Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Polizei fedpol

Informationssystem

HOOGAN

Bearbeitungsreglement

Bern, Mai 2013

INHALT

BEARBEITUNGSREGLEMENT

für das Informationssystem HOOGAN des Bundesamtes für Polizei fedpol

(Bearbeitungsreglement HOOGAN vom 1. Mai 2013, ersetzt Version vom 1. Januar 2010)

Das Bundesamt für Polizei fedpol,

gestützt auf Art. 24*a* ff. Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) vom 21. März 1997 (Stand am 16. Juli 2012)[1];

gestützt auf die Verordnung über verwaltungspolizeiliche Massnahmen des Bundesamtes für Polizei und über das Informationssystem HOOGAN (VVMH) vom 4. Dezember 2009 (Stand am 1. Februar 2013)[2];

gestützt auf Art. 21 der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) vom 14. Juni 1993 (Stand am 1. Dezember 2010)[3];

gestützt auf die Verordnung über den Schutz von Informationen des Bundes (Informationsschutzverordnung, ISchV) vom 4. Juli 2007 (Stand am 1. August 2010)[4];

gestützt auf die Weisung des EJPD über die Einrichtung von Online-Verbindungen und die Erteilung von Zugriffsbewilligungen auf Informatikanwendungen des EJPD (Online-Weisung EJPD) vom 30. September 2004;

in Berücksichtigung des Konkordats über Massnahmen gegen Gewalt anlässlich von Sportveranstaltungen vom 15. November 2007 der Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren

erlässt die folgenden Weisungen:

Die in dieser Richtlinie verwendeten Personenbezeichnungen beziehen sich auf beide Geschlechter.

1 SR 120.
2 SR 120.52.
3 SR 235.11.
4 SR 510.411.

ABSCHNITT 1: ALLGEMEINE BESTIMMUNGEN

Art. 1 Inhalt

Das Bearbeitungsreglement umschreibt insbesondere die Datenbearbeitungs- und Kontrollverfahren sowie den Betrieb des Informationssystems HOOGAN (HOOGAN). Es enthält Angaben über das für den Datenschutz und die Datensicherheit verantwortliche Organ, über die Herkunft der Daten und die Zwecke, für welche sie regelmässig bekannt gegeben werden und beschreibt das Verfahren für die Erteilung der Zugriffsrechte auf HOOGAN.

Art. 2 Begriffe

Definitionen:

a. *Departement*: das Eidgenössische Justiz- und Polizeidepartement EJPD;

b. *Bundesamt*: das Bundesamt für Polizei fedpol;

c. *Datenherr*: das für HOOGAN verantwortliche Bundesamt;

d. *HOOGAN-Verantwortlicher*: Stelle bei fedpol, die die Hauptverantwortung für HOOGAN trägt und Leiter des Projektausschusses ist;

e. *HOOGAN-Applikationsverantwortlicher*: Stelle bei fedpol, die benutzerseitig für HOOGAN verantwortlich ist. Der HOOGAN-Applikationsverantwortliche ist Mitglied des Projektausschusses, verantwortlich für Planung, Weiterentwicklung und Betrieb des Systems sowie Anlaufstelle für die Benutzer. Er versieht zudem die Aufgaben des HOOGAN-Benutzerverwalters und des HOOGAN-Schulungsverantwortlichen, der Schulungsunterlagen und Handbücher erstellt sowie Grund- und Wiederholungskurse für die zugriffsberechtigten Mitarbeiter des Bundes, der Kantone und Städte, der Schweizerischen Zentralstelle Hooliganismus (SZH) und des Grenzwachtkorps (GWK) organisiert und durchführt;

f. *HOOGAN-Qualitätssicherung:* Stelle bei fedpol, die für die Erfassung und die Kontrolle der Daten sowie für die Einhaltung der gesetzlichen Grundlagen verantwortlich ist. Sie kontrolliert die von den zuständigen Stellen in den Kantonen und Städten vorerfassten Daten auf ihre Richtigkeit und überführt sie anschliessend in das produktive System oder weist sie mit Begründung an die erfassende Stelle zurück;

g. *HOOGAN-Sachbearbeiter*: Stelle bei fedpol, welche für die Bewirtschaftung der unpersönlichen Stammdaten von HOOGAN (Erfassung von Veranstaltungen, Organisationen, etc.) verantwortlich ist;

h. *Sektion Hooliganismus (SH)*: Stelle bei fedpol, die HOOGAN betreibt. Ihr gehören der HOOGAN-Applikationsverantwortliche, die HOOGAN-Qualitätssicherung und der HOOGAN-Sachbearbeiter an;

i. *Datenschutz- und Informationsschutzberater/in DSBO fedpol*: Stelle des Rechtsdienstes fedpol, welche für die Einhaltung der Datenschutzvorschriften der Applikationen von fedpol verantwortlich ist;

j. *Informatiksicherheitsbeauftragter ISBO fedpol*: ist zuständig für die Prüfung und Einhaltung der Informatiksicherheitsaspekte;

k. *Grenzwachtkorps (GWK):* es vollzieht Einreiseverbote und Ausreisebeschränkungen;

l. *ISC EJPD*: das Informatik Service Center des Departements;

m. *SZH:* Schweizerische Zentralstelle Hooliganismus;

n. *Kantonaler Benutzerverwalter*: erfasst und verwaltet die Benutzer der Kantons-, Städte- und Gemeindepolizeien und meldet sie via Zugriffsantrag dem HOOGAN-Applikationsverantwortlichen;

o. *Organisator von Sportveranstaltungen*: er kann Daten aus HOOGAN erhalten;

p. *Ausländische Behörde*: zuständiges ausländisches Sicherheitsorgan, das Daten aus HOOGAN erhalten kann;

q. *RIPOL*: automatisiertes Fahndungssystem;

r. *Sportveranstaltungen*: alle nationalen und internationalen Sportveranstaltungen;

s. *Sportveranstaltungsbericht (SVB)*: nicht personenbezogene Informationen über Polizeieinsätze anlässlich von Sportveranstaltungen;

t. *Vollzugriff:* Zugriff auf HOOGAN, der das Lesen, das Erfassen, das Mutieren oder das Löschen von Daten ermöglicht;

u. *Kurzzugriff:* Zugriff auf HOOGAN via RIPOL, der nur das Lesen von aktuellen aktiven Daten ermöglicht;

v. *SSO Portal EJPD*: Elektronisches Single Sign On (SSO)-Portal des Departements, welches einen Single Sign On auf alle Fachanwendungen des Departements zur Verfügung stellt, wie beispielsweise den Vollzugriff auf HOOGAN.

w. *Benutzer*: Mitarbeiter einer kantonalen oder städtischen Polizeibehörde, der sogenannten dezentralen Fachstelle.

Art. 3 Zweck

Fedpol betreibt nach Art. 24*a* Abs. 1 BWIS das elektronische Informationssystem HOOGAN, in das Daten über Personen aufgenommen werden, die sich anlässlich von Sportveranstaltungen im In-und Ausland gewalttätig verhalten haben. Die eingetragenen Ereignisse und Sportveranstaltungsberichte bilden die Grundlagen für Analyseberichte und Statistiken.

Art. 4 Struktur von HOOGAN

In HOOGAN sind Personendaten, welche dem Bundesgesetz vom 19. Juni 1992[5] über den Datenschutz (DSG) unterstehen und Daten zu Sportveranstaltungen, welche nicht personenbezogen sind und dem DSG daher nicht unterstehen, gespeichert.

5 SR 235.1.

ABSCHNITT 2: BEHÖRDEN UND STELLEN

Art. 5 Organe des Bundesamtes

[1] Fedpol ist das verantwortliche Bundesorgan und Datenherr von HOOGAN[6]. Innerhalb von fedpol liegt die Verantwortung für HOOGAN bei der Sektion Hooliganismus (SH) der Hauptabteilung Dienste.

[2] Der HOOGAN-Applikationsverantwortlicher ist benutzerseitig verantwortlich für HOOGAN. Er ist Mitglied des Projektausschusses, verantwortlich für Planung, Weiterentwicklung und Betrieb des Systems sowie Anlaufstelle für die Kantone. Er versieht zudem die Aufgaben des HOOGAN-Benutzerverwalters und des HOOGAN-Schulungsverantwortlichen. Er erstellt Schulungsunterlagen und Handbücher und organisiert Grund- und Wiederholungskurse für die zugriffsberechtigten Mitarbeiter des Bundes, der Kantone und Städte, der SZH und des GWK.

[3] Die HOOGAN-Qualitätssicherung der SH sorgt bei den Benutzern für die Einhaltung der gesetzlichen Grundlagen, insbesondere des BWIS und der VVMH, des DSG sowie des Bearbeitungsreglements. Sie prüft, korrigiert und übernimmt oder weist provisorisch erfasste Daten zurück.

[4] Der HOOGAN-Sachbearbeiter ist für die Bewirtschaftung der nicht personenbezogenen Stammdaten von HOOGAN verantwortlich.

Art. 6 ISC EJPD

Das ISC EJPD ist als Leistungserbringer von HOOGAN zuständig für den Betrieb sowie verantwortlich für die Einhaltung der geltenden Bundesvorschriften im Bereich der Informatiksicherheit.

Art. 7 SZH

Die SZH ist für die Vorprüfung der eingegangenen Meldungen über Stadionverbote und Sportveranstaltungsberichte besorgt. Sie prüft, korrigiert und übernimmt oder weist provisorisch erfasste Daten zurück.

Art. 8 GWK

[1] Das GWK kann zur Identitätsabklärung Personendaten und deren Massnahmen in HOOGAN abfragen. Designierte Mitarbeiter des GWK[7] haben Vollzugriff auf HOOGAN.

[2] Fedpol teilt dem GWK verfügte Ausreisebeschränkungen mit[8].

6 Art. 24*a* Abs. 1 BWIS.
7 Art. 9 Abs. 1 lit. d VVMH.
8 Art. 7 Abs. 7 VVMH.

Art. 9 Kantonale Organe

[1] Verantwortliche Mitarbeiter der Polizeibehörden der Kantone und Städte[9] geben ihre Daten in HOOGAN ein, mutieren sie und leiten sie an die HOOGAN-Qualitätssicherung zur Freigabe im produktiven System weiter oder löschen sie umgehend. Die übrigen Dienststellen haben ausschliesslich Zugang zu HOOGAN zur Personenidentifikation im Zusammenhang mit Gewalt an Sportveranstaltungen.

[2] Jedes Polizeikorps ist gehalten, die Personen zu ernennen, die vor Ort für das Funktionieren von HOOGAN sorgen. Es bestimmt insbesondere:

a. Benutzer, die Daten in HOOGAN vorerfassen und die nötigen Belege an die SZH respektive an die SH weiterleiten. Sie sind dafür verantwortlich, dass die Daten, die sie der Stelle melden oder selbst im HOOGAN erfassen, richtig und vollständig sind;

b. mindestens eine Person als kantonaler Benutzerverwalter. Sie unterstützt und überprüft im kantonalen Polizeikorps, den angeschlossenen Gemeinde- und Städtepolizeien die Einhaltung von BWIS, der VVMH und des Bearbeitungsreglements;

c. eine Person als Schulungsbeauftragte. Sie ist Ansprechpartnerin im Kanton für sämtliche Belange der Ausbildung HOOGAN. Sie setzt sich dafür ein, dass die kantonalen Benutzer von HOOGAN die nötigen Ausbildungen im Kanton oder bei der SH besuchen können. Sie erhält vom HOOGAN-Schulungsverantwortlichen die nötige Beratung und Unterstützung sowie Schulungsunterlagen, um die Schulungen im eigenen Korps durchzuführen. Sie leitet ebenfalls die von der SH erhaltenen Informationen an die zuständigen Städte- und Gemeindepolizeien weiter.

[3] Die Kantone bestimmen ein Kontrollorgan, welches für die Einhaltung des Datenschutzes im Zusammenhang mit HOOGAN zuständig ist. Das Kontrollorgan gewährleistet die Einhaltung der Datenschutz- und Informationssicherheitsbestimmungen und ist Ansprechpartner für fedpol.

ABSCHNITT 3: BENUTZER UND DATENZUGRIFF

Art. 10 Benutzer

[1] HOOGAN steht den zuständigen Stellen von fedpol sowie den dezentralen Fachstellen der Polizeibehörden der Kantone und Städte, der SZH und dem GWK über ein Abrufverfahren zur Verfügung[10].

[2] Es werden für die Erteilung der Zugriffsberechtigung die zeitgemässen Sicherheitsmittel angewendet.

9 Art. 24a Abs. 7 BWIS und Art. 9 Abs. 1 VVMH.
10 Art. 24a Abs. 7 BWIS.

Art. 11 Persönliche Zugriffsberechtigung

[1] Die Zugriffsberechtigung zu HOOGAN wird jedem Benutzer persönlich erteilt (Zugriffsprofil) und darf nicht an Dritte weitergegeben werden.

[2] Alle Anträge für Zugriffsberechtigungen sind mit dem vom Vorgesetzten visierten, im Internet zur Verfügung gestellten EJPD-Formular an die SH zu richten. Diese prüft die Anträge auf Vollständigkeit und Einhaltung der im 4. Abschnitt der Online-Weisung aufgeführten Grundsätze und entscheidet über den Antrag[11].

[3] Die SH erfasst und verwaltet sämtliche Benutzer.

[4] Anträge für die individuellen Zugriffsberechtigungen für die an der Entwicklung und am Unterhalt von HOOGAN arbeitenden Mitarbeiter des ISC EJPD werden an die SH weitergeleitet. Diese prüft die Anträge auf Vollständigkeit und Einhaltung der im 4. Abschnitt der Online-Weisung aufgeführten Grundsätze und leitet sie an den Leiter oder Stv. Leiter der SH zum Entscheid weiter. Die SH erfasst und verwaltet die Zugriffe der Mitarbeiter des ISC EJPD. Sie prüft periodisch, ob die erlaubten Zugriffe immer noch gerechtfertigt sind.

[5] Zugriffsberechtigungen für Schulungsbenutzer dürfen vereinfacht erteilt werden. Schulungsbenutzer haben Zugriff auf das vom produktiven System abgetrennte System HOOGAN-Schulung.

[6] Die Erteilung von Zugriffsberechtigungen erfolgt nach den Bestimmungen der Online-Weisung, namentlich nach denjenigen des 4. Abschnitts, sowie nach der VVMH.

Art. 12 Aufhebung der Zugriffsberechtigung

[1] Die persönliche HOOGAN-Zugriffsberechtigung wird aufgehoben, wenn die Bedingungen von Art. 14 des Bearbeitungsreglements nicht mehr erfüllt sind oder die Person für ihre gesetzliche Tätigkeit keinen HOOGAN-Zugriff mehr benötigt. Die Vorgesetzten haben solche Mutationen der SH umgehend zu melden.

