# „Datenschutz vermitteln und effektiver gestalten“

## Ursprung dieser Initiative

Dieser Bericht hat seinen Ursprung in der Rede von Alex Türk, dem Vorsitzenden der französischen Datenschutzbehörde (CNIL), anlässlich einer im Mai 2006 vom polnischen Generalinspektor für Datenschutz in Warschau abgehaltenen Konferenz zum Thema „Öffentliche Sicherheit und Schutz der Privatsphäre“. Alex Türk sprach über seine ernste Besorgnis angesichts der Herausforderungen, denen die Datenschutzbehörden zurzeit gegenüberstehen. Er betonte, dass die Datenschutzbehörden ihre Aktivitäten dringend auf diese Herausforderungen ausrichten müssten, da andernfalls Gefahr bestehe, dass die den Datenschutzbestimmungen zugrunde liegende Philosophie in kürzester Zeit an Gehalt verliere.

Im Anschluss an die Konferenz lud der Europäische Datenschutzbeauftragte (EDPS) den CNIL ein, eine gemeinsame Initiative ins Leben zu rufen, um die Notwendigkeit dieser dringlichen Maßnahmen bei der Konferenz in London zu präsentieren. Der britische Datenschutzbeauftragte gab der Initiative sofort volle Unterstützung. Vorliegender Bericht wurde in enger Zusammenarbeit der drei genannten Datenschutzbehörden erstellt.

Durch ihren Beitritt zu dieser Initiative verpflichten sich die teilnehmenden Datenschutzbehörden, ihre Aktivitäten im Hinblick auf die folgenden Ziele zu koordinieren:

- Entwicklung von Kommunikationsaktivitäten auf der Grundlage gemeinsamer Ideen, von denen einige in beigefügtem Text zum Ausdruck gebracht werden
- Anpassung der eigenen Verfahrensweisen und Methoden durch eingehende Beurteilung ihrer Effektivität und Effizienz sowie durch Ausweitung ihrer Kapazitäten in den Bereichen technische Kompetenz, Trendprognose und Intervention im technologischen Bereich
- Beitrag zur institutionellen Anerkennung von Datenschutzbehörden auf internationaler Ebene und Förderung der Einbeziehung anderer relevanter Interessenvertreter auf nationaler und internationaler Ebene

Zum gegenwärtigen Zeitpunkt haben die folgenden Datenschutzbehörden bestätigt, diese Initiative grundsätzlich zu unterstützen:

- Commission nationale de l’informatique et des libertés (Frankreich)
- European Data Protection Supervisor (Europäische Union)
- Information Commissioner (Großbritannien und Nordirland)
- Privacy Commissioner of Canada (Kanada)
- Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (Deutschland)
- Agencia Española de Protección de Datos (Spanien)
- Garante per la Protezione dei Dati Personali (Italien)
- College Bescherming Persoonsgegevens (Niederlande)
- Privacy Commissioner (Neuseeland)
- Préposé fédéral à la protection des données et à la transparence (Suisse) / Eidgenössische Datenschutz und Öffentlichkeitsbeauftragte (Switzerland)

Die gemeinsame Initiative wird während der geschlossenen Sitzung der Internationalen Konferenz der Datenschutzbeauftragten in London am 2.-3. November präsentiert. Sie ist nicht als Beschluss formuliert. Das Dokument wird als gemeinsame Initiative des französischen, europäischen und britischen Datenschutzbeauftragten präsentiert, unterstützt von den oben genannten Datenschutzbehörden, die sich auf diese Weise verpflichten, die Initiative in ihren Aktivitäten zu berücksichtigen. Die anderen bei der Konferenz vertretenen Datenschutzbehörden werden eingeladen, ihre Unterstützung der Initiative zum Ausdruck zu bringen oder auch beizutreten, wenn sie dies wünschen. Sie werden nicht aufgefordert, dieses Dokument offiziell zu verabschieden.

