Internationale Rotkreuz- und Rothalbmondbewegung
Suchdienst-Netzwerk

Datenschutz-Verhaltensregeln

Version 1.0

November 2015

Vorwort

Diese Verhaltensregeln (Code of Conduct, CoC) wurden von einer Arbeitsgruppe verfasst, die sich aus Vertretern des Österreichischen Roten Kreuzes (Claire Schocher-Döring), Belgischen Roten Kreuzes (Flanders) (Axel Vande Veegaete, Nadia Terweduwe), Britischen Roten Kreuzes (Mark Baynham und Emily Knox), Deutschen Roten Kreuzes (Jutta Hermanns), des EU-Büros des Roten Kreuzes (Olivier Jenard), des Internationalen Komitees des Roten Kreuzes (Romain Bircher, Massimo Marelli, Katja Gysin) und der Internationalen Föderation der Rotkreuz- und Rothalbmond-Gesellschaften (Christopher Rassi) (Arbeitsgruppe) zusammensetzte. Es haben auch andere Vertreter dieser Organisationen an dem Entwurf mitgewirkt, an den Diskussionen und Treffen teilgenommen und wichtige Beiträge geleistet. Die Arbeitsgruppe nahm die Gespräche zu diesem Projekt Ende 2013 auf. Es gab mehrere Treffen in Mechelen (April 2014), Brüssel (Juli 2014), Wien (September 2014), Sofia (November 2014) und London (Januar 2015) sowie zahlreiche Telefonkonferenzen und E-Mail-Wechsel. Der CoC wurde von der Arbeitsgruppe einvernehmlich angenommen, wobei Rückmeldungen von zahlreichen Nationalen Gesellschaften ebenfalls mit eingearbeitet wurden.

Der CoC wurde aufgrund der (1) vielen Akteure der Internationalen Rotkreuz- und Rothalbmondbewegung (die Bewegung), die im Suchdienst-Netzwerk tätig sind, und aufgrund der Notwendigkeit der Übertragung von Daten innerhalb der Bewegung selbst sowie an andere Akteure und (2) der sich ändernden regulatorischen Rahmenbedingungen in Bezug auf Datenschutzgesetze und -standards in Europa und auf der ganzen Welt für notwendig befunden. Der CoC legt die Mindestgrundsätze, -verpflichtungen und -verfahren fest, die die Mitglieder der Bewegung bei der Datenverarbeitung innerhalb des Suchdienst-Netzwerks einzuhalten haben. Der CoC versucht den strengsten Datenschutzvorschriften, insbesondere der diesbezüglichen Gesetzgebung der Europäischen Union, zu entsprechen. Anwender dieses CoC müssen darüber hinaus auch sicherstellen, dass sie ihre eigenen nationalen Gesetze einhalten. Der CoC stellt ein Referenzdokument dar, das Teil der wichtigsten Restoring Family Links (RFL)[1] Leitlinien der Bewegung ist. Einzelne Mitglieder der Bewegung werden ihn übernehmen und in die von ihnen entwickelten Standardverfahren umsetzen müssen.

Dieser CoC ist ein Instrument, das alle Mitglieder der Bewegung zum Schutz von Grundrechten und Grundfreiheiten einsetzen können, insbesondere zum Schutz des Rechts auf Wahrung der

[1] Unter Restoring Family Links sind insbesondere die Aufgaben der Suche und Familienzusammenführung zu verstehen.

Privatsphäre und des Rechts auf Schutz personenbezogener Daten, die von RFL-Aktivitäten betroffen sind. Der CoC wird hoffentlich das Vertrauen sowohl der Menschen als auch der Regulierungsbehörden in die Arbeit der Bewegung und in ihre Mitglieder stärken, die für die Bearbeitung von Suchanfragen untereinander Daten austauschen müssen.

Inhaltsverzeichnis

DEFINITIONEN

Internationale Rotkreuz- und Rothalbmondbewegung (die Bewegung)

Die Bewegung ist eine weltweit tätige humanitäre Bewegung, deren Auftrag „die Vermeidung und Linderung menschlichen Leids, egal wo dieses auftritt, der Schutz des Lebens und der Gesundheit, die Wahrung der Menschenwürde, besonders in Zeiten bewaffneter Konflikte und anderer Notsituationen, die Krankheitspräventionsarbeit und Förderung der Gesundheit und des sozialen Wohlergehens, die Förderung ehrenamtlicher Arbeit und ständige Bereitschaft der Mitglieder, der Gesellschaft Hilfe zu leisten, sowie eine umfassende Solidarität gegenüber allen Menschen, die Schutz und Hilfe benötigen“, ist.

Das Internationale Komitee vom Roten Kreuz (IKRK), die nationalen Rotkreuz- und Rothalbmondgesellschaften (Nationale Gesellschaften) und die Internationale Föderation der Rotkreuz- und Rothalbmondgesellschaften (IFRC) sind die Komponenten der Bewegung.

Zentraler Suchdienst (Central Tracing Agency, CTA)

Der Zentrale Suchdienst (CTA) ist eine ständige Einrichtung innerhalb des IKRK nach den Bestimmungen der vier Genfer Konventionen und deren Zusatzprotokollen, für die die Statuten der Bewegung gelten. Der Zentrale Suchdienst übernimmt – in Zusammenarbeit mit anderen Komponenten der Bewegung – die Suchdienstaufgaben in Zeiten bewaffneter Konflikte und in anderen Situationen, in denen Gewalt, Katastrophen oder sonstige Umstände vorherrschen, die ein humanitäres Einschreiten erforderlich machen. Nach dem Abkommen von Sevilla 1997, den ergänzenden Maßnahmen aus dem Jahr 2005 und der RFL-Strategie der Bewegung für die Jahre 2008–2018 kommt dem Zentralen Suchdienst innerhalb der Bewegung eine zentrale Rolle in allen RFL-bezogenen Angelegenheiten zu. Er koordiniert Einsätze und agiert als technischer Berater der Nationalen Gesellschaften.

Verantwortliche Stelle

Verantwortliche Stelle bezeichnet jede Komponente der Bewegung, die - allein oder gemeinsam mit anderen - die Zwecke und Methoden zur Verarbeitung personenbezogener Daten festlegt.

Auftragsverarbeiter

Auftragsverarbeiter bezeichnet eine Person, öffentliche Behörde, ein Amt oder andere Körperschaft, die personenbezogene Daten im Auftrag der verantwortlichen Stelle verarbeitet.

Datenschutzbeauftragter für den Suchdienst

Datenschutzbeauftragter für den Suchdienst bezeichnet die Person oder Einheit, die auf die Einhaltung des CoC hinwirkt.

Betroffene Person

Betroffene Person bezeichnet eine natürliche Person (d.h. ein Individuum), deren Identität unmittelbar oder mittelbar über personenbezogene Daten festgestellt werden kann.

Um zu bestimmen, ob die Identität einer Person feststellbar ist, müssen alle Mittel eingesetzt werden, die die verantwortliche Stelle oder eine andere Person nach vernünftigem Ermessen voraussichtlich nutzen, um die Identität der Person unmittelbar oder mittelbar festzustellen. Um zu ermitteln, ob ein Mittel nach vernünftigem Ermessen voraussichtlich eingesetzt wird, um die Identität einer Person festzustellen, müssen alle objektiven Faktoren wie Kosten und Zeitaufwand zur Feststellung der Identität berücksichtigt und alle zum Zeitpunkt der Verarbeitung verfügbaren Technologien und technischen Entwicklungen einbezogen werden. Personenbezogene Daten umfassen daher keine anonymen Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person oder auf Daten beziehen, die so anonymisiert wurden, dass die Identität der betroffenen Person nicht mehr festgestellt werden kann. Dieser CoC behandelt daher nicht die Verarbeitung solcher anonymer Informationen, beispielsweise für statistische oder Forschungszwecke.

Bei der Nutzung von Online-Diensten können Personen Online-Identifikatoren zugewiesen werden, die von ihren Geräten, Anwendungen, Hilfsmitteln und Protokollen bereitgestellt werden, wie Internet-Protokolladressen oder Cookie-Identifikatoren. Das kann Spuren hinterlassen, die, wenn sie mit eindeutigen Identifikatoren und anderen von Servern übermittelten Informationen kombiniert werden, verwendet werden können, um Profile dieser Personen zu erstellen und ihre Identität festzustellen. Nummern, Standortdaten, Online-Identifikatoren (z. B. IP-Adresse oder Cookie-Identifikatoren) oder ähnliche eindeutige Faktoren gelten nicht als personenbezogene Daten, wenn sie die Identität einer Person nicht feststellen oder feststellbar machen.

Familienmitglieder

Als Familienmitglieder gelten zumindest folgende Personen:

- ehelich und außerehelich geborene Kinder, adoptierte Kinder und Stiefkinder;
- Lebenspartner, unabhängig davon ob sie verheiratet sind oder nicht;
- Eltern, einschließlich Schwiegermütter, Schwiegerväter und Adoptiveltern;
- Vollgeschwister, Halbgeschwister und adoptierte Geschwister.

- enge Verwandte[2]

Es sollte auch die im nationalen Recht enthaltene Definition berücksichtigt werden.

Minderjährige

Jede Person unter achtzehn Jahren, außer die für ein Kind geltende Rechtsordnung legt fest, dass die Volljährigkeit früher erreicht wird.

Sonstige Personen

Suchdienstaktivitäten können sich nicht nur auf die anfragende und gesuchte Person, sondern auch auf andere Personen, wie andere Familienmitglieder, Zeugen, Nachbarn, führende Gemeindevertreter, andere gesuchte Personen etc. beziehen.

Personenbezogene Daten

Personenbezogene Daten bezeichnen alle Informationen über eine identifizierte oder identifizierbare Person. Eine identifizierbare natürliche Person ist eine Person, deren Identität unmittelbar oder mittelbar, insbesondere unter Bezugnahme auf einen Identifikator, wie einen Namen, audio-visuelles Material, eine Nummer, Aufenthaltsdaten, einen Online-Identifikator oder über eines oder mehrere Merkmale der physischen, physiologischen, genetischen, geistigen, wirtschaftlichen, kulturellen oder sozialen Identität dieser Person, festgestellt werden kann.

Personenbezogene Daten umfassen keine anonymisierten Informationen, die (i) sich nicht auf eine identifizierte oder identifizierbare natürliche Person oder auf Daten beziehen, (ii) so anonymisiert wurden, dass die Identität der betroffenen Person nicht mehr festgestellt werden kann.

Verletzung des Schutzes personenbezogener Daten

Verletzung des Schutzes von personenbezogenen Daten bezeichnet eine Sicherheitsverletzung, die dazu führt, dass ein Risiko der rechtswidrigen Vernichtung, des Verlusts, der Manipulation oder der unbefugten Offenlegung bzw. des unbefugten Zugriffs auf bzw. von übermittelte(n), gespeicherte(n) oder auf andere Weise verarbeitete(n), personenbezogene(n) Daten besteht oder tatsächlich eines der oben angeführten Ereignisse eintritt.

[2] In vielen Kulturen kann eine Familie alle Personen beinhalten, die unter demselben Dach leben oder zueinander enge Beziehungen pflegen. Daher ist das Konzept von Familien stets vor dem jeweiligen sozialen Hintergrund zu verstehen.