[2] Bei Nichtbenutzung während 60 Tagen kann die persönliche Zugriffsberechtigung provisorisch gesperrt werden. Die Aufhebung der Sperre muss bei der SH beantragt werden.

[3] Wird das System von einem berechtigten Benutzer länger als ein Jahr nicht benutzt, kann die SH die entsprechende Zugriffsberechtigung aufheben.

[4] Bei Missbrauch der Zugriffsberechtigung informiert fedpol die betroffene Dienststelle und hebt die entsprechende Zugriffsberechtigung auf.

Art. 13 Ausbildung der Benutzer

[1] Alle HOOGAN-Benutzer haben vor der Zugriffsberechtigung eine ihren Zugriffsprofilen angepasste Ausbildung zu absolvieren.

[2] Der HOOGAN- Applikationsverantwortliche organisiert die notwendigen deutsch- und französischsprachigen Ausbildungen und Wiederholungskurse für Personen mit

---

[11] Art. 9 Abs. 8 VVMH.

Vollzugriff. Er bildet von jedem Kanton sowie vom GWK Ausbildner aus. Diese bilden die Benutzer in ihrem Zuständigkeitsbereich aus.

[3] Der Benutzer wird im ganzen System feldbezogen vom Anwendungshandbuch unterstützt. Das Anwendungshandbuch ist dreisprachig (d/f/i) ausgearbeitet.

Art. 14 Datenzugriff

Die Benutzer der verschiedenen Kategorien verfügen nur über diejenigen Berechtigungen, die sie tatsächlich benötigen. Die Zugriffsberechtigungen für jede einzelne Benutzerkategorie sind in der VVMH geregelt. Das Recht, Daten zu erfassen und zu modifizieren, ist auf diejenigen Personen beschränkt, die solche Arbeiten tatsächlich ausführen. Die Zugriffsberechtigungen auf HOOGAN (vorerfassen, verifizieren, erfassen, zurückweisen, vernichten, archivieren) sind für jede einzelne Benutzerkategorie im Anhang der VVMH geregelt.

Art. 15 Zugriff auf die Personen- und Ereignisdaten

[1] Der Zugriff für das (Vor-)Erfassen von Personendaten (Foto, Name, Vorname, Geburtsdatum, Geburtsort, Heimatort, Wohnadresse, Art und Grund der Massnahme, Nachweis des gewalttätigen Verhaltens) und von Ereignisdaten (Sachverhaltsrapporte, Berichte über Sportveranstaltungen, Ort, Ereignisse, Organisationen, Videoaufnahmen) in HOOGAN ist pro Kanton beschränkt.

[2] Die Zugriffsberechtigungen sind im Art. 24*a* Abs. 7 BWIS und im Art. 9 der VVMH geregelt.

ABSCHNITT 4: BEARBEITUNG DER DATEN

Art. 16 Eintragung in HOOGAN

In Anwendung von Art. 24*a* Abs. 2 BWIS muss eine der folgenden Voraussetzungen vorhanden sein, um Informationen über Personen, gegen die Massnahmen wie Stadionverbote, Rayonverbote, Meldeauflagen, Polizeigewahrsam oder Ausreisebeschränkungen verhängt worden sind, in das Informationssystem aufzunehmen:

a. Die Massnahme ist von einer richterlichen Behörde ausgesprochen oder bestätigt worden;

b. Die Massnahme ist aufgrund einer strafbaren Handlung ausgesprochen worden, die zur Anzeige an die zuständigen Behörden gebracht wurde; oder

c. Die Massnahme ist zur Wahrung der Sicherheit von Personen oder der Sportveranstaltung notwendig und es kann glaubhaft gemacht werden, dass die Massnahme begründet ist.

Art. 17 Massnahmen

[1] Massnahmen[12] gegen Gewalt anlässlich von Sportveranstaltungen sind namentlich:

a. Stadionverbote
b. Rayonverbote
c. Ausreisebeschränkungen
d. Meldeauflagen
e. Polizeigewahrsam

[2] Sie werden, mit Ausnahme der Ausreisebeschränkungen und den Stadionverboten, von den zuständigen Stellen der Kantone und Städte vorerfasst. Die SZH ist Vortriagestelle für Stadionverbote und Sportveranstaltungsberichte Die Kantone melden ihre personenbezogenen Daten direkt an die SH. Die SZH kontrolliert die Angaben auf ihre Richtigkeit und Erheblichkeit und übermittelt entweder die Massnahme an die SH oder weist sie an die kantonale Stelle zurück.

Art. 18 Ausreisebeschränkungen

Fedpol ist zuständig für das Verfügen von Ausreisebeschränkungen. Die Kantone und die SZH können Ausreisebeschränkungen beantragen. Zusätzlich zur Ausschreibung im RIPOL wird die verfügte Ausreisebeschränkung dem GWK sowie den zuständigen Zoll- und Polizeibehörden im Ausland mitgeteilt.

Art. 19 Erfassung und Kontrolle der Daten

[1] Die dezentrale Fachstelle des Kantons erfasst ihre Daten und Bilder in einem Vorerfassungsmodul von HOOGAN. Personenbezogene Daten werden durch die SH geprüft und erfasst, veranstaltungsbezogene Daten durch die SZH.

[2] Die SH prüft gemäss Art. 24*a* Abs. 6 BWIS, ob die Informationen, die ihr übermittelt werden, richtig und erheblich im Sinne von Art. 24*a* Abs. 2 BWIS sind, und weist unrichtige oder unerhebliche Informationen mit Begründung an den Absender zur Vervollständigung oder Löschung zurück.

[3] Meldungen vom Ausland gelangen direkt an die SH in ihrer Funktion als Nationale Fussball-Informationsstelle (NFIP). Sie prüft die Daten, entscheidet über die Aufnahme und erfasst sie in HOOGAN.

Art. 20 Datenerfassung

Daten können in HOOGAN in Französisch, Deutsch oder Italienisch eingegeben werden. Die in den plausibilisierten Feldern eingegebenen Daten werden automatisch übersetzt.

12 Die Massnahmen Rayonverbot, Meldeauflage und Polizeigewahrsam sind im Konkordat über Massnahmen gegen Gewalt anlässlich von Sportveranstaltungen geregelt.

Art. 21 Aufbewahrungsdauer

Die Aufbewahrungsdauer der Personendaten richtet sich nach Art. 12 der VVMH. Demnach werden die Personendaten und die Informationen zu einer einzelnen Massnahme 3 Jahre nach Ablauf dieser Massnahme gelöscht. Wird während dieser 3 Jahre eine weitere Massnahme gegen dieselbe Person eingetragen, so verlängert sich die Dauer der ersten Eintragung auf 3 Jahre ab dem Datum der zweiten Eintragung; für die anschliessende Löschung gilt wiederum dieselbe Bedingung. Die jeweilige Massnahme wird jedoch spätestens nach 10 Jahren gelöscht.

Art. 22 Datenweitergabe

[1] Die Datenweitergabe aus HOOGAN richtet sich nach Art. 24*a* Abs. 8 und 9 BWIS und Art. 10 und 11 der VVMH. Diese Daten können zwecks Erfüllung ihrer gesetzlichen Aufgaben an Organisatoren von Sportveranstaltungen in der Schweiz und an ausländische Polizeibehörden, Grenzbehörden und Sicherheitsorgane weitergegeben werden. Die Weitergabe ins Ausland richtet sich nach Art. 17 Abs. 3 bis 5 BWIS.

[2] Die von der SH an Organisatoren von Sportveranstaltungen in der Schweiz gelieferten Daten sind nach der Sportveranstaltung von den Sicherheitsverantwortlichen oder von den Organisatoren der Sportveranstaltung umgehend zu vernichten. Die SH ist innert 24 Stunden unaufgefordert über die Vernichtung zu unterrichten.

[3] Über die gesetzeskonforme Verwendung der Daten führt die SH stichprobenweise bei den Sportveranstaltern und deren Sicherheitsverantwortlichen Kontrollen durch.

[4] Die Richtlinie für die Verwendung und Bearbeitung von Daten des Informationssystems HOOGAN durch Organisatoren von Sportveranstaltungen und deren Sicherheitsverantwortliche vom 1. Januar 2010 sowie die Richtlinie für die elektronische Übermittlung von Daten des Informationssystems HOOGAN an Organisatoren von Sportveranstaltungen zur Durchführung von Zutrittskontrollen mit Abgleich von Ausweisen (*HOOGAN+*) sind direkt anwendbar.

Art. 23 Ausdruck und Weiterverwendung von Daten

[1] HOOGAN bietet die Möglichkeit zum Ausdrucken von Daten und zum Erstellen von Listen.

[2] Die Benutzer dürfen aus HOOGAN einzelne Fälle mit den dazugehörigen Hauptentitäten zum Erstellen eines Polizei- oder Übergaberapportes auf dem PC speichern. Dabei ist Art. 13 der VVMH zu beachten.

[3] Die Benutzer dürfen Rohdatenfiles erstellen, d.h. den Inhalt der ausgewählten Felder nach einer erfolgten Recherche auf den PC herunterladen. Die erhaltenen Daten, welche zur Aufklärung der Straftaten dienen können, dürfen für die Kriminalanalyse weiterverwendet werden.

[4] Die Benutzerverwalter dürfen zu Kontrollzwecken aus der Benutzerverwaltung Rohdatenfiles erstellen.

[5] Alle obgenannten zur lokalen temporären Behandlung gespeicherten Daten und Listen müssen sofort nach Verwendung unwiderruflich gelöscht werden.

[6] Ausgedruckte Daten und Listen unterstehen den gleichen Vorschriften über die Aufbewahrung, die Bearbeitung, die Weitergabe und die Vernichtung wie die elekt-

ronisch in HOOGAN bearbeiteten Daten. Bei Weitergabe von Ausdrucken von Daten, welche von einer anderen Erfassungsstelle in einer anderen Geschäftskategorie erfasst worden sind, ist den Verwendungsmöglichkeiten besondere Aufmerksamkeit zu schenken.

Art. 24 Auskunftserteilung an betroffene Personen

Die Wahrnehmung der Rechte der Betroffenen richtet sich nach Art. 24*a* Abs. 10 BWIS. Jede Person kann vom Datenschutz- und Informationsschutzbeauftragten von fedpol Auskunft darüber verlangen, ob in HOOGAN Daten über sie bearbeitet werden und verlangen, dass unrichtige Daten berichtigt werden.

ABSCHNITT 5: LÖSCHUNG UND BUNDESARCHIV

Art. 25 Löschung der Daten

[1] Die absolute Aufbewahrungsdauer der Personendaten richtet sich nach Art. 12 der VVMH.

[2] Personendaten werden jeweils beim Erreichen des Löschdatums gelöscht.

Art. 26 Abgabe der Daten und Dokumente an das Bundesarchiv

[1] Die in HOOGAN gelöschten Daten werden dem Bundesarchiv zur Archivierung angeboten. Nicht angeboten werden klassifizierte Daten aus dem direkten Verkehr mit ausländischen Sicherheitsbehörden und vom Ausland importierte Daten.

[2] Die in HOOGAN gelöschten Daten werden im Modul «BAR» sichergestellt. Der HOOGAN-Applikationsverantwortliche verwaltet die im Modul «BAR» gespeicherten Daten und ist für die organisatorische und technische Abwicklung der Datenübergabe an das BAR und deren anschliessende Löschung im BAR-Modul zuständig.

[3] Die vom Bundesarchiv als nicht archivwürdig bezeichneten Unterlagen werden vernichtet. Vorbehalten bleiben diesbezüglich weitere gesetzliche Bestimmungen über die Datenvernichtung.

ABSCHNITT 6: INFORMATIKSICHERHEIT

Art. 27 Informatiksicherheit

[1] Für die Informatiksicherheit gelten die Weisungen des IRB vom 27. September 2004 über die Informatiksicherheit in der Bundesverwaltung (Informatiksicherheitsweisung IRB) sowie die nachfolgenden Bestimmungen des Bearbeitungsreglements.

[2] Vor der erstmaligen Inbetriebnahme eines HOOGAN-Anschlusses muss von der anzuschliessenden Stelle der Nachweis über die Umsetzung der entsprechenden Vorgaben erbracht werden[13].

Art. 28 Datensicherung

[1] Die Benutzer geben ihre Daten in HOOGAN ein, wo sie gespeichert werden. Diese Daten können durch die Benutzer, die dazu gemäss Anhang der VVMH berechtigt sind, mutiert werden.

[2] Die HOOGAN-Daten werden durch das ISC EJPD gemäss den geltenden Weisungen der Bundesverwaltung gesichert. Regelmässig werden vom ISC EJPD Sicherheitskopien erstellt.

[3] Die Wiederherstellung der Datenkonsistenz und Datenintegrität auf dem Informationssystem nach einem Datenverlust oder dem Ausfall von Systemkomponenten ist garantiert.

Art. 29 Massnahmen zum Schutz der Daten (Vertraulichkeit) im Bereich der Datenendgeräte

[1] Die Datenendgeräte müssen in geschützten Zonen platziert sein. Der Zugang zu den geschützten Zonen muss nachvollziehbar kontrolliert sein.

[2] Ausgedruckte Daten sind so aufzubewahren, dass Drittpersonen sie nicht einsehen und/oder kopieren können. Diese Daten müssen sofort vernichtet werden, wenn sie den Zweck ihrer Erstellung erfüllt haben.

Art. 30 Sichere Übermittlung

Die Übermittlung der Daten erfolgt direkt in HOOGAN.

Art. 31 Benutzerunterstützung und Meldepflicht

[1] Fachlich werden die Benutzer in den Kantonen primär durch die SH unterstützt. Diese steht den Benutzern während den Bürozeiten zur Verfügung.

[2] Die technische Unterstützung für die Datenendgeräte und das Netzwerk ist zunächst durch den IT-Verantwortlichen zu erbringen. Kann dieser die Probleme nicht lösen, wendet er sich ans ISC EJPD. Dieses stellt während der Bürozeiten das IT Help Desk zur Verfügung.

[3] Die Benutzer sind über die Sicherheitseinstufung von HOOGAN und den Vorschriften im Umgang mit dem System und dessen Daten orientiert. Mögliche Sanktionen bei vorsätzlichen oder fahrlässigen Verletzungen der Informatiksicherheit sind den Benutzern bekannt. Sämtliche Benutzer sind verpflichtet, folgende Feststellungen dem HOOGAN-Applikationsverantwortlichen zu melden:

13 Art. 5 Abs. 1 Online-Weisung.

a. Fehler in den erfassten Daten, bei der Identität der registrierten Personen und in den Stammdaten oder deren Strukturen;

b. beobachtete oder vermutete Schwachstellen bzw. Sicherheitsmängel des Systems;

c. nicht umgesetzte oder nicht eingehaltene Sicherheitsmassnahmen;

d. unvorhergesehene Ereignisse, die eine Auswirkung auf die Informatiksicherheit haben könnten.

