità cantonali responsabili degli organi dei Cantoni collegativi.

#### **Art. 24 Entrata in vigore**

La presente direttiva entra in vigore il 1° ottobre 2004.

30 settembre 2004 Dipartimento federale di giustizia e polizia:  
Blocher

## ALLEGATO 3: ISTRUZIONI DEL CIC DEL 27 SETTEMBRE 2004 SULLA SICUREZZA INFORMATICA NELL'AMMINISTRAZIONE FEDERALE (ISTRUZIONI CIC SULLA SICUREZZA INFORMATICA)

*Il Consiglio informatico della Confederazione (CIC),*

visto l'articolo 13 capoversi 4 e 5 dell'ordinanza del 26 settembre 20031 sull'informatica nell'Amministrazione federale (OIAF) adotta le seguenti istruzioni:

### **1. Disposizioni generali**

#### **1.1 Scopo e oggetto**

<sup>1</sup> Le presenti istruzioni disciplinano in ambito di sicurezza informatica nell'Amministrazione federale:

- a. l'organizzazione;
- b. la procedura di sicurezza;
- c. la sicurezza della rete.

<sup>2</sup> Esse stabiliscono requisiti e misure tecniche, edilizie, organizzative e personali per garantire:

- a. la protezione dell'integrità e della disponibilità delle tecnologie dell'informazione e della comunicazione (hardware e software);
- b. la protezione della confidenzialità, dell'integrità e della disponibilità dei dati;
- c. la verificabilità dell'elaborazione dei dati.

<sup>3</sup> I dipartimenti, la Cancelleria federale e le unità organizzative possono stabilire esigenze e misure di protezione più ampie.

#### **1.2 Campo di applicazione**

Il campo di applicazione delle presenti istruzioni è disciplinato dall'articolo 2 OIAF.

### **2. Competenze**

#### **2.1 Incaricato della sicurezza informatica**

<sup>1</sup> I dipartimenti e la Cancelleria federale designano un incaricato della sicurezza informatica. L'incaricato coordina tutti gli aspetti della sicurezza informatica all'interno del dipartimento e con i servizi sovra dipartimentali.

<sup>2</sup> Le unità organizzative designano un incaricato della sicurezza informatica. L'incaricato coordina tutti gli aspetti della sicurezza informatica all'interno dell'unità organizzativa e con i servizi dipartimentali.

#### **2.2 Beneficiari di prestazioni**

<sup>1</sup> I responsabili delle applicazioni, i responsabili dei processi aziendali e i titolari delle raccolte di dati dei beneficiari di prestazioni stabiliscono in collaborazione con l'incaricato della sicurezza informatica le esigenze di sicurezza per i progetti, le applicazioni e le raccolte di dati e organizzano periodicamente i controlli di attuazione delle misure di sicurezza con il concorso dei committenti e dei partner contrattuali.

<sup>2</sup> Le unità organizzative sono responsabili affinché i loro collaboratori conoscano in funzione delle loro mansioni i servizi/organismi competenti e i processi della sicurezza informatica nell'Amministrazione federale.

<sup>3</sup> I collaboratori dell'Amministrazione federale che utilizzano mezzi TIC sono responsabili del loro utilizzo sicuro. Essi devono essere regolarmente istruiti e sensibilizzati sugli aspetti della sicurezza TIC.

#### **2.3 Fornitori di prestazioni**

<sup>1</sup> Le direttive stabilite nei confronti dei beneficiari di prestazioni si applicano per analogia ai progetti, alle applicazioni e alle raccolte di dati dei fornitori di prestazioni.

<sup>2</sup> I responsabili garantiscono l'attuazione su tutti i sistemi delle misure di sicurezza nell'esercizio di mezzi TIC.

## 2.4 Livello operativo

Le responsabilità a livello operativo sono stabilite in modo dettagliato negli accordi di progetto e nei Service Level Agreements tra beneficiari e fornitori di prestazioni.

