

# **WELTWEITE PRINZIPIEN ZUR NATIONALEN SICHERHEIT UND DEM RECHT AUF INFORMATIONEN („DIE TSHWANE PRINZIPIEN“)**

vollendet in Tshwane, Südafrika  
veröffentlicht am 12. Juni 2013

## **EINLEITUNG**

Diese Prinzipien wurden entwickelt, um Leitlinien für jene zur Verfügung zu stellen, die am Verfassen, Überarbeiten und Umsetzen solcher Gesetze oder Bestimmungen beteiligt sind, die mit der Befugnis des Staates in Verbindung stehen, Informationen aus Gründen der nationalen Sicherheit zurückzuhalten oder die Offenlegung solcher Informationen zu bestrafen.

Sie basieren auf internationalem (einschließlich regionalem) und nationalem Recht, Standards, bewährter Praktiken und den Abhandlungen von Experten.

Sie befassen sich mit der nationalen Sicherheit – und nicht so sehr mit anderen Gründen für das Zurückhalten von Informationen. Alle anderen Gemeinwohlgründe für Zugangsbeschränkungen sollten mindestens diesen Standards entsprechen.

Diese Prinzipien wurden von 22 Organisationen und wissenschaftlichen Zentren (im Anhang aufgeführt) verfasst. Dies geschah in Abstimmung mit mehr als 500 Experten aus mehr als 70 Ländern bei 14 Treffen, die weltweit abgehalten wurden mit Unterstützung der Open Society Justice Initiative und in Abstimmung mit den vier Sonderberichterstattern für Meinungsfreiheit und/oder Medienfreiheit und dem Sonderberichterstatter für Terrorismusbekämpfung und der Menschenrechte:

- dem Sonderberichterstatter der Vereinten Nationen (UN) für Meinungs- und Redefreiheit,
- dem Sonderberichterstatter der Vereinten Nationen (UN) für Terrorismusbekämpfung und Menschenrechte,
- dem Sonderberichterstatter der Afrikanischen Kommission der Menschenrechte und der Rechte der Völker (ACHPR) für Meinungsfreiheit und Informationszugang,
- dem Sonderberichterstatter der Organisation Amerikanischer Staaten (OAS) für Meinungsfreiheit und
- den Beauftragten der Organisation für Sicherheit und Zusammenarbeit in Europa (OSCE) für die Medienfreiheit

## **HINTERGRUND UND MOTIVATION**

Die nationale Sicherheit und die Informationsfreiheit werden häufig als entgegengesetzt wirkende Kräfte wahrgenommen. Zuweilen kommt es zu Spannungen zwischen dem Bedürfnis einer Regierung, Informationen aus Gründen der nationalen Sicherheit geheim

zu halten, und dem Recht der Öffentlichkeit auf Zugang zu Informationen, über welche die Behörden verfügen. Ein unverstellter Blick auf die jüngste Vergangenheit legt jedoch nahe, dass legitime Interessen der öffentlichen Sicherheit in der Praxis am besten gewahrt werden, wenn die Öffentlichkeit über die Aktivitäten des Staates umfassend informiert ist, einschließlich jener Aktivitäten, die zum Schutz der nationalen Sicherheit durchgeführt werden.

Zugang zu Informationen schützt dadurch, dass der Öffentlichkeit das Überprüfen staatlicher Handlungen ermöglicht wird, nicht nur vor dem Missbrauch durch Beamte, sondern erlaubt es der Öffentlichkeit zugleich, eine Rolle bei der Festlegung der Politik des Staates zu spielen, und stellt damit eine entscheidende Komponente wohlverstandener nationaler Sicherheit, demokratischer Partizipation und fundierter politischer Arbeit dar. Um die umfassende Ausübung der Menschenrechte zu sichern, mag es unter bestimmten Umständen notwendig sein, Informationen geheim zu halten, um legitime nationale Sicherheitsinteressen zu schützen.

Die richtige Balance zu finden, ist noch herausfordernder aufgrund der Tatsache, dass in vielen Staaten die Gerichte die geringste Unabhängigkeit und die größte Bereitschaft zur Fügsamkeit gegenüber den Forderungen der Regierung zeigen, sobald sich diese auf die nationale Sicherheit beruft. Diese Fügsamkeit wird verstärkt durch Bestimmungen in den Sicherheitsgesetzen vieler Staaten, die Ausnahmen vom Recht auf Informationszugang, von den generellen Beweisregeln und von den Rechten der Angeklagten schon dann auslösen, wenn seitens der Regierung ein minimales Indiz oder auch nur die bloße Behauptung eines Risikos für die nationale Sicherheit vorgebracht wird. Die überzogene Geltendmachung von Bedenken aufgrund der nationalen Sicherheit kann die wichtigsten institutionellen Sicherungsmaßnahmen gegen Missbrauch durch die Regierung ernsthaft untergraben: die Unabhängigkeit der Gerichte, die Rechtsstaatlichkeit, die Aufsicht durch die Legislative, die Medienfreiheit und Open Government.

Diese Prinzipien sind eine Reaktion auf die oben beschriebenen seit langem bestehenden Herausforderungen sowie auf die Tatsache, dass in den letzten Jahren eine signifikante Anzahl an Staaten weltweit angefangen haben, Systeme zur Einstufung von Geheimnissen und damit in Zusammenhang stehenden Gesetze zu verabschieden oder zu überarbeiten. Dieser Trend wiederum wurde durch zahlreiche Entwicklungen entfacht. Vielleicht am wichtigsten war die rasche Verabschiedung von Gesetzen zur Informationsfreiheit seit dem Fall der Berliner Mauer, mit dem Ergebnis, dass zum Zeitpunkt der Veröffentlichung dieser Prinzipien mehr als 5,2 Milliarden Menschen in 95 Ländern weltweit das Recht auf Informationsfreiheit genießen können – zumindest laut Gesetz, wenn nicht bereits in der Praxis. Menschen in diesen Ländern setzen sich – häufig erstmals – mit der Frage auseinander, ob und unter welchen Umständen Informationen geheim gehalten werden können. Andere Entwicklungen, die zu einem Zuwachs an Vorschlägen für Geheimhaltungsregelungen beigetragen haben, waren die Reaktionen der Regierungen auf Terrorismus oder terroristische Bedrohungen und das Interesse, die Geheimhaltung im Rahmen des demokratischen Übergangs gesetzlich zu regeln.

# WELTWEITE PRINZIPIEN ZUR NATIONALEN SICHERHEIT UND DEM RECHT AUF INFORMATIONEN

(„DIE TSHWANE PRINZIPIEN“)

vollendet in Tshwane, Südafrika  
veröffentlicht am 12. Juni 2013

Einleitung .....	i
Hintergrund und Motivation .....	i
Präambel .....	1
Definitionen .....	4
Teil I: Allgemeine Prinzipien .....	6
Teil II: Informationen, die aus Gründen nationaler Sicherheit zurückgehalten werden dürfen und Informationen, die offengelegt werden sollten .....	11
Teil III.A: Regeln für die Einstufung von Informationen als geheim und für die Aufhebung dieser Einstufung .....	19
Teil III.B: Regeln zur Bearbeitung von informationsanfragen .....	23
Teil IV: Justizielle Aspekte von nationaler Sicherheit und dem Recht auf Informationszugang .....	26
Teil V: Stellen, die den Sicherheitssektor beaufsichtigen .....	29
Teil VI: Offenlegung durch öffentliche Beschäftigte im öffentlichen Interesse .....	32
Teil VII: Grenzen für Maßnahmen zur Sanktionierung oder Begrenzung von Offenlegungen gegenüber der Öffentlichkeit .....	38
Teil VIII: Abschließendes Prinzip .....	41

## PRÄAMBEL

Die Organisationen und Einzelpersonen, die an der Ausarbeitung der vorliegenden Grundsätze beteiligt waren:

*Erinnern daran*, dass der Zugang zu Informationen, über die der Staat verfügt, ein Recht eines jedes Menschen ist, und dass dieses Recht daher durch Gesetze geschützt werden sollte, die genau und mit eng gezogenen Ausnahmen formuliert sein sollten, und deren Einhaltung durch unabhängige Gerichte, parlamentarische Kontrollgremien und andere unabhängige Institutionen überwacht werden sollte;

*Erkennen an*, dass Staaten ein berechtigtes Interesse an der Zurückhaltung bestimmter Informationen, unter anderem aus Gründen der nationalen Sicherheit, haben können, und betonen, dass die richtige Balance zwischen der Offenlegung und Vorenthaltung von Informationen für eine demokratische Gesellschaft lebenswichtig ist und entscheidend ist für ihre Sicherheit, ihren Fortschritt, ihre Entwicklung und ihr Wohlergehen sowie für den uneingeschränkten Genuss der Menschenrechte und Grundfreiheiten;

*Bekräftigen*, dass es, wenn die Menschen in der Lage sein sollen, das Verhalten ihrer Regierung zu überwachen und in vollem Umfang an einer demokratischen Gesellschaft teilzunehmen, notwendig ist, dass sie Zugang zu den Informationen haben, über welche die öffentlichen Stellen verfügen, einschließlich jener Informationen, welche die nationale Sicherheit betreffen;

*Weisen darauf hin*, dass diese Prinzipien auf internationalem Recht und auf Standards zum Recht der Öffentlichkeit auf Zugang zu den bei öffentlichen Stellen verfügbaren Informationen und auf anderen Menschenrechten, auf einer sich weiterentwickelnden Staatenpraxis (wie sie sich unter anderem in Urteilen internationaler und nationaler Gerichte widerspiegelt), auf den von der Gemeinschaft der Nationen anerkannten allgemeinen Rechtsgrundsätzen und auf den Abhandlungen von Experten beruhen;

*Berücksichtigen* dabei die einschlägigen Bestimmungen der Allgemeinen Erklärung der Menschenrechte, des Internationalen Pakts über bürgerliche und politische Rechte, der Afrikanischen Charta der Menschenrechte und Rechte der Völker, der amerikanischen Menschenrechtskonvention, der Europäischen Konvention zum Schutze der Menschenrechte und der [Konvention des Europarats über den Zugang zu amtlichen Dokumenten](#);

*Berücksichtigen* dabei darüber hinaus die [Erklärung von Prinzipien der Freiheit der Meinungsäußerung der Inter-Amerikanischen Kommission für Menschenrechte](#); [das Inter-Amerikanische-Modellgesetz über den Zugang zu Informationen](#), die [Erklärung von Prinzipien der Freiheit der Meinungsäußerung in Afrika](#), und das [Modellgesetz über den Zugang zu Informationen für Afrika](#);

*Erinnern an* die [Gemeinsame Erklärung](#) des UN-Sonderberichterstatters für Meinungsfreiheit, des OSZE-Beauftragten für die Freiheit der Medien und des Sonderberichterstatters für Meinungsfreiheit der Inter-Amerikanischen Kommission für Menschenrechte von [2004](#); die Gemeinsamen Erklärungen jener drei Experten sowie des Sonderberichterstatters für Meinungs- und Informationsfreiheit der Afrikanischen Kommission für Menschenrechte und die Rechte der Völker von [2006](#), [2008](#), [2009](#) und [2010](#); die [Gemeinsame Erklärung der UN und der Inter-Amerikanischen Sonderberichterstatter zu WikiLeaks vom Dezember 2010](#); und den [Bericht über Maßnahmen zur Terrorismusbekämpfung und Menschenrechte](#), der von der Venedig-Kommission im Jahr 2010 verabschiedet wurde;

*Erinnern außerdem an* die [Johannesburg-Prinzipien zur Nationalen Sicherheit, Meinungsfreiheit und Zugang zu Informationen](#), die von einer Gruppe von Experten auf Einladung von „Artikel 19“ im Jahr 1995 beschlossen wurden und an die [Prinzipien der Kontrolle und Rechenschaftspflicht von Sicherheitsinstitutionen in einer konstitutionellen Demokratie](#), die im Jahr 1997 durch das Center for National Security Studies (CNSS) und die polnische Helsinki-Stiftung für Menschenrechte erarbeitet wurden;

*Weisen darauf hin*, dass es internationale Prinzipien gibt – wie jene, die enthalten sind im [Modellgesetz über den Zugang zu Informationen in Afrika](#), den [UN-Leitprinzipien für Wirtschaft und Menschenrechte](#) ("Ruggie Principles"), dem [Vertrag über den](#)

[Waffenhandel](#), den [OECD-Leitsätzen für multinationale Unternehmen](#) und im [Montreux-Dokument über die einschlägigen völkerrechtlichen Verpflichtungen und guten Praktiken von Staaten im Hinblick auf die Tätigkeit von privaten Militär- und Sicherheitsunternehmen während eines bewaffneten Konflikts](#) – welche die entscheidende Bedeutung des Zugangs zu Informationen von oder im Bezug auf geschäftliche Unternehmen unter bestimmten Umständen anerkennen, und von denen einige explizit die Notwendigkeit ansprechen, dass private Militär- und Sicherheitsunternehmen, die innerhalb des nationalen Sicherheitssektors tätig sind, bestimmte Informationen veröffentlichen;

*Stellen fest*, dass diese Prinzipien die materiellen Standards für die Sammlung nachrichtendienstlicher Informationen, das Management persönlicher Daten und den Austausch nachrichtendienstlicher Erkenntnisse nicht ansprechen; jene Aspekte werden behandelt in den ["good practices on legal and institutional frameworks for intelligence services and their oversight"](#), welche im Jahr 2010 auf Anfrage des UN-Menschenrechtsrats von Martin Scheinin veröffentlicht wurden, der zu jener Zeit der UN-Sonderberichterstatter für die Förderung und den Schutz der Menschenrechte und Grundfreiheiten bei der Bekämpfung des Terrorismus war;

*Erkennen* die Bedeutung eines wirksamen Austausches von Geheimdienstinformationen zwischen den Staaten, wie er durch die Resolution 1373 des UN-Sicherheitsrates gefordert wird, an;

*Erkennen weiterhin an*, dass Einschränkungen öffentlicher und unabhängiger Kontrolle, die im Namen der nationalen Sicherheit geschaffen werden, das Risiko erhöhen, dass illegales, korruptes und betrügerisches Verhalten auftritt und nicht aufgedeckt wird, und dass Verletzungen der Privatsphäre und anderer Rechte des Einzelnen häufig unter dem Deckmantel der Geheimhaltung zum Schutz der nationalen Sicherheit stattfinden;

*Sind besorgt* über die Kosten für die nationale Sicherheit, die durch überzogene Geheimhaltung, einschließlich der Beeinträchtigung des Informationsaustausches zwischen Behörden und zwischen Verbündeten entstehen, über die Unfähigkeit, legitime Geheimnisse zu schützen, über die Unfähigkeit, wichtige Informationen inmitten ungeordneter Daten zu finden, über wiederholtes Sammeln von Informationen durch verschiedene Institutionen und über die Überlastung der Sicherheits-Manager;

*Betonen*, dass die Prinzipien sich auf das Recht der Öffentlichkeit auf Informationsfreiheit konzentrieren, und dass sie die Informationsrechte von Gefangenen, von Opfern von Menschenrechtsverletzungen und von anderen Personen mit erhöhten Ansprüchen auf Informationszugang nur in dem Maße ansprechen, wie diese Rechte mit dem Recht der Öffentlichkeit auf Informationsfreiheit in engem Zusammenhang stehen;

*Erkennen an*, dass bestimmte Informationen, die nicht aus Gründen der nationalen Sicherheit zurückgehalten werden sollten, möglicherweise dennoch aus verschiedenen anderen, im internationalen Recht anerkannten Gründen zurückgehalten werden dürfen – einschließlich z. B. aufgrund der internationalen Beziehungen, der Fairness von Gerichtsverfahren, der Rechte von Prozessparteien und aus Gründen des Datenschutzes –

dies immer unter Geltung des Prinzips, dass Informationen nur dann zurückgehalten werden dürfen, wenn das öffentliche Interesse an der Geheimhaltung das öffentliche Interesse am Zugang zu jenen Informationen eindeutig überwiegt;

*Streben an*, einen praktischen Leitfaden anzubieten für die Exekutive, die Legislative und Regulierungsstellen, Behörden, Verfasser von Gesetzesentwürfen, die Gerichte, andere Aufsichtsstellen und die Zivilgesellschaft zu einigen der größten Herausforderungen an den Schnittstellen von nationaler Sicherheit und Informationsfreiheit, vor allem jenen, die die Achtung der Menschenrechte und der demokratischen Rechenschaftspflicht betreffen;

*Sind bestrebt*, Prinzipien auszuarbeiten, die von universeller Aussagekraft und Anwendbarkeit sind;

*Erkennen an*, dass die Staaten bei der Abwägung zwischen dem öffentlichen Interesse an der Offenlegung und der Notwendigkeit der Geheimhaltung zum Schutz legitimer nationaler Sicherheitsinteressen vor sehr unterschiedlichen Herausforderungen stehen, und dass, während die Prinzipien universell sind, deren Anwendung in der Praxis auf die örtlichen Gegebenheiten, einschließlich der vielfältigen Rechtsordnungen abgestimmt werden kann;

*Empfehlen*, dass die entsprechenden Stellen auf nationaler, regionaler und internationaler Ebene Schritte unternehmen, um diese Prinzipien zu verbreiten und zu diskutieren, und um sie soweit wie möglich zu unterstützen, zu übernehmen und/oder umzusetzen mit der Zielrichtung, fortschreitend die umfassende Verwirklichung des Rechts auf Informationsfreiheit, wie dieses in Prinzip 1 dargelegt wird, zu erreichen.