Verarbeitung / verarbeiten / verarbeitet

Verarbeitung / verarbeiten / verarbeitet bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen. die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Weitergabe durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung oder das Löschen. Eine Übermittlung von Daten innerhalb oder außerhalb der Bewegung stellt einen Verarbeitungsvorgang dar.

Verarbeitungsmeilensteine

Verarbeitungsmeilensteine sind wichtige Schritte in der Datenverarbeitung. Diese Meilensteine müssen von der verantwortlichen Stelle dokumentiert werden und beinhalten:

- Datum und Rechtsgrundlage der Datenerhebung;
- wenn die Rechtsgrundlage der Verarbeitung eine Einwilligung ist, alle Einschränkungen der Einwilligung, die die betroffene Person geäußert hat;
- Datum, Art und Ergebnis der Anfrage der betroffenen Person auf Ausübung ihrer Rechte;
- Datum und Empfänger sämtlicher Datenübermittlungen;
- Datum und Methoden der Veröffentlichung;
- Datenschutz-Folgenabschätzung (DSFA), sofern diese durchgeführt wurde;
- Schließen der Akte;
- Archivierung, falls erfolgt.

Empfänger

Empfänger bezeichnet eine Person, Behörde, Einrichtung oder jede andere Stelle, an die personenbezogene Daten weitergegeben werden, die jedoch nicht die betroffene Person, verantwortliche Stelle oder der Auftragsverarbeiter ist.

Suchdiensttätigkeiten und Suchdienst-bezogene Aufgaben

Suchdienst[3] ist ein Oberbegriff, der eine Bandbreite von Tätigkeiten beschreibt, die darauf abzielen, die Trennung von Familienmitgliedern zu verhindern und diese bei der Wiederherstellung und Aufrechterhaltung des Kontakts zu unterstützen, sowie Tätigkeiten, die darauf ausgerichtet sind, das Schicksal und den Aufenthalt von vermissten Personen zu klären.

[3] Im englischen Originaldokument wird der Begriff „Restoring Family Links (RFL)“ verwendet.

Diese Tätigkeiten können mit anderen Unterstützungsleistungen verbunden sein, wie der Bereitstellung psychologischer und psychosozialer, rechtlicher, administrativer und materieller Unterstützung für Familien und andere betroffene Personen, sowie mit Resettlement- und Wiedereingliederungsprogrammen und Sozialdiensten (nähere Informationen finden Sie in Anhang 1).

Suchdienst[4]

Nationale Gesellschaften und IKRK-Delegationen auf der ganzen Welt setzen aus ihren Reihen Mitarbeiter ein, die Suchdiensttätigkeiten und Suchdienst-bezogene Aufgaben ausgestalten und umsetzen.

Das Suchdienst-Netzwerk

Wenn infolge von bewaffneten Konflikten oder anderen Situationen, in denen Gewalt, Katastrophen, Migration oder andere humanitäre Krisen vorherrschen, Familien getrennt und Menschen vermisst werden, muss alles Menschenmögliche getan werden, um ihr Schicksal und ihren Aufenthaltsort zu klären, den Kontakt zwischen diesen Menschen wiederherzustellen und sie gegebenenfalls wieder zusammenzuführen.

Die Suchdienste der Nationalen Gesellschaften und des IKRK sind in einem gemeinsamen weltweiten Netzwerk zusammengefasst, das den Namen **Suchdienst-Netzwerk** trägt. Die CTA agiert als technischer Berater und Koordinator dieses Suchdiensts-Netzwerks. Die Stärke dieses humanitären Netzwerks liegt in seiner globalen Fähigkeit zur Mobilisierung von Mitarbeitern und Freiwilligen und in seiner Fähigkeit in von bewaffneten Konflikten, anderen Gewaltsituationen, Katastrophen, Migration und sonstigen humanitären Krisen betroffenen Gebieten auf einer einheitlichen Grundlage und nach einer einheitlichen Methode grenzüberschreitend zu arbeiten.

Weitere Informationen über das Suchdienst-Netzwerk finden Sie auf der Family Links-Homepage unter: http://familylinks.icrc.org.

Besonders schutzbedürftige Person

Besonders schutzbedürftige Person bezeichnet im Kontext dieses CoC jede Person mit einer verminderten Fähigkeit zur freien Äußerung einer Willensbekundung, die ohne Zwang für den konkreten Fall und in Kenntnis der Sachlage erfolgt. Diese Fähigkeit kann eingeschränkt sein aufgrund

[4] Im englischen Originaldokument wird der Begriff „RFL Services“ verwendet.

(i) der emotionalen und psychologischen Auswirkungen, die die Trennung von der Familie und die diese Person belastenden humanitären Bedingungen haben, oder (ii) der Komplexität der erforderlichen Verarbeitung, die es für diese Person schwierig macht, die damit verbundenen Risiken und/oder Chancen umfassend abzuschätzen, oder auch aufgrund einer Kombination aus beiden Umständen.

1. Einleitung

1.1 Zweck dieser Verhaltensregeln (Code of Conduct, CoC)

Dieser CoC legt die Mindestgrundlagen, -verpflichtungen und -verfahren fest, die die Suchdienstmitarbeiter des IKRK, der Nationalen Gesellschaften und der IFRK bei der Datenverarbeitung im Rahmen von Suchdiensttätigkeiten einzuhalten haben, um: (1) die geltenden Datenschutzstandards und -gesetze einzuhalten; (2) den nahtlosen Informationsfluss der für Suchdiensttätigkeiten benötigten personenbezogenen Daten zu ermöglichen und (3) die Grund- und Freiheitsrechte des/der Anfragenden, der gesuchten Person(en) und anderer Personen, wie Zeugen oder anderer Familienmitglieder in Bezug auf Suchdiensttätigkeiten gemäß dem humanitären Völkerrecht (HVR), dem internationalen Menschenrechtsschutz und anderer internationaler Standards, wie insbesondere dem Recht auf Achtung der Privatsphäre und dem Recht auf Schutz personenbezogener Daten, zu schützen.

1.2 Anwendungsbereich dieses CoC

1.2.1 Restoring Family Links (RFL)

Dieser CoC gilt für die Suchdiensttätigkeiten und Suchdienst-bezogene Aufgaben der verantwortlichen Stellen (siehe Anhang 1).

1.2.2 Personenbezogene Daten

Dieser CoC gilt für die Verarbeitung personenbezogener Daten (einschließlich Daten verstorbener Personen) von anfragenden, gesuchten und anderen Personen durch die verantwortlichen Stellen im Rahmen von Suchdiensttätigkeiten.

1.3 Das Suchdienst-Netzwerk

Die Genfer Konventionen von 1949 sowie deren Zusatzprotokolle aus dem Jahr 1977, die Statuten der Internationalen Rotkreuz- und Rothalbmondbewegung (die Statuten der Bewegung), von der Delegiertenversammlung angenommene Beschlüsse und Beschlüsse der Internationalen Konferenz der Rotkreuz- und Rothalbmondbewegung statten die verantwortlichen Stellen mit dem Mandat aus, Suchdiensttätigkeiten auszuüben.

Die Nationalen Gesellschaften erfüllen diese Tätigkeiten als Hilfsgesellschaften der jeweiligen Behörden im humanitären Bereich und nehmen weltweit eine besondere Rolle bei der Suchdienstarbeit ein. Sie sorgen, in Zusammenarbeit mit den Behörden, für unterschiedliche

Angebote, die die Opfer von bewaffneten Konflikten, Naturkatastrophen und anderen Notsituationen, die Hilfe benötigen, unterstützen.

1.4 Grundsätze und Leitlinien der Bewegung

1.4.1 Rotkreuzgrundsätze

Die verantwortlichen Stellen üben ihre Tätigkeit gemäß den Grundsätzen der Bewegung aus: Menschlichkeit, Unparteilichkeit, Neutralität, Unabhängigkeit, Freiwilligkeit, Einheit und Universalität. Alle Datenverarbeitungsschritte der verantwortlichen Stellen im Rahmen der Suchdienstaufgaben müssen unter Einhaltung dieser Grundsätze erfolgen.

1.4.2. Niemandem Schaden zufügen

Im Rahmen der Suchdienstaufgaben unternehmen die verantwortlichen Stellen alles in ihrer Macht stehende, um Menschen durch die Verarbeitung personenbezogener Daten keinen Schaden zuzufügen.

1.4.3 Vertraulichkeit bzw. Offenlegungsvorschriften

Wenn betroffene Personen den verantwortlichen Stellen vertrauliche Informationen anvertrauen, müssen die verantwortlichen Stellen die Vertraulichkeit dieser Informationen respektieren und sie dementsprechend schützen.

Die verantwortlichen Stellen halten sich, vorbehaltlich der in diesem Abschnitt 1.4 enthaltenen Einschränkungen, an alle nationalen, regionalen und internationalen rechtlichen Verpflichtungen. Bei der Entscheidung, ob diese Verpflichtungen gelten oder nicht, werden folgende Faktoren berücksichtigt: (1) alle Privilegien, Immunitäten oder Pflichtausnahmen, die für die verantwortlichen Stellen im fraglichen Land bzw. der fraglichen Region gelten; und (2) jeder Rechtsschutz, der aus dem Völkerrecht, einschließlich HVR, und dem Mandat im Rahmen der Statuten der Bewegung abgeleitet wird.

1.4.4 Bestehende operative Leitlinien

Die Verarbeitung personenbezogener Daten erfolgt gemäß den Suchdienst-Leitlinien des Suchdienst-Netzwerks, wie beispielsweise „Restoring Family links – a guide to National Red Cross and Red Crescent Societies“[5], „Assessing Restoring Family Links Needs – Handbook for National Societies and the ICRC“, „Restoring Family Links in Disasters – Field Manual“ und „Guidelines on Providing

[5] In Überarbeitung

Restoring Family Links Services to Persons Separated as a Result of Migration“[6] sowie den einschlägigen „Professional Standards for Protection Work“[7](in Englisch).

2. Grundlegende Verarbeitungsprinzipien und Pflichten der verantwortlichen Stelle

2.1 Zweckbindung

Zum Zeitpunkt der Datenerhebung wird die verantwortliche Stelle den/die konkreten, eindeutigen und rechtlichen Zweck(e) festlegen und darlegen, zu dem/denen die Daten verarbeitet werden dürfen.

Die Datenverarbeitung erfolgt in erster Linie zum humanitären Zweck der Suche und Familienzusammenführung von Menschen, die infolge eines bewaffneten Konflikts, sonstiger Situationen von Gewalttätigkeit, Katastrophen, Migration oder anderer Situationen, die ein humanitäres Einschreiten erfordern, getrennt wurden.

Daten können zu anderen als den ursprünglich zum Zeitpunkt ihrer Erhebung angegebenen Zwecken verarbeitet werden, wenn zur Erfüllung eines damit vereinbaren Zwecks, wie suchdienstbezogene Aufgaben, eine weitere Verarbeitung vonnöten ist und alle geltenden Datenschutzgesetze durchgehend eingehalten werden (nähere Informationen finden Sie in Anhang 1).

2.2 Rechtmäßige und angemessene Verarbeitung

Der Verarbeitung personenbezogener Daten durch die verantwortliche Stelle erfolgt auf Grundlage einer oder mehrerer der nachstehenden Voraussetzungen:

- Einwilligung der betroffenen Person;
- Lebenswichtiges Interesse der betroffenen Person oder anderer Personen;
- Öffentliches Interesse;
- Berechtigtes Interesse der verantwortlichen Stelle;
- Erfüllung einer rechtlichen Verpflichtung.