## 2.5 Definizione dei ruoli

Le definizioni dei ruoli si fondano sui processi IT dell'Amministrazione federale.

## 3. Procedura di sicurezza

### 3.1 Applicazione della procedura di sicurezza

La procedura di sicurezza concerne l'intero ciclo di vita di un sistema informatico, dalla sua pianificazione alla sua messa fuori servizio.

### 3.2 Standard internazionali

Le misure concrete di sicurezza si orientano sui pertinenti standard internazionali attuali, come ISO/CEI 17799/27001 o i cataloghi concernenti la sicurezza di base IT del BSI (Ufficio Federale per la Sicurezza Informatica con sede a Bonn).

### 3.3 Analisi del bisogno di protezione / valutazione dei rischi

<sup>1</sup> Un'analisi del bisogno di protezione deve essere effettuata per ogni progetto informatico. Il momento dell'analisi è disciplinato dal modello HERMES di procedura in materia di progetti.

<sup>2</sup> Prima di essere applicate nell'Amministrazione federale, le nuove tecnologie dell'informazione e della comunicazione (hardware e software) devono essere sottoposte a una valutazione dei rischi. Questa deve essere effettuata dai beneficiari. Il risultato della valutazione dei rischi deve essere presentata al competente incaricato della sicurezza informatica.

### 3.4 Bisogno generale di protezione

Se dall'analisi risulta un bisogno generale di protezione, devono essere rispettate le esigenze minime di sicurezza dell'allegato 1 delle presenti istruzioni.

### 3.5 Bisogno elevato di protezione

<sup>1</sup> Se dall'analisi risulta un bisogno elevato di protezione, bisogna inoltre definire un concetto di sicurezza, sempre che a livello dipartimentale non esistano direttive generali in materia di sicurezza relative all'elevato bisogno di protezione.

<sup>2</sup> Il responsabile presso il beneficiario delle prestazioni definisce i concetti di sicurezza delle applicazioni e il responsabile presso il fornitore delle prestazioni definisce i concetti di sicurezza dei prodotti e delle piattaforme di sistema.

<sup>3</sup> Nella definizione dei concetti di sicurezza si può rinviare a concetti di sicurezza già esistenti relativi a tematiche specifiche.

<sup>4</sup> I concetti di sicurezza devono essere definiti in collaborazione con l'incaricato della sicurezza informatica.

### 3.6 Rischio residuo

<sup>1</sup> Un eventuale rischio residuo deve essere in ogni caso accertato e comunicato ai decisori.

<sup>2</sup> Tale rischio deve essere assunto dai servizi di linea responsabili.

### 3.7 Documentazione scritta

<sup>1</sup> Tutte le misure di sicurezza e la loro attuazione devono essere documentate per scritto.

<sup>2</sup> Per tutte le applicazioni/progetti e piattaforme di sistema/prodotti occorre tenere un portafoglio con le informazioni rilevanti ai fini della sicurezza. L'incaricato della sicurezza informatica può accedere al portafoglio o lo tiene personalmente.

### 3.8 Controlli

<sup>1</sup> I responsabili dei dipartimenti e delle unità organizzative verificano periodicamente in collaborazione con l'incaricato della sicurezza informatica l'adeguatezza delle misure di sicurezza e l'avvenuta attuazione.

<sup>2</sup> In caso di modifica dei compiti, dell'organizzazione, dei processi, dei dati o dei mezzi TIC utilizzati, essi ne verificano il bisogno di protezione stabilito, nonché l'adeguatezza delle misure di sicurezza prese sino ad allora.

### **3.9 Costi**

I costi della sicurezza TIC sono parte dei costi di progetto e di esercizio. Essi sono pianificati in modo corrispondente.

## **4. Sicurezza della rete**

### **4.1 Direttive in materia di sicurezza**

<sup>1</sup> Ai fini della sicurezza della rete si applicano le definizioni e le direttive in materia di sicurezza dell'allegato 2 delle presenti istruzioni.