## DEFINITIONEN

In diesen Prinzipien bedeutet, soweit der Zusammenhang nichts anderes erfordert:

**"Wirtschaftsunternehmen im nationalen Sicherheitssektor"** eine juristische Person, die Handel oder andere Geschäftstätigkeiten im nationalen Sicherheitssektor ausübt oder ausgeübt hat, jedoch nur insoweit, als sie in dieser Funktion tätig wurde, entweder als Auftragnehmer oder als Anbieter von Dienstleistungen, Einrichtungen, Personal oder Produkten einschließlich, aber nicht beschränkt auf Waffen, Ausrüstung oder geheimdienstliche Tätigkeiten. Dazu gehören private Militär- und Sicherheitsunternehmen (PMSCs). Juristische Personen, die als nicht gewinnorientiert oder als Nicht-Regierungsorganisationen organisiert sind, sind hiervon nicht umfasst.

**"Unabhängig"** bedeutet institutionell, finanziell und operativ frei von dem Einfluss, den Vorgaben oder der Kontrolle der Exekutive, einschließlich aller Behörden des Sicherheitssektors zu sein.

**"Information"** ist jedes Original und jede Kopie dokumentarischen Materials unabhängig von dessen physikalischen Eigenschaften, und jedes andere materielle oder immaterielle Material, unabhängig von der Form oder dem Medium, in der bzw. dem es vorgehalten wird. Dies beinhaltet, ist aber nicht beschränkt auf: Aufzeichnungen, Schriftwechsel,

Fakten, Meinungen, Ratschläge, Denkschriften, Daten, Statistiken, Bücher, Zeichnungen, Pläne, Landkarten, Diagramme, Fotografien, Tonaufzeichnungen oder visuelle Aufzeichnungen, Dokumente, E-Mails, Logbücher, Muster, Modelle und in jeglichem elektronischen Format vorgehaltene Daten.

**"Informationen von öffentlichem Interesse"** bezieht sich auf Informationen, die von Bedeutung oder Nutzen für die Öffentlichkeit, nicht lediglich im Interesse Einzelner sind, und deren Offenlegung "im Interesse der Öffentlichkeit" ist, zum Beispiel, weil sie für das Verständnis des Handelns der Exekutive nützlich sind.

**"Legitimes nationalen Sicherheitsinteresse"** bezieht sich auf Interessen, deren eigentlicher Zweck und deren primäre Wirkung der Schutz der nationalen Sicherheit ist, im Einklang mit internationalem und nationalem Recht. (Kategorien von Informationen, deren Zurückhaltung zum Schutze eines legitimen nationalen Sicherheitsinteresses notwendig sein kann, werden in Prinzip 9 dargelegt). Ein nationales Sicherheitsinteresse ist nicht legitim, wenn sein eigentlicher Zweck oder seine primäre Wirkung ist, ein Interesse zu schützen, welches keinen Zusammenhang mit der nationalen Sicherheit aufweist, wie z.B.: den Schutz der Regierung oder von Beamten vor Unannehmlichkeiten oder vor der Aufdeckung von Fehlverhalten; die Verheimlichung von Informationen über Menschenrechtsverletzungen, jede andere Verletzung der Gesetze oder die Funktionsfähigkeit öffentlicher Institutionen; die Stärkung oder Perpetuierung von bestimmten politischen Interessen, Parteien oder Ideologien; oder die Unterdrückung rechtmäßiger Proteste.

**"Nationale Sicherheit"** wird in diesen Prinzipien nicht definiert. Prinzip 2 enthält eine Empfehlung, dass "nationale Sicherheit" im nationalen Recht präzise definiert werden sollte, in einer Weise, die in Einklang mit den Bedürfnissen einer demokratischen Gesellschaft steht.

**"Öffentliche Stellen"** sind alle Stellen innerhalb der Exekutive, Legislative und Judikative auf allen staatlichen Ebenen, durch Verfassung oder Gesetze geschaffene Behörden einschließlich der Sicherheitsorgane; und ebenso nicht-staatliche Stellen, die im Eigentum des Staates oder unter dessen Kontrolle stehen oder die als Vertreter des Staates agieren. "Öffentliche Stellen" umfasst auch private oder andere Einrichtungen, die öffentliche Aufgaben erfüllen oder öffentliche Dienstleistungen erbringen oder mittels erheblicher öffentlicher Mittel oder Förderungen agieren, dies jedoch nur in Bezug auf diese Aufgaben, Dienstleistungen oder auf öffentlich finanzierte oder geförderte Tätigkeiten.

**"Öffentlicher Beschäftigter"** oder **"Beamter"** bezieht sich auf aktuelle und ehemalige Beschäftigte des öffentlichen Dienstes, Auftragnehmer und Subunternehmer von öffentlichen Stellen, einschließlich des Sicherheitssektors. "Öffentlicher Beschäftigter" oder "Beamter" umfasst auch Personen, die bei nicht-staatlichen Einrichtungen beschäftigt sind, soweit diese im Eigentum oder unter der Kontrolle des Staates stehen oder als Vertreter des Staates tätig sind; ebenso Mitarbeiter von privaten oder anderen Einrichtungen, die öffentliche Aufgaben oder Dienstleistungen erbringen oder mittels erheblicher öffentlicher

Mittel oder Förderungen agieren, dies jedoch nur in Bezug auf diese Aufgaben, Dienstleistungen oder auf öffentlich finanzierte oder geförderte Tätigkeiten.

**"Sanktion"**, bezieht sich, wo es als Nomen verwendet wird, auf jede Form von Strafe oder Nachteil, einschließlich straf-, zivil- und verwaltungsrechtlicher Maßnahmen. Als Verb verwendet bedeutet "sanktionieren", dass solche Strafen oder Nachteile vollzogen werden.

**"Sicherheitssektor"** wird dahingehend definiert, dass er umfasst: (i) Anbieter von Sicherheit, einschließlich, aber nicht beschränkt auf die Streitkräfte, die Polizei und andere Verfolgungsbehörden, paramilitärische Kräfte und Geheim- und Sicherheitsdienste (sowohl militärische als auch zivile) und (ii) alle exekutiven Stellen, Abteilungen und Ministerien, die für die Koordination, Steuerung und Überwachung von Sicherheitsanbietern verantwortlich sind.

## **TEIL I: ALLGEMEINE PRINZIPIEN**

### **Prinzip 1: Recht auf Informationszugang**

- (a) Jeder hat das Recht Informationen zu suchen, zu empfangen, zu verwenden und weiterzugeben, die durch oder im Namen von öffentlichen Stellen vorgehalten werden, oder hinsichtlich derer öffentliche Stellen kraft Gesetzes ein Recht auf Zugang haben.
- (b) Internationale Grundsätze erkennen auch an, dass Wirtschaftsunternehmen im nationalen Sicherheitssektor, einschließlich der privaten Militär- und Sicherheitsfirmen, die Verantwortung haben, Informationen offenzulegen in Bezug auf Situationen, Aktivitäten oder Verhaltensweisen, die aller Voraussicht nach einen Einfluss auf die Wahrnehmung der Menschenrechte haben können.
- (c) Diejenigen, die eine Verpflichtung zur Offenlegung von Informationen gemäß den Prinzipien 1(a) und 1(b) haben, müssen Informationen auf Anfrage zur Verfügung stellen, wobei nur begrenzte Ausnahmen bestehen, die gesetzlich bestimmt und notwendig sein müssen, um genau bezeichnete, feststellbare Schäden für legitime Interessen, einschließlich der nationalen Sicherheit, zu vermeiden.
- (d) Nur öffentlichen Stellen, zu deren spezifischen Aufgaben der Schutz der nationalen Sicherheit gehört, können sich auf die nationale Sicherheit als Grund für die Zurückhaltung von Informationen berufen.
- (e) Die Geltendmachung der nationalen Sicherheit zur Rechtfertigung einer Zurückhaltung von Informationen durch ein Wirtschaftsunternehmen bedarf der ausdrücklichen Ermächtigung oder Bestätigung durch eine mit dem Schutz der nationalen Sicherheit beauftragte öffentliche Stelle.

*Hinweis: Die Staatsgewalt, und nur diese, trägt die oberste Verantwortung für die nationale Sicherheit, und somit können nur staatliche Stellen geltend machen, dass die Informationen nicht freigegeben werden dürfen, wenn dies der nationalen Sicherheit schaden würde.*

- (f) Die öffentlichen Stellen haben auch eine ausdrückliche Verpflichtung, bestimmte Informationen von öffentlichem Interesse eigeninitiativ zu veröffentlichen.

## **Prinzip 2: Die Anwendung dieser Prinzipien**

- (a) Diese Prinzipien gelten für die Ausübung des Rechts auf Zugang zu Informationen, wie dies in Prinzip 1 beschrieben wurde, soweit staatliche Stellen feststellen oder bestätigen, dass die Freigabe solcher Informationen Schäden für die nationale Sicherheit verursachen könnte.
- (b) Da die nationale Sicherheit einer der gewichtigsten Gemeinwohlgründe für die Beschränkung des Informationszugangs ist, müssen öffentliche Stellen, wenn sie andere Gemeinwohlgründe für die Beschränkung des Zugangs geltend machen - einschließlich der internationalen Beziehungen, der öffentlichen Ordnung, der öffentlichen Gesundheit und Sicherheit, der Strafverfolgung, der Möglichkeit, in der Zukunft frei und offen beraten zu können, der effektiven Formulierung von Politik, und der wirtschaftlichen Interessen des Staates - zumindest den Standards für die Einschränkungen des Rechts auf Informationszugang genügen, die in diesen Prinzipien als relevant festgelegt sind.
- (c) Es ist eine gute Praxis, dass dort, wo die nationale Sicherheit benutzt wird, um das Recht auf Informationszugang zu beschränken, diese in der Rechtsordnung des Staates präzise und im Einklang mit einer demokratischen Gesellschaft definiert wird.

## **Prinzip 3: Anforderungen an Beschränkung der Informationsfreiheit aus Gründen der nationalen Sicherheit**

Eine Einschränkung des Rechts auf Informationsfreiheit aus Gründen der nationalen Sicherheit darf nur dann vorgenommen werden, wenn der Staat nachweisen kann, dass: (1) die Beschränkung (a) gesetzlich bestimmt ist und (b) in einer demokratischen Gesellschaft notwendig ist (c) zum Schutz eines legitimen Interesses der nationalen Sicherheit, und (2) das Gesetz angemessene Schutzvorkehrungen gegen Missbrauch beinhaltet, einschließlich einer umgehenden, umfassenden, zugänglichen und wirksamen Kontrolle der Gültigkeit der Beschränkung durch eine unabhängige Aufsichtsbehörde sowie einer vollständigen Überprüfung durch die Gerichte.

- (a) *Gesetzlich vorgeschrieben.* Das Gesetz muss zugänglich sein, eindeutig, eng und präzise formuliert sein, um dem Einzelnen zu ermöglichen zu verstehen, welche Informationen zurückbehalten werden dürfen, welche offengelegt werden sollten und welches Verhalten in Bezug auf die Informationen Sanktionen unterliegt.
- (b) *Notwendig in einer demokratischen Gesellschaft.*

- (i) Die Offenlegung der Information muss ein reales und feststellbares Risiko eines erheblichen Schadens für ein legitimes Interesse der nationalen Sicherheit darstellen.
  - (ii) Das Risiko eines Schadens durch die Offenlegung muss das allgemeine öffentliche Interesse an der Offenlegung überwiegen.
  - (iii) Die Einschränkung muss dem Prinzip der Verhältnismäßigkeit genügen und muss das am wenigsten einschränkende Mittel sein, welches zur Verfügung steht, um vor dem Schaden zu schützen.
  - (iv) Die Einschränkung darf den Wesensgehalt des Rechts auf Informationszugang nicht antasten.
- (c) *Schutz eines legitimen Interesses der nationalen Sicherheit.* Die eng gefassten Kategorien von Informationen, die aus Gründen der nationalen Sicherheit zurückgehalten werden können, sollten gesetzlich klar festgelegt werden.

*Hinweise: Siehe die Definition von "legitimes nationalen Sicherheitsinteresse" im obigen Abschnitt Definitionen. Prinzip 3(b) ist umso wichtiger, wenn der Begriff „nationale Sicherheit“ entgegen der Empfehlung in Prinzip 2 gesetzlich nicht eindeutig definiert ist.*

*„Öffentliches Interesse“ wird in diesen Prinzipien nicht definiert. Eine Liste von Kategorien von besonders großem öffentlichem Interesse, die eigeninitiativ veröffentlicht und niemals zurückgehalten werden sollten, ist in Prinzip 10 enthalten. Eine Liste der Kategorien von Fehlverhalten, welche von großem Interesse für die Öffentlichkeit sind, und die öffentliche Beschäftigte ohne Angst vor Vergeltung offenlegen dürfen und sollten, ist in Prinzip 37 enthalten.*

*Bei der Abwägung des Risikos eines Schadens gegen das öffentliche Interesse an der Offenlegung sollte die Möglichkeit der Verringerung des durch die Offenlegung entstehenden Schadens berücksichtigt werden, auch wenn dementsprechende Maßnahmen den Einsatz angemessener finanzieller Mittel erforderlich machen. Nachfolgend finden Sie eine beispielhafte Auflistung der Faktoren, die bei der Entscheidung, ob das öffentliche Interesse an der Offenlegung das Risiko eines Schadens überwiegt, berücksichtigt werden sollten:*

- *Faktoren die für eine Offenlegung sprechen: Es kann vernünftiger Weise davon ausgegangen werden, dass die Offenlegung (a) die offene Diskussion öffentlicher Angelegenheiten fördert, (b) die Rechenschaftspflicht der Regierung verbessert, (c) zu einer positiven und sachlichen Debatte über wichtige Probleme oder Angelegenheiten, die von ernsthaftem Interesse sind, beiträgt, (d) die wirksame Kontrolle der Ausgaben öffentlicher Mittel fördert, (e) die Gründe für eine staatliche Entscheidung aufzeigt, (f) zum Schutz der Umwelt beiträgt, (g) Gefahren für die öffentliche Gesundheit oder Sicherheit offenlegt oder Verletzungen der Menschenrechte oder des humanitären Völkerrechts aufdeckt oder hilft, diesbezügliche Verantwortlichkeit festzustellen.*

- *Faktoren, die für eine Nicht-Offenlegung sprechen: Die Offenlegung würde wahrscheinlich ein reales und feststellbares Risiko eines Schadens für ein legitimes Interesse der nationalen Sicherheit darstellen;*
- *Faktoren, die irrelevant sind: es kann vernünftiger Weise davon ausgegangen werden, dass die Offenlegung (a) Unannehmlichkeiten für oder einen Verlust von Vertrauen in staatliche Stellen oder Beamte, oder (b) eine Schwächung einer politischen Partei oder Ideologie verursachen wird.*

*Die Tatsache, dass die Offenlegung der Wirtschaft eines Landes Schaden könnte ist für die Entscheidung relevant, ob Informationen aus diesem Grund zurückgehalten werden sollten, aber nicht aber für Gründe der nationalen Sicherheit.*

#### **Prinzip 4: Beweislast der öffentlichen Stelle hinsichtlich der Legitimität jeglicher Einschränkungen**

- (a) Die Beweislast zum Nachweis der Legitimität jeglicher Einschränkung liegt bei der öffentlichen Stelle, die Informationen zurückhalten möchte.
- (b) Das Recht auf Information sollte weit interpretiert und angewandt werden, und alle Einschränkungen sollten eng ausgelegt werden.
- (c) Zur Erfüllung dieser Beweislast ist es nicht ausreichend für eine öffentliche Stelle, einfach zu behaupten, dass es ein Schadensrisiko gibt; die öffentliche Stelle ist verpflichtet, spezifische, stichhaltige Gründe zum Nachweis ihrer Behauptungen vorzubringen.