[6] Einschlägige Referenzdokumente finden Sie im Family Links Extranet (im Aufbau)

[7] https://www.icrc.org/eng/resources/documents/publication/p0999.htm

2.2.1 Einwilligung der betroffenen Person

Einwilligung als bevorzugte Option: Eine Einwilligung der betroffenen Person ist die bevorzugte Grundlage für die Verarbeitung personenbezogener Daten. Die Einwilligung gilt als eindeutig erteilt, wenn sie auf eine Weise erfolgt, die der betroffenen Person die Äußerung ihrer Wünsche ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage durch eine schriftliche, mündliche oder sonstige Erklärung oder durch eine eindeutige, ihre Einwilligung zum Ausdruck bringende Handlung ermöglicht, mit der sie ihre Zustimmung zur Verarbeitung ihrer personenbezogenen Daten ausdrückt. Die Einwilligung umfasst alle Verarbeitungsschritte, die zum selben Zweck erfolgen. Der betroffenen Person sollten nachstehende Dinge in einfacher Sprache erklärt werden:

- die Identität und die Kontaktdaten der verantwortlichen Stelle;
- der konkrete Zweck der Erhebung ihrer personenbezogenen Daten sowie mögliche Risiken und Vorteile;
- die Tatsache, dass die verantwortliche Stelle ihre personenbezogenen Daten zu anderen als den ursprünglich zum Zeitpunkt der Erhebung angegebenen Zwecken verwenden kann, wenn diese mit dem oben erwähnten Zweck vereinbar sind;
- die Umstände, unter denen es gegebenenfalls nicht möglich ist, ihre personenbezogenen Daten vertraulich zu behandeln;
- die Rechte und Grenzen des Rechts der betroffenen Person auf Auskunft, Berichtigung und Löschung ihrer personenbezogenen Daten und ihr Recht auf späteren Widerruf der Verarbeitungseinwilligung;
- die von der verantwortlichen Stelle bezüglich der Datenverarbeitung eingesetzten Sicherheitsmaßnahmen;
- dass es erforderlich sein kann, Daten in ein anderes Land zu übermitteln; und
- die Richtlinie der verantwortlichen Stelle bezüglich der Aufbewahrung von Akten (wie lange Akten aufbewahrt werden und alle Schritte, die unternommen werden, um zu gewährleisten, dass die Akten genau und aktuell sind)
- ob ihre personenbezogenen Daten an andere Organisationen (einschließlich andere Komponenten der Bewegung), staatliche Stellen des Landes, in dem die Datenerhebung erfolgte, oder eines anderen Landes weitergegeben werden oder veröffentlicht werden dürfen sowie die Bestätigung, dass ihre personenbezogenen Daten wie erläutert verwendet werden dürfen.

Die Einwilligung kann unter Einschränkungen erteilt werden. Die Einzelheiten der erteilten Einwilligung, der erforderliche Umfang der Vertraulichkeit und alle geltenden Einschränkungen

werden dokumentiert und liegen den personenbezogenen Daten während der gesamten Verarbeitung bei.

Alternativen zur Einwilligung – besonders wenn keine Einwilligung eingeholt werden kann/das Einholen unzumutbar ist, werden personenbezogene Daten auf folgender Grundlage verarbeitet:

- lebenswichtiges Interesse
- öffentliches Interesse
- berechtigtes Interesse der verantwortlichen Stelle
- Erfüllung einer rechtlichen Verpflichtung

In diesen Fällen wird die verantwortliche Stelle nach Möglichkeit gewährleisten, dass die betroffene Person von dieser Verarbeitung weiß und in der Lage ist, sich - auf Wunsch - dagegen auszusprechen.

2.2.2 Lebenswichtiges Interesse

Es gilt die Annahme, dass die Verarbeitung personenbezogener Daten durch Suchdienstleistungen der verantwortlichen Stelle zum Zwecke der Familienzusammenführung und Klärung des Schicksals und Aufenthalts vermisster Personen sowie der Leistung von Nothilfe und Schutz unter bestimmten Umständen ein lebenswichtiges Interesse der betroffenen Person oder anderer Personen darstellen. Zu diesen Umständen zählen insbesondere:

- wenn eine betroffene Person von ihren Verwandten gesucht oder als vermisst gemeldet, ihrer Freiheit beraubt oder misshandelt wird oder möglicherweise tot ist;
- wenn die betroffene Person besonders schutzbedürftig und/oder nicht in der Lage ist, ihre freiwillige und auf Kenntnis der Sachlage gegründete Einwilligung zu erteilen und die Risiken und Vorteile der Verarbeitung ihrer personenbezogenen Daten weder einschätzen noch verstehen kann.

2.2.3 Öffentliches Interesse

Suchdiensttätigkeiten und suchdienstbezogene Aufgaben der verantwortlichen Stelle liegen im öffentlichen Interesse, weil sie ausschließlich humanitärer Natur sind, wie in Abschnitt 1.3 dargelegt. (Beispiele finden Sie in Anhang 2)

2.2.4 Berechtigtes Interesse

Personenbezogene Daten werden auch in Situationen verarbeitet, in denen ein berechtigtes Interesse der verantwortlichen Stelle an der Verarbeitung vorliegt, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen. (Beispiele finden Sie in Anhang 3).

2.2.5 Erfüllung einer rechtlichen Verpflichtung

Die verantwortliche Stelle wird die personenbezogenen Daten auch in Einklang mit allen geltenden rechtlichen Verpflichtungen, wie beispielsweise Einhaltung nationaler und regionaler Gesetze und gerichtlicher Anordnungen, unter Vorbehalt der grundlegenden Prinzipien der Bewegung, verarbeiten. Die rechtlichen Verpflichtungen können sich in Abhängigkeit von Ländern und Situationen unterscheiden.

2.3 Pflichten betreffend die Verarbeitung

2.3.1 Verantwortlichkeit / Rechenschaftspflicht

Die verantwortliche Stelle gewährleistet, dass jede Person oder Einheit, die Zugang zu personenbezogenen Daten hat und in ihrem Auftrag handelt (und daher ein Auftragsverarbeiter ist), diese personenbezogenen Daten ausschließlich in einer mit diesem CoC vereinbaren Weise verarbeiten wird. Die verantwortliche Stelle gewährleistet zudem, dass die Verantwortlichkeiten jeder an der Verarbeitung von personenbezogenen Daten beteiligten Einheit eindeutig zugewiesen und in entsprechenden Vertragsbestimmungen festgehalten werden. In Abschnitt 4 finden Sie weitere Informationen über die Datenübermittlung an Dritte. Dort ist festgelegt, dass die empfangende dritte Partei die Daten ausschließlich gemäß den Anweisungen der verantwortlichen Stelle verarbeiten wird.

2.3.2 Verarbeitung angemessener, sachlich relevanter und aktualisierter Daten

Datenminimierung – von dem Suchdienst der verantwortlichen Stelle erhobene und verarbeitete personenbezogene Daten werden laufend überprüft, um zu gewährleisten, dass sie dem Zeck angemessen, sachlich relevant und nicht unverhältnismäßig sind, sofern es sich nicht um archivierte Daten handelt.

Richtigkeit – personenbezogene Daten müssen im Hinblick auf den Zweck, für den sie erhoben und verarbeitet wurden, sachlich richtig, vollständig und auf dem neuesten Stand sein.

2.3.3 Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen

Es werden geeignete technische und organisatorische Maßnahmen ergriffen, um die Anforderungen dieses CoC beim Aufbau von Datenmanagementsystemen und der Entwicklung von Verfahren zur Erhebung personenbezogener Daten zu erfüllen.

2.3.4 Datenschutz-Folgenabschätzung (DSFA)

Wenn die Verarbeitung voraussichtlich konkrete Risiken für die Rechte und Freiheiten der betroffenen Personen, wie Übermittlung, Veröffentlichung und Offenlegung mit sich bringt, wird die verantwortliche Stelle vor der Verarbeitung, wenn möglich, in Abstimmung mit der betroffenen Person und anderen Beteiligten eine DSFA vornehmen, um insbesondere Nachstehendes festzustellen und zu beurteilen:

- die Vorteile der Datenverarbeitung;
- Ursprung, Art, Wahrscheinlichkeit und Schweregrad der Risiken;
- geeignete Maßnahmen um nachzuweisen, dass die Risiken minimiert werden und die Verarbeitung der personenbezogenen Daten unter Einhaltung des CoC und aller geltenden Gesetze erfolgt.

Das Ergebnis der DSFA sollte die Minimierung des Risikos einer Verletzung und/oder möglichen Beschneidung der Rechte und Freiheiten der betroffenen Person sein. Die verantwortliche Stelle wird das Ergebnis und die Gründe, warum dieses Ergebnis erzielt wurde, dokumentieren. Die verantwortliche Stelle wird ebenfalls sicherstellen, dass die infolge der DSFA einzuleitenden Schritte entsprechend umgesetzt werden und die gewünschte Wirkung entfalten.

2.3.5 Dokumentation der Verarbeitung

Die verantwortliche Stelle gewährleistet, dass elektronische Aufzeichnungen bzw. Aufzeichnungen in Papierform aufbewahrt werden, die Folgendes enthalten: (i) die Datenbanken, in denen die Verarbeitung der personenbezogenen Daten erfolgt und (ii) die Schlüsseldaten für die Verarbeitungsmeilensteine. Diese Meilensteine werden in den Datenbanken/der einzelnen Datei der betroffenen Person verzeichnet.

2.3.6 Datenaufbewahrung

Personenbezogene Daten werden unter Einhaltung der Daten-/Aktenaufbewahrungsrichtlinie der Suchdienste der verantwortlichen Stelle archiviert oder gelöscht, wenn sie für die Zwecke, für die sie erfasst wurden, oder für die Verarbeitung auf anderer berechtigter/rechtlicher Grundlage nicht länger benötigt werden (siehe auch Abschnitt 3.3).

2.3.7 Datensicherheit

Während des gesamten Verarbeitungsprozesses werden angemessene technische, physische und organisatorische Sicherheitsmaßnahmen ergriffen, um die personenbezogenen Daten vor Verlust, Diebstahl, unberechtigtem(r) oder rechtswidrigem(r) Zugriff oder Offenlegung zu schützen. Der Zugang zu personenbezogenen Daten ist auf jene Mitarbeiter der verantwortlichen Stelle beschränkt,

die diesen Zugang benötigen, um eine konkrete Aufgabe zu erfüllen. Es gelten Sicherheitsmaßnahmen und Zugangsbeschränkungen (nähere Einzelheiten finden Sie in Anhang 4).

2.3.8 Verletzung des Schutzes personenbezogener Daten

Die verantwortliche Stelle benachrichtigt die betroffene Person im Falle einer Verletzung des Schutzes personenbezogener Daten, wenn diese voraussichtlich Auswirkungen auf die Rechte und Freiheiten der betroffenen Person haben wird.

Die Benachrichtigung der betroffenen Person über die Verletzung des Schutzes personenbezogener Daten erfolgt mit dem Ziel, die Risiken nachteiliger Auswirkungen auf die betroffene Person zu minimieren.