<sup>2</sup> Al dominio blu si applicano inoltre le direttive dell'allegato 3 delle presenti istruzioni.

### **4.2 Altri domini della Confederazione**

<sup>1</sup> I titolari di altri domini della Confederazione devono stabilire in merito una corrispondente policy (norma di comportamento).

<sup>2</sup> Le policy di dominio della Confederazione e gli accordi bilaterali tra domini della Confederazione e domini di terzi devono essere approvati dal Comitato per la sicurezza informatica (C-SI).

<sup>3</sup> Gli accordi bilaterali tra domini della Confederazione oppure tra domini della Confederazione e domini di terzi devono parimenti essere approvati dal C-SI.

<sup>4</sup> L'unità organizzativa competente deve, mediante accordo (ad es. contratto, Service Level Agreement), obbligare al rispetto delle direttive in materia di sicurezza delle presenti istruzioni chiunque è direttamente allacciato a un dominio della Confederazione, senza essere sottoposto alle presenti istruzioni.

## **5. Disposizioni finali**

### **5.1 Abrogazione di normative previgenti**

Le seguenti istruzioni e normative sono abrogate:

- a. istruzione sulla sicurezza informatica n. S01 (WS S01) dell'UFI, del 18 agosto 1993;
- b. istruzione sulla sicurezza informatica n. S02 (WS S02) dell'UFI, del 2 ottobre 1998;
- c. istruzione sulla sicurezza informatica n. S03 (WS S03) dell'UFI, del 25 giugno 1997;
- d. Network Security Policy (NSP) dell'UFI, del 25 giugno 1997.

### **5.2 Disposizioni transitorie**

Per l'attuazione dei requisiti di cui ai numeri 5.7, 6.3 e 6.4 dell'allegato 1 alle presenti istruzioni vige un termine transitorio fino a fine 2009.

### **5.3 Entrata in vigore**

Le presenti istruzioni entrano in vigore il 1° novembre 2004.

Berna, 27 settembre 2004 Per il Consiglio informatico della Confederazione:

Il presidente:

Peter Grütter

## ALLEGATO 4: DIRETTIVA DEL 1° GENNAIO 2010 SULL'UTILIZZO E IL TRATTAMENTO DEI DATI DEL SISTE- MA D'INFORMAZIONE HOOGAN DA PARTE DEGLI ORGA- NIZZATORI DI MANIFESTAZIONI SPORTIVE E DEI LORO RESPONSABILI DELLA SICUREZZA

*L'Ufficio federale di polizia fedpol,*

visto l'articolo 24a capoverso 8 della legge federale del 21 marzo 1997 sulle misure per la salvaguardia della sicurezza interna (LMSI; RS 120),  
visto l'articolo 10 dell'ordinanza del 4 dicembre 2009 sulle misure di polizia amministrativa e i sistemi d'informazione dell'Ufficio federale di polizia (RS 120.52),  
visto l'articolo 22 del regolamento sul trattamento dei dati HOOGAN del 1° gennaio 2010,  
emana la direttiva seguente:

### **SEZIONE 1: DISPOSIZIONI GENERALI**

Le denominazioni utilizzate nella presente direttiva si riferiscono a persone di entrambi i sessi.

#### **Art. 1 Contenuto**

La direttiva disciplina l'utilizzo, la comunicazione, il trattamento, il ritorno e l'eliminazione dei dati del sistema d'informazione HOOGAN da parte degli organizzatori di manifestazioni sportive e dei loro responsabili della sicurezza. Inoltre stabilisce i destinatari dei dati e i loro obblighi. Sono inoltre definiti gli scopi per cui i dati sono comunicati agli organizzatori di manifestazioni sportive. Infine la presente direttiva descrive lo svolgimento della comunicazione dei dati e la procedura per controllare il suo rispetto. Essa è parte dell'allegato del regolamento per il trattamento dei dati HOOGAN.