*Hinweis: Jede Person, die Zugang zu Informationen zu sucht, sollte im Einklang mit den Prinzipien 26 und 27 eine faire Chance haben, die angeführten Grundlagen für eine Risikobewertung vor einer Verwaltungsbehörde ebenso wie vor einem Gericht anzugreifen.*

- (d) In keinem Fall darf die bloße Versicherung, wie die Erteilung einer Bescheinigung durch einen Minister oder einen anderen Beamten, wonach die Offenlegung zu einem Schaden für die nationale Sicherheit führen würde, als bindend hinsichtlich des Punktes gelten, für welchen sie erstellt wurde.

#### **Prinzip 5: Keine Ausnahmegenehmigung für irgendeine öffentliche Stelle**

- (a) Keine öffentliche Stelle – einschließlich der Justiz, des Gesetzgebers, der Aufsichtsstellen, der Geheimdienste, der Streitkräfte, der Polizei, anderen Sicherheitsbehörden, der Büros der Staats- und Regierungschefs, und aller anderen im vorstehenden Sinne zuständiger Stellen – darf von der Pflicht zur Offenlegung ausgenommen werden.
- (b) Informationen dürfen nicht aus Gründen der nationalen Sicherheit einfach deshalb zurückgehalten werden, weil sie durch einen ausländischen Staat oder eine

zwischenstaatliche Einrichtung oder eine spezielle öffentliche Stelle oder eine Einheit innerhalb einer öffentlichen Stelle erstellt oder mit diesem Staat, dieser Einrichtung oder einer dieser Stellen geteilt wurden.

*Hinweis: Hinsichtlich Informationen, die von einem ausländischen Staat oder einer zwischenstaatlichen Einrichtung erzeugt wurden, siehe Prinzip 9(a)(v).*

### **Prinzip 6: Zugang zu Informationen von Aufsichtsstellen**

Alle Aufsichts-, Ombudsmann- und Beschwerdestellen, einschließlich der Gerichte, sollten, unabhängig vom Grad der Geheimhaltungsstufe, Zugang zu allen Informationen, einschließlich Informationen der nationalen Sicherheit, haben, soweit diese für ihre Fähigkeit zur Erfüllung ihrer Aufgaben relevant sind.

*Hinweis: Auf dieses Prinzip wird in Prinzip 32 näher eingegangen. Es bezieht sich nicht auf Offenlegungen durch Aufsichtsstellen gegenüber der Öffentlichkeit. Aufsichtsstellen sollten, wie in Prinzip 35 dargelegt, die Geheimhaltung aller gemäß dieser Prinzipien rechtmäßig als geheimhaltungsbedürftig eingestuften Informationen wahren.*

### **Prinzip 7: Ressourcen**

Die Staaten sollten die notwendigen Mittel einsetzen und andere notwendige Schritte unternehmen, wie z.B. die Herausgabe von Verordnungen und die ordnungsgemäße Verwaltung von Archiven, um sicherzustellen, dass diese Prinzipien in der Praxis eingehalten werden.

### **Prinzip 8: Notstandssituationen**

In Zeiten eines öffentlichen Notstandes, der die Existenz einer Nation bedroht, und dessen Vorliegen offiziell und rechtmäßig im Einklang sowohl mit nationalem als auch mit internationalem Recht proklamiert wurde, kann eine Staat von seinen Pflichten hinsichtlich des Rechts, Informationen zu suchen, zu empfangen und zu verbreiten nur in jenem Maße abweichen, wie dies aufgrund der Erfordernisse der Situation unbedingt notwendig ist und dies nur dann und solange, wie die Abweichung mit den anderen Verpflichtungen des Staates nach internationalem Recht vereinbar ist und keine Form von Diskriminierung mit sich bringt.

*Hinweis: Bestimmte Aspekte des Rechts, Informationen und Gedankengut zu suchen, zu empfangen und zu verbreiten sind von so grundlegender Bedeutung für die Wahrnehmung der unveräußerlichen Rechte, dass diese Aspekte immer, sogar in Zeiten öffentlichen Notstandes in vollem Umfang beachtet werden sollten. Dies würde beispielsweise – nicht nur aber auch – auf einige oder alle der in Prinzip 10 erwähnten Informationen zutreffen.*

## TEIL II: INFORMATIONEN, DIE AUS GRÜNDEN NATIONALER SICHERHEIT ZURÜCKGEHALTEN WERDEN DÜRFEN UND INFORMATIONEN, DIE OFFENGELEGT WERDEN SOLLTEN

### Prinzip 9: Informationen, die berechtigter Weise zurückgehalten werden können

(a) Eine Behörde darf das Recht der Öffentlichkeit auf Zugang zu Informationen aus Gründen der nationalen Sicherheit beschränken, dies aber nur, wenn solche Einschränkungen allen anderen Bestimmungen dieser Prinzipien genügen, die Informationen im Besitz einer öffentlichen Stelle sind und die Information einer der nachfolgenden Kategorien angehören:

(i) Informationen über laufende Verteidigungsplanungen, -operationen und -fähigkeiten für die Dauer des Zeitraums, innerhalb dessen die Informationen von operativem Nutzwert sind.

*Hinweis: Der Ausdruck "für die Dauer des Zeitraums, innerhalb dessen die Informationen von operativem Nutzwert sind" ist so zu verstehen, dass eine Information offenzulegen ist, sobald sie nichts mehr enthüllt, was von Feinden benutzt werden könnte, um die Verteidigungsbereitschaft, -fertigkeiten oder -pläne des betreffenden Staates zu verstehen.*

(ii) Informationen über die Produktion, die Fähigkeiten oder den Einsatz von Waffensystemen und anderen militärischen Systemen einschließlich Kommunikationssystemen.

*Hinweis: Diese Informationen umfassen technische Daten und Erfindungen sowie Informationen über Produktion, Fähigkeiten oder Verwendung. Information über die einzelnen Budgetposten für Waffen und andere militärische Systeme sollten der Öffentlichkeit zugänglich gemacht werden. Dazu Prinzipien 10C(3) & 10F. Es ist gute Staatenpraxis, eine Kontrollliste über Waffen zu führen und zu veröffentlichen, wie dies durch den Vertrag über den Waffenhandel mit konventionellen Waffen angeregt wird. Es ist auch gute Praxis, Informationen über Waffen, Ausrüstung und Truppenstärke zu veröffentlichen.*

(iii) Informationen über spezifische Maßnahmen zur Sicherung des Hoheitsgebietes des Staates, kritischer Infrastruktur oder wesentlicher nationaler Institutionen (*institutions essentielles*) gegen Bedrohungen oder die Anwendung von Gewalt oder Sabotage, deren Wirksamkeit auf Geheimhaltung angewiesen ist;

*Hinweis: "Kritische Infrastruktur" bezieht sich auf strategische Ressourcen, Anlagen und Systeme, gleichgültig ob physisch oder virtuell, die für den Staat so wichtig sind, dass die Zerstörung oder Unbrauchbarkeit solcher Ressourcen, Anlagen und Systeme eine lähmende Wirkung auf die nationale Sicherheit haben würde.*

- (iv) Informationen in Bezug auf, oder hergeleitet aus den Operationen, Quellen und Methoden der Geheimdienste, soweit sie Fragen der nationalen Sicherheit betreffen, und
- (v) Informationen über Angelegenheiten nationaler Sicherheit, die von einem ausländischen Staat oder einer zwischenstaatlichen Einrichtung unter der ausdrücklichen Erwartung ihrer Geheimhaltung zur Verfügung gestellt wurden; und andere diplomatische Kommunikation, soweit sie Angelegenheiten der nationalen Sicherheit betrifft.

*Hinweis: Es ist gute Praxis hinsichtlich solcher Erwartungen, dass sie schriftlich aufgezeichnet werden.*

*Hinweis: In dem Maße, in dem bestimmte Informationen, die Terrorismus und Maßnahmen zur Terrorismusbekämpfung betreffen, einer der oben genannten Kategorien unterfallen, kann das Recht der Öffentlichkeit auf Zugang zu derartigen Informationen in Übereinstimmung mit dieser und anderen Regelungen der Prinzipien Beschränkungen aus Gründen der nationalen Sicherheit unterliegen. Gleichzeitig können einige Informationen über Terrorismus oder Maßnahmen zur Terrorismusbekämpfung von besonders großem öffentlichem Interesse sein: siehe z.B. die Prinzipien 10A, 10B und 10H(1).*

- (b) Es ist gute Praxis des nationalen Rechts, eine abschließende Liste der Kategorien von Informationen festzulegen, die mindestens so eng definiert sind wie die oben genannten Kategorien.
- (c) Ein Staat kann eine Kategorie von Informationen zu der vorstehenden Liste von Kategorien hinzufügen, dies aber nur, wenn die Kategorie genau beschrieben und eng definiert ist und die Wahrung der Geheimhaltung der Informationen erforderlich ist, um ein, wie in Prinzip 2(c) vorgesehen durch Gesetz festgelegtes, legitimes Interesse der nationalen Sicherheit zu schützen. Beim Vorschlag der Kategorie sollte der Staat erklären, wie die Offenlegung von Informationen dieser Kategorie die nationale Sicherheit schädigen würde.

### **Prinzip 10: Kategorien von Informationen, bei denen eine starke Vermutung oder ein überwiegendes Interesse zugunsten einer Offenlegung besteht**

Einige Kategorien von Informationen, einschließlich der unten aufgeführten, sind wegen ihrer besonderen Bedeutung für den Prozess der demokratischen Kontrolle und der Rechtsstaatlichkeit von besonders großem öffentlichem Interesse. Folglich gibt es eine sehr starke Vermutung, und in einigen Fällen ein vorrangiges Gebot, dass derartige Informationen öffentlich verfügbar sein und eigeninitiativ offengelegt werden sollten.

Informationen aus den folgenden Kategorien sollten mindestens zu einer starken Vermutung zugunsten der Offenlegung führen, und dürfen aus Gründen der nationalen Sicherheit nur in ganz außergewöhnlichen Ausnahmefällen und im Einklang mit den anderen Prinzipien geheim gehalten werden; dies nur für einen eng begrenzten Zeitraum, nur aufgrund eines Gesetzes, und nur, wenn es keine angemessenen Mittel gibt, um den

Schaden einzugrenzen, der mit deren Offenlegung verbunden wäre. Für bestimmte Unterkategorien von Informationen, die im Folgenden bezeichnet werden, als Informationen, für die ihrer Natur nach ein überwiegendes öffentliches Interesse an der Offenlegung besteht, kann eine Geheimhaltung aus Gründen der nationalen Sicherheit niemals gerechtfertigt werden.

#### **A. Verletzungen der internationalen Menschenrechte und des humanitären Völkerrechts**

- (1) Es besteht ein überwiegendes öffentliches Interesse an der Offenlegung von Informationen über schwere Menschenrechtsverletzungen oder schwere Verstöße gegen das humanitäre Völkerrecht, einschließlich Verbrechen nach dem Völkerrecht, und über systematische oder weit verbreitete Verletzungen der Rechte auf persönliche Freiheit und Sicherheit. Diese Informationen dürfen aus Gründen der nationalen Sicherheit unter keinen Umständen geheim gehalten werden.
- (2) Informationen über andere Verletzungen der Menschenrechte oder des humanitären Völkerrechts unterliegen einer starken Vermutung zugunsten der Offenlegung, in keinem Fall dürfen sie aus Gründen der nationalen Sicherheit in einer Art und Weise zurückgehalten werden, die es verhindern würde, dass die Verantwortlichen zur Rechenschaft gezogen werden oder dass Opfer Zugang zu einem effektiven Rechtsbehelf erlangen.
- (3) Wenn sich ein Staat in einer Übergangsphase des Rechtssystems befindet, während dessen er besonders verpflichtet ist, Wahrheit, Gerechtigkeit, Wiedergutmachung und Garantien für den Ausschluss einer Wiederholung sicherzustellen, gibt es ein überwiegendes öffentliches Interesse der Gesellschaft als Ganzes an der Offenlegung von Informationen über Menschenrechtsverletzungen, die unter dem früheren Regime begangen wurden. Eine Nachfolge-Regierung sollte sofort die Unversehrtheit aller Aufzeichnungen, die derartige, von einer Vorgänger-Regierung geheim gehaltene Informationen enthalten, schützen und bewahren und diese auch ohne Verzögerung veröffentlichen.

*Hinweis: Siehe Prinzip 21 (c) in Bezug auf die Pflicht, nach Informationen über Menschenrechtsverletzungen zu suchen oder diese wiederherzustellen.*

- (4) Wird die Existenz von Verstößen bestritten oder nur befürchtet, anstatt bereits gesichert zu sein, gilt dieses Prinzip auch in Bezug auf Informationen, die für sich genommen oder in Verbindung mit anderen Informationen zur Erhellung der Wahrheit hinsichtlich der mutmaßlichen Verstöße beitragen würden.
- (5) Dieses Prinzip findet Anwendung auf Informationen über Verstöße, die eingetreten sind oder stattfinden und gilt unabhängig davon, ob die Verstöße von Dritten oder von dem Staat begangen wurden, der über die Informationen verfügt.
- (6) Die von diesem Prinzip erfassten Informationen über Verstöße umfassen, ohne dass dies abschließend zu verstehen ist, die folgenden:

- (a) Vollständige Beschreibungen und alle Aufzeichnungen, die Handlungen oder Unterlassungen belegen, welche Verstöße darstellen sowie die Daten und Umstände unter denen sie aufgetreten sind und gegebenenfalls den Aufenthaltsort von vermissten Personen oder sterblichen Überresten.
- (b) Die Identität aller Opfer, soweit dies mit dem Recht auf Privatsphäre und anderen Rechten der Opfer, ihrer Angehörigen und von Zeugen im Einklang steht; und aggregiertes und anderes anonymes Datenmaterial hinsichtlich ihrer Zahl und ihrer Charakteristiken, welches zur Wahrung der Menschenrechte relevant sein könnte.

*Hinweis: Die Namen und andere persönliche Daten von Opfern, ihren Angehörigen und von Zeugen können von der Offenlegung gegenüber der Öffentlichkeit in dem Maße zurückgehalten werden, in welchem dies notwendig ist, um sie vor weiterem Schaden zu bewahren, wenn die betroffenen Personen, oder im Falle verstorbener Personen deren Familienangehörige ausdrücklich und freiwillig die Geheimhaltung fordern oder diese aus anderen Gründen offensichtlich mit den Wünschen dieser Personen oder den Bedürfnissen von gefährdeten Gruppen im Einklang steht. Die Namen und andere persönliche Daten von Opfern sexueller Gewalt sollten nur mit deren ausdrücklicher Zustimmung offengelegt werden. Kinder (unter 18 Jahren), die Opfer wurden, sollten gegenüber der Öffentlichkeit nicht identifiziert werden. Bei der Auslegung dieses Prinzip sollte berücksichtigt werden, dass in der Praxis unterschiedliche Regierungen zu verschiedenen Zeiten das Argument des Datenschutzes benutzt haben um Menschenrechtsverletzungen vor der Öffentlichkeit und auch vor jenen Personen geheim zu halten, deren Rechte massiv verletzt werden oder wurden, ohne dabei auf die wahren Wünsche der Betroffenen Personen Rücksicht zu nehmen. Die vorgenannten Einschränkungen sollten außerdem der Veröffentlichung von aggregierten oder in anderer Weise anonymen Daten nicht entgegenstehen.*

- (c) Die Namen der Einrichtungen und Einzelpersonen, welche die Verstöße begangen haben oder in anderer Weise für diese verantwortlich waren, sowie allgemein von allen zum Zeitpunkt der Verstöße anwesenden oder in anderer Weise verwickelten Einheiten der Sicherheitsdienste, ihrer Vorgesetzten und der Befehlshabenden sowie Informationen über den Umfang ihrer Befehle und Kontrolle.
- (d) Informationen über die Ursachen der Verstöße und die Versäumnisse, sie zu verhindern.