Die verantwortliche Stelle kann entscheiden, dass die Benachrichtigung über eine Verletzung des Schutzes personenbezogener Daten der betroffenen Person nicht erforderlich ist, wenn eine oder mehrere der folgenden Voraussetzungen vorliegen:

- die verantwortliche Stelle hat geeignete organisatorische, technische oder physische Schutzmaßnahmen umgesetzt und diese Maßnahmen wurden auf die von der Verletzung des Schutzes personenbezogener Daten betroffenen Daten angewendet;
- die verantwortliche Stelle hat in der Folge Maßnahmen ergriffen, die gewährleisten, dass die Rechte und Freiheiten der betroffenen Personen wahrscheinlich nicht länger maßgeblich betroffen sind;
- die Benachrichtigung würde einen unverhältnismäßigen Aufwand bedeuten, insbesondere im Hinblick auf die vorherrschenden logistischen oder Sicherheitsumstände oder die Anzahl der betroffenen Fälle. In diesem Fall wird die verantwortliche Stelle stattdessen die Herausgabe einer öffentlichen Mitteilung oder eine ähnliche Maßnahme erwägen, mithilfe derer betroffene Personen auf ebenso wirksame Weise benachrichtigt werden;
- die Benachrichtigung würde sich nachteilig auf ein wesentliches öffentliches Interesse, wie z. B. die Durchführbarkeit der Arbeit der verantwortlichen Stelle, auswirken;
- die Kontaktaufnahme mit der betroffenen Person könnte aufgrund der vorherrschenden Umstände die betroffene Person selbst gefährden.

3. Rechte der betroffenen Personen

3.1 Informationspflicht und Auskunftsrecht

Die verantwortliche Stelle wird der betroffenen Person zum Zeitpunkt der Erhebung personenbezogener Daten bzw. so schnell wie möglich danach, mündlich oder schriftlich und vorbehaltlich logistischer und sicherheitstechnischer Einschränkungen, auf dem geeignetsten Weg Informationen über die Verarbeitung ihrer personenbezogenen Daten zukommen lassen (eine Liste mit Informationen, die darin enthalten sein müssen, finden Sie in Anhang 5).

Betroffene Personen haben das Recht jederzeit eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden. Ist dies der Fall, so sind sie berechtigt, Auskunft über ihre personenbezogenen Daten zu erhalten und Informationen über den Zweck der Verarbeitung sowie die Empfänger dieser Daten und die getroffenen Sicherheitsvorkehrungen einzuholen.

Auf Anfrage wird ihnen eine Kopie des/der Dokuments/Dokumente zur Verfügung gestellt, das/die ihre personenbezogenen Daten enthält/enthalten.

Dieser Abschnitt gilt nicht, wenn die Auskunft infolge nachstehender Umstände eingeschränkt werden muss:

- vorrangiges öffentliches Interesse
- Datenschutzinteressen sowie Rechte und Freiheiten anderer
- die fraglichen Dokumente können nicht aussagekräftig bearbeitet werden

Die verantwortliche Stelle führt Aufzeichnungen über Auskunftsanfragen und die Ergebnisse dieser Anfragen sowie die Art der offengelegten personenbezogenen Daten und/oder die Verweigerung des Zugriffs auf Informationen.

3.2 Weitergabe an Familienmitglieder und Vormünder

Eine Anfrage auf Weitergabe personenbezogener Daten eines Familienmitglieds oder gesetzlichen Vormunds eines Kindes oder anderer Personen, die keine Einwilligung geben können, gilt als im Wohl dieser Person gelegen und ihr wird daher stattgegeben, sofern kein ausreichender Grund vorliegt, etwas anderes anzunehmen. Die betroffene Person sollte, wenn möglich, gefragt werden um festzustellen, ob sie dieser Weitergabe widerspricht.

3.3 Berichtigung und Löschung

Berichtigung – Die verantwortliche Stelle wird auf Anfrage personenbezogene Daten berichtigen, insbesondere wenn die Daten unzutreffend oder unvollständig sind. Die verantwortliche Stelle wird den Empfängern von personenbezogenen Daten vorgenommene Berichtigungen mitteilen, sofern die Berichtigung nicht unwesentlich ist oder die Mitteilung einen unverhältnismäßigen Aufwand bedeutet.

Löschung – Eine betroffene Person hat in allen nachstehenden Fällen das Recht auf Löschung ihrer personenbezogenen Daten aus den aktiven Datenbanken der verantwortlichen Stelle:

- ihre personenbezogenen Daten werden für die Zwecke, für die sie ursprünglich erfasst wurden oder für eine weitere Verarbeitung nicht länger benötigt;
- die betroffene Person hat ihre Einwilligung zur Verarbeitung widerrufen und es existiert keine andere Grundlage für die Verarbeitung ihrer personenbezogenen Daten;
- die betroffene Person erhebt erfolgreich Widerspruch gegen die Verarbeitung ihrer personenbezogenen Daten;
- die Verarbeitung der personenbezogenen Daten einer betroffenen Person entspricht diesem CoC aus einem anderen Grund nicht.

Eine weitere Speicherung personenbezogener Daten einer betroffenen Person ist jedoch erlaubt, wenn diese aus folgenden Gründen erforderlich oder gerechtfertigt ist:

- für historische, statistische oder wissenschaftliche Zwecke, wie zur Dokumentation einer von einer verantwortlichen Stelle in Erfüllung ihres Auftrags im Rahmen der Genfer Konventionen von 1945, der dazu erlassenen Zusatzprotokolle aus dem Jahr 1977 und/oder der Statuten der Bewegung gesetzten Handlung;
- aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit; oder
- im Hinblick auf die Veröffentlichung von journalistischem, literarischem oder künstlerischem Material durch eine beliebige Person in Ausübung des Rechts auf freie Meinungsäußerung und Information.

Außerdem ist die weitere Aufbewahrung der personenbezogenen Daten einer betroffenen Person zulässig, wenn diese gesetzlich vorgeschrieben ist. Eine betroffene Person wird über eine Entscheidung betreffend ihre Anfrage benachrichtigt und diese Entscheidung wird von der verantwortlichen Stelle dokumentiert.

Die verantwortliche Stelle behält sich das Recht vor, eine Anfrage der betroffenen Person auf Berichtigung oder Löschung abzulehnen, wenn sie der Meinung ist, dass die betroffene Person diese Anfrage unter ungebührendem Druck gestellt hat und/oder wenn die Löschung lebenswichtigen Interessen der betroffenen Person zuwider laufen würde.

Die verantwortliche Stelle wird die Empfänger über die Löschung der personenbezogenen Daten benachrichtigen und sie bitten, alle Verknüpfungen oder Kopien dieser Daten zu löschen, sofern die gelöschten Daten nicht unbedeutend sind oder die Benachrichtigung einen unverhältnismäßigen Aufwand darstellt.

3.4 Widerspruchsrecht

Eine betroffene Person hat das Recht gegen die auf berechtigten Interessen der verantwortlichen Stelle beruhende oder im öffentlichen Interesse gelegene Verarbeitung ihrer personenbezogenen Daten aus nachvollziehbaren Gründen, die sich aus ihrer besonderen Situation ergeben, Widerspruch einzulegen. Wenn dem Widerspruch stattgegeben wird, werden die betroffenen personenbezogenen Daten nicht mehr verarbeitet, es sei denn, die verantwortliche Stelle kann vorrangige schutzwürdige Gründe für deren weitere Verarbeitung nachweisen.

Wenn dem Widerspruch stattgegeben wird, wird die verantwortliche Stelle die Datenempfänger über diesen Widerspruch benachrichtigen, sofern dies keinen unverhältnismäßigen Aufwand darstellt.

3.5 Rechtsbehelfe

Eine betroffene Person richtet ihre Anfrage an die verantwortliche Stelle, die diese innerhalb einer angemessenen, jedenfalls jedoch innerhalb der gesetzlich vorgeschriebenen Frist beantwortet.

Das Personal, das eine Anfrage einer betroffenen Person erhält, wird:

- der Anfrage stattgeben und die anfragende Person benachrichtigen, wie der Anfrage entsprochen wird oder wurde; oder
- die anfragende betroffene Person informieren, warum der Anfrage nicht entsprochen wird oder entsprochen werden kann; und
- die betroffene Person über die Möglichkeit der Einbringung einer Beschwerde bei der verantwortlichen Stelle informieren.

4. Besondere Vorschriften betreffend die Übermittlung von Daten

4.1 Allgemeine Grundsätze

4.1.1 Hintergrund

Suchdiensttätigkeiten und suchdienstbezogene Aufgaben machen oft eine grenzüberschreitende Datenübermittlung personenbezogener Daten zwischen verantwortlichen Stellen erforderlich.

Die Suchdienste der verantwortlichen Stelle können auch die Übermittlung personenbezogener Daten an Stellen wie nicht-staatliche Organisationen (NGO), internationale Organisationen, Behörden oder andere Dritte erforderlich machen, um Suchdiensttätigkeiten und suchdienstbezogene Aufgaben wahrnehmen zu können.

Diese Übermittlungen erfolgen in Einklang mit den Aktivitäten des Suchdienst-Netzwerks wie in Abschnitt 1.3 dargelegt; sie erfolgen daher aus wichtigen Gründen des öffentlichen Interesses und im Sinne der in Abschnitt 1.4 dargestellten Grundsätze und Leitlinien der Bewegung.

Zudem erfolgen diese Übermittlungen in den meisten Fällen auf Grundlage der Einwilligung und/oder des Schutzes lebenswichtiger Interessen der betroffenen Person oder anderer Personen.

4.1.2 Allgemeine Grundsätze der Datenübermittlung

Eine Übermittlung von Daten innerhalb oder außerhalb der Bewegung stellt einen Verarbeitungsvorgang dar. Daher unterliegt sie den in Kapitel 2 dargestellten grundlegenden Prinzipien und den in Kapitel 3 dargestellten Rechten der betroffenen Personen. Eine Übermittlung ist jedoch ein besonders sensibler Verarbeitungsvorgang. Dementsprechend sind einige Verarbeitungsanforderungen wie DSFA, Benachrichtigung der betroffenen Person und Datensicherheit besonders wichtig.

Wie in Abschnitt 3.1 oben dargelegt, wird eine Übermittlung an alle vorhersehbaren Dritten vor dem/zum Zeitpunkt der Erhebung der Daten vorausgesehen und die Einwilligung zur Übermittlung personenbezogenen Daten der betroffenen Person wird, wenn möglich, eingeholt.

Personenbezogene Daten dürfen nicht an Personen oder Organisationen übermittelt werden, wenn keine angemessenen und geeigneten Garantien vorgesehen sind, die der sensiblen Natur der Daten, der Dringlichkeit des humanitären Einschreitens und den logistischen und sicherheitstechnischen Grenzen, die in diesem CoC beschrieben werden, Rechnung tragen.

4.1.3 Datenschutz-Folgenabschätzung für Datenübermittlungen

Das Erfordernis der Durchführung einer DSFA ist im Zusammenhang mit Datenübermittlungen besonders wichtig. Dementsprechend wird die verantwortliche Stelle, wenn die Übermittlung voraussichtlich konkrete Risiken für die Rechte und Freiheiten der betroffenen Personen mit sich

bringt, vor der Übermittlung eine DSFA (nachzuschlagen in Anhang 6), wie in Abschnitt 2.3.4 oben dargestellt, vornehmen.