#### **Art. 2 Principi**

<sup>1</sup> La direttiva disciplina il trattamento dei dati registrati nel sistema d'informazione HOOGAN.

<sup>2</sup> Sono oggetto della direttiva le manifestazioni sportive nazionali e internazionali che si svolgono in Svizzera.

<sup>3</sup> La direttiva si applica per analogia anche alle trasmissioni di manifestazioni sportive mediante maxi schermi (Public-Viewing).

<sup>4</sup> Non sono oggetto della direttiva i dati degli organizzatori di manifestazioni sportive (elenchi delle persone cui è vietato accedere agli stadi) oppure i dati dei Cantoni, segnatamente i dati preventivi. La Confederazione non assume nessuna responsabilità per questi dati.

### **SEZIONE 2: AUTORITÀ E SERVIZI COINVOLTI**

#### **Art. 3 Organizzatori di manifestazioni sportive**

<sup>1</sup> Le federazioni sportive comunicano al settore Tifoseria violenta dell'Ufficio federale di polizia fedpol il nome del responsabile della sicurezza per le attuali manifestazioni sportive. Egli funge da interlocutore per la Confederazione e i Cantoni.

<sup>2</sup> Il responsabile della sicurezza chiede alla competente autorità di polizia del Cantone, ovvero al servizio specializzato decentralizzato (servizio specializzato), che gli siano comunicati i dati personali registrati nel sistema d'informazione HOOGAN. Il servizio specializzato informa immediatamente il settore Tifoseria violenta della richiesta. In occasione delle partite delle squadre nazionali, il responsabile della sicurezza si rivolge direttamente al settore Tifoseria violenta per ottenere i dati personali.

<sup>3</sup> Il responsabile della sicurezza garantisce che all'interno del luogo della manifestazione i dati personali sono utilizzati conformemente alle prescrizioni e istruisce il personale di sicurezza in merito.

#### **Art. 4 Servizi specializzati decentralizzati dei Cantoni**

<sup>1</sup> I servizi specializzati inoltrano su richiesta ai responsabili della sicurezza i dati delle persone sottoposte a misure attive.

<sup>2</sup> I servizi specializzati controllano che l'utilizzo, la comunicazione e la distruzione dei dati avvenga conformemente alle prescrizioni.

<sup>3</sup> I servizi specializzati dopo il termine di una manifestazione sportiva compilano un foglio di controllo e lo trasmettono al settore Tifoseria violenta.

#### **Art. 5 Settore Tifoseria violenta**

<sup>1</sup> Quale gestore del sistema d'informazione HOOGAN, il settore Tifoseria violenta può delegare ai servizi specializzati il compito di comunicare i dati agli organizzatori di manifestazioni sportive in Svizzera.

<sup>2</sup> In occasione delle partite delle squadre nazionali il settore Tifoseria violenta trasmette direttamente i dati al responsabile della sicurezza della federazione competente. Inoltre informa della comunicazione dei dati il servizio specializzato responsabile della manifestazione.

<sup>3</sup> Con l'ausilio dei fogli di controllo il settore Tifoseria violenta garantisce il rispetto delle basi legali, del regolamento sul trattamento dei dati e della presente direttiva, verificandone il rispetto con controlli saltuari. In occasione delle partite delle squadre nazionali controlla che l'utilizzo, la comunicazione, il trattamento, il ritorno e l'eliminazione dei dati avvengano secondo le prescrizioni.

### **SEZIONE 3: UTENTI E TIPO DI COMUNICAZIONE**

#### **Art. 6 Utenti**

Gli organizzatori di manifestazioni sportive ricevono soltanto i dati personali di cui hanno veramente bisogno per adempiere i loro compiti di sicurezza. Il servizio specializzato competente consegna i dati personali necessari sotto forma di elenchi stampati, di cui il numero esatto delle copie è riportato sul foglio di controllo, ai responsabili della sicurezza richiedenti che apponendo la loro firma sul foglio di controllo confermano di averli ricevuti. I servizi specializzati possono farsi sostituire dai locali servizi di polizia cantonale. In occasione delle partite delle squadre nazionali i dati sono comunicati dal settore Tifoseria violenta.