### **B. Maßnahmen zum Schutze des Rechts auf Freiheit und auf Sicherheit der Person, zur Verhinderung von Folter und anderen Misshandlungen sowie zum Schutz des Rechts auf Leben**

Die von diesem Prinzip umfassten Informationen beinhalten:

- (1) Gesetze und Regelungen, die den Entzug des Lebens einer Person durch den Staat erlauben, und Gesetze und Regelungen über Freiheitsentziehungen, einschließlich jener, welche die Gründe, Verfahren, Verbringung, Behandlungen oder Haftbedingungen von betroffenen Personen, einschließlich der Verhörmethoden regeln.

Es besteht ein überwiegendes öffentliches Interesse an der Offenlegung solcher Gesetze und Regelungen.

*Hinweise: "Gesetze und Regelungen" im Sinne von Prinzip 10 umfassen jegliche primäre oder delegierte Gesetzgebung, Statuten, Verordnungen und Verfügungen ebenso wie Dekrete oder Anordnungen durch einen Präsidenten, Premierminister, Minister oder eine andere öffentliche Stelle sowie gerichtliche Entscheidungen, die Gesetzeskraft haben. "Gesetze und Regelungen" umfassen auch jede Regel oder Gesetzesinterpretation, die von Beamten als verbindlich angesehen wird.*

*Freiheitsentziehung umfasst jede Form von Arrest, Festnahme, Inhaftierung oder Internierung.*

(2) Die Lage aller Orte, an denen Personen die Freiheit durch oder im Namen des Staates vorenthalten wird, ebenso wie die Identität und Anklage gegen, oder die Gründe für die Inhaftierung aller Personen, denen die Freiheit entzogen ist, auch während eines bewaffneten Konflikts.

(3) Informationen über den Tod von Personen in Gewahrsam und Informationen über andere Todesfälle, für die ein Staat verantwortlich ist, einschließlich der Identität der getöteten Person oder Personen, der Umstände ihres Todes und des Ortes, an dem sich ihre Überreste befinden.

*Hinweis: Unter keinen Umständen dürfen Informationen aus Gründen der nationalen Sicherheit zurückgehalten werden, wenn diese zur geheimen Inhaftierung einer Person, zur Errichtung und dem Betrieb von geheimen Haftanstalten oder zu geheimen Hinrichtungen führen würden. Auch gibt es keine Umstände, unter denen das Schicksal oder der Verbleib von jemandem, dessen Freiheit durch den Staat oder mit Ermächtigung, Unterstützung oder Duldung des Staates entzogen wurde, gegenüber dessen Familienangehörigen oder Dritten, die ein legitimes Interesse am Wohlergehen der Person haben, verborgen oder in anderer Weise vorenthalten werden darf.*

*Die Namen und andere persönliche Daten von Personen, deren Freiheit entzogen wurde, die in Haft gestorben sind oder deren Tod durch Vertreter des Staates verschuldet wurde, können von der Offenlegung gegenüber der Öffentlichkeit in jenem Umfang ausgenommen werden der erforderlich ist, um das Recht auf Schutz der Privatsphäre zu gewährleisten, soweit die betroffenen Personen oder, im Falle von Verstorbenen, deren Familienangehörigen dies ausdrücklich und freiwillig verlangen und die Nichtoffenlegung auch ansonsten im Einklang mit den Menschenrechten steht. Die Identität von Kindern, denen die Freiheit entzogen wurde, sollte der Öffentlichkeit nicht zugänglich gemacht werden. Diese Einschränkungen sollten jedoch der Veröffentlichung von aggregierten oder sonstigen anonymen Daten nicht entgegenstehen.*

### **C. Strukturen und Kompetenzen der Exekutive**

Die von diesem Prinzip betroffenen Informationen umfassen, ohne Einschränkung, die folgenden:

- (1) Die Existenz aller Militär-, Polizei-, Sicherheits- und Nachrichtendienste und ihrer Untereinheiten.
- (2) Die geltenden Gesetze und Regelungen, die auf diese Behörden und deren Aufsichtsstellen und auf interne Mechanismen der Rechenschaftspflicht anwendbar sind sowie die Namen der Beamten, die diese Behörden leiten.
- (3) Informationen, die nötig sind zur Evaluation und zur Kontrolle öffentlicher Ausgaben einschließlich der Brutto-Gesamtbudgets, wichtiger Einzelposten und der Informationen über die grundlegenden Ausgaben solcher Behörden.
- (4) Das Bestehen und der Wortlaut von abgeschlossenen bilateralen und multilateralen Abkommen und anderer wichtiger internationaler Verpflichtungen, die der Staat in Angelegenheiten der nationalen Sicherheit eingegangen ist.

#### **D. Entscheidungen über die Anwendung militärischer Gewalt oder den Erwerb von Massenvernichtungswaffen**

- (1) Die von diesem Prinzip umfassten Informationen beinhalten jene mit Bedeutung für eine Entscheidung über den Einsatz von Kampftruppen oder über andere militärische Maßnahmen einschließlich der Bestätigung der Tatsache der Vornahme einer solchen Maßnahme, ihrer generellen Größe und ihres Umfangs sowie eine Erläuterung der Gründe dafür, und ebenso alle Informationen, die belegen, dass eine Tatsache, welche als Teil der öffentlichen Begründung angegeben wurde, unzutreffend war.

*Hinweis: Die Bezugnahme auf die „generelle“ Größe und den Umfang einer Maßnahme erkennt an, dass es in der Regel möglich sein sollte, das starke öffentliche Interesse am Zugang zu Informationen, die für die Entscheidung über den Einsatz von Kampftruppen relevant sind zu erfüllen, ohne alle Details der operationellen Aspekte der fraglichen Militäraktion offenzulegen (siehe Prinzip 9).*

- (2) Der Besitz oder Erwerb von Atomwaffen oder anderen Massenvernichtungswaffen durch einen Staat, nicht unbedingt aber alle Details über ihre Herstellung oder operativen Fähigkeiten, ist eine Angelegenheit von überwiegenden öffentlichen Interesse und sollte nicht geheim gehalten werden.

*Hinweis: Dieses Unterprinzip sollte nicht so verstanden werden, als ob dadurch in irgendeiner Weise der Erwerb solcher Waffen befürwortet würde.*

#### **E. Überwachung**

- (1) Der allgemeine Rechtsrahmen hinsichtlich jeglicher Form von Überwachung sowie die zu beachtenden Verfahren zur Genehmigung von Überwachung, zur Auswahl der Ziele der Überwachung, und zur Nutzung, zum Austausch, und über die Speicherung und Zerstörung des abgefangenen Materials sollten der Öffentlichkeit zugänglich sein.

*Hinweis: Diese Informationen umfassen: (a) die einschlägigen Gesetze hinsichtlich aller Formen der Überwachung, sowohl der verdeckten als auch der offenen, einschließlich der indirekten Überwachung wie Profiling und Data-Mining, und der Arten von Überwachungsmaßnahmen, die verwendet werden können; (b) die zulässigen Ziele der*

*Überwachung; (c) die Schwelle des Verdachts, der erforderlich ist um eine Überwachung einzuleiten oder fortzusetzen; (d) Beschränkungen der Dauer von Überwachungsmaßnahmen; (e) Verfahren für die Zulassung und Überprüfung der Nutzung solcher Maßnahmen; (f) die Arten von persönlichen Daten, die für Zwecke der nationalen Sicherheit gesammelt und/oder verarbeitet werden dürfen; und (g) die Kriterien, die auf die Verwendung, Aufbewahrung, Löschung und Weitergabe dieser Daten Anwendung finden.*

- (2) Die Öffentlichkeit sollte auch Zugang zu den Informationen darüber haben, welche Stellen befugt sind, die Überwachung durchzuführen und über Statistiken über die Anwendung dieser Überwachungsmaßnahmen.

*Hinweise: Diese Informationen umfassen für jedes Jahr die Identität jeder staatlichen Stelle, der eine spezifische Genehmigung für die jeweilige Überwachung gewährt wurde, die Zahl der jedes Jahr jeder solchen Stelle gewährten Überwachungsgenehmigungen sowie die besten verfügbaren Informationen über die Anzahl der Personen und die Anzahl der Mitteilungen, die jedes Jahr von einer Überwachungsmaßnahme betroffen waren, und, ob eine Überwachungsmaßnahme ohne spezifische Genehmigung durchgeführt wurde und wenn ja, von welcher staatlichen Stelle.*

*Das Recht der Öffentlichkeit auf Information erstreckt sich nicht zwangsläufig auf die Fakten oder operativen Einzelheiten einer gesetzmäßig und im Einklang mit menschenrechtlichen Verpflichtungen durchgeführten Überwachungsmaßnahme. Diese Informationen können der Öffentlichkeit und den von der Überwachung Betroffenen mindestens bis zum Ende des Überwachungszeitraums vorenthalten werden.*

- (3) Zusätzlich sollte die Öffentlichkeit umfassend über jegliche illegale Überwachung informiert werden. Informationen über solche Überwachung sollten im größtmöglichen Umfang offengelegt werden, der ohne Verletzung des Rechts auf Privatsphäre der überwachten Personen möglich ist.

- (4) Diese Prinzipien beziehen sich auf das Recht der Öffentlichkeit auf Zugang zu Informationen und gelten unbeschadet der darüber hinaus bestehenden materiellen und verfahrensmäßigen Rechte jener Personen, die Gegenstand von Überwachungsmaßnahmen waren oder dies annehmen.

*Hinweis: Es entspricht guter Praxis, dass öffentliche Stellen verpflichtet sind, Personen, die Gegenstand verdeckter Überwachungsmaßnahmen waren, hierüber zu unterrichten (unter Angabe von mindestens: Informationen über die Art der Maßnahme, die angewandt wurde, den Zeitpunkten und der für die Genehmigung der Überwachungsmaßnahme zuständigen Stelle), soweit dies ohne Beeinträchtigung laufender Maßnahmen oder von Quellen und Methoden getan werden kann.*

- (5) Die in diesem Prinzip anerkannten starken Vermutungen zugunsten der Offenlegung finden keine Anwendung auf Informationen, die sich ausschließlich auf die Überwachung der Aktivitäten ausländischer Regierungen beziehen.

*Hinweis: Über verdeckte Überwachung erlangte Informationen, einschließlich jener über Aktivitäten ausländischer Regierungen, sollten unter den in Prinzip 10a beschriebenen Umständen Gegenstand einer Offenlegung sein.*

#### **F. Finanzinformationen**

Die von diesem Prinzip umfassten Informationen beinhalten jene Informationen, die der Öffentlichkeit in ausreichender Weise ermöglichen, die Finanzierung des Sicherheitssektors und ebenso jene Vorschriften, welche die Finanzen des Sicherheitssektors regeln, zu verstehen. Diese Informationen sollten beinhalten, aber nicht beschränkt sein auf:

- (1) Die Budgets und die Überschriften der Einzeltitel von Abteilungen und Einrichtungen;
- (2) Die finanziellen Jahresabschlüsse mit den Überschriften der Einzeltitel;
- (3) Die Regeln des Finanzmanagements und die Kontrollmechanismen;
- (4) Vergabevorschriften und
- (5) Berichte der Rechnungshöfe und sonstigen Einrichtungen, die für die Überprüfung der finanziellen Aspekte des Sicherheitssektors verantwortlich sind, einschließlich von Zusammenfassungen von etwaig als geheim eingestuften Abschnitten solcher Berichte.

#### **G. Rechenschaftspflicht hinsichtlich der Verletzung von verfassungsrechtlichen und gesetzlichen Pflichten und andere Fällen von Machtmissbrauch**

Die von diesem Prinzip umfassten Informationen beinhalten Informationen über die Existenz, die Art und Weise und den Umfang von Verletzungen der Verfassung oder der Gesetze sowie von anderen Fällen von Machtmissbrauch durch öffentliche Stellen oder Beschäftigte.

#### **H. Öffentliche Gesundheit, öffentliche Sicherheit und Umwelt**

Die von diesem Prinzip betroffenen Informationen beinhalten:

- (1) Im Falle einer bevorstehenden oder tatsächlichen Gefährdung der öffentlichen Gesundheit, der öffentlichen Sicherheit oder der Umwelt, alle Informationen, die es der Öffentlichkeit ermöglichen könnten, die Gefahr zu verstehen oder Maßnahmen zu ergreifen, Schädigungen infolge dieser Gefährdung zu vermeiden oder zu mindern, unabhängig davon, ob die Gefahr durch natürliche Ursachen oder menschliche Aktivitäten, einschließlich der Handlungen von Staaten oder von privaten Unternehmen, hervorgerufen wurde.
- (2) Sonstige, regelmäßig aktualisierte Informationen über die Ausbeutung natürlicher Ressourcen, Umweltverschmutzungen und Emissionskataster, Umweltauswirkungen von vorgeschlagenen oder bereits bestehenden großen öffentliche Bauvorhaben oder Ressourcennutzungen sowie Risikobewertungen und Managementpläne von besonders gefährlichen Einrichtungen.

## **TEIL III.A: REGELN FÜR DIE EINSTUFUNG VON INFORMATIONEN ALS GEHEIM UND FÜR DIE AUFHEBUNG DIESER EINSTUFUNG**

### **Prinzip 11: Pflicht zur Angabe von Gründen für eine Einstufung von Informationen als geheim**

- (a) Unabhängig davon, ob in einem Staat ein formales Verfahren zur Festlegung von Geheimhaltungsstufen besteht oder nicht, sind Behörden verpflichtet, Gründe dafür anzugeben, wenn sie Informationen als geheim einstufen.

*Hinweis: "Einstufung als geheim" ist der Prozess, in welchem Unterlagen, die sensible Informationen enthalten, bewertet und gekennzeichnet werden, um festzulegen, wer Zugang zu ihnen bekommen kann und wie die Unterlagen zu behandeln sind. Es ist gute Praxis, ein formales System dieses Einstufungsprozesses einzuführen, um Willkür und übermäßige Zurückhaltung von Informationen zu vermindern.*

- (b) Die Gründe sollten unter Benutzung der in Prinzip 9 aufgelisteten Kategorien angeben, zu welcher der dortigen engen Informationskategorien die Informationen gehören und den möglichen Schaden beschreiben, der durch ihre Offenlegung entstehen könnte, einschließlich des Grades seiner Schwere und der Wahrscheinlichkeit seines Eintritts.
- (c) Geheimhaltungsstufen sollten, wenn sie angewandt werden, dem Niveau und der Wahrscheinlichkeit des in der Begründung dargelegten Schadens angemessen sein.
- (d) Wenn Informationen als geheim eingestuft werden, sollte (i) eine Sicherungskennzeichnung auf den Unterlagen angebracht werden, aus der – soweit vorhanden – die Stufe und der maximale Zeitraum der Geheimhaltung hervorgeht, und (ii) eine Erklärung sollte hinzugefügt werden, welche die Notwendigkeit der Geheimhaltung auf dieser Stufe und für diesen Zeitraum rechtfertigt.

*Hinweis: Die Erstellung einer Begründung für jede Entscheidung über eine Geheimhaltungsstufe wird empfohlen, da dies die Beamten dazu bringt, das spezifische, von einer Offenlegung verursachte Schadenspotential zu betrachten, und da so das Verfahren der Aufhebung der Geheimhaltung und Offenlegung vereinfacht wird. Eine absatzweise Kennzeichnung erleichtert die Konsistenz bei der Offenlegung von nicht als geheim eingestuften Teilen von Dokumenten zusätzlich.*

### **Prinzip 12: Zugang der Öffentlichkeit zu den Einstufungsregeln**

- (a) Die Öffentlichkeit sollte die Möglichkeit haben, die Verfahren und Standards für eine Einstufung als geheim vor ihrem Wirksamwerden zu kommentieren.
- (b) Die Öffentlichkeit sollte Zugang zu den schriftlich festgelegten Verfahren und Standards der Einstufung als geheim haben.