4.1.4 Voraussetzungen

Datenübermittlungen müssen alle nachstehenden Voraussetzungen erfüllen:

- Die Verarbeitung durch den Empfänger ist streng auf die Zwecke von Suchdiensttätigkeiten und suchdienstbezogene Aufgaben und auf damit vereinbare Zwecke beschränkt;
- Umfang und Art der personenbezogenen Daten sind streng auf die Bedürfnisse des Empfängers für die Zwecke der angegebenen oder beabsichtigten weiteren Verarbeitung beschränkt;
- Die Übermittlung ist mit den nachvollziehbaren Erwartungen der betroffenen Person vereinbar.

4.1.5 Dokumentation der Datenübermittlung

Die verantwortliche Stelle gewährleistet die Führung von Aufzeichnungen über die Übermittlungen in elektronischer bzw. Papierform (siehe auch 2.3.5).

Die Übermittlungsaufzeichnungen sollten Folgendes enthalten:

- Name des Empfängers
- angegebenen Zweck der Übermittlung;
- Datum der Übermittlung;
- Beschreibung der Art der personenbezogenen Daten, die übermittelt wurden;
- alle Einschränkung hinsichtlich der vom Empfänger genehmigten Nutzung.

4.1.6 Vereinbarungen

Wie in Abschnitt 4.1.2 dargelegt, kann eine Datenübermittlung stattfinden, wenn die verantwortliche Stelle sich davon überzeugt hat, dass vom Empfänger geeignete Garantien zum Schutz von personenbezogenen Daten vorgesehen wurden. Geeignete Garantien können, wenn möglich, durch Vereinbarungen über die Behandlung personenbezogener Daten mit Dritten außerhalb der Bewegung vorgesehen werden, sobald regelmäßige Datenübermittlungen erwogen werden.

Auch wenn Vereinbarungen abgeschlossen werden, kann die Übermittlung bestimmter Arten von Daten dennoch unangemessen sein.

4.2 Übermittlungsmethoden

Im Falle einer Übermittlung müssen geeignete Vorkehrungen zur Sicherung der an Dritte übermittelten personenbezogenen Daten ergriffen werden. Der Standard und die Methode der

angewandten Sicherheitsmaßnahmen richten sich nach der Art und Sensibilität der personenbezogenen Daten sowie nach den in der DSFA ermittelten Risiken.

5. Besondere Vorschriften betreffend die Veröffentlichung von Daten

5.1 Allgemeine Grundsätze

Die Veröffentlichung personenbezogener Daten durch die verantwortliche Stelle stellt einen Datenverarbeitungsvorgang dar. Daher unterliegt sie den in Kapitel 2 dargestellten allgemeinen Prinzipien und den in Kapitel 3 dargestellten Rechten der betroffenen Personen. Eine Veröffentlichung ist jedoch ein besonders sensibler Verarbeitungsvorgang. Nach der Veröffentlichung von personenbezogenen Daten können die verantwortliche Stelle und die betroffene Person größtenteils nicht mehr kontrollieren, auf welche Weise diese verarbeitet werden. Dementsprechend sind auch die in diesem Kapitel dargestellten, zusätzlichen Prinzipien einzuhalten.

Vorbehaltlich DSFA und geltender rechtlicher Verpflichtungen, können die Suchdienste der verantwortlichen Stelle personenbezogene Daten veröffentlichen, um Familien zu suchen und zusammenzuführen, die infolge von bewaffneten Konflikten, anderen Situationen der Gewalttätigkeit, Naturkatastrophen und Migration getrennt wurden. Zu diesen Daten zählen Namen, Bilder und Zustand (wie z.B. am Leben und gesund, verwundet, verstorben, vermisst, vertrieben), die online, in den Medien, auf Postern, Broschüren oder auf andere geeignete Weise veröffentlicht werden können.
Gemäß Abschnitt 2.2.1 ist die Einwilligung der betroffenen Person die bevorzugte Grundlage für die Veröffentlichung von personenbezogenen Daten.

5.2 Datenschutz-Folgenabschätzung für die Veröffentlichung von Daten

Das in Abschnitt 2.3.4 oben und Anhang 6 dargelegte Erfordernis der Durchführung einer DSFA ist im Kontext der Datenveröffentlichung besonders wichtig.

Neben den in Abschnitt 2.3.4 „Datenschutz-Folgenabschätzung“ oben dargelegten Punkten, hat die DSFA im Kontext der Veröffentlichung folgende Punkte zu berücksichtigen:

- die für die Datenveröffentlichung geltenden, nationalen Datenschutzgesetze und -vorschriften;
- die Sicherheitslage, die Einhaltung der Menschenrechte und des HVR sowie die Sicherheit der betroffenen Personen im jeweiligen Land;

- ob anonymisierte/verallgemeinerte Daten ausreichen oder ob die Veröffentlichung von personenbezogenen Daten erforderlich ist; ob andere Methoden zum Schutz der Identität der betroffenen Personen den angegebenen Zweck der Veröffentlichung erfüllen (dazu zählt beispielsweise zu einem Bild keine Namen/Erkennungsmerkmale/konkreten Orte anzugeben);
- die Art und Voraussetzungen der Veröffentlichung;
- die Möglichkeit zur Einschränkung der weiteren Nutzung gegenüber Dritten, die die veröffentlichten Daten verwenden möchten;
- die Möglichkeit der Festlegung des Zeitraums, in dem bestimmte Daten in einem bestimmten Medium veröffentlicht bleiben und der Löschungsmethode nach der Erfüllung des für die Veröffentlichung angegebenen Zwecks;
- die Feststellung der Erforderlichkeit und Angemessenheit der Veröffentlichungen durch regelmäßige Überprüfungen seitens der verantwortlichen Stelle;
- im Kontext der öffentlichen Kommunikation die Wichtigkeit, besonders schutzbedürftige Personen vor öffentlicher Aufmerksamkeit zu schützen.

Wenn die betroffene Person besonders schutzbedürftig ist, müssen gegebenenfalls weitere Überlegungen, wie Sicherheitsvorkehrungen zum Schutz der Vertraulichkeit und Anonymität, angestellt werden. Das grundlegende Prinzip des Opferschutzes lautet „niemandem Schaden zuzufügen“ und zum Wohl von besonders schutzbedürftigen betroffenen Personen zu handeln.

5.3 Dokumentation der Datenveröffentlichung

Die verantwortliche Stelle führt ein Verzeichnis über die Veröffentlichungen.

Die Veröffentlichungsaufzeichnungen sollten Folgendes enthalten:

- Datum der Veröffentlichung;
- sofern relevant, Datum, an dem die Grundlage der Veröffentlichung im Sinne der DSFA zu überprüfen ist;
- sofern relevant, Datum, an dem die Daten nicht mehr veröffentlicht werden dürfen;
- Beschreibung der Art der personenbezogenen Daten, die veröffentlicht wurden;
- wenn möglich, Einzelheiten zu den eingesetzten Medien.

5.4 Für Suchdienstzwecke zu veröffentlichende Daten

Daten, die veröffentlicht werden dürfen, müssen für jeden einzelnen Kontext festgelegt werden; für bestimmte betroffene Personen können genauere Leitlinien verfügbar sein. Auf Grundlage der DSFA können bestimmte Risikominderungsmaßnahmen festgelegt werden wie:

- Eine Beschränkung der Veröffentlichung auf jene Daten, die unbedingt erforderlich sind, damit der Leser/Hörer die Identität der Personen, deren Namen/Bilder veröffentlicht werden, feststellen und mit ihnen in Kontakt treten kann.
- Bilder besonders schutzbedürftiger Personen werden nicht in Verbindung mit anderen personenbezogenen Daten (z.B. Name) veröffentlicht; die Anschrift von Minderjährigen wird niemals veröffentlicht.

5.5 Für öffentliche Archive zu veröffentlichende Daten

Archivierte personenbezogene Daten können in Übereinstimmung mit geltendem Recht öffentlich gemacht werden.

5.6 Für die öffentliche Kommunikation zu veröffentlichende Daten

Personenbezogene Daten können zum Zwecke der Bewerbung von Suchdiensttätigkeiten und/oder im Rahmen der Sensibilisierung für Situationen, die Anlass zur Besorgnis geben, in Übereinstimmung mit geltendem Recht veröffentlicht werden. Die öffentliche Kommunikation steht in Zusammenhang mit dem Recht auf freie Meinungsäußerung und Information sowie mit der öffentlichen Rechenschaftspflicht. Wie bei jeder Veröffentlichung werden jedoch die in diesem CoC dargelegten Prinzipien eingehalten und es wird eine DSFA vorgenommen.

5.7 Recht auf Widerruf der Einwilligung/auf Löschung von veröffentlichten Materialien

Wenn die Veröffentlichung auf der Grundlage einer Einwilligung erfolgt, kann eine betroffene Person diese Einwilligung zur Veröffentlichung von Materialien, in denen ihre Identität feststellbar ist, jederzeit widerrufen. In diesem Fall wird die verantwortliche Stelle unter Berücksichtigung der Probleme bei der Löschung von öffentlichen (insbesondere Online-)Dokumenten alle zumutbaren Schritte unternehmen, um die veröffentlichten Materialien zurückzuziehen und/oder deren Veröffentlichung zu verhindern.

Wenn die Veröffentlichung auf einer anderen Grundlage als einer Einwilligung erfolgt, wird nach den in Abschnitt 3.4 „Widerspruchsrecht“ dargestellten Verfahren vorgegangen.

6. Anwendung des CoC

Eine Arbeitsgruppe für die Einhaltung des CoC wird die weltweite Umsetzung des CoCs durch Förderung eines fortlaufenden Lernprozesses und einer fortlaufenden Entwicklung unterstützen.

Der vorliegende CoC muss, unter Vorbehalt der nationalen Gesetze, von allen verantwortlichen Stellen wie folgt wirksam angewendet werden:

- Der CoC wird in die Suchdienststrategien, -leitfäden und -programme aufgenommen.
- Der CoC wird ein integraler Bestandteil des Suchdienst-Personalmanagements und der Schulung aller verantwortlichen Stellen.
- Es wird ein Datenschutzbeauftragter für den Suchdienst ernannt, dessen Kontaktdaten bekannt gegeben werden.
- Teilnahme an regelmäßigen Erhebungen betreffend die Umsetzung dieses CoC.
- Zusammenarbeit mit der Arbeitsgruppe für die Einhaltung des CoC.
- Eine Überwachung, die eine Selbstüberwachung, einen Dialog, eine Begutachtung durch Kollegen und andere Formen der Überprüfung umfasst, wird vorgenommen, um eine fortlaufende Verbesserung und einen Lernprozess innerhalb der Organisation zu gewährleisten.

Die Arbeitsgruppe für die Einhaltung des CoC wird diesen CoC bei Bedarf überprüfen und aktualisieren.