#### **Art. 7 Dati personali**

I dati personali sono dati operativi, importati e concernenti una determinata manifestazione. Sono comunicati i dati personali seguenti: fotografia, cognome, nome, data di nascita, indirizzo e misure pronunciate.

### **SEZIONE 4: TRATTAMENTO E CONTROLLO DEI FLUSSI DEI DATI**

#### **Art. 8 Ulteriore utilizzo e controllo dei dati**

<sup>1</sup> Il responsabile della sicurezza distribuisce ai responsabili del personale di sicurezza l'elenco dei dati personali al massimo tre ore prima dell'apertura degli stadi. Entro un'ora dal termine della manifestazione sportiva tutti gli elenchi distribuiti devono essere restituiti al responsabile della sicurezza. Egli ritira gli elenchi e li distrugge immediatamente in presenza dell'autorità di polizia responsabile.

<sup>2</sup> Ai responsabili della sicurezza e al personale di sicurezza è vietato copiare gli elenchi distribuiti, riprodurli in qualche modo o memorizzarli. Gli elenchi non devono in nessun momento essere comunicati, trasmessi o resi visibili a terzi.

### **SEZIONE 5: CANCELLAZIONE E CONTROLLO PERIODICO DEI DATI PERSONALI**

#### **Art. 9 Cancellazione dei dati e comunicazione al settore Tifoseria violenta**

<sup>1</sup> I rappresentanti della polizia responsabili sorvegliano sul luogo la distruzione dei dati personali. Conformemente all'articolo 10 capoverso 3 dell'ordinanza sulle misure di polizia amministrativa e i sistemi d'informazione dell'Ufficio federale di polizia la comunicazione della distruzione dei dati personali deve avvenire entro le 24 ore dalla trasmissione dei dati personali da parte delle autorità. Esse verbalizzano sul foglio di controllo la distribuzione e la restituzione degli elenchi e registrano una copia del foglio di controllo nel sistema d'informazione HOOGAN sotto alla relativa manifestazione sportiva.

<sup>2</sup> Se il servizio specializzato constata delle irregolarità, egli richiama i responsabili della sicurezza e informa il settore Tifoseria violenta. Quest'ultimo decide l'ulteriore procedura dopo aver consultato gli addetti alla sicurezza della federazione.

#### **Art. 10 Controllo periodico degli organizzatori di manifestazioni sportive da parte del settore Tifoseria violenta**

<sup>1</sup> Il settore Tifoseria violenta controlla saltuariamente che gli organizzatori di manifestazioni sportive e i loro responsabili della sicurezza utilizzino i dati conformemente alla legge.

<sup>2</sup> Se il settore Tifoseria violenta constata delle irregolarità, chiede all'addetto alla sicurezza della federazione di applicare delle sanzioni contro le persone inadempienti, dopo essersi consultato con il servizio specializzato responsabile.

**SEZIONE 6: DISPOSIZIONI FINALI**

**Art. 11 Entrata in vigore e pubblicazione**

La presente direttiva sostituisce la versione del 1° novembre 2007 ed entra in vigore il 1° gennaio 2010.

Berna, 31 dicembre 2009

UFFICIO FEDERALE DI POLIZIA fedpol  
del Dipartimento federale di giustizia e polizia

La Direttrice supplente

Nicoletta della Valle

## ALLEGATO 5: CONCORDATO DEL 15 NOVEMBRE 2007 DELLA CONFERENZA DEI DIRETTORI CANTONALI DI GIUSTIZIA E POLIZIA SULLE MISURE CONTRO LA VIOLENZA IN OCCASIONE DI MANIFESTAZIONI SPORTIVE

*La Conferenza delle direttrici e dei direttori dei dipartimenti cantonali di giustizia e polizia approva il seguente testo del concordato:*

### **Capitolo 1: Disposizioni generali**

#### **Art. 1 Scopo**

I Cantoni adottano, in collaborazione con la Confederazione, le misure preventive di polizia ai sensi del presente concordato, per impedire un comportamento violento nonché per rilevare e combattere tempestivamente la violenza in occasione di manifestazioni sportive.