### **Prinzip 13: Einstufungsbefugnis**

(a) Nur gemäß gesetzlicher Regelung dazu besonders autorisierte oder bezeichnete Beamte sind zur Einstufung von Informationen als geheim befugt. Wenn ein nicht befugter Beamter der Überzeugung ist, dass Informationen als geheim eingestuft werden sollten, können diese Informationen für eine kurze und genau bestimmte Zeitspanne bis zur Überprüfung der Empfehlung der Geheimhaltung durch einen befugten Beamten als geheim angesehen werden.

*Hinweis: Wenn gesetzliche Regelungen über die Befugnis zur Einstufung als geheim fehlen, entspricht es guter Praxis, die Delegation solcher Befugnisse wenigstens in einer Verordnung zu regeln.*

(b) Zur Sicherstellung der Rechenschaftspflicht sollte die Identität der Person, die die für eine Entscheidung über die Geheimhaltung verantwortlich ist, ermittelbar oder auf dem Dokument angegeben sein, es sei denn, es gibt zwingende Gründe, ihre Identität geheim zu halten.

(c) Die gesetzlich bestimmten Beamten sollten die Befugnis zur Einstufung als geheim nur an die geringste Anzahl hochrangiger Untergebener weitergeben, mit der eine effiziente Verwaltung noch möglich ist.

*Hinweis: Es ist eine gute Praxis, Informationen darüber zu veröffentlichen, wie viele Personen die Befugnis zur Einstufung als geheim haben und wie viele Personen Zugang zu den als geheim eingestuften Informationen haben.*

### **Prinzip 14: Förderung eines internen Vorgehens gegen Geheimhaltungseinstufungen**

Öffentliche Beschäftigte, einschließlich derjenigen mit Beziehungen zum Sicherheitssektor, die der Auffassung sind, dass Informationen unangemessener Weise als geheim eingestuft wurden, können gegen diese Einstufung vorgehen.

*Hinweis: Beschäftigte des Sicherheitssektors zeichnen sich dadurch aus, dass sie einer besonderen Ermutigung zu einem Vorgehen gegen Geheimhaltung bedürfen, dies vor dem Hintergrund der ausgeprägten Kultur der Geheimhaltung in Sicherheitsbehörden und angesichts der Tatsachen, dass die meisten Staaten keine unabhängigen Stellen geschaffen oder bezeichnet haben, um Beschwerden von Sicherheitspersonal entgegenzunehmen, und dass die Offenlegung von Informationen aus dem Sicherheitssektor häufig zu schärferen Strafen führt als bei der Offenlegung anderer Informationen.*

## **Prinzip 15: Pflicht zur Aufbewahrung, Verwaltung und Pflege von Informationen zur nationalen Sicherheit**

- (a) Die Behörden haben die Pflicht, Informationen gemäß internationaler Standards<sup>1</sup> aufzubewahren, zu verwalten und zu pflegen. Informationen können nur mittels gesetzlicher Regelung von der Aufbewahrung, Verwaltung und Pflege ausgenommen werden.
- (b) Die Informationen sollten ordnungsgemäß gepflegt werden. Ablagesysteme sollten konsistent, transparent (ohne Offenlegung rechtmäßig als geheim eingestufte Informationen) und umfassend sein, so dass bei spezifischen Zugangsanfragen alle relevanten Informationen aufgefunden werden, auch wenn die Informationen nicht offengelegt werden.
- (c) Jede öffentliche Stelle sollte eine detaillierte und genaue Liste der in ihrem Besitz befindlichen, als geheim eingestufteten Datenbestände erstellen, öffentlich machen und in regelmäßigen Abständen überprüfen und aktualisieren; dies nur mit Ausnahmen für jene außergewöhnlichen Dokumente – soweit vorhanden –, deren Existenz zulässigerweise gemäß Prinzip 19 geheim gehalten werden darf.

*Hinweis: Es ist gute Praxis, solche Listen jährlich zu aktualisieren.*

## **Prinzip 16: Fristen für die Dauer der Geheimhaltung**

- (a) Informationen dürfen aus Gründen der nationalen Sicherheit nur so lange zurückgehalten werden, wie dies nötig ist, um ein berechtigtes Interesse nationaler Sicherheit zu schützen. Entscheidungen, Informationen zurückzuhalten sollten regelmäßig überprüft werden, um sicherzustellen, dass dieses Prinzip eingehalten wird.

*Hinweis: Es ist eine gute Praxis, gesetzlich eine Überprüfung mindestens alle fünf Jahre vorzuschreiben. Mehrere Staaten verlangen Überprüfungen in kürzeren Zeiträumen.*

- (b) Die Stelle, welche die Einstufung als geheim vornimmt, sollte das Datum, die Bedingungen oder das Ereignis benennen, an welchem bzw. bei welchen die Einstufung als geheim endet.

*Hinweis: Es ist gute Praxis, dass diese Frist oder die festgelegten Bedingungen oder das Ereignis, bei welchem die Einstufung als geheim endet bzw. enden einer regelmäßigen Überprüfung unterzogen wird.*

---

<sup>1</sup> Dazu gehören: International Council on Archives (ICA), [Principles of Access to Archives](#) (2012); ICA, [Universal Declaration on Archives](#) (2010; unterstützt durch die UNESCO); Europarat, [Recommendation No R\(2000\)13 on a European policy on access to archives](#) (2000); Antonio González Quintana, ICA, [Archival policies in the protection of human rights](#): an updated and fuller version of the report prepared by UNESCO and the International Council on Archives (1995), concerning the management of the archives of the state security services of former repressive regimes (2009).

- (c) Keinerlei Informationen dürfen auf unbestimmte Zeit als geheim eingestuft bleiben. Der mutmaßliche maximale Zeitraum für eine Einstufung als geheim aus Gründen der nationalen Sicherheit sollte durch Gesetz festgelegt werden.
- (d) Informationen dürfen über den mutmaßlichen Ablaufzeitpunkt hinaus nur unter außergewöhnlichen Umständen und nach Maßgabe einer, von einem anderen Entscheidungsträger getroffenen, neuen Geheimhaltungseinstufung unter Festlegung eines geänderten Ablaufzeitpunktes zurückgehalten werden.

### **Prinzip 17: Verfahren zur Aufhebung einer Einstufung als geheim**

- (a) Die nationalen Rechtsvorschriften sollten eine Verantwortung der Regierung vorsehen, Maßnahmen zur Aufhebung von Einstufungen als geheim zu koordinieren, zu überwachen und umzusetzen sowie Leitlinien zur Aufhebung von Geheimhaltungseinstufungen zu konsolidieren und regelmäßig zu aktualisieren.
- (b) Es sollten Verfahren eingeführt werden, mit welchen Informationen von öffentlichem Interesse identifiziert werden, um diese einer vorrangigen Aufhebung der Geheimhaltungseinstufung zuzuführen. Wenn Informationen von öffentlichem Interesse einschließlich jener Informationen, die in eine der in Prinzip 10 aufgeführten Kategorien fallen, aufgrund besonderer Sensibilität als geheim eingestuft sind, sollte deren Einstufung als geheim so schnell wie möglich aufgehoben werden.
- (c) Nationale Rechtsvorschriften sollten Verfahren zur en-bloc-Aufhebung von Geheimhaltungseinstufungen (in großen Blöcken und/oder mittels Stichproben) vorsehen.
- (d) Nationale Rechtsvorschriften sollten feste Zeiträume vorgeben, innerhalb derer die Geheimhaltungseinstufung verschiedener Kategorien von als geheim eingestuften Informationen automatisch aufgehoben werden. Um Belastungen durch die Aufhebung von Geheimhaltungseinstufungen zu minimieren, sollte die Geheimhaltungseinstufung von Unterlagen wo immer möglich automatisch ohne Überprüfung aufgehoben werden.
- (e) Nationale Rechtsvorschriften sollten ein zugängliches und öffentliches Verfahren für die Beantragung der Aufhebung von Geheimhaltungseinstufungen von Dokumenten festlegen.
- (f) Dokumente, deren Geheimhaltungseinstufungen aufgehoben wurden, einschließlich derjenigen, die von Gerichten oder anderen Beschwerde-, Ombuds- oder Aufsichtsstellen aufgehoben wurden, sollen eigeninitiativ offengelegt oder in anderer Weise öffentlich zugänglich gemacht werden (z. B. durch eine Harmonisierung jener Rechtsvorschriften mit jenen über nationale Archive oder über Informationsfreiheit oder beides).

*Hinweis: Dieses Prinzip gilt unbeschadet der Regelungen zu anderen im vorstehenden Prinzip 15 genannten Gründen für die Zurückhaltung von Informationen.*

*Hinweis: Zu weiteren guten Praktiken gehören die folgenden:*

- *regelmäßige Prüfung der Möglichkeiten neuer Technologien im Verfahren zur Aufhebung von Geheimhaltungseinstufungen und*
- *regelmäßige Konsultation mit Experten auf dem Gebiet der Verfahren zur Erstellung von Prioritäten bei der Aufhebung von Geheimhaltungseinstufungen sowohl hinsichtlich automatischer als auch en bloc-Aufhebung.*

## **TEIL III.B: REGELN ZUR BEARBEITUNG VON INFORMATIONSANFRAGEN**

### **Prinzip 18: Pflicht zur Bearbeitung von Anfragen - auch hinsichtlich als geheim eingestufter Informationen**

Die Tatsache, dass Informationen als geheim eingestuft wurden, ist dafür, wie auf eine diese Informationen betreffende Anfrage reagiert wird, nicht entscheidend. Vielmehr sollte die Behörde, die über die Informationen verfügt, die Anfrage nach diesen Prinzipien beurteilen.

### **Prinzip 19: Pflicht zur Bestätigung oder Verneinung**

- (a) Nach Eingang eines Antrags auf Zugang zu Informationen sollte eine Behörde bestätigen oder verneinen, dass sie über die angeforderten Informationen verfügt.
- (b) Ist in einer Rechtsordnung die Möglichkeit erlaubt, dass unter außergewöhnlichen Umständen bereits die Tatsache der Existenz oder Nicht-Existenz von bestimmten Informationen in Übereinstimmung mit Prinzip 3 als geheim eingestuft wird, so sollte jede Ablehnung der Bestätigung oder Verneinung der Existenz der Informationen, die auf eine spezifische Anfrage hin erfolgt, auf den Nachweis gestützt werden, dass schon die bloße Bestätigung oder Verneinung der Existenz der Informationen die Gefahr einer Schädigung einer spezifischen, gesetzlich oder durch Rechtsverordnung bestimmten Informationskategorie mit sich bringen würde, die einer solchen außergewöhnlichen Behandlung bedarf.

### **Prinzip 20: Pflicht zur schriftlichen Begründung von Ablehnungen**

- (a) Wenn eine Behörde einen Antrag auf Informationszugang ganz oder teilweise ablehnt, sollte sie, innerhalb des hierfür gesetzlich vorgesehenen Zeitraums und im Einklang mit den Prinzipien 3 und 9 eine spezifische schriftliche Begründung hierfür abgeben.

*Hinweis: Zur Notwendigkeit der gesetzlichen Festlegung eines Zeitraums, innerhalb dessen eine Antwort abgegeben werden muss, siehe Prinzip 25.*

- (b) Die Behörde sollte dem Antragsteller auch ausreichende Informationen über den Entscheidungsprozess und darüber zur Verfügung stellen welche(r) Beamte(r) diese Entscheidung getroffen hat, es sei denn, dass dies zur Offenlegung als geheim eingestufter Informationen führen würde; der Antragssteller ist auch über Rechtsmittel zur Überprüfung der Rechtmäßigkeit der Behördenentscheidung zu informieren.

## **Prinzip 21: Pflicht zur Wiederherstellung oder Rekonstruktion fehlender Informationen**

- (a) Wenn eine Behörde nicht in der Lage ist, die zur Beantwortung einer Anfrage nötigen Informationen aufzufinden, sie Unterlagen, in welchen diese Informationen enthalten sind, aber gepflegt, gesammelt oder produziert haben müsste, so sollte die Behörde angemessene Anstrengungen unternehmen, um die fehlenden Informationen wiederherzustellen oder zu rekonstruieren, um sie gegenüber dem Antragsteller offenlegen zu können.

*Hinweis: Dieses Prinzip gilt für Informationen, die gleichgültig aus welchem Grund nicht vorliegen, so z.B. weil sie niemals gesammelt wurden, zerstört wurden oder unauffindbar sind.*

- (b) Ein Vertreter der Behörde sollte verpflichtet werden, innerhalb einer angemessenen und gesetzlich festgelegten Zeitspanne unter Eid vollständig darzulegen, welche Bemühungen unternommen wurden, um die Informationen wiederherzustellen oder zu rekonstruieren; dies sollte in einer Art und Weise geschehen, die diese Bemühungen einer gerichtlichen Überprüfung zugänglich macht.

*Hinweis: Wenn Informationen, deren Vorliegen gesetzlich vorgeschrieben ist, nicht aufgefunden werden können, sollte diese Angelegenheit einer Untersuchung durch die Polizei oder Verwaltungsbehörden zugeführt werden. Das Ergebnis dieser Untersuchung sollte öffentlich gemacht werden.*

- (c) Die Pflicht, Informationen wiederherzustellen oder zu rekonstruieren ist besonders stark, wenn diese Informationen sich beziehen auf (i) Vorwürfe von schwerwiegenden oder systematischen Menschenrechtsverletzungen und / oder (ii) den Übergang von einer durch weit verbreitete Menschenrechtsverletzungen charakterisierten Regierung zu einer demokratischen Regierungsform.

## **Prinzip 22: Pflicht zur Offenlegung von Teilen von Dokumenten**

Ausnahmen von der Offenlegung gelten nur für bestimmte Informationen und nicht für ganze Dokumente oder andere Unterlagen. Nur spezifische Informationen, für welche die Gültigkeit einer Einschränkung nachgewiesen wurde ("ausgenommene Information") dürfen zurückgehalten werden. Soweit ein Dokument sowohl ausgenommene als auch nicht-ausgenommene Informationen enthält, haben die Behörden die Pflicht, beide Kategorien zu trennen und die nicht-ausgenommenen Informationen offenzulegen.

## **Prinzip 23: Pflicht zur Kenntlichmachung zurückgehaltener Informationen**

Eine Behörde, die über Informationen verfügt, deren Herausgabe sie ablehnt, sollte diese Informationen so spezifisch wie irgend möglich beschreiben. Die Behörde sollte mindestens den Umfang der Informationen angeben, hinsichtlich derer sie die Offenlegung verweigert, z.B. durch Schätzung der Anzahl der Seiten.

## **Prinzip 24: Pflicht, Informationen in verfügbaren Formaten herauszugeben**

Behörden sollten Informationen soweit möglich in dem vom Antragsteller bevorzugten Format herausgeben.

*Hinweis: Dazu gehört z. B. die Verpflichtung der Behörden, geeignete Maßnahmen zu treffen, um Informationen, im Einklang mit der UN-Konvention über die Rechte von Menschen mit Behinderungen, auch Menschen mit Behinderungen in diesen zugänglichen Formaten und Technologien rechtzeitig und ohne zusätzliche Kosten zur Verfügung zu stellen.*

## **Prinzip 25: Fristen für die Beantwortung von Anträgen auf Informationszugang**

(a) Die Fristen für die Beantwortung von Anträgen, einschließlich einer Entscheidung über deren Begründetheit, einer internen Überprüfung, soweit anwendbar der Entscheidung durch eine unabhängige Stelle und der gerichtlichen Kontrolle sollten durch Gesetz festgelegt werden und sollten so kurz wie in der Praxis möglich sein.

*Hinweis: Es wird in Übereinstimmung mit den Vorgaben der meisten Gesetze über den Zugang zu Informationen als gute Praxis angesehen, eine Frist von 20 Arbeitstagen oder weniger für die inhaltliche Beantwortung eines Antrages vorzusehen. Wo Fristen zur Beantwortung von Anfragen nicht gesetzlich vorgegeben sind, sollte die Frist für die Beantwortung einer Standard-Anfrage 30 Tage nicht überschreiten. Gesetzliche Regelungen können unterschiedliche Fristen vorsehen, um Unterschieden in Volumen, Komplexitätsniveau und Sensibilität von Dokumenten Rechnung zu tragen.*

(b) Verkürzte Fristen sollten dort gelten, wo es ein dargelegtes Eilbedürfnis für die Offenlegung gibt, wie z. B. dort, wo die Informationen notwendig sind, um das Leben oder die Freiheit einer Person zu schützen.