7. Quellenangaben

7.1 Rechtsgrundlagen/Leitfäden

- UN Guidelines for the Regulation of Computerized Personal Data Files, as adopted by General Assembly resolution 49/95 of 14 December 1990;
- Art. 17 International Covenant on Civil and Political Rights;
- International Standard on the protection of personal data and privacy by the International Conference of Data Protection and Privacy Commissioners, 5 November 2009, http://privacyconference2011.org/htmls/adoptedResolutions/2009_Madrid/2009_M1.pdf;
- Convention of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data, 108, 28 January 1981, BRON
- Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 24 October 1995, *OJ* L 281 23 November 1995, p. 31-50;
- Art. 8 European Convention for the protection of Human Rights and fundamental freedoms, 4 November 1950;
- Art. 16 Treaty on the Functioning of the European Union (TFEU), 13 December 2007, *OJ* C 236, 26 November 2012, p. 0001-0390;
- Articles 7 - 8 Charter of Fundamental Rights of the European Union, *OJ*. C 303/1, 14 December 2007;
- Organisation for Economic Cooperation and Development (OECD), Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 1980 (update 2013), oe.cd/privacy;
- OECD Guidelines for Consumer Protection in the Context of Electronic Commerce, 9 December 1999, www.oecd.org/sti/consumer/34023811.pdf ;
- APEC Privacy Framework, 2005, http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

- Statutes of the International Red Cross and Red Crescent Movement, as amended in 2006;
- Resolution 4 by the Council of Delegates on Restoring Family links Strategy for the International Red Cross and Red Crescent Movement, 24 November 2007;
- International Conference of Data Protection and Privacy Commissioners, Resolution on Privacy and International Humanitarian Action, Amsterdam, Netherlands, 2015, https://icdppc.org/document-archive/adopted-resolutions/

7.2 Handbücher

- INTERNATIONAL COMMITTEE OF THE RED CROSS (ICRC), *Restoring family links in disasters: field manual,* Switzerland, ICRC, 2009, 211 p.;
- INTERNATIONAL COMMITTEE OF THE RED CROSS (ICRC), *Assessing restoring family links needs: handbook for national societies and the ICRC*, Switzerland, ICRC, 2010, 103 p.;
- INTERNATIONAL COMMITTEE OF THE RED CROSS (ICRC), *Guidelines on providing restoring family links services to persons separated as a result of migration: an Internal document for the International Red Cross and Red Crescent Movement*, Switzerland, ICRC, 2010, 59 p.;
- INTERNATIONAL COMMITTEE OF THE RED CROSS (ICRC), *Restoring family links strategy: including legal references*, Switzerland, ICRC, 2009, 64 p.;
- Morgan, O., Tidball- Binz, M., van Alphen, D. (*EDS.), Management of dead bodies after disasters: A field manual for first responders*, Washington D.C., 2009, 53 p.;

ANHÄNGE

Anhang 1: Suchdiensttätigkeiten und suchdienstbezogene Aufgaben

Suchdiensttätigkeiten können, abhängig von Situation und Kontext, in verschiedene Kategorien unterteilt werden:

- Organisation des Austauschs von Familiennachrichten;
- Suche von Personen;
- Registrierung und Nachverfolgung von Personen (Kindern oder Erwachsenen), um deren Verschwinden zu verhindern und ihre Familien zu informieren;
- Zusammenführung und Rückführung von Familien;
- Erfassung, Management und Weiterleitung von Informationen über Verstorbene;
- Übermittlung von offiziellen Dokumenten, wie Geburtsurkunden, Ausweisen oder anderen von einer Behörde ausgestellten Dokumenten;
- Ausstellung von Haftzeitbescheinigungen und von anderen Dokumenten zur Bestätigung von Umständen, die zur Registrierung einer Person geführt haben;
- Ausstellung von IKRK-Reisedokumenten;
- Begleitung der Eingliederung von mit ihren Familienmitgliedern wiedervereinten Personen;
- Förderung und Unterstützung der Einführung von Verfahren zur Klärung des Schicksals und Aufenthalts von als vermisst gemeldeten Personen;

Siehe auch: http://familylinks.icrc.org

Suchdienstbezogene Aufgaben – andere humanitäre Dienstleistungen in Bezug auf Suchdiensttätigkeiten, die von Suchdienstmitarbeitern erbracht werden:

- Materielle, rechtliche, psychologische und psychosoziale Unterstützung von Familien vermisster Personen und anderer von einem bewaffneten Konflikt, anderen Situationen von Gewalttätigkeiten, Katastrophen, Migration und anderen humanitären Krisen betroffenen Personen
- Unterstützung der zuständigen Behörden beim Umgang mit und der Identifizierung von menschlichen Überresten
- (Verweis an) Sozialdienste
- Resettlement-Leistungen oder (Verweis an) Integrationshilfen für besonders schutzbedürftige Personen

- Archivierung (persönliche/Familienerinnerungen; Weltkulturerbe; individuelle administrative Bedürfnisse, Rechenschaftspflicht der Parteien, historische, statistische und medizinische Forschung)
- Öffentliche Kommunikation zur Bewerbung von Suchdiensttätigkeiten und suchdienstbezogenen Aufgaben

Anhang 2: Öffentliches Interesse

Einige Beispiele für öffentliches Interesse:

- Bei der Bewältigung großer Krisen, die ein unverzügliches Handeln erfordern und das Einholen von Einwilligungen unmöglich machen und nicht eindeutig festgestellt werden kann, ob ein lebenswichtiges Interesse als Rechtsgrundlage vorliegt. Ein Beispiel dafür ist die Rettung einer großen Anzahl von Migranten auf dem Meer.
- Im Falle, dass die betroffenen Verarbeitungsvorgänge sehr komplex sind und unterschiedliche externe Verarbeiter und komplexe Technologien umfassen, die eine umfassende Einschätzung der Risiken und Vorteile der betroffenen Verarbeitungsschritte und eine Entscheidung in voller Sachkenntnis für die betroffene Person auf dieser Grundlage schwierig machen. Wenn lebenswichtige Interessen der betroffenen Person oder einer anderen Person nicht festgestellt werden können (entweder aufgrund fehlender Dringlichkeit oder weil die betroffene Person gesucht wird), kann die Verarbeitung auf Grundlage des Auftrags der verantwortlichen Stelle erfolgen, wenn eine ausreichende DSFA durchgeführt wurde.
- Zuweisung von Hilfeleistungen, wenn das Einholen der Einwilligung aller potenziellen Berechtigten nicht durchführbar ist, und wenn das Leben und die Unversehrtheit der betroffenen Person oder anderer Personen voraussichtlich nicht auf dem Spiel stehen (in diesem Fall wäre ein „lebenswichtiges Interesse“ die geeignetste Grundlage für die Verarbeitung).
- Die Verarbeitung von personenbezogenen Daten einer inhaftierten betroffenen Person. Das kann beispielsweise bei der Verarbeitung von Daten von im Zuge eines bewaffneten Konflikts oder einer anderen Situation der Gewalttätigkeit ihrer Freiheit beraubten Personen vorkommen, wenn das IKRK (oder die Nationale Gesellschaft) noch nicht in der Lage war, die ihrer Freiheit beraubten betroffene Person zu besuchen und ihre Einwilligung einzuholen, und wenn die vorherrschenden Haftbedingungen im fraglichen Fall die Vermutung zulassen, dass ein „lebenswichtiges Interesse" vorliegt.

Anhang 3: Berechtigtes Interesse

Einige Beispiele für ein berechtigtes Interesse:

- Die Verarbeitung ist für die wirksame Erfüllung des Mandats der verantwortlichen Stelle gemäß den Rotkreuzgrundsätzen (insbesondere Neutralität, Unabhängigkeit und Unparteilichkeit) und den Standardarbeitsmodalitäten erforderlich;
- Die Verarbeitung von Daten nur im ausdrücklich erforderlichen Umfang zur Sicherstellung der Informationssysteme und Informationssicherheit sowie der Sicherheit der damit verbundenen Dienstleistungen, die von öffentlichen Behörden, Computer Emergency Response Teams (CERT), Computer Security Incident Response Teams (CSIRT), Anbietern elektronischer Kommunikationsnetzwerke und -dienstleistungen und Anbietern von Sicherheitstechnologien und –dienstleistungen über diese Informationssysteme angeboten werden bzw. über diese Informationssysteme abgerufen werden können. Dazu zählen beispielsweise die Verhinderung des unbefugten Zugriffs auf elektronische Kommunikationsnetzwerke und der Verbreitung störender Programmcodes sowie die Abwehr von „Denial of Service“-Angriffen und der Beschädigung von Computern und elektronischer Kommunikationssysteme;
- Die Verarbeitung personenbezogener Daten im ausdrücklich zur Verhinderung, des Nachweises und der Unterbindung von Betrug oder Diebstahl erforderlichen Umfang;
- Die Verarbeitung personenbezogener Daten zum Zweck der Anonymisierung und Pseudonymisierung von personenbezogenen Daten;
- Wenn es zur Feststellung, Durchsetzung oder Abwehr von Rechtsansprüchen im Rahmen eines Gerichts-, Verwaltungs- oder außergerichtlichen Verfahrens erforderlich ist; Direktmarketing und/oder öffentliche Kommunikation.

Anhang 4: Datensicherheit

Personenbezogene Daten müssen in einer Art und Weise verarbeitet werden, die eine angemessene Sicherheit der Daten sowie die Verhinderung eines unbefugten Zugriffs oder einer unbefugten Nutzung dieser personenbezogenen Daten und der bei der Verarbeitung verwendeten Infrastruktur gewährleistet.

Alle der verantwortlichen Stelle unterstellten Personen, die Zugriff auf personenbezogene Daten haben, dürfen diese nur in einer mit dem CoC und der geltenden Datenschutzrichtlinie vereinbarten Weise verarbeiten, worauf in diesem Anhang näher eingegangen wird.

Zur Wahrung der Sicherheit und zur Verhinderung einer gegen diesen CoC verstoßenden Verarbeitung wird die verantwortliche Stelle eine Abschätzung der mit den Verarbeitungs- und Umsetzungsmaßnahmen verbundenen konkreten Risiken vornehmen, um diese zu mindern.

Diese Maßnahmen müssen einen in Bezug auf die Risiken und die Natur der zu schützenden personenbezogenen Daten ausreichenden Sicherheitsstandard (unter Berücksichtigung der verfügbaren Technologien, der vorherrschenden sicherheitstechnischen und logistischen Voraussetzungen und der Umsetzungskosten) gewährleisten. Dazu zählen Maßnahmen in Bezug auf:

- Schulungen
- das Management der Zugriffsrechte auf Datenbanken, die personenbezogene Daten enthalten;
- die physische Sicherheit von Datenbanken;
- die IT-Sicherheit;
- Verschwiegenheitsklauseln;
- Vernichtungsmethoden für personenbezogene Daten;
- alle übrigen geeigneten Maßnahmen.

Ziel dieser Maßnahmen ist zu gewährleisten, dass personenbezogene Daten sowohl aus technischer als auch aus organisatorischer Sicht sicher aufbewahrt und durch angemessene und geeignete Vorkehrungen vor unbefugter Änderung, Vervielfältigung, Manipulation, gesetzwidriger Vernichtung, versehentlichem Verlust und unzulässiger Offenlegung und Übertragung geschützt werden.

Datensicherheitsvorkehrungen können unter anderem in Abhängigkeit folgender Faktoren variieren:

- Art des Vorgangs;
- Natur und Sensibilität der betroffenen personenbezogenen Daten;
- Speicherform oder -format;
- Umgebung/Standort der konkreten personenbezogenen Daten; und
- vorherrschende sicherheitstechnische und logistische Bedingungen.

Datensicherheitsvorkehrungen müssen regelmäßig überprüft und auf den neuesten Stand gebracht werden, um einen Datenschutzstandard zu gewährleisten, der der Sensibilität der personenbezogenen Daten Rechnung trägt.