Art. 32 HOOGAN-Programmentwicklung

[1] Es wird eine klare Trennung zwischen Entwicklung, Test, Integration, Schulung und Produktion praktiziert.

[2] Anträge für die Weiterentwicklung des Systems werden zusammengefasst und als Wartungsvorhaben oder Projekt definiert, angemeldet, budgetiert und realisiert.

[3] Programme, die entwickelt und / oder getestet werden, greifen nicht auf produktive HOOGAN-Daten zu.

[4] Programmübernahmen in die Produktion werden im ISC EJPD durch den Prozess "operationelle Changes" gemacht.

Art. 33 Protokollierung

Jede Bearbeitung von Daten in HOOGAN wird in einem Protokoll festgehalten[14]. Die Protokollierungsdaten werden während eines Jahres aufbewahrt.

Art. 34 Aufsicht und Verantwortlichkeit

[1] Fedpol trägt die Verantwortung für HOOGAN.

[2] Der HOOGAN-Applikationsverantwortliche beaufsichtigt, ob die Benutzer die gesetzlichen Grundlagen einhalten.

Art. 35 Missbräuchliche Verwendung von HOOGAN

[1] Wird eine missbräuchliche Verwendung von HOOGAN durch einen Benutzer innerhalb der Bundesverwaltung festgestellt oder vermutet, namentlich indem ein missbräuchlicher Datenzugriff oder ein missbräuchlicher Eintrag vermutet wird, muss unverzüglich der Datenschutz- und Informationsschutzberater DSBO von fedpol informiert werden. Um den Sachverhalt zu belegen, kann dieser die HOOGAN-Qualitätssicherung damit beauftragen, den Sachverhalt festzustellen und ihm diesen vertraulich mitzuteilen. Anschliessend informiert dieser den Direktor von fedpol, welcher den Sachverhalt bei strafrechtlicher Relevanz der zuständigen Behörde anzeigt.

[2] Wird eine missbräuchliche Verwendung von HOOGAN durch einen Benutzer ausserhalb der Bundesverwaltung festgestellt oder vermutet, namentlich indem

14 Gemäss Art. 10 der Verordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993 (SR 235.11).

ein missbräuchlicher Datenzugriff oder ein missbräuchlicher Eintrag vermutet wird, muss unverzüglich entweder die zuständige Strafverfolgungsbehörde des Kantons oder der Datenschutz- und Informationsschutzberater DSBO fedpol informiert werden. Er kann die HOOGAN-Qualitätssicherung damit beauftragen, den Sachverhalt festzustellen und ihm vertraulich mitzuteilen. Anschliessend informiert er den Direktor von fedpol, welcher bei strafrechtlicher Relevanz seinerseits die zuständige kantonale Strafverfolgungsbehörde informiert.

Art. 36 Technische Anforderungen

[1] Die in der Bundesverwaltung und den kantonalen Polizeikorps sowie dem GWK angeschlossenen Datenendgeräte müssen den technischen Vorschriften des Bundes entsprechen.

[2] Diese Anforderungen werden zusammen mit dem ISC EJPD in Berücksichtigung der VDSG festgelegt.

Art. 37 Anhänge zum HOOGAN-Bearbeitungsreglement

[1] Die im Bearbeitungsreglement erwähnten Anhänge sind integrierender Bestandteil dieses Bearbeitungsreglementes.

[2] Der HOOGAN-Applikationsverantwortliche verwaltet und aktualisiert das Bearbeitungsreglement[15].

ABSCHNITT 7: ABSCHLIESSENDE BESTIMMUNGEN

Art. 38 Inkrafttreten und Publikation

Das vorliegende Bearbeitungsreglement ersetzt dasjenige vom 1. Januar 2010 und tritt am 1. Mai 2013 in Kraft.

Bern, 30. April 2013

BUNDESAMT FÜR POLIZEI fedpol

des Eidgenössischen Justiz- und Polizeidepartements

Direktor fedpol

Jean-Luc Vez

15 Gemäss Art. 11 der Verordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993 (SR 235.11).

ANHANG 1: VERORDNUNG ÜBER VERWALTUNGSPOLIZEILICHE MASSNAHMEN DES BUNDESAMTES FÜR POLIZEI UND ÜBER DAS INFORMATIONSSYSTEM HOOGAN

Verordnung 120.52
über verwaltungspolizeiliche Massnahmen des Bundesamtes für Polizei und über das Informationssystem HOOGAN (VVMH)[1]

vom 4. Dezember 2009 (Stand am 1. Februar 2013)

Der Schweizerische Bundesrat,
gestützt auf die Artikel 24a Absätze 7 und 8 sowie 30 des Bundesgesetzes vom 21. März 1997[2] über Massnahmen zur Wahrung der inneren Sicherheit (BWIS),[3]
verordnet:

1. Abschnitt: Allgemeine Bestimmungen

Art. 1 Gegenstand

Diese Verordnung regelt:

a. die Durchführung verwaltungspolizeilicher Massnahmen, gestützt auf das BWIS, durch das Bundesamt für Polizei (fedpol);
b. das Informationssystem HOOGAN von fedpol;
c. …[4]

Art. 2[5]

2. Abschnitt:
Verwaltungspolizeiliche Massnahmen gegen Propagandamaterial

Art. 3

[1] Über die Beschlagnahme und die Einziehung von Propagandamaterial im Sinne von Artikel 13*e* BWIS entscheidet fedpol nach Anhörung des Nachrichtendienstes des Bundes (NDB).[6]
[2] Die sicherstellende Behörde übermittelt das Propagandamaterial umgehend an den NDB und informiert diesen über die Umstände der Sicherstellung sowie über die beteiligten Personen und Firmen.
[3] Fedpol zieht das Propagandamaterial ein, wenn der Aufruf zur Gewalt konkret und ernsthaft ist.
[4] Fedpol vernichtet das eingezogene Material, sofern es nicht zu Instruktionszwecken verwendet werden kann.

3. Abschnitt:
Verwaltungspolizeiliche Massnahmen gegen Gewalt anlässlich von Sportveranstaltungen

Art. 4 Gewalttätiges Verhalten

[1] Gewalttätiges Verhalten und Gewalttätigkeiten liegen namentlich vor, wenn eine Person im Vorfeld einer Sportveranstaltung, während der Veranstaltung oder im Nachgang dazu folgende Straftaten begangen oder dazu angestiftet hat:[7]

a.[8] strafbare Handlungen gegen Leib und Leben nach den Artikeln 111–113, 117, 122, 123, 125 Absatz 2, 126 Absatz 1, 129, 133 und 134 des Strafgesetzbuches[9] (StGB)[10];
b. Sachbeschädigungen nach Artikel 144 StGB;

---

1 Fassung gemäss Beilage 2 Ziff. 1 der V vom 21. Nov. 2012, in Kraft seit 1. Jan. 2013 (AS **2012** 6781).
2 SR 120
3 Fassung gemäss Ziff. I der V vom 14. Dez. 2012, in Kraft seit 1. Febr. 2013 (AS **2013** 1).
4 Aufgehoben durch Beilage 2 Ziff. 1 der V vom 21. Nov. 2012, mit Wirkung seit 1. Jan. 2013 (AS **2012** 6781).
5 Aufgehoben durch Beilage 2 Ziff. 1 der V vom 21. Nov. 2012, mit Wirkung seit 1. Jan. 2013 (AS **2012** 6781).
6 Fassung gemäss Ziff. I der V vom 14. Dez. 2012, in Kraft seit 1. Febr. 2013 (AS **2013** 1).
7 Fassung gemäss Ziff. I der V vom 14. Dez. 2012, in Kraft seit 1. Febr. 2013 (AS **2013** 1).
8 Fassung gemäss Ziff. I der V vom 14. Dez. 2012, in Kraft seit 1. Febr. 2013 (AS **2013** 1).
9 SR **311.0**
10 SR **311.0**

c. Nötigung nach Artikel 181 StGB;
d. Brandstiftung nach Artikel 221 StGB;
e. Verursachung einer Explosion nach Artikel 223 StGB;
f.[11] Gefährdung durch Sprengstoffe und giftige Gase in verbrecherischer Absicht nach Artikel 224 StGB;
g.[12] öffentliche Aufforderung zu Verbrechen oder zur Gewalttätigkeit nach Artikel 259 StGB;
h.[13] Landfriedensbruch nach Artikel 260 StGB;
i.[14] Gewalt und Drohung gegen Behörden und Beamte nach Artikel 285 StGB;
j.[15] Hinderung einer Amtshandlung nach Artikel 286 StGB.

[2] Als gewalttätiges Verhalten gilt ferner die Gefährdung der öffentlichen Sicherheit durch das Mitführen oder Verwenden von Waffen, Sprengmitteln, Schiesspulver oder pyrotechnischen Gegenständen in Sportstätten, in deren Umgebung sowie auf An- und Rückreisewegen zu und von Sportstätten.

Art. 5 Nachweis gewalttätigen Verhaltens

[1] Als Nachweis gewalttätigen Verhaltens gelten:
a. entsprechende Gerichtsurteile oder polizeiliche Anzeigen;
b. glaubwürdige Aussagen oder Bildaufnahmen der Polizei, der Zollverwaltung, des Sicherheitspersonals oder der Sportverbände und -vereine;
c. Stadionverbote der Sportverbände oder -vereine;
d. Meldungen einer zuständigen ausländischen Behörde.

[2] Aussagen nach Absatz 1 Buchstabe b sind schriftlich festzuhalten und zu unterzeichnen.

Art. 6 Zuständigkeit und Meldepflichten

[1] Die Kantone und die in Artikel 13 BWIS genannten Behörden und Amtsstellen erstatten fedpol unaufgefordert Meldung über Informationen und Erkenntnisse betreffend Gewalttätigkeiten anlässlich von Sportveranstaltungen.

[2] Zusätzlich melden die Kantone fedpol:
a. Verfügungen, Aufhebungen und Änderungen folgender Massnahmen:
1. Stadionverbot,
2. Rayonverbot,
3. Meldeauflage,
4. Polizeigewahrsam;
b. Verstösse gegen Massnahmen nach Buchstabe a;
c. die von ihnen festgelegten Rayons unter Beilage der entsprechenden Pläne.

[3] Fedpol bestimmt den Massstab der Pläne nach Absatz 2 Buchstabe c.[16]

Art. 7 Ausreisebeschränkung

[1] Fedpol ist zuständig für die Verfügung einer Ausreisebeschränkung.

[2] In der Verfügung sind die Dauer der Ausreisebeschränkung und die betroffenen Bestimmungsländer genau festzulegen.

[3] Eine Sportveranstaltung beginnt mit dem ersten damit zusammenhängenden offiziellen Akt und endet mit dem letzten damit zusammenhängenden offiziellen Akt.

[4] Dass eine Person sich anlässlich einer Sportveranstaltung in einem bestimmten Land an Gewalttätigkeiten beteiligen wird, ist namentlich anzunehmen, wenn diese Person:
a. sich an Gewalttätigkeiten im Inland beteiligt hat;
b. aufgrund von Informationen ausländischer Polizeistellen über die Beteiligung an Gewalttätigkeiten im Ausland bereits bekannt ist; oder
c. Mitglied einer Gruppierung ist, die schon an Gewalttätigkeiten im In- oder Ausland beteiligt war.

[5] Für die Verfügung einer Ausreisebeschränkung müssen zudem Hinweise vorliegen, dass die Person oder die betreffende Gruppierung beabsichtigt, zum Sportanlass im Ausland zu reisen.

---

11 Fassung gemäss Ziff. I der V vom 14. Dez. 2012, in Kraft seit 1. Febr. 2013 (AS **2013** 1).
12 Fassung gemäss Ziff. I der V vom 14. Dez. 2012, in Kraft seit 1. Febr. 2013 (AS **2013** 1).
13 Fassung gemäss Ziff. I der V vom 14. Dez. 2012, in Kraft seit 1. Febr. 2013 (AS **2013** 1).
14 Fassung gemäss Ziff. I der V vom 14. Dez. 2012, in Kraft seit 1. Febr. 2013 (AS **2013** 1).
15 Fassung gemäss Ziff. I der V vom 14. Dez. 2012, in Kraft seit 1. Febr. 2013 (AS **2013** 1).
16 Fassung gemäss Ziff. I der V vom 14. Dez. 2012, in Kraft seit 1. Febr. 2013 (AS **2013** 1).

[6] Besteht gegen eine Person kein kantonales Rayonverbot wegen Gewalt anlässlich von Sportveranstaltungen, so ist eine Ausreisebeschränkung begründet, wenn konkrete und aktuelle Tatsachen vorliegen, dass:

a. die Person nach Informationen ausländischer Polizeistellen im Ausland gewalttätig gewesen ist;
b. die Person Mitglied einer Gruppierung ist, die schon mehrfach an Gewalttätigkeiten im In- oder Ausland beteiligt war; und
c. als gesichert erscheint, dass die Person oder die Gruppierung beabsichtigt, an einen bestimmten Sportanlass im Ausland zu reisen.

[7] Zusätzlich zur Ausschreibung im automatisierten Polizeifahndungssystem (RIPOL) wird die verfügte Ausreisebeschränkung den Grenzbehörden sowie den zuständigen Zoll- und Polizeibehörden im Ausland mitgeteilt.

Art. 7*a*[17] Stadionverbot, Rayonverbot und Meldeauflage

[1] Fedpol kann den Organisatoren von Sportveranstaltungen empfehlen, gegen Personen Stadionverbote auszusprechen, die sich anlässlich einer Sportveranstaltung innerhalb oder ausserhalb des Stadions gewalttätig verhalten haben. Die Empfehlungen erfolgen unter Angabe der notwendigen Daten nach Artikel 24*a* Absatz 3 BWIS.

[2] Es kann den Polizeibehörden der Kantone beantragen, ein Rayonverbot oder Meldeauflagen zu erlassen.

4. Abschnitt: Informationssystem HOOGAN

Art. 8 Daten

[1] Im elektronischen Informationssystem HOOGAN werden Daten von Personen erfasst, die sich anlässlich einer Sportveranstaltung im Inland oder Ausland gewalttätig verhalten haben und gegen die eine Massnahme nach Artikel 6 Absatz 2 Buchstabe a oder eine Ausreisebeschränkung nach Artikel 7 verfügt wurde.[18]

[2] In HOOGAN werden zudem Sportveranstaltungen sowie damit zusammenhängende Ereignisse und die von den Kantonen bestimmten Rayons erfasst.