## **Prinzip 26: Recht auf Überprüfung der Entscheidung zur Informationsverweigerung**

(a) Ein Antragsteller hat in Bezug auf eine Entscheidung, durch die ihm die Offenlegung der Informationen oder von Angelegenheiten im Zusammenhang mit seinem Antrag verweigert wurde, das Recht auf eine rasche und kostengünstige Überprüfung durch eine unabhängige öffentliche Stelle.

*Hinweis: Als Weigerung kann auch eine implizite oder stillschweigende Zurückweisung angesehen werden. Die Gegenstände einer Überprüfung durch eine unabhängige öffentliche Stelle umfassen Gebühren, Fristen und Format.*

(b) Die unabhängige öffentliche Stelle sollte die Kompetenz und die notwendigen Ressourcen besitzen, um eine wirksame Überprüfung sicherzustellen, einschließlich des uneingeschränkten Zugangs zu allen relevanten Informationen, auch wenn diese als geheim eingestuft sind.

(c) Eine Person sollte das Recht auf eine unabhängige und wirksame Überprüfung aller relevanten Fragen durch ein zuständiges Gericht haben.

- (d) Wenn ein Gericht die Entscheidung trifft, dass das Zurückhalten von Informationen gerechtfertigt ist, sollte es eine fakten spezifische Begründung und seine rechtliche Analyse der Öffentlichkeit in Schriftform zugänglich machen, es sei denn es liegen außergewöhnliche Umstände vor und Prinzip 3 wird beachtet.

## **TEIL IV: JUSTIZIELLE ASPEKTE VON NATIONALER SICHERHEIT UND DEM RECHT AUF INFORMATIONSZUGANG**

### **Prinzip 27: Prinzip der vollständigen gerichtlichen Kontrolle**

- (a) Die Berufung auf Gründe nationaler Sicherheit darf nicht dazu genutzt werden, um das Grundrecht auf ein faires Verfahren vor einem zuständigen, unabhängigen und unparteiischen, auf Gesetz beruhendem Gericht, zu untergraben.
- (b) Wenn eine öffentliche Stelle sich in einem gerichtlichen Verfahren auf Gründe der nationalen Sicherheit beruft, um Informationen zurückzuhalten, sollte ein Gericht die Befugnis haben, die Informationen bei der Entscheidung über die Rechtmäßigkeit, diese zurückzuhalten, zu untersuchen. Ein Gericht sollte normalerweise eine Klage nicht ohne Untersuchung der Informationen zurückweisen.
- Hinweis: Im Einklang mit Prinzip 4(d) sollte das Gericht sich nicht auf Zusammenfassungen oder eidesstattliche Erklärungen stützen, die ein Geheimhaltungsbedürfnis lediglich behaupten ohne Beweise für diese Behauptung vorzulegen.*
- (c) Das Gericht sollte sicherstellen, dass eine Person, die Zugang begehrt, so weit wie möglich, um das Vorbringen der Exekutive zur Begründung der Nicht- Offenlegung wissen und dieses angreifen kann.
- (d) Ein Gericht sollte über die Recht- und Ordnungsmäßigkeit des Vorbringens einer Behörde entscheiden und kann die Offenlegung der Informationen oder - im Falle von ganz oder teilweiser Nicht-Offenlegung - geeignete Ausgleichsmaßnahmen anordnen; dies umfasst auch die Möglichkeit der Einstellung eines Strafverfahrens.
- (e) Das Gericht sollte unabhängig beurteilen, ob die Behörde sich ordnungsgemäß auf eine Rechtsgrundlage zur Nicht-Offenlegung berufen hat; der Umstand der Einstufung einer Information als geheim sollte dabei in Bezug auf die Offenlegungsentscheidung nicht von allein entscheidender Bedeutung sein. Ebenso sollte das Gericht jeglichen von der Behörde behaupteten Schaden, dessen Eintrittswahrscheinlichkeit und das öffentliche Interesse an der Offenlegung im Einklang mit den in Prinzip 3 definierten Standards selbst beurteilen.

## **Prinzip 28: Öffentlicher Zugang zu gerichtlichen Verfahren**

- (a) Die Berufung auf Gründe nationaler Sicherheit darf nicht dazu genutzt werden, um das Grundrecht der Öffentlichkeit auf Zugang zu gerichtlichen Verfahren zu untergraben.
- (b) Urteile – und ebenso alle gerichtlichen Entscheidungen und Anordnungen, die wesentlichen Erkenntnisse, Beweise und rechtlichen Erwägungen – sollten öffentlich gemacht werden, sofern dem nicht die Wahrung der Interessen von Kindern und Jugendlichen unter achtzehn Jahren entgegensteht.

*Hinweise: Das Völkerrecht gestattet es nicht, aus Gründen der nationalen Sicherheit von der Verpflichtung der öffentlichen Verkündung von Urteilen abzuweichen.*

- (c) Aufzeichnungen über Verfahren vor Jugendgerichten sollten nicht öffentlich gemacht werden. In Aufzeichnungen anderer gerichtlicher Verfahren, die Kinder und Jugendliche unter achtzehn Jahren betreffen, sollten deren Namen und andere zur Identifizierung geeignete Informationen ordnungsgemäß geschwärzt werden.
- (d) Das Recht der Öffentlichkeit auf Zugang zu Rechtsschutz sollte einschließen zeitnahen öffentlichen Zugang zu (i) einer gerichtlichen Begründung, (ii) Informationen über die Existenz und den Fortschritt der Verfahren, (iii) schriftlichem Vorbringen gegenüber dem Gericht, (iv) Gerichtsverhandlungen und Anhörungen und (v) Beweismittel in Gerichtsprozessen, auf welche eine Verurteilung gestützt wird; es sei denn, eine Ausnahme hiervon steht im Einklang mit diesen Prinzipien.

*Hinweis: Völkerrechtliche Regelungen zum fairen Verfahren ermöglichen es Gerichten, die Öffentlichkeit oder einen Teil der Öffentlichkeit von einer Verhandlung aus Gründen der nationalen Sicherheit in einer demokratischen Gesellschaft sowie der Moral, der öffentlichen Ordnung, im Interesse der Privatsphäre der Parteien oder zur Vermeidung einer Beeinträchtigung der Interessen der Rechtspflege auszuschließen soweit solche Einschränkungen in jedem Fall notwendig und verhältnismäßig sind.*

- (e) Die Öffentlichkeit sollte die Möglichkeit haben, gegen jedes Vorbringen einer Behörde, dass eine Beschränkung des Zugangs der Öffentlichkeit zu einem gerichtlichen Verfahren aufgrund der nationalen Sicherheit unbedingt erforderlich sei, vorzugehen.
- (f) Wenn ein Gericht eine Entscheidung darüber trifft, ob eine Beschränkung des freien Zugangs zu gerichtlichen Verfahren gerechtfertigt ist, sollte es, außer unter außergewöhnlichen Umständen, im Einklang mit Prinzip 3 seine fakten-spezifische Begründung und rechtliche Analyse in schriftlicher Form öffentlich zugänglich machen.

*Hinweise: Dieses Prinzip ist nicht dazu gedacht, das bestehende Recht eines Staates in Bezug auf vorläufigen Verfahren, zu welchen die Öffentlichkeit im Normalfall keinen Zugang hat, zu modifizieren. Es gilt nur, wenn das Prozessrecht sonst den öffentlichen Zugang erlauben würde und der Versuch, diesen zu unterbinden auf Gründe nationaler Sicherheit gestützt wird.*

*Das Recht der Öffentlichkeit auf Zugang zu Gerichtsverfahren und Materialien ergibt sich aus der Bedeutung jenes Zugangs zur Förderung (i) der tatsächlichen und der wahrgenommenen Fairness und Unparteilichkeit gerichtlicher Verfahren, (ii) des ordnungsgemäßen und*

*ehrlicheren Verhaltens der Parteien, und (iii) der verbesserten Genauigkeit der öffentlichen Kommentierung.*

### **Prinzip 29: Zugang der Parteien zu Informationen in Strafverfahren**

- (a) Das Gericht darf einen Angeklagten von der Teilnahme an seinem Prozess nicht aus Gründen der nationalen Sicherheit ausschließen.
- (b) In keinem Fall sollte eine Verurteilung oder Freiheitsentziehung auf Beweismittel gestützt werden, hinsichtlich derer der Beschuldigte keine Gelegenheit gehabt hatte, diese zu überprüfen und zu widerlegen.
- (c) Im Interesse der Gerechtigkeit sollte eine Behörde gegenüber dem Angeklagten und seinem Verteidiger die Anklage und alle Informationen offenlegen, die notwendig sind, um ein faires Verfahren zu gewährleisten, unabhängig davon, ob die Informationen im Einklang mit den Prinzipien 3-6 , 10, 27 und 28 und unter Berücksichtigung der öffentlichen Interessen als geheim eingestuft wurden.
- (d) Lehnt die Behörde die Offenlegung von für ein faires Verfahren notwendigen Informationen ab, sollte das Gericht das Verfahren aussetzen oder abweisen.

*Hinweis: Die Behörden sollten sich nicht zu ihrem Vorteil auf Informationen stützen, wenn sie sich auf deren Geheimhaltung berufen, allerdings steht es ihnen frei, die Entscheidung zu treffen, die Informationen geheim zu halten und die daraus folgenden Konsequenzen in Kauf zu nehmen.*

*Hinweis: Die Prinzipien 29 und 30 wurden in diese den öffentlichen Zugang zu Informationen betreffenden Prinzipien aufgenommen, um der Tatsache Rechnung zu tragen, dass gerichtliche Kontrolle sowie die Offenlegung im Rahmen gerichtlicher Überprüfungen oft wichtige Mittel zur Gewährleistung der öffentlichen Offenlegung von Informationen darstellen.*

### **Prinzip 30: Zugang der Parteien zu Informationen in Zivilsachen**

- (a) Jedes behördliche Vorbringen zur Vorenthaltung von Informationen in einem Zivilprozess sollte im Einklang mit den Prinzipien 3-6, 10, 27 und 28, einschließlich der Berücksichtigung der öffentlichen Interessen geprüft werden.
- (b) Opfer von Menschenrechtsverletzungen haben ein Recht auf einen wirksamen Rechtsbehelf und Wiedergutmachung, einschließlich der öffentlichen Offenlegung von erlittenen Missbräuchen. Die Behörden sollten Informationen im Zusammenhang mit ihren Ansprüchen nicht in einer Art und Weise zurückhalten, die mit diesem Recht unvereinbar ist.
- (c) Auch die Öffentlichkeit hat ein Recht auf Informationen über massive Menschenrechtsverletzungen und schwere Verstöße gegen das humanitäre Völkerrecht.

## **TEIL V: STELLEN, DIE DEN SICHERHEITSEKTOR BEAUFSICHTIGEN**

### **Prinzip 31: Einrichtung von unabhängigen Aufsichtsstellen**

Die Staaten sollten, soweit sie dies nicht bereits getan haben, unabhängige Aufsichtsstellen einrichten, welche die Einrichtungen des Sicherheitssektors einschließlich deren Tätigkeiten, Richtlinien, Politiken, Finanzen und Verwaltung beaufsichtigen. Solche Aufsichtsstellen sollten institutionell, in ihrem Handeln und in ihrer Finanzierung unabhängig von jenen Institutionen sein, mit deren Beaufsichtigung sie beauftragt sind.

### **Prinzip 32: Uneingeschränkter Zugang zu Informationen, die für die Erfüllung des Mandats notwendig sind**

- (a) Unabhängige Aufsichtsstellen sollten ein gesetzlich garantiertes Zugangsrecht hinsichtlich aller Informationen besitzen, die für die Erfüllung ihres Mandates notwendig sind. Jenseits der Beachtung von angemessenen Sicherheitsvorschriften für den Zugang sollte es unabhängig vom Grad der Geheimhaltungseinstufung oder Vertraulichkeit der Informationen keinerlei Einschränkungen dieses Zugangsrechts geben.
- (b) Die Informationen, zu denen die Aufsichtsstellen Zugang haben sollten, beinhalten, sind aber nicht beschränkt auf:
  - (i) alle im Besitz der Sicherheitsbehörden befindlichen Datensätze, Technologien und Systeme unabhängig von Form oder Medium und unabhängig davon, ob sie von dieser Behörde erstellt wurden;
  - (ii) physische Standorte, Objekte und Einrichtungen und
  - (iii) Informationen im Besitz von Personen, welche die Aufseher als relevant für ihre Aufsichtsfunktionen ansehen.
- (c) Jegliche Verpflichtung öffentlicher Beschäftigter zur Geheimhaltung oder Vertraulichkeit sollte diese nicht daran hindern, Informationen an die Aufsichtsstellen weiterzugeben. Diese Bereitstellung von Informationen sollte nicht als Verstoß gegen jene gesetzlich oder vertraglich begründeten Verpflichtungen angesehen werden.

### **Prinzip 33: Kompetenzen, Ressourcen und Verfahren, die erforderlich sind, um den Zugang zu Informationen zu ermöglichen**

- (a) Unabhängige Aufsichtsstellen sollten über angemessene rechtliche Kompetenzen verfügen, um in der Lage zu sein, alle relevanten Informationen, die sie für die Ausübung ihres Mandates als notwendig ansehen, erlangen und auswerten zu können.
  - (i) Zu diesen Kompetenzen sollten mindestens die Rechte, aktive und ehemalige Mitglieder der Exekutive sowie Beschäftigte und Vertragspartner von Behörden zu

befragen, relevante Akten anzufordern und zu überprüfen und physische Orte und Einrichtungen zu überprüfen, gehören.

- (ii) Unabhängige Aufsichtsstellen sollten, wo nötig mit umfassender Unterstützung der Strafverfolgungsbehörden, auch die Kompetenz haben, Personen vorzuladen, Aufzeichnungen heraus zu verlangen und Personen unter Eid oder Eidesstattlicher Versicherung zu vernehmen, soweit angenommen wird, dass diese Informationen besitzen, die für die Erfüllung des Mandats notwendig sind.
- (b) Unabhängige Aufsichtsstellen sollten beim Umgang mit Informationen und bei der Erlangung von Zeugenaussagen unter anderem die relevanten Bestimmungen des Datenschutzes sowie das Recht, sich nicht selbst belasten zu müssen und andere Anforderungen eines fairen Verfahrens beachten.
- (c) Unabhängige Aufsichtsstellen sollten Zugang zu den notwendigen finanziellen, technologischen und personellen Ressourcen haben, die es ihnen ermöglichen, jene Informationen, die für eine effektive Durchführung ihrer Aufgaben nötig sind, zu erkennen, sich zugänglich zu machen und zu analysieren.
- (d) Das Gesetz sollte die Institutionen des Sicherheitssektors verpflichten, die unabhängigen Aufsichtsstellen bei der Erlangung und Auswertung von Informationen, die jene für die Erfüllung ihrer Aufgaben benötigen, zu unterstützen.
- (e) Das Gesetz sollte die Institutionen des Sicherheitssektors verpflichten, den unabhängigen Aufsichtsstellen eigeninitiativ und zeitnah jene speziellen Kategorien von Informationen zur Verfügung zu stellen, welche die Aufsichtsstellen als für die Erfüllung ihrer Aufgaben notwendig festgelegt hat. Solche Informationen sollten beinhalten, jedoch nicht beschränkt sein auf: mögliche Verletzungen von Gesetzen und Menschenrechtsstandards.

## **Prinzip 34: Transparenz der unabhängigen Aufsichtsstellen**

### **A. Anwendbarkeit von Gesetzen über den Zugang zu Informationen**

Gesetze, die die Erfüllung des Rechts der Öffentlichkeit auf Zugang zu Informationen, welche im Besitz öffentlicher Stellen sind, regeln, sollten auf diejenigen Stellen Anwendung finden, die den Sicherheitssektor beaufsichtigen.

### **B. Berichterstattung**

- (1) Unabhängige Aufsichtsstellen sollten gesetzlich verpflichtet sein, regelmäßige Berichte zu erstellen und diese der Öffentlichkeit zugänglich zu machen. Diese Berichte sollten mindestens beinhalten: Informationen über die Aufsichtsstelle selbst einschließlich ihres Mandats, ihrer Mitglieder, ihres Budgets sowie ihrer Leistungen und Aktivitäten.