Die verantwortliche Stelle ist für die Koordinierung folgender Dinge verantwortlich:

- Einrichtung eines Systems zum Management der Informationssicherheit. Zu diesem Zweck wird er eine auf international anerkannten Standards und einer Risikobewertung beruhende Datenschutzrichtlinie einführen und regelmäßig aktualisieren, die beispielsweise aus Leitlinien zur physischen Sicherheit, einer IT-Sicherheitsrichtlinie, Leitlinien zur Sicherheit von E-Mails, Leitlinien zur Nutzung der IT-Ausrüstung, einer Typologie für den Umgang mit Informationen, einem Notfallplan und Leitlinien zur Vernichtung von Dokumenten besteht.
- die Entwicklung einer Kommunikationsinfrastruktur und von Datenbanken zur Erhaltung der Unversehrtheit und Sicherheit der Daten gemäß der eingeführten Sicherheitsrichtlinie.
- Ergreifung aller im Sinne dieses CoC geeigneten Maßnahmen zum Schutz der Sicherheit der im Informationssystem der verantwortlichen Stelle verarbeiteten personenbezogenen Daten.

1. Zugriffsrechte auf Datenbanken

Die verantwortliche Stelle ist verantwortlich für:

- die Gewährung von Zugriffsrechten auf Datenbanken, die personenbezogene Daten enthalten;
- die Sicherheit der Anlagen, die den berechtigen Mitarbeitern, den Zugriff auf dieses System ermöglichen;
- die Einhaltung der in diesem Anhang beschriebenen Sicherheitsvorschriften;
- die Gewährleistung, dass Mitarbeiter, denen Zugriff gewährt wurde, in der Lage sind, diesen CoC einzuhalten. Das erfordert vor der Gewährung des Zugriffs auf Datenbanken entsprechende Schulungen und die Unterzeichnung einer Verschwiegenheitsverpflichtung im Dienstvertrag;
- die Gewährleistung, dass nur Mitarbeitern der Zugriff gewährt wird, die diesen tatsächlich benötigen;
- Führung eines Registers der Mitarbeiter, die Zugriff auf jede einzelne Datenbank haben, und gegebenenfalls eine Aktualisierung dessen (z. B. wenn Mitarbeiter, denen verschiedene Verantwortlichkeiten übertragen wurden, nicht länger Zugriff benötigen);
- Sofern machbar, sollte ein Verlaufsprotokoll der Mitarbeiter, die Zugriff auf eine Datenbank hatten, geführt werden, um – so lange sich die von diesen Mitarbeitern verarbeiteten Daten in der Datenbank befinden – eine entsprechende Rechenschaftspflicht zu gewährleisten.

Die Mitarbeiter müssen die Daten innerhalb der Grenzen der ihnen gewährten Verarbeitungsrechte verarbeiten.

Mitarbeitern mit erweiterten Zugriffsrechten oder Mitarbeitern, die für die Verwaltung der Zugriffsrechte verantwortlich sind, können zusätzliche vertragliche Verschwiegenheitsverpflichtungen auferlegt werden.

2. Physische Sicherheit

Jede verantwortliche Stelle ist verantwortlich für:

- die Erlassung von Sicherheitsvorschriften, die prozessuale, technische und administrative Sicherheitskontrollen festlegen, um auf der Grundlage der ermittelten Risiken einen angemessenen Standard bezüglich der Vertraulichkeit, physischen Unversehrtheit und Verfügbarkeit von (physischen oder IT-basierten) Datenbanken zu gewährleisten;
- die Sicherstellung, dass alle Mitarbeiter über diese Sicherheitsvorschriften informiert sind und sich daran halten;
- die Entwicklung geeigneter Kontrollmechanismen zur Gewährleistung der Erhaltung der Datensicherheit;
- die Gewährleistung, dass an Speicherstandorten ausreichende Sicherheitsnormen für den Brandschutz und den Schutz elektrischer Anlagen gelten;
- die Gewährleistung, dass die Speicherkapazitäten auf ein strenges Minimum reduziert werden.

3. IT-Sicherheit

Die verantwortliche Stelle wird:

- Sicherheitsvorschriften erlassen, die prozessuale, technische und administrative Sicherheitskontrollen festlegen, um auf Grundlage einer Risikobewertung einen angemessenen Standard bezüglich der Vertraulichkeit, Unversehrtheit und Verfügbarkeit der eingesetzten Informationssysteme gewährleisten;
- geeignete Kontrollmechanismen zur Gewährleistung der Erhaltung der Datensicherheit entwickeln;
- konkrete Sicherheitsvorschriften für einen Teil der IT-Kommunikationsstruktur, eine Datenbank oder eine konkrete Abteilung erlassen, wenn er dies für notwendig erachtet;

Die gesamte interne und externe E-Mail-Korrespondenz, die personenbezogene Daten enthält, wird nur von Mitarbeitern bearbeitet, die diese Informationen unbedingt benötigen. Die Empfänger einer

E-Mail-Korrespondenz müssen sorgfältig erwogen werden, um die unnötige Verbreitung personenbezogener Daten zu vermeiden.

Der Fernzugriff auf Server und der Einsatz von privaten Standgeräten oder Laptops müssen den in der IT-Sicherheitsrichtlinie der verantwortlichen Stelle festgelegten Sicherheitsstandards entsprechen. Die Nutzung von Internetzugängen und ungesicherten Drahtlosverbindungen zum Abruf, zur Weitergabe, Übermittlung oder Übertragung von personenbezogenen Daten muss, wenn sie nicht aus betrieblichen Gründen unbedingt erforderlich ist, vermieden werden.

Mitarbeiter müssen beim Umgang mit personenbezogenen Daten angemessene Sorgfalt walten lassen, wenn sie sich über Fernzugriff mit den Servern der verantwortlichen Stelle verbinden. Passwörter müssen stets geschützt werden und die Mitarbeiter müssen überprüfen, dass sie sich ordnungsgemäß von ihrem Computersystem abgemeldet und alle Browserfenster geschlossen haben.

Laptops, Smartphones und andere tragbare Geräte bedürfen besonderer Sicherheitsvorkehrungen, insbesondere, wenn mit ihnen an einem anderen Ort gearbeitet wird. Tragbare Medienausrüstungen müssen stets an sicheren Standorten verwahrt werden.

Tragbare oder mobile Geräte dürfen nicht für die Speicherung von Dokumenten verwendet werden, die personenbezogene Daten enthalten, welche als besonders sensibel klassifiziert wurden. Wenn es sich nicht vermeiden lässt, müssen personenbezogene Daten so schnell wie praktisch machbar auf geeignete Computersysteme und Datenbankanwendungen übertragen werden. Wenn Flashspeicher wie USB-Flashlaufwerke und Speicherkarten zur vorübergehenden Speicherung personenbezogener Daten verwendet werden, müssen diese sicher verwahrt und das elektronische Protokoll muss verschlüsselt werden. Wenn die Informationen nicht länger benötigt werden, müssen sie nach der ordnungsgemäßen Speicherung von diesem tragbaren oder mobilen Gerät gelöscht werden.

Wiederherstellung und Sicherung

Es müssen wirksame Wiederherstellungs- und Sicherungsverfahren vorhanden sein, die sämtliche elektronischen Aufzeichnungen umfassen, und der zuständige Beauftragte für Informations- und Kommunikationstechnologie (Information and Communications Technology, ICT) muss gewährleisten, dass regelmäßige Sicherungen durchgeführt werden. Die Häufigkeit der Sicherungen variiert abhängig von der Sensibilität der personenbezogenen Daten. Elektronische Aufzeichnungen müssen automatisiert erfolgen, um eine einfache Wiederherstellung in Situation zu ermöglichen, in denen eine Sicherung unter anderem aufgrund von regelmäßigen Stromausfällen, Systemausfällen oder Naturkatastrophen schwierig ist.

Wenn elektronische Aufzeichnungen und Datenbankanwendungen nicht länger benötigt werden, muss die verantwortliche Stelle den zuständigen ICT-Beauftragten mit der dauerhaften Löschung beauftragen.

4. Verschwiegenheitspflicht und Mitarbeiterverhalten

Die Verschwiegenheitspflicht ist eines der wichtigsten Elemente der Sicherheit von personenbezogenen Daten. Die Verschwiegenheitspflicht bedeutet:

- dass alle Mitarbeiter und externen Berater Verschwiegenheits- und Vertraulichkeitsvereinbarungen als Teil ihrer Dienst-/Beraterverträge unterzeichnen. Diese Anforderung korreliert mit der Anforderung, dass Mitarbeiter Daten nur gemäß den Anweisungen der verantwortlichen Stelle verarbeiten dürfen;
- alle externen Auftragsverarbeiter sind vertraglich durch Vertraulichkeitsklauseln gebunden. Diese Anforderung korreliert mit der Anforderung, dass der Auftragsverarbeiter Daten nur gemäß den Anweisungen der verantwortlichen Stelle verarbeiten darf;
- die strenge Einhaltung der Typologie für den Umgang mit Informationen auf Grundlage des Vertraulichkeitsstatus; und
- sicherzustellen, dass alle Forderungen von betroffenen Personen, ihre personenbezogenen Daten auf eine bestimmte Weise zu verarbeiten und insbesondere diese vertraulich zu behandeln und nicht an Dritte weiterzugeben, in der Akte der betroffenen Person genau verzeichnet werden.

Um das Risiko von Sicherheitslücken zu minimieren, dürfen nur befugte Mitarbeiter mit der Erfassung und dem Management von Daten aus vertraulichen Quellen beauftragt werden und gemäß der Typologie für den Umgang mit Informationen Zugriff auf Dokumente haben;

Die Mitarbeiter sind für die Festlegung der Vertraulichkeitsstandards der Daten verantwortlich, die sie auf der Grundlage der geltenden Typologie für den Umgang mit Informationen bearbeiten, sowie für die Wahrung der Vertraulichkeit der Daten, die sie für externe Verarbeitungszwecke aufrufen, übermitteln oder nutzen.

Mitarbeiter, die für Daten ursprünglich einen Vertraulichkeitsstandard festgelegt haben, können diesen jederzeit ändern, insbesondere ihnen einen geringeren Vertraulichkeitsstandard als den ursprünglich angegebenen zuweisen, wenn sie der Meinung sind, dass diese Daten weniger schutzwürdig sind.

5. Notfallplanung

Die verantwortliche Stelle ist für die Erstellung und Umsetzung eines Plans zur Evakuierung der Aufzeichnungen im Notfall verantwortlich.

6. Vernichtungsmethoden

Wenn festgestellt wird, dass die Aufbewahrung von personenbezogenen Daten nicht länger erforderlich ist, müssen alle Aufzeichnungen und Sicherungen vernichtet oder anonymisiert werden.
Die Vernichtungsmethode ist unter anderem abhängig von:

- der Art und Sensibilität der personenbezogenen Daten;
- dem Format oder Speichermedium; und
- dem Umfang der Aufzeichnungen in elektronischer oder Papierform.

Der Verantwortliche sollte vor der Vernichtung eine Bewertung der Sensibilität vornehmen, um sicherzustellen, dass geeignete Methoden zur Vernichtung der personenbezogenen Dateien eingesetzt werden.

Vernichtung von Aufzeichnungen in Papierform
Aufzeichnungen in Papierform werden durch Shreddern oder Verbrennen vernichtet, da dadurch gewährleistet ist, die diese in der Zukunft nicht wiederverwendet oder wiederhergestellt werden können.
Wenn entschieden wird, dass Aufzeichnungen in Papierform digitalisiert werden, müssen nach einer genauen Konvertierung in ein elektronisches Format alle Hinweise auf die Aufzeichnungen in Papierform vernichtet werden, sofern die Aufbewahrung der Aufzeichnungen in Papierform nicht durch geltendes Recht vorgeschrieben wird oder eine Kopie in Papierform zu Archivierungszwecken aufbewahrt werden muss.