#### **Art. 2 Definizione di comportamento violento**

<sup>1</sup> Un comportamento violento e gli atti violenti sono considerati tali segnatamente se una persona ha commesso o incitato a commettere:

- a. reati contro la vita e l'integrità della persona ai sensi degli articoli 111–113, 117, 122, 123, 125 capoverso 2, 129, 133 e 134 del Codice penale (CP) <sup>17</sup>;
- b. danneggiamenti ai sensi dell'articolo 144 CP;
- c. coazione ai sensi dell'articolo 181 CP;
- d. incendio intenzionale ai sensi dell'articolo 221 CP;
- e. esplosione ai sensi dell'articolo 223 CP;
- f. pubblica istigazione a un crimine o alla violenza ai sensi dell'articolo 259 CP;
- g. sommossa ai sensi dell'articolo 260 CP;
- h. violenza o minaccia contro le autorità e i funzionari ai sensi dell'articolo 285 CP.

<sup>2</sup> È inoltre considerato un comportamento violento, minacciare la sicurezza pubblica, trasportando o utilizzando armi, esplosivi, polvere da sparo o pezzi pirotecnici in impianti sportivi, in loro prossimità e nel viaggio di andata e ritorno.

#### **Art. 3 Prova del comportamento violento**

<sup>1</sup> Sono considerate prove di un comportamento violento ai sensi dell'articolo 2:

- a. pertinenti sentenze giudiziarie o denunce della polizia;
- b. dichiarazioni attendibili o registrazioni visive della polizia, dell'amministrazione delle dogane, del personale addetto alla sicurezza o delle federazioni e delle società sportive;
- c. divieti di accedere a stadi pronunciati dalle federazioni e dalle società sportive;
- d. comunicazioni di un'autorità straniera competente in materia.

<sup>2</sup> Le dichiarazioni ai sensi del capoverso 1 lettera b sono messe per scritto e firmate.

### **Capitolo 2: Misure di polizia**

#### **Art. 4 Aree vietate**

<sup>1</sup> Le autorità competenti possono vietare a una persona di accedere, in determinati orari, a un'area esattamente delimitata in prossimità di una manifestazione sportiva (area vietata), se è provato che in occasione di manifestazioni sportive ha partecipato ad atti violenti contro persone o cose. L'autorità cantonale competente definisce i confini delle singole aree vietate.

<sup>2</sup> Il divieto è valido per la durata massima di un anno.

<sup>3</sup> Il divieto è pronunciato mediante decisione formale dalle autorità del Cantone in cui la persona risiede o in cui ha partecipato agli atti violenti. Le autorità del Cantone in cui si sono verificati gli atti violenti hanno la precedenza. Il Servizio centrale svizzero in materia di tifoseria violenta (Servizio centrale) può presentare la relativa richiesta.

#### **Art. 5 Decisione d'interdizione d'accesso a un'area**

<sup>1</sup> La decisione d'interdizione d'accesso a un'area stabilisce la durata dell'interdizione e l'area interdetta. La decisione è accompagnata da una piantina in cui sono indicati esattamente i luoghi interessati dall'interdizione e le relative aree interdette.

<sup>2</sup> Se la decisione è pronunciata dall'autorità del Cantone in cui si sono verificati gli atti violenti, quest'ultima informa senza indugio l'autorità competente del Cantone di domicilio della persona interessata.

<sup>3</sup> Per la prova della partecipazione ad atti violenti è applicabile l'articolo 3.