Art. 9 Zugriffsrechte

[1] Auf HOOGAN haben die folgenden Behörden ausschliesslich zu den folgenden Zwecken Zugriff:

a. die folgenden Stellen innerhalb von fedpol:
   1.[19] die Sektion Hooliganismus: für den Betrieb von HOOGAN, das Verfügen von Ausreisebeschränkungen, für den gesetzlich vorgesehenen Informationsaustausch sowie für Analyse- und Lagebeurteilungen,
   2. die Einsatzzentrale von fedpol: zur Personenidentifikation im Zusammenhang mit Gewalt an Sportveranstaltungen,
   3. die oder der Datenschutz- und Informationsschutzbeauftragte von fedpol: für die Bearbeitung der Auskunfts- und Löschgesuche für HOOGAN;
b. die für die Verhinderung von Gewalt an Sportveranstaltungen verantwortlichen Mitarbeiter und Mitarbeiterinnen der Polizeibehörden der Kantone: für den Erlass von Rayonverboten, Meldeauflagen und Polizeigewahrsam, für die Analyse- und Lagebeurteilung und die Weitergabe von Personendaten an Organisatoren von Sportveranstaltungen in der Schweiz;
c. die Dienststellen der Polizeibehörden der Kantone: zur Personenidentifikation im Zusammenhang mit Gewalt an Sportveranstaltungen;
d. die Dienststellen des Grenzwachtkorps (GWK) der Eidgenössischen Zollverwaltung (EZV): zum Vollzug von Ausreisebeschränkungen und von Einreiseverboten;
e. die Dienststellen der Schweizerischen Zentralstelle Hooliganismus (SZH): zur Vorprüfung der eingegangenen Meldungen über Stadionverbote und Sportveranstaltungsberichte der Organisatoren von Sportveranstaltungen sowie zur Beantragung von Ausreisebeschränkungen, Rayonverboten und Meldeauflagen.

---

[17] Eingefügt durch Ziff. I der V vom 14. Dez. 2012, in Kraft seit 1. Febr. 2013 (AS **2013** 1).

[18] Eingefügt durch Ziff. I der V vom 14. Dez. 2012, in Kraft seit 1. Febr. 2013 (AS **2013** 1).

[19] Eingefügt durch Ziff. I der V vom 14. Dez. 2012, in Kraft seit 1. Febr. 2013 (AS **2013** 1).

[2] Für HOOGAN können Berechtigungen für Voll- und Kurzzugriffe erteilt werden. Der Vollzugriff ermöglicht das Lesen, das Erfassen, das Mutieren und das Löschen von Daten. Der Kurzzugriff ermöglicht nur das Lesen von jeweils aktiven Daten im konkreten Fall.20[20]
[3] Über den Vollzugriff verfügen:
- a.[21] die Sektion Hooliganismus;
- b. die SZH;
- c. die für die Verhinderung von Gewalt an Sportveranstaltungen verantwortlichen Mitarbeiter und Mitarbeiterinnen der Polizeibehörden der Kantone und des GWK.

[4] Über den Kurzzugriff verfügen:
- a. die Einsatzzentrale von fedpol;
- b. die oder der Datenschutz- und Informationsschutzbeauftragte von fedpol;
- c. die Polizeibehörden der Kantone;
- d. das GWK.

[5] Der Kurzzugriff der Polizeibehörden der Kantone und des GWK erfolgt via Schnittstelle im Informationssystem RIPOL.
[6] Die Datenfelder und Bearbeitungsrechte sind im Anhang aufgeführt.[22]
[7] Die Behörden nach Absatz 1 stellen sicher, dass die Datenschutz- und Informatiksicherheitsbestimmungen eingehalten werden.[23]
[8] Die Leiterin oder der Leiter der Sektion Hooliganismus von fedpol oder deren oder dessen Stellvertreterin oder Stellvertreter entscheidet über individuelle Zugriffsanträge der Behörden nach Absatz 1.[24]
[9] Die Verantwortung für HOOGAN liegt bei der Sektion Hooliganismus.[25]

Art. 10 Verwendung und Weitergabe der Daten durch Organisatoren von Sportveranstaltungen
[1] Die Organisatoren von Sportveranstaltungen dürfen die in HOOGAN gespeicherten Daten nur mit Zustimmung der datenliefernden Behörde und nur zur Umsetzung von Massnahmen gegen Gewalt anlässlich von Sportveranstaltungen an die Sicherheitsverantwortlichen dieser Veranstaltungen weitergeben.
[2] Die Sicherheitsverantwortlichen dürfen die Daten nur in Bezug auf die von der Behörde bezeichnete Sportveranstaltung bearbeiten. Sie dürfen dazu die Daten in elektronischen Personenerkennungssystemen bearbeiten.
[3] Die Sicherheitsverantwortlichen und gegebenenfalls die Organisatoren von Sportveranstaltungen müssen die Daten nach der Sportveranstaltung umgehend vernichten. Sie haben die datenliefernde Behörde innert 24 Stunden über die Vernichtung zu unterrichten.
[4] Fedpol regelt im Bearbeitungsreglement die Verwendung und die Bearbeitung der Daten durch die Organisatoren von Sportveranstaltungen und die Sicherheitsverantwortlichen.

Art. 11 Weitergabe der Daten an ausländische Behörden
[1] Fedpol kann Personendaten an ausländische Polizeibehörden und Sicherheitsorgane weitergeben, die für die Sicherheit bei Sportveranstaltungen zuständig sind.
[2] Es registriert die Weitergabe an ausländische Behörden.
[3] Es setzt bei der Weitergabe von Informationen und Personendaten den Empfänger oder die Empfängerin über die Bewertung und die Aktualität der Daten in Kenntnis.
[4] Es weist den Empfänger oder die Empfängerin darauf hin, dass:
- a. die Informationen und Personendaten nur für den Zweck verwendet werden dürfen, zu dem sie weitergegeben wurden;
- b. sich fedpol vorbehält, Auskunft über die vorgenommene Verwendung zu verlangen.

Art. 12 Aufbewahrungsdauer und Löschung der Daten
[1] Die Personendaten und die Informationen zu einer einzelnen Massnahme werden 3 Jahre nach Ablauf dieser Massnahme gelöscht.
[2] Wird während dieser 3 Jahre eine weitere Massnahme gegen dieselbe Person eingetragen, so verlängert sich die Dauer der ersten Eintragung auf 3 Jahre ab dem Datum der zweiten Eintragung.

---

20 Fassung gemäss Ziff. I der V vom 14. Dez. 2012, in Kraft seit 1. Febr. 2013 (AS **2013** 1).
21 Fassung gemäss Ziff. I der V vom 14. Dez. 2012, in Kraft seit 1. Febr. 2013 (AS **2013** 1).
22 Fassung gemäss Ziff. I der V vom 14. Dez. 2012, in Kraft seit 1. Febr. 2013 (AS **2013** 1).
23 Fassung gemäss Ziff. I der V vom 14. Dez. 2012, in Kraft seit 1. Febr. 2013 (AS **2013** 1).
24 Fassung gemäss Ziff. I der V vom 14. Dez. 2012, in Kraft seit 1. Febr. 2013 (AS **2013** 1).
25 Fassung gemäss Ziff. I der V vom 14. Dez. 2012, in Kraft seit 1. Febr. 2013 (AS **2013** 1).

[3] Die Daten zu einer einzelnen Massnahme werden in jedem Fall spätestens nach 10 Jahren gelöscht.

Art. 13 Organisatorische Bestimmungen
[1] Für die Gewährleistung der Datensicherheit gelten:

a. Artikel 20 der Verordnung vom 14. Juni 1993[26] zum Bundesgesetz über den Datenschutz (VDSG);
b. die Verordnung vom 26. September 200327[27] (BinfV) über die Informatik und Telekommunikation in der Bundesverwaltung.

[2] Fedpol regelt in einem Bearbeitungsreglement:

a. die organisatorischen und die technischen Massnahmen gegen unbefugtes Bearbeiten der Daten;
b. die automatische Protokollierung der eingegebenen Daten;
c. die technischen Anforderungen, denen die Endgeräte der Benutzerinnen und Benutzer genügen müssen.

5. Abschnitt: …

Art. 14–28[28]

6. Abschnitt: Inkrafttreten
Art. 29
Diese Verordnung tritt am 1. Januar 2010 in Kraft.

26 SR **235.11**
27 SR **172.010.58**
28 Aufgehoben durch Beilage 2 Ziff. 1 der V vom 21. Nov. 2012, mit Wirkung seit 1. Jan. 2013 (AS **2012** 6781).

Anhang[29]
(Art. 9 Abs. 6)

Datenfelder und Bearbeitungsrechte

L = Lesen
A = Aktualisieren
V = Vernichten
R-Aktiv = nur Personen und untergeordnete Objekte, gegen die im Zeitpunkt der Anfrage eine Massnahme verhängt ist
SH = Sektion Hooliganismus
ISC = Informatik Service Center EJPD
EZV = Eidgenössische Zollverwaltung
SZH = Schweizerische Zentralstelle Hooliganismus
E = Städte-Polizei
F = Grenzstellen
R = Kantonale Polizei

			Vollzugriff auf HOOGAN im Bereich Produktion							Kurzzugriff auf HOOGAN via RIPOL	
		Dienststelle	fedpol SH	fedpol SH	EZV, Kantone, SZH	fedpol SH	fedpol SH, ISC	Kantone , SZH	SZH	Organisationseinheiten E, F, R	
		Rolle	fedpol Voranalyse –>	fedpol Qualitätssicherung –>	Benutzer/in –>	Administrator/in –>	technische/r Administrator/in –>	Sachbearbeiter/in –>	Sachbearbeiter/in SZH –>	Benutzer/in via RIPOL	Benutzeradministrator/in RIPOL
Datenbereiche	**Datenfelder**	**Bearbeitungsrecht**									
Person	Personalien, Adresse, Massnahmen, Massnahmenverstösse, Personen Ereignis, Beziehung	vorerfassen	LAV	-	-	-	-	LAV	LAV	-	-
		verifizieren	-	LA	-	-	-	-	LA	-	-
		erfassen	-	LA	-	-	-	-	-	-	-
		zurückweisen	-	LA	-	-	-	-	LA	-	-
		vernichten	-	LAV	-	-	-	-	-	-	-
		archivieren	-	LAV	-	LAV	-	-	-	-	-
Veranstaltungen	Ereignis	erfassen	LAV	LAV	-	-	-	LAV	LAV	-	-
		vernichten	-	LAV	-	-	-	-	-	-	-
	Sportveranstaltungsbericht	vorerfassen	-	-	-	-	-	LAV	LAV	-	-
		verifizieren	-	LA	-	-	-	-	LA	-	-
		erfassen	-	LA	-	-	-	-	LA	-	-
		zurückweisen	-	LA	-	-	-	-	LA	-	-
		vernichten	-	LAV	-	LAV	-	-	-	-	-
Person / Veranstaltung	Alle Datenfelder	operative Daten	L	LA	L	L	-	L	L	R-Aktiv	-
Funktion											
		Stammdatenverwaltung	-	-	-	LAV	LAV	-	-	-	-
		Benutzeradministration	-	-	-	-	-	-	-	-	LAV

29 Eingefügt durch Ziff. II der V vom 14. Dez. 2012, in Kraft seit 1. Febr. 2013 (AS **2013** 1).

ANHANG 2: WEISUNG DES EJPD ÜBER DIE EINRICHTUNG VON ONLINE-VERBINDUNGEN UND DIE ERTEILUNG VON ZUGRIFFSBEWILLIGUNGEN AUF INFORMATIKANWENDUNGEN DES EJPD

Weisung des EJPD über die Einrichtung von Online-Verbindungen und die Erteilung von Zugriffsbewilligungen auf Informatikanwendungen des EJPD (Online-Weisung EJPD) vom 30. September 2004

Das Eidgenössische Justiz- und Polizeidepartement,

gestützt auf Artikel 38 des Regierungs- und Verwaltungsorganisationsgesetzes vom 21. März 19971 (RVOG),

verordnet:

1. Abschnitt: Allgemeines
Art. 1 Zweck
[1] Diese Weisung harmonisiert das Verfahren bei der Einrichtung von Online-Verbindungen im Eidgenössischen Justiz- und Polizeidepartement (EJPD).
[2] Sie regelt:
a. das Verfahren und die Voraussetzungen für die Einrichtung einer Online-Verbindung zwischen dem EJPD und den Organen des Bundes und der Kantone, mit welcher Angestellte dieser Organe (Benutzende) Zugang durch ein Abrufverfahren zu einer Informatikanwendung des EJPD erhalten;
b. das Verfahren und die Voraussetzungen für die Erteilung von individuellen Zugriffsbewilligungen oder von Gruppenzugriffsbewilligungen an diese Benutzenden, wenn ihnen Personendaten durch diese Online-Verbindung zugänglich gemacht werden.

Art. 2 Voraussetzungen
Voraussetzungen für die Einrichtung einer Online-Verbindung zwischen einer Informatikanwendung des EJPD und den Benutzenden sind:
a. eine hinreichende gesetzliche Grundlage nach Artikel 19 Absatz 3 des Bundesgesetzes vom 19. Juni 19922 über den Datenschutz (DSG), welche die Zugriffsberechtigungen und ihre wesentlichen Rahmenbedingungen festlegt (Art. 3);
b. die Zweckbindung (Art. 4);
c. die Sicherheit der Online-Verbindung (Art. 5);
d. ein Gesuch der zuständigen kantonalen Behörde, wenn die Einrichtung einer Online-Verbindung einen kantonalen Dienst betrifft (Art. 16).

2. Abschnitt: Grundsätze für die Einrichtung einer Online-Verbindung
Art. 3 Rechtsgrundlage
Eine Online-Verbindung bedarf einer ausdrücklichen Rechtsgrundlage. Sind besonders schützenswerte Personendaten oder Persönlichkeitsprofile betroffen, bedarf es eines formellen Gesetzes.

Art. 4 Zweckbindung
[1] Eine Online-Verbindung darf nur zu den in der Rechtsgrundlage definierten Zwecken eingerichtet werden.
[2] Umschreibt die Rechtsgrundlage den Zweck nur in allgemeiner Weise, muss das Gesuch um Einrichtung einer Online-Verbindung den Zweck präziser umschreiben.