Vernichtung von elektronischen Aufzeichnungen
Die Vernichtung elektronischer Aufzeichnungen muss dem zuständigen ICT-Beauftragten aufgetragen werden, da die Löschung von den Computersystemen nicht notwendigerweise eine vollständige Entfernung gewährleistet.

Auf Anweisung müssen die zuständigen ICT-Mitarbeiter sicherstellen, dass alle Spuren personenbezogener Daten vollständig von den Computersystemen und anderer Software entfernt werden.

Diskettenlaufwerke und Datenbankanwendungen müssen bereinigt werden; alle wiederbeschreibbaren Medien, wie unter anderem CDs, DVDs, Mikrofiche, Video- und Audiobänder, die zur Speicherung von personenbezogenen Daten verwendet werden, müssen vor ihrer Wiederverwendung gelöscht werden. Physische Maßnahmen zur Vernichtung elektronischer Aufzeichnungen wie Wiederverwertung, Pulverisierung oder Verbrennen müssen streng überwacht werden.

Beseitigungsnachweise

Die verantwortliche Stelle muss gewährleisten, dass alle relevanten Dienstverträge, MOU (gemeinsame Absichtserklärungen), Vereinbarungen und schriftlichen Übertragungs- oder Verarbeitungsverträge eine Aufbewahrungsfrist für die Vernichtung von personenbezogenen Daten nach der Erfüllung des angegebenen Zwecks beinhalten. Dritte müssen der verantwortlichen Stelle die personenbezogenen Daten zurückgeben und bestätigen, dass alle Kopien derselben, einschließlich jener personenbezogenen Daten, die gegenüber ihren bevollmächtigen Vertretern offengelegt wurden, vernichtet wurden. Es müssen Beseitigungsnachweise aufbewahrt und den Projekt- oder Evaluierungsberichten beigefügt werden, die die Zeit und Methode der Vernichtung angeben.

Die Vernichtung von umfangreichen Aufzeichnungen in Papierform darf an darauf spezialisierte Unternehmen ausgelagert werden. In diesem Fall muss die verantwortliche Stelle gewährleisten, dass die Vertraulichkeit der personenbezogenen Daten schriftlich zugesichert wird; die Vorlage der Beseitigungs- und Vernichtungsbestätigungen stellt einen Teil der vertraglichen Pflichten von Dritten dar.

7. Sonstige Maßnahmen

Die Datensicherheit erfordert auch angemessene Vorschriften innerhalb der Organisation, wie regelmäßige interne Verbreitung der Datensicherheitsvorschriften und der Pflichten aller Mitarbeiter aus dem Datenschutzgesetz, insbesondere im Hinblick auf die Vertraulichkeitspflicht.

Ernennung eines Sicherheitsbeauftragten

Jede verantwortliche Stelle muss einen oder mehrere Mitarbeiter (wenn möglich Verwaltung/IT) zu Sicherheitsbeauftragten ernennen und mit der Wahrnehmung von Sicherheitsaufgaben beauftragen.

Der Sicherheitsbeauftragte muss insbesondere:

- gewährleisten, dass alle in diesem CoC und den geltenden Sicherheitsvorschriften vorgeschriebenen Sicherheitsverfahren eingehalten werden;

- diese Verfahren auf dem neuesten Stand halten und bei Bedarf aktualisieren;
- weitere Personalschulungen über Datensicherheit abhalten.

Anhang 5: Bereitzustellende Informationen

Bereitzustellende Informationen:	**Einwilligung**	**Lebenswichtiges Interesse/ Öffentliches Interesse**	**Berechtigtes Interesse**	**Vertragliche/Rechtliche Verpflichtung**
Verantwortliche Stelle / zuständige Mitarbeiter	Ja	Ja	Ja	Ja
Verarbeitungszweck	Ja	Ja	Ja	Ja
Geplante externe Auftragsverarbeiter	Ja	DSFA und, sofern möglich, Datenweitergabe	Ja	Ja
Geplante Übermittlungen	Ja	DSFA und, sofern möglich, Datenweitergabe	Ja	Ja
Rechte der betroffenen Person (auf Information, Auskunft, Berichtigung, Löschung, Widerspruch)	Ja	DSFA und, sofern möglich, Datenweitergabe	Ja	Ja
Falls zutreffend, ob die Information gesetzlich/vertraglich vorgeschrieben ist	Nicht zutreffend	Nicht zutreffend	Ja	Ja

Anhang 6: Kurzer Leitfaden zur DSFA

Der Zweck einer Datenschutz-Folgenabschätzung (DSFA) ist die Feststellung, Bewertung und Adressierung der konkreten Risiken für personenbezogene Daten, die sich aus den Suchdiensttätigkeiten ergeben. Eine DSFA sollte Maßnahmen zur Vermeidung, Minimierung oder sonstigen Minderung von Risiken zum Ergebnis haben. Dieser Leitfaden zur DSFA soll Mitarbeiter in die Lage versetzen, selbst eine DSFA vorzunehmen. **Für die Nationalen Gesellschaften steht ein DSFA-Vorlage für Suchdiensttätigkeiten als gesondertes Dokument zur Verfügung**, das Beispiele für die Risikoarten und mögliche Risikominderungsmaßnahmen enthält.

Hier werden Bespiele angegeben, wann Sie die Durchführung einer DSFA erwägen sollten.

- Ihre Organisation speichert ihre Akten auf CDs und in Papierform. Sie möchten nun eine zentrale elektronische Speicherung der Akten einführen. Wie entscheiden Sie, welche Informationen am besten wo gespeichert werden?
- Ein Tsunami spült dutzende Küstendörfer fort. Tausende Menschen werden als vermisst gemeldet. Wie viele personenbezogene Informationen müssen Sie von den Familien der vermissten Personen erfassen? Ein Minimum oder ein Maximum? Sollten auch sensible Informationen (z. B. DNA, Religion, politische Zugehörigkeit) erfasst werden?
- Die Regierung richtet ein System zur Zentralisierung aller Informationen über durch den Tsunami vermisste Personen ein. Sie bittet Sie, alle Informationen zur Verfügung zu stellen, die Sie über die im Zuge dieses Ereignisses vermissten Personen haben. Wie viele personenbezogene Daten dürfen an die Regierung für die Suche nach vermissten Personen weitergegeben werden? Unter welchen Voraussetzungen müssen personenbezogene Daten gegenüber der Regierung offengelegt werden?
- Eine andere humanitäre Organisation bittet Sie um die Herausgabe von Daten über in einem Flüchtlingslager lebende Personen. Sollten/dürfen Sie diese Daten weitergeben? Unter welchen Voraussetzungen? Welche Folgen hat die Weitergabe dieser Daten? Wird diese Organisation mit diesen personenbezogenen Daten genauso sorgfältig umgehen wie Sie?
- Dürfen Sie Bilder unbegleiteter Kinder bei der Suche nach Verwandten im Internet veröffentlichen? Dürfen Sie Poster mit vermissten Kindern einsetzen? Unter welchen Umständen und Voraussetzungen?
- Ein soziales Netzwerk bietet Ihnen an, Sie bei der Vermisstensuche nach einer Katastrophe zu unterstützen. Wie können Sie mit diesem sozialen Netzwerk zusammenarbeiten, ohne die Sicherheit der personenbezogenen Daten und der betroffenen Menschen zu gefährden?
- Morgen plant das IKRK den Besuch einer Haftanstalt, in der sich angeblich eine gesuchte Person aufhält. Dürfen Sie in Anbetracht der Dringlichkeit per E-Mail eine Suchanfrage oder eine Rotkreuz-Familiennachricht an das IKRK übermitteln?

Manchmal fehlt die Zeit, um eine umfassende DSFA durchzuführen oder die Komplexität, Sensibilität und der Umfang des Verarbeitungsvorgangs erfordern keine formelle DSFA. Suchdienstmitarbeiter sollten jedoch immer an eine Risikobewertung im Hinblick auf den Datenschutz denken (und diese nach Möglichkeit aufzeichnen), wenn Sie Entscheidungen über die Übertragung von Daten treffen.

Daher sollten Suchdienstmitarbeiter und Ehrenamtliche mit dem DSFA-Verfahren vertraut sein und die nachstehenden Fragen berücksichtigen.

Ein DSFA-**Verfahren** gliedert sich üblicherweise in folgende Schritte: Diese Schritte müssen im DSFA-Bericht abgebildet sein:

A. Problembestimmung *(Scoping)*

1. Auf der Grundlage der Komplexität, Sensibilität und des Umfangs des Verarbeitungsvorgangs, stellen Sie fest:

- ob eine DSFA notwendig ist;
- wer die DSFA durchführen wird;
- wer die DSFA überprüfen und validieren wird.

2. Beschreiben Sie, wie im Kontext der fraglichen Suchdiensttätigkeit Daten erfasst, genutzt, gespeichert und weitergegeben werden. Das beinhaltet einen Überblick über die Stakeholder sowie eine Beschreibung der Informationsflüsse (d. h. welche Informationen erfasst werden, über wen, durch wen; wie diese Informationen genutzt werden; wie, wo und wie lange sie gespeichert werden; werden Auftragsverarbeiter eingesetzt, die Zugriff auf diese Informationen haben?)

3. Bestimmung der Stakeholder, die zu befragen sind. Das könnten interne Stakeholder sein (wie IT-Experte, Rechtsberater, Psychologe, Programmexperten...) oder externe Stakeholder (wie andere Organisationen, Behörden, Sozialarbeiter, führende Gemeindevertreter, gesetzliche Vormünder...).

B. Bewertung

4. Definieren Sie die Risiken, die sich für Personen aus dem Verarbeitungsvorgang und dem Risiko der Nichteinhaltung der Datenschutz-Verhaltensregeln ergeben.

5. Bewerten Sie die Risiken.

6. Legen Sie Maßnahmen zur Vermeidung, Minimierung oder sonstigen Minderung der Risiken fest.

7. Sprechen Sie Empfehlungen aus.

C. Validierung und Umsetzung

8. Überprüfen lassen und Validierung einholen.

9. Umsetzung der vereinbarten Empfehlungen.

10. Aktualisierung der DSFA, wenn sich die Tätigkeit ändert

Wenn eine DSFA durchgeführt wird, sollte dies in einem Bericht (der die unter A), B) und C) oben beschriebenen Informationen enthalten sollte) erwähnt werden. Legt man Komplexität, Sensibilität und Umfang des Verarbeitungsvorgangs zugrunde, kann ein DSFA-**Bericht** (das Ergebnis eines DSFA-Verfahrens) sehr kurz sein oder auch umfangreicher und mehr Einzelheiten enthalten. Ein DSFA-

Bericht kann unter Verwendung der den Nationalen Gesellschaften gesondert zur Verfügung stehenden Vorlage verfasst werden.

Anhang 7: Erfüllung einer rechtlichen Verpflichtung

Kann in Abhängigkeit der Situation der verantwortlichen Stelle erforderlich sein

- Einhaltung des nationalen oder internationalen Rechts, beispielsweise in den Bereichen Arbeitsrecht, Rechnungslegung, Betrug, Geldwäsche
- Gerichtliche Anordnungen