Nach einer einführenden Erinnerung, warum Datenschutz für unsere Gesellschaften unerlässlich ist (I), analysiert der Text im Einzelnen die Bedrohungen, denen persönliche Freiheiten und Datenschutz heute weltweit ausgesetzt sind und die ebenso viele Herausforderungen für die Aufsichtsbehörden darstellen (II). Aus den Ausführungen werden verschiedene Vorschläge für koordinierte Aktivitäten und Initiativen hergeleitet (III), wie auch für die Entwicklung einer neuen Kommunikationsstrategie (IV).

## I – DATENSCHUTZ IST FÜR DIE GESELLSCHAFT UNERLÄSSLICH

1. Für die Gesellschaft ist der Schutz der Personendaten ihrer Bürger unerlässlich. Er steht auf gleicher Ebene wie die Presse- und die Bewegungsfreiheit. Da unsere Gesellschaften zunehmend auf Informationstechnologie angewiesen sind und immer mehr Personendaten erhoben oder erstellt werden, ist es wichtiger als je zuvor, dass individuelle Freiheiten und andere legitime Interessen der Bürger durch geeignete Datenschutzpraktiken auf angemessene Weise respektiert werden.

2. Datenschutz ist kein abstraktes, theoretisches, ganz zu schweigen ein „theologisches“ Thema und darf nicht als solches betrachtet werden. Bestimmungen zum *Datenschutz* dienen dem Schutz des *Einzelnen*. Sie zielen auf die Wahrung des Rechts ab, nicht auf missbräuchliche oder unkontrollierte Weise erfasst oder überwacht zu werden. Sie zielen auf die Verteidigung der menschlichen Würde ab und sollen den Einzelnen in die Lage versetzen, seine Rechte auszuüben und seine legitimen Interessen zu schützen.

3. Datenschutz kann nur dann Realität werden, wenn Datenschutzbestimmungen in der Praxis befolgt werden. Datenschutzbehörden spielen eine wichtige Rolle, indem sie dafür sorgen, dass die Bestimmungen eingehalten werden. Sie können aber nur dann erfolgreich sein, wenn sie das Thema Datenschutz auf effektive Weise vermitteln, andere relevante Interessenvertreter involvieren und – falls nötig – ihre Ermittlungs- und Durchsetzungsrechte auf effektive Weise ausüben.

## II – ZWEI GEFAHRENWELLEN, DREI HERAUSFORDERUNGEN

4. Die Freiheit des Einzelnen, aber auch die Datenschutzbehörden selbst sind bislang nicht da gewesenen Risiken ausgesetzt. Sie sind der Bedrohung unterworfen, von zwei Gefahrenwellen überrollt zu werden, stehen aber zusätzlich noch vor einer dritten Herausforderung.

### A – Die erste Herausforderung gründet sich auf viele unterschiedliche Faktoren, die mit dem Tempo technologischer Veränderungen in Zusammenhang stehen

5. **Beschleunigung:** Internet, RFID, Nanotechnologien etc. Datenschutzbehörden sind Innovation und technologischem Fortschritt gegenüber nicht feindlich eingestellt. Aber der Zeitraum von der Entdeckung eines Phänomens bis zu dessen technischer Umsetzung, von

einer Innovation zur nächsten, von der Entwicklung eines Prototyps bis zu dessen industrieller Anwendung wird kürzer und kürzer. Versuche zur Gesetzesanpassung und Gesetzgebung können immer weniger mit der technologischen Entwicklung Schritt halten. Das Tempo der technologischen Entwicklung wird immer schneller, während das Tempo der Gesetzgebung nach wie vor sehr langsam ist, da es an den von demokratischen Verfahrensweisen auferlegten Rhythmus angepasst ist.

6. **Globalisierung:** Die örtliche Verlagerung der Datenverarbeitung steht in voller Blüte. Es lässt sich wohl kaum bestreiten, dass der internationale Datentransfer sehr schwer zu kontrollieren ist. Dieser Trend hin zur Globalisierung steht im Konflikt mit einem der Hauptmerkmale der Rechtsstaatlichkeit – ihrer geografisch beschränkten Anwendbarkeit.