*Hinweis: Diese Berichte sollten auch Informationen beinhalten über das Mandat, die Struktur, das Budget und die allgemeinen Tätigkeiten all jener Institutionen des Sicherheitssektors, die solche Informationen selbst nicht öffentlich verfügbar machen.*

- (2) Unabhängig Aufsichtsstellen sollten auch öffentliche Versionen ihrer Berichte über thematische und fallspezifische Studien und Untersuchungen verfügbar machen, und bezüglich von Angelegenheiten öffentlichen Interesses so viele Informationen wie möglich bereitstellen, dies auch hinsichtlich der in Prinzip 10 genannten Bereiche.
- (3) Bei ihrer öffentlichen Berichterstattung sollten die unabhängigen Aufsichtsstellen die Rechte aller Betroffenen, einschließlich deren Rechts auf Privatsphäre, respektieren.
- (4) Unabhängige Aufsichtsinstitutionen sollten den unter ihrer Aufsicht stehenden Stellen die Möglichkeit einräumen - innerhalb einer gewissen Frist - die zu veröffentlichenden Berichte zu überprüfen, damit diese Bedenken hinsichtlich der Verwendung von möglicherweise als geheim eingestuftem Material äußern können. Die endgültige Entscheidung darüber, was veröffentlicht werden sollte, sollte der Aufsichtsstelle selbst überlassen bleiben.

### **C. Verbreitung und Zugänglichkeit**

- (1) Die Rechtsgrundlagen der Aufsichtsstellen, einschließlich ihrer Mandate und Befugnisse, sollten öffentlich verfügbar und leicht zugänglich sein.
- (2) Unabhängige Aufsichtsstellen sollten Mechanismen und Hilfestellungen schaffen für Menschen, die Analphabeten sind, die Minderheitensprachen sprechen oder Seh- oder Hörbehinderungen aufweisen, damit auch diese auf Informationen über ihre Arbeit zugreifen können.
- (3) Unabhängige Aufsichtsstellen sollten eine Reihe von frei zugänglichen Mechanismen anbieten, durch welche es der Öffentlichkeit - einschließlich Personen aus geografisch abgelegenen Standorten - erleichtert wird, mit ihnen Kontakt aufzunehmen, bzw. falls es sich bei der Stelle um eine Beschwerdestelle handelt, Beschwerden einzulegen oder Bedenken aufnehmen zu lassen.
- (4) Unabhängige Aufsichtsstellen sollten über Mechanismen verfügen, die die Vertraulichkeit der Beschwerden und die Anonymität des Beschwerdeführers effektiv gewährleisten.

### **Prinzip 35: Maßnahmen zum Schutz von Informationen, die von Aufsichtsstellen des Sicherheitssektors verarbeitet werden**

- (a) Das Gesetz sollte unabhängige Aufsichtsstellen verpflichten, alle erforderlichen Maßnahmen zu ergreifen, um die in ihrem Besitz befindlichen Informationen zu schützen.
- (b) Der Gesetzgeber sollte die Macht haben, zu entscheiden, ob (i) die Mitglieder der parlamentarischen Aufsichtsgremien und (ii) die Leiter und Mitglieder der unabhängigen, nicht-legislativen Aufsichtsstellen, sich vor ihrer Ernennung einer Sicherheitsüberprüfung unterziehen müssen.
- (c) Wo eine Sicherheitsüberprüfung gefordert wird, sollte diese durchgeführt werden: (i) innerhalb eines angemessenen Zeitraums, (ii) in Übereinstimmung mit festgelegten

Prinzipien, (iii) frei von politischer Voreingenommenheit oder Motivation, und (iv), wenn möglich, von einer Institution, die nicht der Aufsicht jener Stelle unterliegt, deren Mitglieder/Personal überprüft werden.

(d) Unter Beachtung der in Teil VI und VII niedergelegten Prinzipien sollten die Mitglieder oder Beschäftigten der unabhängigen Aufsichtsstellen, welche Verschlussachen oder anderweitig vertrauliches Material außerhalb der normalen Berichtswege der Stelle offenlegen, angemessenen verwaltungs-, zivil- oder strafrechtlichen Verfahren unterzogen werden.

### **Prinzip 36: Autorität des Gesetzgebers, Informationen öffentlich zu machen**

Der Gesetzgeber sollte - wenn er dies für angemessen erachtet und im Einklang mit einem von ihm festgelegten Verfahren - die Macht haben, jegliche Information der Öffentlichkeit zugänglich zu machen, einschließlich derjenigen Informationen, hinsichtlich derer die Exekutive behauptet, diese aus Gründen der nationalen Sicherheit zurückhalten zu dürfen.

## **TEIL VI: OFFENLEGUNG DURCH ÖFFENTLICHE BESCHÄFTIGTE IM ÖFFENTLICHEN INTERESSE**

### **Prinzip 37: Kategorien von Fehlverhalten**

Die Offenlegung von Informationen, unabhängig von deren Einstufung als geheim, durch öffentliche Beschäftigte, welche Fehlverhalten aufzeigen, welches in eine der folgenden Kategorien fällt, sollte als eine "geschützte Offenlegung" angesehen werden, wenn sie den Bedingungen genügt, die in den Prinzipien 38-40 niedergelegt sind. Eine geschützte Offenlegung kann dabei Fehlverhalten betreffen, das bereits stattgefunden hat, gerade stattfindet oder wahrscheinlich stattfinden wird.

- (a) Straftaten;
- (b) Menschenrechtsverletzungen;
- (c) Verletzungen des internationalen humanitären Völkerrechts;
- (d) Korruption;
- (e) Gefahren für die öffentliche Gesundheit und Sicherheit;
- (f) Gefahren für die Umwelt;

- (g) Missbrauch eines öffentlichen Amtes;
- (h) Fehltritte;
- (i) Misswirtschaft oder Verschwendung von Ressourcen;
- (i) Vergeltung für die Offenlegung von einer der oben aufgeführten Kategorien von Fehlverhalten und
- (k) absichtliches Verschweigen einer Angelegenheit, die einer der vorstehenden Kategorien unterfällt.

### **Prinzip 38: Gründe, Motivation und Beweise für die Offenlegung von Informationen zum Beleg von Fehlverhalten**

- (a) Das Gesetz sollte öffentliche Beschäftigte, welche Informationen offenlegen, die Fehlverhalten belegen, vor Vergeltungsmaßnahmen, wie sie im Prinzip 41 definiert werden, schützen; dies unabhängig davon, ob die Information eine Verschlussangelegenheit oder anderweitig vertraulich ist, sofern zum Zeitpunkt der Offenlegung:
  - (i) die Person, welche die Offenlegung vorgenommen hat, vernünftige Gründe hatte anzunehmen, dass die offengelegte Information dazu geeignet ist, Fehlverhalten aufzuzeigen, welches einer der in Prinzip 37 genannten Kategorien unterfällt und
  - (ii) die Offenlegung im Einklang mit den in den Prinzipien 38 – 40 niedergelegten Bedingungen erfolgte.
- (b) Die Motivation für eine geschützte Offenlegung ist irrelevant, es sei denn, dass nachgewiesen wird, dass die Offenlegung im Wissen um deren Falschheit erfolgte.
- (c) Eine Person, die eine geschützte Offenlegung vornimmt, sollte nicht verpflichtet sein, unterstützende Nachweise vorzulegen oder die Beweislast in Bezug auf ihre Offenlegung zu tragen.

### **Prinzip 39: Verfahren für die Vornahme von und die Reaktion auf geschützte Offenlegungen, die intern oder gegenüber Aufsichtsstellen erfolgen**

#### **A. Interne Offenlegungen**

Das Gesetz sollte öffentlichen Stellen verpflichten interne Verfahren einzurichten und Personen für die Entgegennahme von geschützten Offenlegungen zu benennen.

#### **B. Offenlegungen an unabhängige Aufsichtsstellen**

- (1) Die Staaten sollten außerdem unabhängige Stellen einrichten oder bezeichnen, die geschützte Offenlegungen entgegennehmen und untersuchen. Jene Stellen sollten institutionell und operativ von den Sicherheitsorganen und anderen Stellen, einschließlich der Exekutive, unabhängig sein, aus deren Reihen Offenlegungen erfolgen könnten.
- (2) Die Beschäftigten des öffentlichen Dienstes sollte die Befugnis haben, geschützte Offenlegungen gegenüber einer Aufsichtsstelle oder einer anderen für die

Untersuchung der Angelegenheit zuständigen Stelle vornehmen zu können, ohne verpflichtet zu sein, die Offenlegung zuvor intern vorgenommen zu haben.

- (3) Das Gesetz sollte gewährleisten, dass die unabhängigen Aufsichtsstellen Zugang zu allen relevanten Informationen haben, und ihnen die notwendigen Ermittlungsbefugnisse verleihen, um diesen Zugang sicherzustellen. Diese Kompetenzen sollten die Befugnis umfassen, Vorladungen vorzunehmen und Zeugenaussagen unter Eid oder eidesstattlicher Versicherung zu verlangen.

### **C. Pflichten der internen Stellen und der unabhängigen Aufsichtsstellen, die Offenlegungen entgegennehmen**

Wenn eine Person eine geschützte Offenlegung, wie sie in Prinzip 37 definiert ist, intern oder gegenüber einer unabhängigen Aufsichtsstelle vornimmt, sollte die entgegennehmende Stelle verpflichtet sein

- (1) das angebliche Fehlverhalten zu untersuchen und unverzüglich Maßnahmen im Hinblick auf die Lösung der Angelegenheit innerhalb einer gesetzlich bestimmten Zeitspanne vorzunehmen oder – nach Anhörung der Person, die die Offenlegung vorgenommen hat – diese an eine Stelle weiterzuleiten, die zu deren Untersuchung befugt und qualifiziert ist;
- (2) die Identität der öffentlichen Beschäftigten zu schützen, die vertrauliche Eingaben machen wollen; anonyme Eingaben sollten anhand ihres Inhalts beurteilt werden;
- (3) die offen gelegten Informationen und die Tatsache, dass eine Offenlegung erfolgt ist, zu schützen – außer dass und insoweit als eine Offenlegung der Information gegenüber Dritten zur Behebung der Missstände nötig ist; und
- (4) die Person, welche die Offenlegung vorgenommen hat, über den Fortgang und den Abschluss einer Untersuchung zu unterrichten, soweit möglich gilt dies auch hinsichtlich der ergriffenen Maßnahmen oder Empfehlungen.

### **Prinzip 40: Schutz öffentlicher Offenlegungen**

Das Gesetz sollte Offenlegungen an die Öffentlichkeit, welche die in Prinzip 37 definierten Arten von Fehlverhalten betreffen, vor den in Prinzip 41 definierten Vergeltungsmaßnahmen schützen, wenn die Offenlegung den folgenden Kriterien genügt:

- (a) (1) Die Person hatte eine Offenlegung der gleichen oder von der Substanz her ähnlichen Informationen intern und/oder gegenüber einer unabhängigen Aufsichtsstelle vorgenommen und:
- (i) die Stelle, gegenüber welcher die Offenlegung erfolgte, hat sich geweigert oder es versäumt, die Offenlegung - in Übereinstimmung mit den geltenden internationalen Standards - wirksam zu untersuchen; oder
  - (ii) der Offenlegende, hat innerhalb eines angemessenen und rechtlich definierten Zeitraums kein vernünftiges und angemessenes Ergebnis erhalten.

#### ODER

- (2) Die Person hat vernünftigerweise angenommen, dass bei einer Offenlegung gegenüber einer internen Stelle und/oder gegenüber einer unabhängigen

Aufsichtsstelle ein erhebliches Risiko bestand, dass diese zu einer Zerstörung oder Vertuschung von Beweismitteln, einer Zeugenbeeinflussung oder zu Vergeltungsmaßnahmen gegenüber dieser Person oder gegenüber Dritten geführt hätte;

ODER

(3) Es war keine interne Stelle beziehungsweise keine unabhängige Aufsichtsstelle eingerichtet, gegenüber welcher eine Offenlegung hätte vorgenommen werden können;

ODER

(4) Die Offenlegung bezog sich auf eine Handlung oder Unterlassung, die ein ernstes und unmittelbares Risiko einer Gefahr für das Leben, die Gesundheit oder die Sicherheit von Personen oder für die Umwelt darstellte.

UND

(b) Die Person, die die Offenlegung vornahm, legte nur jene Menge an Informationen offen, die vernünftigerweise notwendig war, um das Fehlverhalten ans Tageslicht zu bringen;

*Hinweis: Wenn bei der Offenlegung von Informationen, welche Fehlverhalten aufzeigen, jemand auch solche Dokumente offenlegt, die keine Relevanz für das Aufzeigen von Fehlverhalten haben, sollte jene Person dennoch vor Vergeltungsmaßnahmen geschützt sein, es sei denn, der durch diese Offenlegung angerichtete Schaden übersteigt das öffentliche Interesse an der Offenlegung.*

UND

(c) Die Person, die die Offenlegung vornahm, nahm vernünftigerweise an, dass das öffentliche Interesse am Bekanntwerden der Information jeden durch die Offenlegung entstehenden Schaden überwiegt.

*Hinweis: Der "nahm vernünftigerweise an"-Test ist ein gemischt subjektiv-objektiver Test. Die Person muss dies tatsächlich angenommen haben (subjektiv) und es muss vernünftig für sie gewesen sein dies zu tun (objektiv). Wenn dies bestritten wird, kann es nötig werden, dass jene Person die Vernünftigkeit ihrer Annahme darlegen muss, wobei es letztlich Aufgabe eines unabhängigen Gerichts oder Spruchkörpers ist, festzustellen, ob dieser Anforderung genüge getan wurde und ob eine geschützte Offenlegung vorlag.*

## **Prinzip 41: Schutz gegen Vergeltung für die Offenlegung von Informationen über Fehlverhalten**

### **A. Zivil- und strafrechtlicher Haftungsausschluss bei geschützter Offenlegung**

Eine Person, die eine Offenlegung in Übereinstimmung mit den Prinzipien 37-40 vorgenommen hat, sollte nicht ausgesetzt werden:

(1) Strafverfahren, einschließlich, aber nicht beschränkt auf die Strafverfolgung für die Offenlegung von als geheim eingestuft oder sonstigen vertraulichen Informationen; oder

- (2) Zivilverfahren wegen der Offenlegung von als geheim eingestuften oder sonstigen vertraulichen Informationen, einschließlich, jedoch nicht beschränkt auf Verfahren wegen Rufschädigung und Schadensersatz.

### **B. Verbot anderer Formen der Vergeltung**

- (1) Das Gesetz sollte Vergeltungsmaßnahmen gegen jede Person verbieten, die eine Offenlegung im Einklang mit den Prinzipien 37-40 vorgenommen hat, möglicherweise vornehmen möchte oder verdächtigt wird, eine solche vorgenommen zu haben.
- (2) Verbotene Formen von Vergeltung umfassen, sind aber nicht beschränkt auf:
- (a) Verwaltungsmaßnahmen oder Strafen, einschließlich, aber nicht beschränkt auf: Abmahnungen, Vergeltungsuntersuchungen, Rückstufungen, Versetzungen, Übertragung anderer Aufgaben, Unterlassen von Beförderungen, Kündigungen, Maßnahmen, die wahrscheinlich eine Rufschädigung bewirken oder auf eine solche abzielen, die Aussetzung oder der Widerruf einer Zugangsberechtigung;
  - (b) Körperliche oder seelische Schädigungen oder Mobbing; oder
  - (c) Androhungen einer der vorgenannten Maßnahmen.
- (3) Maßnahmen gegenüber anderen Personen als jener, die die Offenlegung vorgenommen hat, können unter bestimmten Umständen ebenfalls eine verbotene Vergeltung darstellen.