Art. 5 Sicherheit
[1] Eine Online-Verbindung darf erst dann installiert werden, wenn die korrekte Bearbeitung der Daten und die Datensicherheit gewährleistet werden können, d. h. wenn die technischen und organisatorischen Massnahmen nach Abschnitt 3 erfüllt sind.

[2] Der Zugang zu allen Informationen und Fachanwendungen des EJPD wird von einer zentralen Sicherheitsinfrastruktur (SSO Portal EJPD3) gesteuert. Das SSO Portal EJPD gewährleistet eine standardisierte Benutzerverwaltung und eine starke Benutzerauthentisierung.

3. Abschnitt: Technische und organisatorische Massnahmen
Art. 6 Risikobeurteilung
Vor der Inbetriebnahme einer Informatikanwendung mit einer Online-Verbindung nimmt das für die Anwendung verantwortliche Bundesamt eine Risikobeurteilung nach den entsprechenden Weisungen des Informatikrates Bund (IRB) sowie des Informatikstrategieorgans des Bundes (ISB) vor und setzt die daraus abgeleiteten Massnahmen um.

Art. 7 Sicherheitskonzept der Informatikanwendung
[1] Das für die Informatikanwendung verantwortliche Bundesamt erstellt auf der Grundlage der Schutzbedarfsanalyse (SchubAn) und der Risikobeurteilung ein Konzept über den Informations- und Datenschutz (ISDS), welches hinreichende technische und organisatorische Schutz- und Sicherheitsmassnahmen nach Artikel 20 der Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG4) beschreibt.
[2] Das Sicherheitskonzept der Informatikanwendung legt namentlich fest:
a. die Anwendungsverantwortlichen;
b. die Datenschutzverantwortlichen;
c. die Informatiksicherheitsverantwortlichen;
d. das Aufsichtsorgan;
e. die Protokollierungsregeln;
f. das Verfahren der Benutzeridentifikation und -authentisierung;
g. die Datenchiffrierung;
h. das Zugriffserteilungsverfahren;
i. die Regeln und das Verfahren für die Unterbrechung inaktiver Verbindungen und für die Sperrung nicht beanspruchter Zugriffsrechte;
k. das Verfahren der Kontrolle nach Artikel 9 Absatz 1 VDSG.
[3] Das Informations- und Datenschutzkonzept (ISDS) der Informatikanwendung ist periodisch durch das hierfür verantwortliche Bundesamt zu aktualisieren.
[4] Der Schlussbericht des Informatiksicherheitsbeauftragten des Departements (ISBD) und des Informatikstrategieorgans Bund (ISB) kann das Sicherheitskonzept der Informatikanwendung ersetzen, wenn die in Absatz 2 genannten Punkte im Bearbeitungsreglement aufgeführt werden.

Art. 8 Bearbeitungsreglement
Die für die Informatikanwendungen verantwortlichen Bundesämter erlassen nach Artikel 21 VDSG ein Bearbeitungsreglement ihrer Informatikanwendungen.

4. Abschnitt: Grundsätze für die Erteilung von individuellen Zugriffsbewilligungen
Art. 9 Eignung
Der Online-Zugriff muss geeignet sein, den konkreten Benutzungszweck zu erreichen.

Art. 10 Notwendigkeit
[1] Ein Online-Zugriff muss zur Erfüllung der gesetzlich übertragenen Aufgaben erforderlich sein.
[2] Die Notwendigkeit ist anzunehmen, wenn die Aufgabe ohne den Online-Zugriff nicht ohne unverhältnismässigen Mehraufwand erfüllt werden kann.

Art. 11 Verhältnismässigkeit
[1] Der Online-Zugriff muss verhältnismässig sein.
[2] Er ist verhältnismässig, wenn der Eingriff in die Persönlichkeit der betroffenen Personen in einem angemessenen Verhältnis zum zu erwartenden Nutzen der Datenbearbeitung steht.
[3] Die Zugriffberechtigung ist auf die Daten und Bearbeitungsfunktionen zu beschränken, welche für die Aufgabenerfüllung des Benutzenden notwendig sind.

Art. 12 Beurteilungskriterien
Bei der Beurteilung der Grundsätze nach den Artikeln 9–11 sind namentlich folgende Kriterien massgeblich:
a. voraussichtliche Nutzungsfrequenz des einzelnen Zugriffs;
b. bisherige Nutzungsfrequenz des betreffenden Organs;

c. Anzahl der bereits zugriffsberechtigten Mitarbeitenden des betreffenden Organs;
d. gesamter Zugriffsumfang des betreffenden Organs;
e. Notwendigkeit des unabhängigen und raschen Handelns (z.B. ausserhalb der ordentlichen Geschäftszeiten);
f. beantragte Zugriffsprivilegien (Suchkriterien, Umfang der einsehbaren Daten);
g. beantragte Funktionen (Abfragen, Schreiben, Mutieren, Löschen).

5. Abschnitt: Organisation
Art. 13 Zentrale Authentisierungsstelle
[1] Die zentrale Authentisierungsstelle (Authentisierungsstelle EJPD) ist zuständig für die Authentisierung von Benutzenden, die einen Online-Zugriff auf Informatikanwendungen des EJPD beantragen. Sie führt das SSO Portal EJPD.
[2] Sie nimmt die Gesuche um Zugriffserteilung entgegen, authentisiert die Benutzenden und leitet die Begehren an das für die Informatikanwendung verantwortliche Bundesamt weiter.
[3] Sie koordiniert das Verfahren für die Erteilung von individuellen Zugriffsbewilligungen.

Art. 14 Zuständigkeiten des für die Informatikanwendung verantwortlichen Amtes
[1] Die Datenschutzberaterin oder der Datenschutzberater des für die Informatikanwendung verantwortlichen Bundesamtes (DSBO) überwacht die Planung und die Errichtung von Online-Verbindungen und sorgt für die Einhaltung der Regeln zur Erteilung der individuellen Zugriffsbewilligungen.
[2] Sie oder er prüft das erste individuelle Gesuch um Zugriffsbewilligung aus jedem Organ des Bundes oder der Kantone und kontrolliert, ob die Voraussetzungen nach dem 4. Abschnitt erfüllt sind. Sie oder er überwacht stichprobenweise nach den Ziffern 9–12 die Erteilung der nächsten individuellen Zugriffsbewilligungen.
[3] Sie oder er prüft die Richtigkeit und Vollständigkeit des Bearbeitungsreglements.
[4] Die oder der Informatiksicherheitsbeauftragte der Verwaltungseinheit (ISBO) ist zuständig für die Prüfung der Informatiksicherheitsaspekte. Sie oder er prüft namentlich die Konformität der Sicherheitsmassnahmen zu den Voraussetzungen der Artikel 6 und 7.

Art. 15 Leistungserbringer der Informatikanwendung
Der Leistungserbringer jeder Informatikanwendung ist zuständig für die technische Umsetzung der Online-Verbindungen, wenn die individuellen Zugriffsbewilligungen erteilt sind.

6. Abschnitt: Verfahren für die Einrichtung einer Online-Verbindung
Art. 16 Gesuch der zuständigen kantonalen Behörde
Die zuständige kantonale Behörde richtet das Gesuch um die Einrichtung einer Online-Verbindung an das für die Informatikanwendung verantwortliche Bundesamt. Das Gesuch enthält:
a. den Namen der Organe, für welche sie die Einrichtung einer Online-Verbindung beantragt;
b. den Namen der Informatikanwendung, für welche diese Organe eine Online-Verbindung brauchen;
c. den Zweck, für welchen die Verbindung eingerichtet werden soll, sofern die Rechtsgrundlage den Zweck nur in allgemeiner Weise umschreibt.

Art. 17 Prüfung des Gesuchs zur Einrichtung einer Online-Verbindung
[1] Die oder der DSBO prüft das Gesuch, namentlich:
a. das Bestehen einer hinreichenden Rechtsgrundlage;
b. die Zweckbindung;
c. die Gesuche für Gruppenzugriffsbewilligungen.
[2] Sie oder er stellt das Bearbeitungsreglement der Informatikanwendung der gesuchstellenden kantonalen Behörde zu, wenn das Gesuch angenommen wird.

7. Abschnitt: Verfahren für die Bewilligung von individuellen Online-Zugiffen
Art. 18 Anschlussgesuch
[1] Das Gesuch um die Erteilung einer individuellen Zugriffsbewilligung ist mit einem Formular des EJPD einzureichen, das über das Internet oder Intranet abgerufen werden kann.
[2] Das Gesuch ist elektronisch an die Authentisierungsstelle EJPD zu senden.

Art. 19 Prüfung der individuellen Bewilligungsgesuche zum Online-Zugriff
[1] Das für die Informatikanwendung verantwortliche Bundesamt prüft die individuellen Bewilligungsgesuche zum Online-Zugriff nach den Grundsätzen des 4. Abschnitts.

[2] Beim ersten individuellen Gesuch eines Organs des Bundes oder der Kantone prüft die oder der DSBO sämtliche Bewilligungsvoraussetzungen. Bei der Prüfung von weiteren, individuellen Zugriffsbewilligungen für die Benutzenden desselben Organs werden die Bewilligungsvoraussetzungen stichprobenweise kontrolliert.
[3] Das für die Informatikanwendung verantwortliche Bundesamt bezeichnet die Personen, welche die weiteren Gesuche bearbeiten. Es kann kantonale Organe mit der Prüfung der weiteren Begehren beauftragen.

Art. 20 Gruppenzugriffsbewilligungen (nicht mehr anwendbar)
[1] Eine Gruppenzugriffsbewilligung erlaubt allen Benutzenden einer bestimmten Benutzergruppe die Verwendung der gleichen Identifikationsparameter (Gruppen-Logins) bei der Anmeldung beim SSO Portal EJPD und bei den Informatikanwendungen des EJPD.
[2] Eine Gruppenzugriffsbewilligung kann einer bestimmten Benutzergruppe erteilt werden, wenn die Voraussetzungen nach dem 4. Abschnitt erfüllt sind. Zusätzlich müssen folgende Bedingungen erfüllt sein:

a. die Arbeitsstation wird laufend benutzt;
b. die Verbindung mit einer Anwendung muss sehr schnell erstellt werden, weil der Zugriff dringend ist;
c. die Arbeitsstation kann durch sämtliche Mitglieder der im Zugriffsbegehren erwähnten Benutzergruppe benutzt werden;
d. die Inhaberinnen und Inhaber von Gruppenbewilligungen können im betreffenden Informationssystem Daten nur abfragen;
e. die Schichtpläne der Benutzergruppe werden während eines Jahres aufbewahrt;
f. die Liste der Mitglieder der Benutzergruppe wird dem oder der Anwendungsverantwortlichen weitergegeben; und
g. die Mutationen in der Benutzergruppe werden zweimal jährlich dem oder der Anwendungsverantwortlichen gemeldet.

Art. 21 Aufsicht
Die oder der DSBO überprüft periodisch, ob die gewährten Zugriffe den Anforderungen nach dem 4. Abschnitt entsprechen.

8. Abschnitt: Schlussbestimmungen
Art. 22 Ausführungsbestimmungen
Diese Weisung ist als Anhang integraler Bestandteil der Bearbeitungsreglemente aller Informatikanwendung des EJPD mit Online-Verbindungen.

Art. 23 Übergangsbestimmungen
[1] Die beim Inkrafttreten der vorliegenden Weisung bestehenden individuellen Zugriffsberechtigungen bleiben bis zur Einführung der starken Authentisierung der Benutzenden bestehen. Zu diesem Zeitpunkt werden die individuellen Zugriffsbewilligungen gemäss Artikel 19 überprüft.
[2] Wenn eine bestehende Informatikanwendung durch eine neue ersetzt wird, so bleiben die Bewilligungen zur Einrichtung einer Online-Verbindung (Art. 17) gültig.
[3] Bis zur Einführung der digitalen Signatur im EJPD ist zwingend ein unterschriebener Abdruck des Anschlussbegehrens (Art. 18 Abs. 1) per Post oder per Fax an die Authentisierungsstelle EJPD zu schicken.
[4] Das EJPD stellt die Bearbeitungsreglemente der Informatikanwendungen, die am 31. August 2004 online zugänglich sind, den für die angeschlossenen Organen der Kantone zuständige kantonale Behörde bis zum 31. Dezember 2004 zu.

Art. 24 Inkrafttreten
Diese Weisung tritt am 1. Oktober 2004 in Kraft.

30. September 2004 Eidgenössisches Justiz- und Polizeidepartement:

Christoph Blocher

ANHANG 3: WEISUNG DES IRB ÜBER DIE INFORMATIKSICHERHEIT IN DER BUNDESVERWALTUNG

Weisungen des IRB über die Informatiksicherheit in der Bundesverwaltung vom 27. September 2004 (Stand 1. November 2007)

Der Informatikrat des Bundes (IRB),

gestützt auf Artikel 13 Absätze 4 und 5 der Bundesinformatikverordnung vom 26. September 20031 (BinfV),

erlässt folgende Weisungen:

1. Allgemeine Bestimmungen

1.1 Gegenstand und Zweck

[1] Diese Weisungen regeln für den Bereich der Informatiksicherheit in der Bundesverwaltung:

a. die Organisation;
b. das Sicherheitsverfahren;
c. die Netzwerksicherheit.

[2] Sie bestimmen die technischen, baulichen, organisatorischen und personellen Anforderungen und Massnahmen, um zu gewährleisten:

a. den Schutz der Integrität und Verfügbarkeit der Informations- und Kommunikationstechnik (Hardware und Software);
b. den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Daten;
c. die Nachvollziehbarkeit der Bearbeitung von Daten.

[3] Die Departemente, die Bundeskanzlei und die Verwaltungseinheiten können weiter gehende Sicherheitsanforderungen und -massnahmen festlegen.

1.2 Geltungsbereich

Der Geltungsbereich dieser Weisungen richtet sich nach Artikel 2 BinfV.

2. Zuständigkeiten

2.1 Informatiksicherheitsbeauftragte

[1] Die Departemente und die Bundeskanzlei bestimmen eine Informatiksicherheitsbeauftragte oder einen Informatiksicherheitsbeauftragten. Diese koordinieren alle Informatiksicherheitsaspekte innerhalb des Departements sowie mit den überdepartementalen Stellen.

[2] Die Organisationseinheiten bestimmen eine Informatiksicherheitsbeauftragte oder einen Informatiksicherheitsbeauftragten. Diese koordinieren alle Informatiksicherheitsaspekte innerhalb der Organisationseinheit sowie mit den departementalen Stellen.

2.2 Leistungsbezüger

[1] Die Anwendungsverantwortlichen, Geschäftsprozessverantwortlichen und Inhaber der Datensammlungen bei den Leistungsbezügern legen, in Zusammenarbeit mit den Informatiksicherheitsbeauftragten, die Sicherheitsanforderungen für Projekte, Anwendungen und Datensammlungen fest und organisieren unter Einbezug der Auftraggeber und der Vertragspartner periodisch die Kontrollen der Umsetzung der Sicherheitsmassnahmen.