7. **Ambivalenz:** Technologische Innovation bringt sowohl Fortschritt als auch Gefahren mit sich. Für den Einzelnen mögen die aus Technologie erwachsenden Vorteile und Bequemlichkeiten eine große Verlockung darstellen, die Risiken werden ihm vielleicht jedoch erst dann bewusst, wenn er oder jemand anders zu Schaden gekommen und es zu spät ist. Vielen Menschen ist es egal, dass alle ihre Bewegungen, Aktivitäten und Beziehungen nachvollzogen und potenziell überwacht werden können. Diese Zwiespältigkeit gegenüber der Technologie lässt sich nur schwer mit der Rechtsstaatlichkeit vereinbaren, die definitionsgemäß fest umrissene Antworten geben möchte.

8. **Unvorhersehbarkeit:** Die Anwendung neuer Technologien entwickelt sich manchmal in Richtungen, die anfangs selbst von den Entwicklern der Technologie nicht vorhergesehen wurden. Diese nicht vorhersehbaren Einsatzmöglichkeiten können schwer zu kontrollieren sein, insbesondere wenn die Anwendung einer Technologie von den ursprünglich geplanten Einsatzmöglichkeiten – auf die das Gesetz einfach anwendbar erschien – völlig abweicht.

9. **Unsichtbarkeit (virtuelle Unsichtbarkeit/körperliche Unsichtbarkeit):** Die Datenverarbeitung ist immer weniger sichtbar und greifbar, gleichzeitig auch immer weniger kontrollierbar. Moderne Technologien tendieren zu Unsichtbarkeit, erstens, weil ein großer Teil der Datenverarbeitung stattfindet, ohne dass sich der Einzelne ihrer Existenz bewusst ist (z. B. Nachverfolgbarkeit der Nutzung öffentlicher Verkehrsmittel, des Surfverhaltens im Internet, der elektronischen Kommunikation, der Telefonkommunikation usw.). Da die Prozesse unsichtbar sind, kann man hier von virtueller Unsichtbarkeit sprechen. Technologie wird aber auch unsichtbar aufgrund ihrer extremen Miniaturisierung, die man als körperliche Unsichtbarkeit bezeichnen kann. In ein paar Jahren wird die Entwicklung von Nanotechnologien dazu führen, dass man die in einem Gegenstand enthaltene Technologie mit dem bloßen Auge nicht mehr erkennen kann. Wie will man Verarbeitungsprozesse überwachen, die von unsichtbaren Technologien ausgeführt werden?

10. **Irreversibilität:** Technologischer Fortschritt lässt sich nicht umkehren: Wir werden nie wieder in einer Welt ohne Computer, Internet, Handys, biometrischer Identifizierung, Geolokalisierung und Videoüberwachung leben. In dem Maße, wie diese Technologien konvergieren und immer stärker miteinander verwoben werden, können sie in ihrer Gesamtheit eine echte Gefahr für unsere Gesellschaft darstellen.

## B – Die zweite Herausforderung ist gesetzlicher Art, insbesondere in Bezug auf die neuen Antiterrorgesetze

11. Der Erlass von Antiterrorgesetzen bedeutet eine Herausforderung für die Datenschutzbehörden, die in diesem Zusammenhang Fallen vermeiden, Illusionen aufgeben und Mythen bekämpfen müssen.

12. **Die Notwendigkeit von Ausgewogenheit:** Unabhängige Datenschutzbehörden sind weder Gesetzgeber noch Gerichtshöfe noch Aktivisten, spielen aber dennoch eine äußerst spezifische Rolle. In den seltensten Fällen ist es ihnen möglich, Probleme auf klar umrissene Weise zu lösen. Alle Datenschutzbehörden erkennen die Legitimität von Antiterrorgesetzen an, wie sie in den vergangenen Jahren entwickelt wurden. Vor dem Hintergrund des Auftrags, den die Datenschutzbehörden vom Gesetz erhalten haben, und im Auftrag der Gesellschaft insgesamt ist es jedoch ihre Pflicht, kontinuierlich nach dem richtigen Gleichgewicht zwischen den Erfordernissen der öffentlichen Sicherheit einerseits und der Notwendigkeit des Datenschutzes und des Schutzes der Privatsphäre andererseits zu streben. Sie müssen diese Rolle vollkommen unabhängig erfüllen und die inakzeptablen Anschuldigungen verantwortungslosen Handelns von sich weisen, die gelegentlich gegen sie vorgebracht werden.