### **C. Untersuchung von Vergeltungsmaßnahmen durch eine unabhängige Aufsichtsstelle und Justizbehörden**

- (1) Jede Person sollte das Recht haben, sich wegen einer im Zusammenhang mit einer geschützten Offenlegung stehenden Vergeltungsmaßnahme oder deren Androhung an eine unabhängige Aufsichtsstelle und/oder an eine Justizbehörde zu wenden.
- (2) Unabhängig Aufsichtsstellen sollten verpflichtet werden, Meldungen über Vergeltungsmaßnahmen oder deren Androhung zu untersuchen. Solche Stellen sollten auch die Kompetenz haben, Untersuchungen durchzuführen, ohne dass ihnen eine entsprechende Meldung vorliegt.
- (3) Unabhängige Aufsichtsstellen sollten die Befugnisse und die Ressourcen haben, jede behauptete Vergeltungsmaßnahme effektiv zu untersuchen, einschließlich der Befugnis, Personen vorzuladen, Akten heraus zu verlangen und Zeugen unter Eid oder Eidesstattlicher Versicherung zu vernehmen.
- (4) Unabhängige Aufsichtsstellen sollten alle Anstrengungen unternehmen sicherzustellen, dass Verfahren bezüglich behaupteter Vergeltungsmaßnahmen fair und in Übereinstimmung mit rechtmäßigen prozessualen Standards durchgeführt werden.
- (5) Unabhängige Aufsichtsstellen sollten die Befugnis haben, die betreffende Behörde zu Ausgleichs- und Wiedergutmachungsmaßnahmen zu verpflichten, einschließlich aber nicht begrenzt auf: Wiedereinstellung; Rückübertragung; und/oder Erstattung von Verfahrens- und Anwalts- und anderen angemessenen Kosten, rückständigen Gehaltszahlungen und sonstigen Leistungen, Reiskosten und/oder Schadensersatz.

- (6) Unabhängige Aufsichtsstellen sollten auch die Befugnis haben, einer Behörde Vergeltungsmaßnahmen zu untersagen.
- (7) Solche Stellen sollten ihre Untersuchung von Vergeltungsmaßnahmen innerhalb eines angemessenen und gesetzlich festgelegten Zeitraums abschließen.
- (8) Solche Stellen sollten die betroffenen Personen zumindest über den Abschluss einer Untersuchung und, so weit wie möglich, auch über die ergriffenen Maßnahmen und die ausgesprochenen Empfehlungen unterrichten.
- (9) Gegen die Feststellung, dass Reaktionen auf die Offenlegung keine Vergeltungsmaßnahmen darstellen sowie gegen die Ausgleichs- oder Wiedergutmachungsentscheidungen der unabhängigen Aufsichtsstellen können gerichtliche Rechtsmittel eingelegt werden.

#### **D. Beweislast**

Wenn eine Behörde eine nachteilige Maßnahme gegen eine Person ergreift, trägt die Behörde die Beweislast dafür, dass diese Maßnahme nicht im Zusammenhang mit der Offenlegung erfolgte.

#### **E. Kein Verzicht auf Rechte und Rechtsmittel**

Die in den Prinzipien 37-40 festgelegten Rechte und Rechtsmittel können weder ausgesetzt noch begrenzt werden noch kann wirksam auf sie verzichtet werden, weder durch Vereinbarung noch durch Festlegungen, Normen oder Beschäftigungsbedingungen, einschließlich jeder Form von Mediations- oder Schlichtungsvereinbarung. Jeder Versuch, auf diese Rechte und Rechtsmittel zu verzichten oder diese zu begrenzen sollte als nichtig angesehen werden.

#### **Prinzip 42: Förderung und Erleichterung geschützter Offenlegungen**

Die Staaten sollten öffentliche Beschäftigte ermutigen, geschützte Offenlegungen vorzunehmen. Um solche Offenlegungen zu erleichtern, sollten die Staaten alle öffentlichen Stellen verpflichten, Leitlinien zu erlassen, welche die Prinzipien 37-42 wirksam werden lassen.

*Hinweis: Diese Leitlinien sollten mindestens Angaben enthalten zu: (1) Hinweisen hinsichtlich der Rechte und/oder Verantwortlichkeiten bezüglich der Offenlegung von Fehlverhalten; (2) den Arten von Informationen, die offengelegt werden sollten oder können; (3) den vorgeschriebenen Verfahren zur Durchführung solcher Offenlegungen; und (4) den gesetzlich festgelegten Schutzmechanismen.*

#### **Prinzip 43: Öffentliches Interesse als Rechtfertigungsgrund für Beschäftigte des öffentlichen Dienstes**

- (a) Für alle Fälle, in denen Beschäftigte des öffentlichen Dienstes hinsichtlich einer Offenlegung von Informationen, welche nicht ohnehin bereits durch eines dieser Prinzipien geschützt ist, straf-oder zivilrechtlichen Verfahren oder

verwaltungsrechtlichen Sanktionen ausgesetzt sind, sollte das Recht einen Rechtfertigungsgrund „öffentliches Interesse“ normieren, sofern das öffentliche Interesse an der Offenlegung das öffentliche Interesse an der Geheimhaltung der fraglichen Information übersteigt.

*Hinweis: Dieser Prinzip gilt für alle Offenlegungen von Informationen, die nicht ohnehin bereits geschützt sind, sei es weil die Information nicht zu den in Prinzip 37 genannten Kategorien gehört, oder weil die Offenlegung zwar Informationen betrifft, die den Kategorien aus Prinzip 37 unterfallen, aber nicht im Einklang mit dem in den Prinzipien 38-40 dargelegten Verfahren erfolgte.*

- (b) Bei der Entscheidung, ob das öffentliche Interesse an der Offenlegung das öffentlichen Interesse an der Geheimhaltung überwiegt, sollten Staatsanwaltschaften und Gerichte berücksichtigen:
- (i) ob der Umfang der Offenlegung vernünftiger Weise notwendig war, um die Informationen, welche von öffentlichem Interesse sind, offenzulegen;
  - (ii) das Ausmaß und das Risiko einer Schädigung des öffentlichen Interesses durch die Offenlegung;
  - (iii) ob die Person vernünftiger Weise annehmen durfte, dass die Offenlegung im öffentlichen Interesse sein würde;
  - (iv) ob die Person versucht hat, eine geschützte Offenlegung im Einklang mit den Prinzipien 38-40 vorzunehmen durch Nutzung interner Verfahren und/oder gegenüber einer unabhängigen Aufsichtsstelle und/oder der Öffentlichkeit; und
  - (v) die Existenz von außerordentlichen Umständen, welche die Offenlegung rechtfertigen.

*Hinweis: Jedes Gesetz, welches Strafen für die unbefugte Offenlegung von Informationen vorsieht, sollte im Einklang mit Prinzip 46(b) stehen. Dieses Prinzip beabsichtigt nicht, bereits bestehende Rechte auf freie Meinungsäußerung von Mitarbeitern des öffentlichen Dienstes oder den in den Prinzipien 37-42 oder 46 gewährleisteten Schutz in irgendeiner Weise einzuschränken.*

## **TEIL VII: GRENZEN FÜR MAßNAHMEN ZUR SANKTIONIERUNG ODER BEGRENZUNG VON OFFENLEGUNGEN GEGENÜBER DER ÖFFENTLICHKEIT**

### **Prinzip 44: Schutz gegen Strafen für gutgläubige und vernünftige Offenlegungen durch Informationsbeauftragte**

Personen mit Verantwortung für die Beantwortung von Informationsanfragen aus der Öffentlichkeit sollten nicht dafür sanktioniert werden, dass sie Informationen herausgegeben haben, hinsichtlich derer sie gutgläubig und vernünftiger Weise davon ausgingen, dass sie rechtmäßig offengelegt werden durften.

## **Prinzip 45: Strafen für die Zerstörung oder die Verweigerung der Offenlegung von Informationen**

- (a) Mitarbeiter des öffentlichen Dienstes sollten Strafen unterliegen für die vorsätzliche Vernichtung oder Manipulation von Informationen mit der Absicht, der Öffentlichkeit den Zugang zu verwehren;
- (b) Wenn ein Gericht oder eine unabhängige Stelle die Offenlegung einer Informationen angeordnet hat, und diese Information nicht innerhalb eines angemessenen Zeitraums offengelegt wird, sollte der hierfür verantwortliche Beamte und/oder die verantwortliche Behörde angemessenen Sanktionen unterliegen; dies gilt nicht wenn im Einklang mit dem rechtlich vorgesehen Verfahren ein Rechtsmittel eingelegt wurde.

## **Prinzip 46: Begrenzungen der Strafbarkeit der Offenlegung von Informationen durch Mitarbeiter des öffentlichen Dienstes**

- (a) Die öffentliche Offenlegung von Informationen durch Beschäftigte des öffentlichen Dienstes sollte, selbst wenn diese nicht nach Teil VI geschützt ist, nicht Gegenstand strafrechtlicher Sanktionen sein, mag jedoch zu administrativen Sanktionen führen, wie z.B. dem Verlust von Zugangsberechtigungen oder sogar des Arbeitsplatzes.
- (b) Wenn das Gesetz dennoch strafrechtliche Sanktionen vorsieht für unberechtigte Offenlegungen von Informationen gegenüber der Öffentlichkeit oder gegenüber Personen in der Absicht, dass die Informationen öffentlich gemacht werden, sollten die folgenden Bedingungen gelten:
  - (i) strafrechtliche Sanktionen sollten nur hinsichtlich der Offenlegung bestimmter gesetzlich eindeutig und eng festgelegter Informationskategorien Anwendung finden;  
*Hinweis: Soweit nationales Recht Kategorien von Informationen festlegt, deren Offenlegung Gegenstand strafrechtlicher Sanktionen sein kann, sollten diese hinsichtlich ihrer Spezifizierung und Auswirkungen auf die nationale Sicherheit den folgenden ähneln: technologische Daten über Nuklearwaffen; nachrichtendienstliche Quellen, Codes und Methoden; diplomatische Codes; die Identität von Geheimagenten; und geistiges Eigentum, hinsichtlich dessen die Regierung Eigentümerinteressen hat und dessen Bekanntwerden der nationale Sicherheit schaden könnte.*
  - (ii) Die Offenlegung sollte ein reales und erkennbares Risiko eines erheblichen Schaden darstellen;
  - (iii) Jede strafrechtliche Sanktion sollte in ihrer gesetzlichen Festschreibung und ihrer Anwendung proportional zu dem verursachten Schaden sein; und
  - (iv) Die Person sollte in der Lage sein sich, wie in Prinzip 43 dargelegt, auf den Rechtfertigungsgrund des öffentlichen Interesses zu berufen.

### **Prinzip 47: Schutz vor Sanktionen für Personen, die nicht im öffentlichen Dienst beschäftigt sind hinsichtlich des Besitzes und der Verbreitung von Informationen, die als geheim eingestuft wurden**

- (a) Eine Person, die nicht Beamter ist, darf für die Entgegennahme, den Besitz oder die Veröffentlichung von als geheim eingestuften Informationen nicht sanktioniert werden.
- (b) Eine Person, die nicht Beamter ist, darf nicht wegen Verschwörung oder anderen Straftaten beschuldigt werden, weil sie diese Informationen gesucht und erhalten hat.

*Hinweis: Dieses Prinzip will die Strafverfolgung für den Erwerb oder die Wiedergabe der Informationen verhindern. Allerdings ist mit diesem Prinzip nicht beabsichtigt, die Verfolgung einer Person für andere Verbrechen wie Einbruch oder Erpressung, auszuschließen, die im Zuge der Suche nach oder bei der Beschaffung der Informationen begangen wurden.*

*Hinweis: Offenlegungen durch Dritte dienen als wichtiges Korrektiv gegenüber allgegenwärtiger ausufernder Einstufung als geheim.*

### **Prinzip 48: Schutz von Quellen**

Keine Person, die nicht Beamter ist, sollte im Rahmen einer Untersuchung über die unberechtigte Offenlegung von Informationen gegenüber der Presse oder der Öffentlichkeit gezwungen werden können, eine vertrauliche Quelle oder unveröffentlichte Materialien preisgeben zu müssen.

*Hinweis: Dieses Prinzip bezieht sich nur auf Untersuchungen über unberechtigte Offenlegungen von Informationen, nicht auf andere Straftaten.*

### **Prinzip 49: Vorab-Beschränkungen**

- (a) Vorab-Beschränkungen gegen Veröffentlichungen im Interesse des Schutzes der nationalen Sicherheit sollten verboten werden.

*Hinweis: Vorab-Beschränkungen sind Anordnungen von Gerichten oder anderen staatlichen Stellen, die die Veröffentlichung eines bestimmten Materials untersagen, welches sich bereits im Besitz einer Person befindet, die kein Beamter ist.*

- (b) Soweit Informationen bereits, auf welchem Weg auch immer, sei es rechtmäßig oder nicht, allgemein für die Öffentlichkeit zugänglich gemacht wurden, wird vermutet, dass jeglicher Versuch eine weitere Veröffentlichung dieser Informationen in ihrer bereits öffentlich verfügbaren Form zu unterbinden, unzulässig ist.

*Hinweis: "allgemein ... zugänglich " meint, dass die Informationen bereits ausreichend weit verbreitet wurden, sodass es keine praktisch durchführbaren Maßnahmen gibt, mittels derer die Informationen geheim gehalten werden könnten.*

## **TEIL VIII: ABSCHLIEßENDES PRINZIP**

### **Prinzip 50: Beziehung dieser Prinzipien zu anderen Standards**

Nichts in diesen Prinzipien sollte als Einschränkung oder Begrenzung verstanden werden hinsichtlich irgendeines Rechts auf Informationszugang, welches im Rahmen internationaler, regionaler oder nationaler Rechtsvorschriften oder Standards anerkannt ist, oder hinsichtlich irgendwelcher Vorschriften innerstaatlichen oder internationalen Rechts, die einen besseren Schutz bezüglich der Offenlegung von Informationen durch Mitarbeiter des öffentlichen Dienstes oder andere vorsehen.

## **Anhang: Partner Organisationen**

Die folgenden 22 Organisationen trugen wesentlich zur Ausarbeitung der Prinzipien bei und sind bestrebt, daran mitzuarbeiten, diese zu verbreiten, zu veröffentlichen, und bei deren Umsetzung zu helfen.<sup>2</sup> Nach dem Namen der jeweiligen Organisation ist, soweit vorliegend, die Stadt angegeben, in der sie ihren Sitz hat und das Land oder die Region, in der sie arbeitet. Organisationen, die umfangreiche Arbeit in drei oder mehr Regionen leisten, werden als "global" angeführt.

- Africa Freedom of Information Centre (Kampala/Afrika);
- African Policing Civilian Oversight Forum (APCOF) (Kapstadt/Afrika)
- Alianza Regional por la Libre Expresión e Información (Amerika)
- Amnesty International (London/global);
- Article 19, the Global Campaign for Free Expression (London/global);
- Asian Forum for Human Rights and Development (Forum Asia) (Bangkok/Asien);
- Center for National Security Studies (Washington DC/USA);
- Central European University (Budapest/ Europa);
- Centre for Applied Legal Studies (CALS), Wits University (Johannesburg/Südafrika);
- Centre for European Constitutionalization and Security (CECS), University of Copenhagen (Kopenhagen/Europa);
- Centre for Human Rights, University of Pretoria (Pretoria/Afrika);
- Centre for Law and Democracy (Halifax/global);
- Centre for Peace and Development Initiatives (Islamabad/Pakistan);
- Centre for Studies on Freedom of Expression and Access to Information (CELE), Palermo University School of Law (Buenos Aires/Argentinien);
- Commonwealth Human Rights Initiative (New Delhi/Commonwealth);
- Egyptian Initiative for Personal Rights (Kairo/Ägypten);
- Institute for Defence, Security and Peace Studies (Jakarta/Indonesien);
- Institute for Security Studies (Pretoria/Afrika);
- International Commission of Jurists (Genf/global);
- National Security Archive (Washington DC/global);
- Open Democracy Advice Centre (Kapstadt /Südliches Afrika); und
- Open Society Justice Initiative (New York/global).

---

<sup>2</sup> Darüber hinaus lieferten Aidan Wills und Benjamin Buckland vom Geneva Centre for Democratic Control of the Armed Forces (DCAF), die nicht einer der Partner-Organisationen angehören, besonders bedeutende Beiträge zu Teil V über Aufsichtsstellen und zu Teil VI über Offenlegungen im öffentlichen Interesse und ebenso zu den Prinzipien im Ganzen.

*Deutsche Übersetzung: Whistleblower-Netzwerk e.V. - <http://whistleblower-net.de>*