[2] Die Organisationseinheiten sind dafür verantwortlich, dass ihre Mitarbeitenden die zuständigen Stellen/Organe und die Abläufe der Informatiksicherheit in der Bundesverwaltung stufengerecht kennen.

[3] Die Mitarbeitenden der Bundesverwaltung, die IKT-Mittel nutzen, sind für deren sichere Handhabung verantwortlich. Sie sind regelmässig in den Themen der IKT-Sicherheit zu schulen und zu sensibilisieren.

2.3 Leistungserbringer
[1] Die beim Leistungsbezüger festgehaltenen Vorgaben gelten beim Leistungserbringer sinngemäss für dessen Projekte, Anwendungen und Datensammlungen.
[2] Die Verantwortlichen stellen sicher, dass die Sicherheitsmassnahmen beim Betrieb von IKT-Mitteln auf allen Systemen umgesetzt werden.

2.4 Operative Ebene
Die Verantwortlichkeiten auf der operativen Ebene werden in den Projektvereinbarungen und in den Service Level Agreements zwischen den Leistungsbezügern und den Leistungserbringern detailliert festgehalten.

2.5 Rollenbeschreibungen
Die Rollenbeschreibungen stützen sich auf die IT-Prozesse der Bundesverwaltung.

3. Sicherheitsverfahren

3.1 Anwendung des Sicherheitsverfahrens
Das Sicherheitsverfahren betrifft den gesamten Lebenszyklus eines Informatiksystems von seiner Planung bis zur Ausserbetriebsetzung.

3.2 Internationale Standards
Die konkreten Sicherheitsmassnahmen orientieren sich an den jeweils aktuellen internationalen Standards wie ISO/IEC 17799/27001 oder den IT-Grundschutz-Katalogen des BSI (Bundesamt für Sicherheit in der Informationstechnik).

3.3 Schutzbedarfsanalyse / Risikobetrachtung
[1] Bei jedem Informatikvorhaben ist eine Schutzbedarfsanalyse zwingend durchzuführen. Der Zeitpunkt richtet sich nach dem Projektvorgehensmodell HERMES.
[2] Neue Informations- und Kommunikationstechnologien (Hard- und Software) sind vor deren Einsatz in der Bundesverwaltung einer Risikobetrachtung zu unterziehen. Diese ist durch den Bedürfnisträger vorzunehmen. Das Ergebnis der Risikobetrachtung ist der oder dem zuständigen Informatiksicherheitsbeauftragten vorzulegen.

3.4 Genereller Schutzbedarf
Ergibt die Schutzbedarfsanalyse einen generellen Schutzbedarf, so sind die minimalen Sicherheitsanforderungen nach Anhang 1 dieser Weisungen einzuhalten.

3.5 Erhöhter Schutzbedarf
[1] Ergibt die Schutzbedarfsanalyse einen erhöhten Schutzbedarf, so ist zusätzlich ein Informations- und Datenschutzkonzept (ISDS) zu erstellen, sofern auf departementaler Ebene keine generellen Sicherheitsvorgaben für den erhöhten Schutzbedarf bestehen.
[2] Die Informations- und Datenschutzkonzepte (ISDS) für Anwendungen erstellt der oder die Verantwortliche beim Leistungsbezüger, die Informations- und Datenschutzkonzepte (ISDS) für Produkte und Systemplattformen der oder die Verantwortliche beim Leistungserbringer.
[3] Bei der Erstellung der Informations- und Datenschutzkonzepte (ISDS) darf auf bereits bestehende themenspezifische Informations- und Datenschutzkonzepte (ISDS) verwiesen werden.
[4] Die Informations- und Datenschutzkonzepte (ISDS) sind in Zusammenarbeit mit dem oder der Informatiksicherheitsbeauftragten ISBO oder der Datenschutzberaterin DSBO zu erstellen.

3.6 Restrisiko
[1] Ein allfälliges Restrisiko ist in jedem Fall auszuweisen und den Entscheidungsträgern mitzuteilen.
[2] Es muss durch die verantwortlichen Linienstellen getragen werden.

3.7 Schriftliche Dokumentation
[1] Alle Sicherheitsmassnahmen und ihre Umsetzung sind schriftlich zu dokumentieren.
[2] Für alle Anwendungen/Projekte und Systemplattformen/Produkte wird ein Portfolio mit sicherheitsrelevanten Informationen geführt. Der oder die Informatiksicherheitsbeauftragte ISBO hat Einsicht in das Portfolio oder führt es selber.

3.8 Kontrolle
[1] Die Verantwortlichen der Departemente und Organisationseinheiten überprüfen in Zusammenarbeit mit den Informatiksicherheitsbeauftragten ISBO und der Datenschutzberaterin DSBO periodisch, ob die Informations- und Datenschutzmassnahmen angemessen sind und ob sie umgesetzt werden.
[2] Ändern sich Aufgaben, Organisation, Prozesse, Daten oder die eingesetzten IKT-Mittel, so überprüfen sie den festgelegten Schutzbedarf sowie die Angemessenheit der bisher getroffenen Sicherheitsmassnahmen.

3.9 Kosten
Die Kosten für die IKT-Sicherheit sind Teil der Projekt- und Betriebskosten. Sie werden entsprechend eingeplant.

4. Netzwerksicherheit

4.1 Sicherheitsvorgaben
[1] Für die Netzwerksicherheit gelten die Definitionen und Sicherheitsvorgaben nach Anhang 2 dieser Weisungen.
[2] Für die blaue Domäne gelten zusätzlich die Vorgaben nach Anhang 3 dieser Weisungen.

4.2 Weitere Bundesdomänen
[1] Inhaberinnen oder Inhaber weiterer Bundesdomänen müssen für diese eine entsprechende Policy ausarbeiten.
[2] Policies von Bundesdomänen sowie bilaterale Vereinbarungen zwischen Bundesdomänen und Fremddomänen bedürfen der Genehmigung durch den Ausschuss Informatiksicherheit (A-IS).
[3] Bilaterale Vereinbarungen zwischen Bundesdomänen oder zwischen Bundesdomänen und Fremddomänen bedürfen ebenfalls der Genehmigung durch den A-IS.
[4] Wer direkt an eine Bundesdomäne angeschlossen ist, aber nicht diesen Weisungen untersteht, ist durch die zuständige Organisationseinheit der Bundesverwaltung mittels einer Vereinbarung (z.B. Vertrag, Service Level Agreement) zur Einhaltung der Sicherheitsvorgaben dieser Weisungen zu verpflichten.

5. Schlussbestimmungen

5.1 Aufhebung bisheriger Regelungen
Folgende Weisungen und Regelungen werden aufgehoben:
a. Weisung Informatiksicherheit Nr. S01 (WS S01) des BFI vom 18. August 1993
b. Weisung Informatiksicherheit Nr. S02 (WS S02) des BFI vom 2. Oktober 1998
c. Weisung Informatiksicherheit Nr. S03 (WS S03) des BFI vom 25. Juni 1997
d. Network Security Policy (NSP) des BFI vom 25. Juni 1997

5.2 Übergangsbestimmungen
Für die Umsetzung der Anforderungen gemäss Ziffer 5.7, 6.3 und 6.4 des Anhangs 1 zu diesen Weisungen gilt eine Übergangsfrist bis Ende 2009.

5.3 Inkrafttreten
Diese Weisungen treten am 1. November 2004 in Kraft.
Bern, 27. September 2004

Für den Informatikrat Bund:
Der Vorsitzende: Peter Grütter

ANHANG 4: RICHTLINIE FÜR DIE VERWENDUNG UND BEARBEITUNG VON DATEN DES INFORMATIONSSYSTEM HOOGAN DURCH ORGANISATOREN VON SPORTVERANSTALTUNGEN

Richtlinie für die Verwendung und Bearbeitung von Daten des Informationssystems HOOGAN durch Organisatoren von Sportveranstaltungen

(Richtlinie vom 1. Mai 2013, ersetzt Version vom 1. Januar 2010)

Das Bundesamt für Polizei fedpol,

gestützt auf Art. 24a Abs. 8 des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (BWIS; SR 120);
gestützt auf Art. 10 der Verordnung über verwaltungspolizeiliche Massnahmen des Bundesamtes für Polizei und über das Informationssystem HOOGAN vom 4. Dezember 2009 (VVMH; SR 120.52);
gestützt auf Art. 22 des Bearbeitungsreglements HOOGAN vom 1. März 2013

erlässt folgende Richtlinie:

Abschnitt 1: Allgemeine Bestimmungen

[Die in dieser Richtlinie verwendeten Personenbezeichnungen beziehen sich auf beide Geschlechter.]

Art. 1 Inhalt
Die Richtlinie regelt die Verwendung, die Weitergabe, die Bearbeitung, den Rückfluss und die Vernichtung der Daten aus dem Informationssystem HOOGAN durch Organisatoren von Sportveranstaltungen und deren Sicherheitsverantwortliche. Ausserdem werden die Datenempfänger näher bestimmt und ihre Pflichten ausgeführt. Des Weiteren werden die Zwecke, für welche die Daten den Organisatoren von Sportveranstaltungen bekannt gegeben werden, definiert. Schliesslich beschreibt sie den Ablauf der Datenweitergabe und das Kontrollverfahren zur Einhaltung dieser Richtlinie. Sie ist Teil des Anhangs des Bearbeitungsreglements HOOGAN.

Art. 2 Grundsätze
1 Die Richtlinie regelt den Umgang mit Daten, welche in HOOGAN erfasst sind.
2 Gegenstand der Richtlinie sind nationale und internationale Sportveranstaltungen in der Schweiz.
3 Die Richtlinie gilt sinngemäss für Übertragungen von Sportveranstaltungen mittels Grossbildleinwänden (Public-Viewing).
4 Nicht Gegenstand der Richtlinie sind Daten von Sportveranstaltern (Stadionverbotslisten) oder der Kantone, namentlich Präventivdaten. Für diese trägt der Bund keine Verantwortung.

Abschnitt 2: Beteiligte Behörden und Stellen

Art. 3 Organisatoren von Sportveranstaltungen[1]
1 Die Sportverbände melden der Sektion Hooliganismus (SH) des Bundesamtes für Polizei (fedpol) den Sicherheitsverantwortlichen für die jeweiligen Sportveranstaltungen. Dieser ist Ansprechpartner für Bund und Kantone.
2 Der Sicherheitsverantwortliche beantragt jeweils bei der zuständigen Polizeibehörde des Kantons (nachfolgend: Fachstelle) oder bei fedpol, dass ihm Personendaten aus HOOGAN zur Verfügung gestellt werden. Bei Spielen von Nationalmannschaften wendet sich der zuständige Sicherheitsverantwortliche direkt an die SH.

[1] Art. 24*a* Abs. 8 BWIS.

3 Der Sicherheitsverantwortliche sorgt innerhalb des Veranstaltungsorts für die vorschriftsgemässe Verwendung der Personendaten und instruiert das Sicherheitspersonal entsprechend.

Art. 4 Dezentrale Fachstellen der Kantone
1 Die Fachstellen leiten auf Anfrage die Personendaten mit aktiven Massnahmen an den Sicherheitsverantwortlichen weiter.
2 Die Fachstellen kontrollieren die vorschriftsgemässe Verwendung und Weitergabe sowie die Vernichtung der Daten.
3 Die Fachstellen füllen jeweils nach Beendigung einer Sportveranstaltung ein Kontrollblatt aus, welches sie der SH zukommen lassen.

Art. 5 Sektion Hooliganismus
1 Die SH als Betreiberin von HOOGAN kann die Aufgabe der Datenweitergabe an Organisatoren von Sportveranstaltungen in der Schweiz an die Fachstellen übertragen.
2 Bei Spielen von Nationalmannschaften gibt die SH selber die Daten an den Sicherheitsverantwortlichen des zuständigen Verbandes weiter. Die SH informiert die zuständige Fachstelle des Veranstaltungsortes über die Weitergabe.
3 Die SH sorgt unter Beizug der Kontrollblätter für die Einhaltung der gesetzlichen Grundlagen, des Bearbeitungsreglements und der vorliegenden Richtlinie und kontrolliert stichprobenweise deren Einhaltung. Er kontrolliert bei Spielen von Nationalmannschaften die vorschriftsgemässe Verwendung, die Weitergabe, die Bearbeitung, den Rückfluss und die Vernichtung der Daten.

Abschnitt 3: Benutzer und ART der Weitergabe

Art. 6 Benutzer
Die Organisatoren von Sportveranstaltungen erhalten jeweils nur diejenigen Personendaten, die sie zur Erfüllung ihrer Sicherheitsaufgaben tatsächlich benötigen. Die zuständige Fachstelle oder die SH übergibt die benötigten Personendaten in Form von ausgedruckten Listen mit einer im Kontrollblatt genau bezifferten Anzahl von Kopien den antragsstellenden Sicherheitsverantwortlichen gegen eine handschriftliche Empfangsbestätigung auf dem Kontrollblatt. Die Fachstellen können sich durch örtliche Polizeistellen vertreten lassen. Bei Spielen von Nationalmannschaften werden die Daten durch die SH weitergegeben.

Art. 7 Personendaten
Bei Personendaten handelt es sich um operative[2], importierte[3] und anlassbezogene Daten. Es werden jeweils folgende Personendaten bekannt gegeben: Foto, Name, Vorname, Geburtsdatum, Wohnadresse und die verhängte Massnahmen.

Abschnitt 4: Weiterverwendung und Kontrolle der Daten

Art. 8 Weiterverwendung und Kontrolle der Daten
1 Der Sicherheitsverantwortliche verteilt frühestens drei Stunden vor Stadionöffnung jeweils eine Liste der Personendaten unter den zuständigen Personen des Sicherheitspersonals. Innerhalb einer Stunde nach Beendigung der Sportveranstaltung sind sämtliche verteilten Listen an den Sicherheitsverantwortlichen zu retournieren. Er sammelt die Listen ein und vernichtet diese im Beisein der zuständigen Polizeibehörde umgehend.

2 Den Sicherheitsverantwortlichen und dem Sicherheitspersonal ist es untersagt, die verteilten Listen zu kopieren, in einer anderen Form zu vervielfältigen oder zu speichern. Die Listen dürfen zu keinem Zeitpunkt an Dritte weitergegeben, übermittelt oder sichtbar gemacht werden.

[2] Die Massnahmen sind aktiv, d.h. sie sind zum Zeitpunkt der Datenweitergabe in Kraft.