13. **Die Gefahr, in einen Teufelskreis zu geraten:** Dieses Risiko – eine Art „schleichende Funktionsausweitung" – sieht folgendermaßen aus: Eine Datenbank wird zu einem bestimmten Zeitpunkt in einer bestimmten Situation angelegt. Die Aufsichtsbehörde ist in die Entwicklung der Datenbank involviert. Zu einem späteren Zeitpunkt erweitert sich der Wirkungsbereich dieser Datenbank. Beispielsweise werden zunächst die Kategorien der erfassten Personen erweitert, dann die Gründe, warum jemand registriert werden kann, später wiederum die Kategorien der Personen, die Zugriff auf die Datenbank haben. In diesen späteren Phasen steht die Behörde dem Argument gegenüber, dass sie eine einfache Erweiterung nicht verweigern kann, da sie das Prinzip zur Erstellung der ursprünglichen Datenbank akzeptiert hat, und so weiter. Und dies, obwohl der ursprünglich akzeptierte Umfang des Systems zwischen der ersten und der letzten Entwicklungsphase so stark vergrößert wurde, dass er nicht länger akzeptabel ist.

14. **Das Trugbild der mustergültigen Natur von Präzedenzfällen in anderen Ländern:** Landesregierungen bringen als Angriff auf die landeseigene Datenschutzbehörde häufig das Argument vor, dass ein anderes Land bereits ein bestimmtes System eingeführt hat, wenn diese sich sträubt, ein in anderen Ländern verwendetes System diskussionslos zu akzeptieren. Dies führt zu ernsten Harmonisierungsproblemen und dazu, dass die Datenschutzbehörden einen gemeinsamen Nenner finden und gemeinsam nachdenken müssen.

15. **Die Illusion der Datenbank als Allheilmittel:** Die Datenschutzbehörden müssen Öffentlichkeit und Regierung fortwährend daran erinnern, dass durch die Schaffung von Datenbanken mit immer mehr Personendaten nicht alle Probleme gelöst werden können. Der „Glorienschein" der angeblich unfehlbaren Computerdatei erweist sich häufig als Illusion. Außerdem steigt mit der Verarbeitung von immer mehr Personendaten auch das Risiko falscher Zuordnungen, veralteter Informationen und anderer Fehler. Dies kann den Lebenschancen, der Gesundheit, dem Wohlstand und selbst der Freiheit des Einzelnen ernstlich schaden.

16. **Der Mythos der unfehlbaren Datei (das „Mehrheits-/Minderheitsproblem"):** Nur allzu häufig wird völlig unfundiert angenommen, dass wir alle aus gutem Grund in einer Datenbank erfasst werden – mit dem Ergebnis, dass sich Personen, die unnötig oder unangemessen erfasst werden („die Minderheit"), gelegentlich in unmöglichen Situationen wiederfinden, da jeder der Ansicht ist, es sei praktisch unmöglich, in einem derart effizienten System grundlos erfasst zu werden. Aus diesem Grund ist es aus ethischer Sicht äußerst wichtig, immer wieder darauf hinzuweisen, dass Technologie nicht unfehlbar ist, und die automatische Entscheidungsfindung, insbesondere in Bereichen wie Sicherheit und Recht, zu verbieten.

## C – Bei der dritten Herausforderung geht es um den Ruf

17. Zumindest in einigen Ländern genießen Datenschutz und Datenschutzbehörden nicht den guten Ruf, den sie verdienen. Es kann die Auffassung herrschen, dass die Bestimmungen komplex sind und sich in der Praxis nur schwer auf konsequente, vorhersehbare und realistische Weise umsetzen lassen. Manche kritisieren die Kontrolle des Datenschutzes als übertrieben abstrakt und nicht ausreichend auf tatsächliche und potenzielle Gefahren ausgerichtet, die sowohl für den Einzelnen als auch für die Gesellschaft insgesamt erwachsen, wenn die Bestimmungen nicht beachtet werden. Andere kritisieren die Art und Weise, in der diese Bestimmungen umgesetzt und durchgesetzt werden, und den Mangel an positiven oder negativen Anreizen zur Einhaltung der Bestimmungen oder zur Investition in angemessene Maßnahmen. Negative Auffassungen wie diese werden von Politikern, Verwaltungsbeamten, Unternehmen, den Medien und manchmal auch von Privatpersonen vertreten. Es ist wichtig, gegen derartige Ansichten vorzugehen, die praktische Bedeutung des Datenschutzes aufzuzeigen, die viel besprochenen Grundrechte und Grundfreiheiten zur Realität zu machen und die derzeitigen Praktiken – sofern angemessen – zu überdenken.