#### **Art. 6 Obbligo di presentarsi alla polizia**

<sup>1</sup> Una persona può essere obbligata a presentarsi alla polizia in determinati orari se:

- a. negli ultimi due anni ha violato il divieto di accedere a un'area determinata, secondo l'articolo 4, o il divieto di recarsi in un Paese determinato, secondo l'articolo 24c LMSI<sup>18</sup> ;
- b. in base a elementi concreti e attuali si deve presumere che altre misure non la distolgono dal commettere atti violenti in occasione di manifestazioni sportive; oppure
- c. l'obbligo di presentarsi alla polizia rappresenta nel caso particolare la misura meno severa.

<sup>2</sup> La persona interessata deve presentarsi al posto di polizia designato nella decisione, negli orari indicati. Di principio si tratta di un posto di polizia nel luogo di residenza. Nel designare luogo e orari, l'autorità tiene conto della situazione personale della persona interessata.

<sup>3</sup> L'obbligo di presentarsi alla polizia è imposto con decisione formale dall'autorità del Cantone di residenza della persona interessata. Il Servizio centrale può presentare la relativa richiesta.

#### **Art. 7 Applicazione dell'obbligo di presentarsi alla polizia**

<sup>1</sup> Si deve presumere che misure diverse dall'obbligo di presentarsi alla polizia non impediscono a una persona di commettere atti violenti in occasione di manifestazioni sportive (art. 6 cpv. 1 lett. b), segnatamente se:

- a. le autorità sono a conoscenza di affermazioni o attività correnti della persona interessata che inducono a credere che eluderebbe misure meno severe; oppure
- b. misure meno severe non le impedirebbero di commettere in futuro atti violenti a causa di circostanze personali, ad esempio perché il luogo di domicilio o di lavoro è situato nelle immediate vicinanze di uno stadio.

<sup>2</sup> Se la persona soggetta all'obbligo di presentarsi alla polizia, per motivi importanti e giustificabili non è in grado, conformemente all'articolo 6 capoverso 2, di presentarsi presso il servizio competente (posto di polizia), lo comunica senza indugio a quest'ultimo informandolo sul luogo in cui si trova. L'autorità di polizia competente verifica se le informazioni e il luogo indicato dalla persona interessata sono esatti.

<sup>3</sup> Il posto di polizia informa senza indugio l'autorità che ha pronunciato l'obbligo di presentarsi alla polizia se le persone interessate si sono presentate o meno.

#### **Art. 8 Fermo preventivo di polizia**

<sup>1</sup> Una persona può essere sottoposta a un fermo preventivo di polizia se:

- a. vi sono indizi concreti e attuali che in occasione di una manifestazione sportiva nazionale o internazionale parteciperà a gravi atti violenti contro persone o cose; e
- b. è l'unica possibilità per impedirle di commettere tali atti violenti.

<sup>2</sup> Il fermo preventivo di polizia termina quando non ne sussistono più i presupposti e in ogni caso dopo 24 ore.

<sup>3</sup> La persona interessata deve presentarsi all'ora indicata al posto di polizia del luogo di residenza o a un altro posto di polizia designato nella decisione e restarvi per la durata del fermo.

<sup>4</sup> Se la persona interessata non si presenta al posto di polizia, può esservi condotta dalla polizia.

<sup>5</sup> Su richiesta della persona interessata, un'autorità giudiziaria esamina la legalità della privazione della libertà.

<sup>6</sup> Il fermo preventivo di polizia è pronunciato con decisione formale dalle autorità del Cantone in cui la persona interessata risiede o dalle autorità del Cantone in cui si temono gli atti violenti. Le autorità del Cantone in cui si temono gli atti violenti hanno la precedenza.

#### **Art. 9 Applicazione del fermo preventivo di polizia**

<sup>1</sup> Sono considerate manifestazioni sportive nazionali ai sensi dell'articolo 8 capoverso 1 lettera a, le manifestazioni organizzate dalle federazioni sportive o dalle leghe nazionali oppure a cui partecipano società che fanno parte di tali organizzazioni.