[3] Ausländische Personendaten, welche anlassbezogen für die jeweilige Sportveranstaltung in HOOGAN importiert werden.

Abschnitt 5: Löschung und periodische Überprüfung

Art. 9 Löschung der Daten und Mitteilung an die SH
1 Die zuständigen Polizeivertreter beaufsichtigen vor Ort die Vernichtung der Personendaten. Die Meldung der Vernichtung muss gemäss Art. 10 Abs. 3 VVMH spätestens 24 Stunden nach Übergabe der Personendaten durch die Behörden erfolgen. Diese protokollieren die Verteilung und Rückgabe der Listen auf dem Kontrollblatt und erfassen eine Kopie des Kontrollblatts in HOOGAN unter der betreffenden Sportveranstaltung.
2 Stellt die Fachstelle Unregelmässigkeiten fest, mahnt sie den Sicherheitsverantwortlichen und informiert die SH. Diese entscheidet über das weitere Vorgehen.

Art. 10 Periodische Kontrolle der Sportveranstalter durch die SH
1 Die SH überprüft die gesetzeskonforme Verwendung der Daten bei den Sportveranstaltern und deren Sicherheitsverantwortlichen stichprobenweise.
2 Stellt die SH Unregelmässigkeiten fest, beantragt er Sanktionen gegen die fehlbaren Personen nach Absprache mit der zuständigen Fachstelle beim Sicherheitsbeauftragten des Verbandes.

Abschnitt 6: Abschliessende Bestimmung

Art. 11 Inkrafttreten
Die vorliegende Richtlinie ersetzt diejenige vom 1. Januar 2010 und tritt am 1. Mai 2013 in Kraft.
Bern, 30. April 2013

BUNDESAMT FÜR POLIZEI fedpol
des Eidgenössischen Justiz- und Polizeidepartements

Direktor fedpol

Jean-Luc Vez

ANHANG 5: RICHTLINIE FÜR DIE ELEKTRONISCHE ÜBERMITTLUNG VON DATEN DES INFORMATIONSSYSTEMS HOOGAN AN ORGANISATOREN VON SPORTVERANSTALTUNGEN ZUR DURCHFÜHRUNG VON ZUTRITTSKONTROLLEN MIT ABGLEICH VON AUSWEISEN (*HOOGAN+*)

Richtlinie für die elektronische Übermittlung von Daten des Informationssystems HOOGAN an Organisatoren von Sportveranstaltungen zur Durchführung von Zutrittskontrollen mit Abgleich von Ausweisen (*HOOGAN+*)

(Richtlinie, 1. Version vom 30.04.2013)

Das Bundesamt für Polizei fedpol,

gestützt auf Art. 24*a* Abs. 8 des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (BWIS; SR 120);
gestützt auf Art. 10 der Verordnung über verwaltungspolizeiliche Massnahmen des Bundesamtes für Polizei und über das Informationssystem HOOGAN vom 4. Dezember 2009 (VVMH, SR 120.52);
gestützt auf Art. 22 des Bearbeitungsreglements HOOGAN vom März 2013

erlässt folgende Richtlinie:

Abschnitt 1: Allgemeine Bestimmungen

[Die in dieser Richtlinie verwendeten Personenbezeichnungen beziehen sich auf beide Geschlechter.]

Art. 1 Inhalt

1 Diese Richtlinie regelt die Verwendung, die Weitergabe, die Bearbeitung, den Rückfluss und die Vernichtung von elektronischen Personendaten aus dem Informationssystem HOOGAN durch Organisatoren von Sportveranstaltungen und deren Sicherheitsverantwortliche für nationale und internationale Sportveranstaltungen in der Schweiz.
2 Sie bestimmt die Datenempfänger näher und führt ihre Pflichten aus.
3 Sie definiert die Zwecke, für welche die Daten den Organisatoren von Sportveranstaltungen bekannt gegeben werden.
4 Sie beschreibt den Ablauf der Datenweitergabe und das Kontrollverfahren zur Einhaltung dieser Richtlinie. Sie ist Teil des Bearbeitungsreglements HOOGAN.

Abschnitt 2: Beteiligte Behörden und Stellen

Art. 2 Organisatoren von Sportveranstaltungen

1 Die Organisatoren von Sportveranstaltungen[1] melden der Sektion Hooliganismus (SH) des Bundesamtes für Polizei (fedpol) ihr Interesse an einer Zutrittskontrolle mit Ausweisen an und melden den Sicherheitsverantwortlichen für die jeweiligen Sportveranstaltungen. Der Sicherheitsverantwortliche ist Ansprechpartner und Verantwortlicher für den Empfang von Daten aus dem Informationssystem HOOGAN.
2 Der Sicherheitsverantwortliche stellt sicher, dass den Mitarbeitern der SH im Rahmen einer Begehung und einer Testphase Zugang zur Infrastruktur der Stadien, namentlich den Einlasszonen, gewährt wird.
3 Der Sicherheitsverantwortliche kann im Anschluss an eine erfolgreiche Testphase durch die SH mit elektronischen Personendaten aus HOOGAN beliefert werden.

---

1 Art. 24*a* Abs. 8 BWIS.

4 Der Sicherheitsverantwortliche sorgt innerhalb des Veranstaltungsorts für die vorschriftsgemässe Verwendung der Personendaten und instruiert das Sicherheitspersonal entsprechend.

Art. 3 Polizeiliche dezentrale Fachstellen der Kantone
1 Die Fachstellen unterstützen die lokalen Organisatoren von Sportveranstaltungen bei der Testphase der Zutrittskontrolle mit dem Abgleich eines Ausweises mit Daten aus HOOGAN.
2 Die Fachstellen können die vorschriftsgemässe Verwendung und Weitergabe sowie die Vernichtung der elektronischen Daten kontrollieren.

Art. 4 Sektion Hooliganismus
1 Die SH als Betreiberin des Informationssystems HOOGAN kann Daten aus HOOGAN an Organisatoren von Sportveranstaltungen übermitteln. Sie kann diese Aufgabe an die Fachstellen übertragen.
2 Die SH informiert die zuständige Fachstelle des Veranstaltungsortes über den Einsatz von *HOOGAN+*.
3 Die SH überprüft unter Beizug der Kontrollblätter die Einhaltung der gesetzlichen Grundlagen, des Bearbeitungsreglements und der vorliegenden Richtlinie. Sie kontrolliert insbesondere die vorschriftsgemässe Verwendung, die Weitergabe, die Bearbeitung, den Rückfluss und die Vernichtung der Daten.

Abschnitt 3: Benutzer und Weitergabe

Art. 5 Benutzer
1 Die Organisatoren von Sportveranstaltungen erhalten von fedpol die elektronischen Daten als gesicherte Datei. Die Bedingungen für die regelmässige elektronische Datenweitergabe werden in einer schriftlichen Vereinbarung zwischen fedpol und dem jeweiligen Organisator von Sportveranstaltungen festgelegt. Der Organisator muss im Rahmen der Zutrittskontrolle mit Abgleich eines Ausweises über die notwendigen Voraussetzungen, namentlich im Bereich der eingesetzten Soft- und Hardware, gemäss der jeweiligen Vereinbarung verfügen.
2 Die Weitergabe erfolgt über einen verschlüsselten FTP-Server oder durch persönliche Übergabe eines gesicherten Datenträgers. Die Organisatoren von Sportveranstaltungen bestätigen den Erhalt der Daten mit einer handschriftlichen Empfangsbestätigung auf dem Kontrollblatt.
3 Die eingesetzte Soft- und Hardware darf einzig zum Zweck der Zutrittskontrolle mit Daten aus dem Informationssystem HOOGAN eingesetzt werden. Es dürfen keine Schnittstellen zu anderen Systemen, z.B. Drehkreuzen, Ticketkontrollen, bestehen.

Art. 6 Personendaten
1 Bei den elektronischen Daten handelt es sich um operative, importierte[2] und anlassbezogene Daten von Personen mit aktiven[3] Massnahmen zum Zeitpunkt der Veranstaltung.
2 Die SH kann jeweils folgende Personendaten bekannt geben: Foto, Name, Vorname, Geschlecht, Geburtsdatum, Wohnadresse und die Art der verhängten Massnahmen.

Abschnitt 4: Bearbeitung und Kontrolle

Art. 7 Weiterverwendung und Kontrolle der Daten
1 Der Sicherheitsverantwortliche fügt die elektronischen Daten frühestens drei Stunden vor Stadionöffnung in die eingesetzten und in der Vereinbarung festgelegten Zutrittssysteme ein. Spätestens nach einer Stunde nach Beendigung der Sportveranstaltung sind die elektronischen Daten aus den Zutrittssystemen zu entfernen und die Daten auf den eingesetzten Speichermedien zu löschen. Sowohl der Zeitpunkt des Einsatzes wie auch die Löschung der Daten müssen auf dem Kontrollblatt Datenweitergabe festgehalten werden.
2 Nach der Löschung übermittelt der Sicherheitsverantwortliche das elektronische Auswertungsprotokoll sowie das Kontrollblatt der Datenweitergabe an die Sektion Hooliganismus.

---

[2] Ausländische Personendaten, welche anlassbezogen für die jeweilige Sportveranstaltung in HOOGAN importiert werden.

[3] Die Massnahmen sind aktiv, d.h. sie sind zum Zeitpunkt der Datenweitergabe in Kraft.

3 Den Sicherheitsverantwortlichen und dem Sicherheitspersonal ist es untersagt, die verteilten Daten in einer anderen Form als in der Vereinbarung festgelegt, zu vervielfältigen oder zu speichern. Die Daten dürfen zu keinem Zeitpunkt an Dritte weitergegeben, übermittelt oder sichtbar gemacht werden.
abschnitt 5: Löschung und periodische Überprüfung

Art. 8 Löschung der Daten und Mitteilung an die SH
1 Die Meldung der Vernichtung muss gemäss Art. 10 Abs. 3 VVMH innert 24 Stunden nach Übergabe der Daten mittels Kontrollblatt an die SH erfolgen. Diese protokolliert die Übermittlung und Rückgabe der Daten und erfasst eine Kopie des Kontrollblatts in HOOGAN unter der betreffenden Sportveranstaltung.
2 Stellt die SH Unregelmässigkeiten fest, mahnt sie den Sicherheitsverantwortlichen und informiert die dezentrale Fachstelle. Die SH entscheidet nach Absprache mit der dezentralen Fachstelle über das weitere Vorgehen.

Art. 9 Periodische Kontrolle der Sportveranstalter durch die SH
1 Die SH überprüft die gesetzeskonforme Verwendung der Daten bei den Sportveranstaltern und deren Sicherheitsverantwortlichen stichprobenweise.
2 Stellt die SH Unregelmässigkeiten fest, beantragt sie nach Absprache mit der zuständigen Fachstelle Sanktionen gegen die fehlbaren Personen beim Sicherheitsbeauftragten des jeweiligen Verbandes.

Abschnitt 6: Abschliessende Bestimmung

Art. 10 Inkrafttreten
Die vorliegende Richtlinie tritt am 1. Mai 2013 in Kraft.

Bern, 30. April 2013

BUNDESAMT FÜR POLIZEI fedpol
des Eidgenössischen Justiz- und Polizeidepartements

Direktor fedpol

Jean-Luc Vez

ANHANG 6: KONKORDAT ÜBER MASSNAHMEN GEGEN GEWALT ANLÄSSLICH VON SPORTVERANSTALTUNGEN VOM 15. NOVEMBER 2007; ÄNDERUNG VOM 2. FEBRUAR 2012

Die Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren verabschiedet folgenden Konkordatstext:

1. Kapitel: Allgemeine Bestimmungen

Art. 1 Zweck
Die Kantone treffen in Zusammenarbeit mit dem Bund zur Verhinderung gewalttätigen Verhaltens vorbeugende polizeiliche Massnahmen nach diesem Konkordat, um frühzeitig Gewalt anlässlich von Sportveranstaltungen zu erkennen und zu bekämpfen.

Art. 2 Definition gewalttätigen Verhaltens
[1] Gewalttätiges Verhalten und Gewalttätigkeiten liegen namentlich vor, wenn eine Person im Vorfeld einer Sportveranstaltung, während der Veranstaltung oder im Nachgang dazu folgende Straftaten begangen oder dazu angestiftet hat:
a. Strafbare Handlungen gegen Leib und Leben nach den Artikeln 111–113, 117, 122, 123, 125 Absatz 2, 126 Abs. 1, 129, 133, 134 des Strafgesetzbuches (StGB)[1];
b. Sachbeschädigungen nach Artikel 144 StGB;
c. Nötigung nach Artikel 181 StGB;
d. Brandstiftung nach Artikel 221 StGB;
e. Verursachung einer Explosion nach Artikel 223 StGB;
f. Gefährdung durch Sprengstoffe und giftige Gase in verbrecherischer Absicht nach Artikel 224 StGB
g. Öffentliche Aufforderung zu Verbrechen oder zur Gewalttätigkeit nach Art. 259 StGB;
h. Landfriedensbruch nach Artikel 260 StGB;
i. Gewalt und Drohung gegen Behörden und Beamte nach Artikel 285 StGB;
j. Hinderung einer Amtshandlung nach Artikel 286 StGB.
[2] Als gewalttätiges Verhalten gilt ferner die Gefährdung der öffentlichen Sicherheit durch das Mitführen oder Verwenden von Waffen, Sprengmitteln, Schiesspulver oder pyrotechnischen Gegenständen an Sportstätten, in deren Umgebung sowie auf dem An- und Rückreiseweg.

Art. 3 Nachweis gewalttätigen Verhaltens
[1] Als Nachweis für gewalttätiges Verhalten nach Artikel 2 gelten:
a. entsprechende Gerichtsurteile oder polizeiliche Anzeigen;
b. glaubwürdige Aussagen oder Bildaufnahmen der Polizei, der Zollverwaltung, des Sicherheitspersonals oder der Sportverbände und -vereine;
c. Stadionverbote der Sportverbände oder -vereine;
d. Meldungen einer zuständigen ausländischen Behörde.
[2] Aussagen nach Absatz 1 Buchstabe b sind schriftlich festzuhalten und zu unterzeichnen.