# III – AUFGABEN UND INITIATIVEN FÜR DATENSCHUTZBEHÖRDEN

18. Die Datenschutzbehörden müssen dringend Maßnahmen ergreifen, um in ihren Bürgern ein gesteigertes Bewusstsein und ein besseres Verständnis der ernsten Risiken zu wecken, die ihre persönlichen Freiheiten in ihrem jeweiligen Land bedrohen. Sie müssen ferner ihre Arbeitsmethoden und ihre Effizienz und Effektivität überdenken.

## A – Die Datenschutzbehörden müssen gemeinsam Änderungen und koordinierte Strategien vorbringen, um so auf neue, effektivere und sachdienlichere Weise zu handeln

19. **Stärkung der Kapazitäten in den Bereichen Fachwissen, fortgeschrittene Studien und Intervention im Technologiesektor:** Der Datenschutz leidet zurzeit unter seinem übermäßig „rechtsbetonten“ Image. Die Glaubwürdigkeit unserer Institutionen hängt jedoch schon heute und auch in Zukunft immer mehr von unserer Fähigkeit ab, technologische Entwicklungen zu verstehen, zu analysieren und vorherzusehen.

20. Zur Analyse dieser neuen Trends müssen die Datenschutzbehörden Strategien erarbeiten, um sich die Arbeit abhängig vom jeweiligen Fall, ihren Erfahrungen, Zuständigkeiten und praktischen Maßnahmen zu teilen.

21. Sie müssen überlegen, welche Beziehungen sie im Bereich neue Technologien zu Forschung und Industrie aufbauen wollen. Sie müssen die Vorteile eines guten Datenschutzes gegenüber Wirtschaft und öffentlichen Körperschaften betonen.

22. **Beurteilung unserer Effektivität und Änderung unserer Praktiken:** Wir müssen unbedingt eine detaillierte und ehrliche Beurteilung der Effektivität einer jeden Behörde durchführen. Zeigt die Arbeit der jeweiligen Behörde wirklich Auswirkungen, erreicht sie etwas in der Praxis? Werden Worte in Taten umgesetzt? Durch derartige Beurteilungen lernen wir, wie wir unsere Ergebnisse verbessern können.

23. Die Beurteilung der Effektivität aller Behörden wird sicherlich dazu führen, dass einige von ihren Gesetzgebern verlangen, sie mit ausreichend Befugnissen und Mitteln auszustatten. Möglicherweise werden auch Fragen zu den Praktiken einiger Behörden aufgeworfen. Wir alle müssen Prioritäten setzen, insbesondere was Gefahr und Schwere eines möglichen

Unheils anbelangt. Wir müssen uns primär auf die Hauptrisiken konzentrieren, denen der Einzelne ausgesetzt ist, und vorsichtig sein, dass wir bei Angelegenheiten, die es nicht verdienen, nicht übermäßig puristisch und rigide vorgehen. Wir müssen zu größerem Pragmatismus und mehr Flexibilität bereit sein.