<sup>2</sup> Sono considerati gravi atti violenti ai sensi dell'articolo 8 capoverso 1 lettera a segnatamente i reati di cui agli articoli 111–113, 122, 123 numero 2, 129, 144 capoverso 3, 221, 223 o 224 CP.

<sup>3</sup> L'autorità competente del luogo di domicilio della persona interessata designa il posto di polizia presso cui essa deve presentarsi e determina l'inizio e la durata del fermo preventivo.

<sup>4</sup> I Cantoni designano l'istanza giudiziaria competente per l'esame della legalità del fermo preventivo di polizia.

<sup>5</sup> Con la decisione s'informa la persona interessata del suo diritto di far verificare la legalità della privazione della libertà (art. 8 cpv. 5).

<sup>6</sup> Il posto di polizia designato per l'esecuzione del fermo preventivo informa l'autorità di decisione dell'esecuzione. Se la persona interessata non si presenta, l'informazione avviene senza indugio.

#### **Art. 10 Raccomandazione divieto di accedere a stadi**

L'autorità competente per le misure secondo gli articoli 4–9 e il Servizio centrale possono raccomandare agli organizzatori di manifestazioni sportive di pronunciare divieti di accedere a stadi per coloro che hanno dimostrato un comportamento violento fuori dallo stadio in occasione di manifestazioni sportive. La raccomandazione viene rilasciata indicando i dati necessari in conformità dell'art. 24a cpv. 3 LMSI.

#### **Art. 11 Età minima**

Le misure secondo gli articoli 4–7 sono pronunciate solo contro persone che hanno compiuto i 12 anni. Il fermo preventivo di polizia secondo gli articoli 8–9 è pronunciato solo contro persone che hanno compiuto i 15 anni.

### **Capitolo 3: Disposizioni procedurali**

#### **Art. 12 Effetto sospensivo**

Il ricorso contro le misure secondo gli articoli 4–9 ha effetto sospensivo solo se non ne risulta pregiudicato lo scopo della misura e se l'autorità di ricorso o il giudice lo accorda espressamente in una decisione incidentale.

#### **Art. 13 Competenza e procedura**

<sup>1</sup> I Cantoni designano l'autorità competente per le misure secondo gli articoli 4–9.

<sup>2</sup> Per l'esecuzione delle misure di cui al Capitolo 2, l'autorità competente rinvia alla comminatoria dell'articolo 292 CP.

<sup>3</sup> I Cantoni comunicano all'Ufficio federale di polizia (fedpol) in virtù dell'art. 24a cpv. 4 LMSI:

- a. le decisioni e le revoche delle misure secondo gli articoli 4–9 e 12;
- b. le violazioni delle misure secondo gli articoli 4–9, nonché le decisioni penali corrispondenti;
- c. le aree vietate da essi designate, allegando le relative piantine.

### **Capitolo 4: Disposizioni finali**

#### **Art. 14 Informazione della Confederazione**

La Segreteria generale della Conferenza delle direttrici e dei direttori dei dipartimenti cantonali di giustizia e polizia (CDDGP) informa la Cancelleria federale sul presente Concordato. La procedura si svolge secondo l'articolo 27o OLOGA.

#### **Art. 15 Entrata in vigore**

Il presente Concordato entra in vigore non appena vi aderiscono almeno due Cantoni, al più presto tuttavia il 1° gennaio 2010.

#### **Art. 16 Rescissione**

Un Cantone membro può rescindere il Concordato alla fine di un anno con un termine di preavviso di un anno. Gli altri Cantoni decidono se lasciare o meno in vigore il Concordato.

#### **Art. 17 Informazione del Segretariato generale della CDDGP**

I Cantoni informano il Segretariato generale della CDDGP sulla loro adesione, l'autorità competente in virtù dell'articolo 13 cpv. 1 e la loro rescissione. Il Segretariato generale della CDDGP tiene una lista aggiornata con lo stato di validità del Concordato.