2. Kapitel: Bewilligungspflicht und Auflagen

Art. 3a Bewilligungspflicht
[1] Fussball- und Eishockeyspiele mit Beteiligung der Klubs der jeweils obersten Spielklasse der Männer sind bewilligungspflichtig. Spiele der Klubs unterer Ligen oder anderer Sportarten können als bewilligungspflichtig erklärt werden, wenn im Umfeld der Spiele eine Gefährdung der öffentlichen Sicherheit zu befürchten ist.
[2] Zur Verhinderung gewalttätigen Verhaltens im Sinn von Artikel 2 kann die zuständige Behörde eine Bewilligung mit Auflagen verbinden. Diese können insbesondere bauliche und technische Massnahmen, den Einsatz bestimmter personeller oder anderer Mittel durch den Veranstalter, die Regeln für den Verkauf der Eintrittskarten, den Verkauf alkoholischer Getränke oder die Abwick-

[1] SR **311.0**

lung der Zutrittskontrollen umfassen. Die Behörde kann insbesondere bestimmen, wie die Anreise und Rückreise der Anhänger der Gastmannschaft abzuwickeln ist und unter welchen Voraussetzungen ihnen Zutritt zu den Sportstätten gewährt werden darf.
[3] Die Behörde kann anordnen, dass Besucherinnen und Besucher beim Besteigen von Fantransporten oder beim Zutritt zu Sportstätten Identitätsausweise vorweisen müssen und dass mittels Abgleich mit dem Informationssystem HOOGAN sichergestellt wird, dass keine Personen eingelassen werden, die mit einem gültigen Stadionverbot oder Massnahmen nach diesem Konkordat belegt sind.
[4] Werden Auflagen verletzt, können adäquate Massnahmen getroffen werden. Unter anderem kann eine Bewilligung entzogen werden, für künftige Spiele verweigert werden, oder eine künftige Bewilligung kann mit zusätzlichen Auflagen versehen werden. Vom Bewilligungsnehmer kann Kostenersatz für Schäden verlangt werden, die auf eine Verletzung von Auflagen zurückzuführen sind.

3. Kapitel: Polizeiliche Massnahmen

Art. 3b Durchsuchungen

[1] Die Polizei kann Besucherinnen und Besucher im Rahmen von Zutrittskontrollen zu Sportveranstaltungen oder beim Besteigen von Fantransporten bei einem konkreten Verdacht durch Personen gleichen Geschlechts auch unter den Kleidern am ganzen Körper nach verbotenen Gegenständen durchsuchen. Die Durchsuchungen müssen in nicht einsehbaren Räumen erfolgen. Eigentliche Untersuchungen des Intimbereichs erfolgen unter Beizug von medizinischem Personal.
[2] Die Behörden können private Sicherheitsunternehmen, die vom Veranstalter mit den Zutrittskontrollen zu den Sportstätten und zu den Fantransporten beauftragt sind, ermächtigen, Personen unabhängig von einem konkreten Verdacht über den Kleidern durch Personen gleichen Geschlechts am ganzen Körper nach verbotenen Gegenständen abzutasten.
[3] Der Veranstalter informiert die Besucherinnen und Besucher seiner Sportveranstaltung über die Möglichkeit von Durchsuchungen.

Art. 4 Rayonverbot

[1] Einer Person, die sich anlässlich von Sportveranstaltungen nachweislich an Gewalttätigkeiten gegen Personen oder Sachen beteiligt hat, kann der Aufenthalt in einem genau umschriebenen Gebiet im Umfeld von Sportveranstaltungen (Rayon) zu bestimmten Zeiten verboten werden. Die zuständige Behörde bestimmt, für welche Rayons das Verbot gilt.
[2] Das Rayonverbot wird für eine Dauer von einem bis zu drei Jahren verfügt. Es kann Rayons in der ganzen Schweiz umfassen.
[3] Das Verbot kann von den folgenden Behörden verfügt werden:
a. von der zuständigen Behörde im Kanton, in dem die Gewalttätigkeit erfolgte;
b. von der zuständigen Behörde im Kanton, in dem die betroffene Person wohnt;
c. von der zuständigen Behörde im Kanton, in dem der Klub seinen Sitz hat, zu dem die betroffene Person in Beziehung steht.
Der Vorrang bei sich konkurrenzierenden Zuständigkeiten folgt der Reihenfolge der Aufzählung in diesem Absatz.
[4] Die Schweizerische Zentralstelle Hooliganismus (Zentralstelle) und das Bundesamt für Polizei fedpol können den Erlass von Rayonverboten beantragen.

Art. 5 Verfügung über ein Rayonverbot

[1] In der Verfügung über ein Rayonverbot sind die Geltungsdauer und der räumliche Geltungsbereich festzulegen. Der Verfügung sind Angaben beizufügen, die es der betroffenen Person erlauben, genaue Kenntnis über die vom Verbot erfassten Rayons zu erhalten.
[2] Die verfügende Behörde informiert umgehend die übrigen in Art. 4 Abs. 3 und 4 erwähnten Behörden.
[3] Für den Nachweis der Beteiligung an Gewalttätigkeiten gilt Artikel 3.

Art. 6 Meldeauflage

[1] Eine Person kann verpflichtet werden, sich für eine Dauer von bis zu drei Jahren zu bestimmten Zeiten bei einer von der zuständigen Behörde bezeichneten Amtsstelle zu melden, wenn:
a. sie sich anlässlich von Sportveranstaltungen nachweislich an Gewalttätigkeiten gegen Personen im Sinne von Artikel 2 Absatz 1 Buchstaben a und c-j beteiligt hat. Ausgenommen sind Tätlichkeiten nach Art. 126 Abs. 1 StGB;
b. sie Sachbeschädigungen im Sinne von Art. 144 Abs. 2 und 3 StGB begangen hat;

c. sie Waffen, Sprengstoff, Schiesspulver oder pyrotechnische Gegenstände in der Absicht verwendet hat, Dritte zu gefährden oder zu schädigen oder wenn sie dies in Kauf genommen hat;
d. gegen sie in den letzten zwei Jahren bereits eine Massnahme nach diesem Konkordat oder eine Ausreisebeschränkung nach Artikel 24c BWIS[2] verfügt wurde und sie erneut gegen Artikel 2 dieses Konkordats verstossen hat;
e. aufgrund konkreter und aktueller Tatsachen anzunehmen ist, dass sie sich durch andere Massnahmen nicht von Gewalttätigkeiten anlässlich von Sportveranstaltungen abhalten lässt; oder
f. die Meldeauflage im Verhältnis zu anderen Massnahmen im Einzelfall als milder erscheint.
[2] Die betroffene Person hat sich bei der in der Verfügung genannten Amtsstelle zu den bezeichneten Zeiten zu melden. Nach Möglichkeit ist dies eine Amtsstelle am Wohnort der betroffenen Person. Die verfügende Behörde berücksichtigt bei der Bestimmung von Meldeort und Meldezeiten die persönlichen Umstände der betroffenen Person.
[3] Die für den Wohnort der betroffenen Person zuständige Behörde verfügt die Meldeauflage. Die Zentralstelle und fedpol können den Erlass von Meldeauflagen beantragen.

Art. 7 Handhabung der Meldeauflage
[1] Dass eine Person sich durch andere Massnahmen als eine Meldeauflage nicht von Gewalttätigkeiten anlässlich von Sportveranstaltungen abhalten lässt (Art. 6 Abs. 1 Bst. e), ist namentlich anzunehmen, wenn:
a. aufgrund von aktuellen Aussagen oder Handlungen der betreffenden Person behördlich bekannt ist, dass sie mildere Massnahmen umgehen würde; oder
b. die betreffende Person aufgrund ihrer persönlichen Verhältnisse, wie Wohnlage oder Arbeitsplatz in unmittelbarer Umgebung eines Stadions, durch mildere Massnahmen nicht von künftigen Gewalttaten abgehalten werden kann.
[2] Kann sich die meldepflichtige Person aus wichtigen und belegbaren Gründen nicht nach Artikel 6 Absatz 2 bei der zuständigen Stelle (Meldestelle) melden, so hat sie die Meldestelle unverzüglich und unter Bekanntgabe des Aufenthaltsortes zu informieren. Die zuständige Polizeibehörde überprüft den Aufenthaltsort und die Angaben der betreffenden Person.
[3] Die Meldestelle informiert die Behörde, die die Meldeauflage verfügt hat, unverzüglich über erfolgte oder ausgebliebene Meldungen.
[4] Wird eine Meldeauflage ohne entschuldbare Gründe nach Abs. 2 verletzt, wird ihre Dauer verdoppelt.

Art. 8 Polizeigewahrsam
[1] Gegen eine Person kann der Polizeigewahrsam verfügt werden, wenn:
a. konkrete und aktuelle Hinweise dafür vorliegen, dass sie sich anlässlich einer nationalen oder internationalen Sportveranstaltung an schwerwiegenden Gewalttätigkeiten gegen Personen oder Sachen beteiligen wird; und
b. dies die einzige Möglichkeit ist, sie an solchen Gewalttätigkeiten zu hindern.
[2] Der Polizeigewahrsam ist zu beenden, wenn seine Voraussetzungen weggefallen sind, in jedem Fall nach 24 Stunden.
[3] Die betroffene Person hat sich zum bezeichneten Zeitpunkt bei der Polizeistelle ihres Wohnortes oder bei einer anderen in der Verfügung genannten Polizeistelle einzufinden und hat für die Dauer des Gewahrsams dort zu bleiben.
[4] Erscheint die betreffende Person nicht bei der bezeichneten Polizeistelle, so kann sie polizeilich zugeführt werden.
[5] Die Rechtmässigkeit des Freiheitsentzuges ist auf Antrag der betroffenen Person richterlich zu überprüfen.
[6] Der Polizeigewahrsam kann von den Behörden des Kantons verfügt werden, in dem die betroffene Person wohnt, oder von den Behörden des Kantons, in dem die Gewalttätigkeit befürchtet wird. Die Behörde des Kantons, in dem die Gewalttätigkeit befürchtet wird, hat dabei Vorrang.

Art. 9 Handhabung des Polizeigewahrsams
[1] Nationale Sportveranstaltungen nach Artikel 8 Absatz 1 Buchstabe a sind Veranstaltungen, die von den nationalen Sportverbänden oder den nationalen Ligen organisiert werden, oder an denen Vereine dieser Organisationen beteiligt sind.

---

[2] SR **120**

[2] Schwerwiegende Gewalttätigkeiten im Sinne von Artikel 8 Absatz 1 Buchstabe a sind namentlich strafbare Handlungen nach den Artikeln 111–113, 122, 123 Ziffer 2, 129, 144 Absatz 3, 221, 223 oder nach Artikel 224 StGB.
[3] Die zuständige Behörde am Wohnort der betreffenden Person bezeichnet die Polizeistelle, bei der sich die betreffende Person einzufinden hat und bestimmt den Beginn und die Dauer des Gewahrsams.
[4] Die Kantone bezeichnen die richterliche Instanz, die für die Überprüfung der Rechtmässigkeit des Polizeigewahrsams zuständig ist.
[5] In der Verfügung ist die betreffende Person auf ihr Recht, den Freiheitsentzug richterlich überprüfen zu lassen, hinzuweisen (Art. 8 Abs. 5).
[6] Die für den Vollzug des Gewahrsams bezeichnete Polizeistelle benachrichtigt die verfügende Behörde über die Durchführung des Gewahrsams. Bei Fernbleiben der betroffenen Person erfolgt die Benachrichtigung umgehend.

Art. 10 Empfehlung Stadionverbot
Die zuständige Behörde für die Massnahmen nach den Artikeln 4–9, die Zentralstelle und fedpol können den Organisatoren von Sportveranstaltungen empfehlen, gegen Personen Stadionverbote auszusprechen, welche in Zusammenhang mit einer Sportveranstaltung innerhalb oder ausserhalb des Stadions gewalttätig wurden. Die Empfehlung erfolgt unter Angabe der notwendigen Daten gemäss Art. 24a Abs. 3 BWIS.

Art. 11 Untere Altersgrenze
Massnahmen nach den Artikeln 4–7 können nur gegen Personen verfügt werden, die das 12. Altersjahr vollendet haben. Der Polizeigewahrsam nach den Artikeln 8–9 kann nur gegen Personen verfügt werden, die das 15. Altersjahr vollendet haben.

4. Kapitel: Verfahrensbestimmungen

Art. 12 Aufschiebende Wirkung
[1] Beschwerden gegen Verfügungen der Behörden, die in Anwendung von Artikel 3a ergehen, haben keine aufschiebende Wirkung. Die Beschwerdeinstanz kann die aufschiebende Wirkung auf Antrag der Beschwerdeführer gewähren.
[2] Einer Beschwerde gegen eine Verfügung über Massnahmen nach den Artikeln 4–9 kommt aufschiebende Wirkung zu, wenn dadurch der Zweck der Massnahme nicht gefährdet wird und wenn die Beschwerdeinstanz oder das Gericht diese in einem Zwischenentscheid ausdrücklich gewährt.

Art. 13 Zuständigkeit und Verfahren
[1] Die Kantone bezeichnen die zuständigen Behörden für die Bewilligungen nach Artikel 3a Abs. 1 und die Massnahmen nach den Artikeln 3a Abs. 2-4, 3b und 4–9.
[2] Die zuständige Behörde weist zum Zwecke der Vollstreckung der Massnahmen nach Kapitel 3 auf die Strafdrohung von Artikel 292 StGB hin.
[3] Die zuständigen Behörden melden dem Bundesamt für Polizei (fedpol) gestützt auf Art. 24a Abs. 4 BWIS:
a. Verfügungen und Aufhebungen von Massnahmen nach den Artikeln 4–9 und 12;
b. Verstösse gegen Massnahmen nach den Artikeln 4–9 sowie die entsprechenden Strafentscheide;
c. die von ihnen festgelegten Rayons.

5. Kapitel: Schlussbestimmungen

Art. 14 Information des Bundes
Das Generalsekretariat der Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) informiert die Bundeskanzlei über das vorliegende Konkordat. Das Verfahren richtet sich nach Artikel 27o RVOV[3].

Art. 15 Inkrafttreten
[1] Dieses Konkordat tritt in Kraft, sobald ihm mindestens zwei Kantone beigetreten sind, frühestens jedoch auf den 1. Januar 2010.
[2] Die Änderungen vom 2. Februar 2012 treten für Kantone, die ihnen zustimmen, an jenem Datum in Kraft, an dem ihr Beitrittsbeschluss rechtskräftig wird.

Art. 16 Kündigung
Ein Mitgliedkanton kann das Konkordat mittels einjähriger Vorankündigung auf Ende eines Jahres kündigen. Die anderen Kantone entscheiden, ob das Konkordat in Kraft zu lassen ist.

Art. 17 Benachrichtigung Generalsekretariat KKJPD
Die Kantone informieren das Generalsekretariat KKJPD über ihren Beitritt, die zuständigen Behörden nach Artikel 13 Absatz 1 und ihre Kündigung. Das Generalsekretariat KKJPD führt eine Liste über den Geltungsstand des Konkordats.

[3] SR **172.010.1**