### B – Datenschutzbehörden müssen gemeinsam überlegen, wie sie auf internationaler Ebene eine bessere institutionelle Anerkennung ihrer Aktivitäten erzielen und andere Interessenvertreter involvieren können

24. **Eine notwendige Umstrukturierung der Internationalen Konferenz:** Globale Herausforderungen brauchen globale Lösungen. Die Internationale Konferenz der Datenschutzbeauftragten muss an der Spitze unserer Aktivitäten auf internationaler Ebene stehen. Wir müssen für die Lebens- und Existenzfähigkeit der Konferenz sorgen, ihre Funktionsweise verbessern, sie sichtbarer und effizienter machen und einen Aktionsplan – ein Kommunikationsprogramm – erarbeiten. Dazu gehört möglicherweise, dass wir darüber nachdenken, ein permanentes Sekretariat für die Konferenz einzurichten. Die Konferenz muss zu einem unvermeidbaren Gesprächspartner bei allen internationalen Initiativen werden, die einen Einfluss auf den Datenschutz haben. Sie muss Raum für Gespräche bieten und Vorschläge aufkommen lassen, damit internationale Initiativen besser verfolgt, Praktiken aufeinander abgestimmt und gemeinsame Standpunkte bezogen werden.

25. **Ausarbeitung einer internationalen Konvention und anderer globaler Instrumente:** In der Erklärung von Montreux (2005) forderten die Datenschutzbeauftragen eine universelle Konvention für den Datenschutz. Diese Initiative muss von den Datenschutzbehörden mit den zuständigen Institutionen unterstützt werden, mit gebührlichem Respekt für deren institutionelle Position und ggf. für die notwendigen Vorbedingungen einer landesinternen Koordination. Innerhalb dieses Rahmenwerks sollten sich die Datenschutzbehörden bemühen, die Initiative in ihrem jeweiligen Einflussbereich voranzutreiben, vor allem innerhalb der regionalen Organisationen und der Sprachzonen, in denen sie tätig sind. In bestimmten Sektoren (z. B. Internetkontrolle, Finanztransaktionen, Flugverkehr) kann die Notwendigkeit globaler Lösungen zur Respektierung von Privatsphäre und Datenschutz entstehen, worauf die Datenschutzbehörden mit allen geeigneten Mitteln eingehen müssen.

26. **Involvierung anderer Interessenvertreter (Einrichtungen der Zivilgesellschaft, Nichtregierungsorganisationen usw.):** Zurzeit sind sowohl national als auch international diverse andere Interessenvertreter für den Datenschutz und den Schutz der Privatsphäre aktiv, auf unterschiedlichen Ebenen und in unterschiedlichen Sektoren. Derartige Organisationen können als strategische Partner agieren und wesentlich dazu beitragen, dass die Datenschutzbehörden effektiver werden. Die Kooperation mit anderen geeigneten Interessenvertretern sollte daher gefördert oder aktiv entwickelt werden.

## IV – EINER NEUEN KOMMUNIKATIONSSTRATEGIE ENTGEGEN

27. Kommunikation ist eine Hauptvoraussetzung, um Datenschutz effektiver zu machen. Eine Botschaft, die nicht ankommt und nicht verstanden wird, ist im Grunde genommen nicht existent. Eine Meinung oder Entscheidung, auf die sich nicht zugreifen lässt, ist in ihrer Wirkung begrenzt und möglicherweise nicht die auf ihre Ausarbeitung verwendete Mühe wert.

### A – Wir müssen dringend eine neue Kommunikationsstrategie entwickeln, sowohl auf nationaler als auch auf internationaler Ebene

28. **Kommunikation als Ziel.** Eine sehr viel bessere Kommunikation mit der Öffentlichkeit muss eines der Hauptziele aller Datenschutzbehörden sein. Es ist inakzeptabel, dass in einigen Ländern, in denen das Recht auf Datenschutz – ebenso wie die Bewegungs- und Pressefreiheit – zu den Grundrechten gehört, die große Mehrheit unserer Mitbürger sich dieser Rechte und ihrer Bedeutung nicht bewusst ist. Noch viel weniger akzeptabel ist dies, wenn eine negative Einstellung gegenüber dem Datenschutz herrscht.

29. Wir müssen wirkungsvolle Kampagnen zur langfristigen Bewusstseinssteigerung ins Leben rufen, die den Einzelnen über die Existenz und den Inhalt seiner Rechte informieren. Die Wirksamkeit dieser Maßnahmen muss gemessen werden. Dabei gibt es zwei spezifische Ziele:

    - Gewählte Vertreter auf landesweiter und kommunaler Ebene – die meisten von ihnen sind nicht besser informiert als der Durchschnittsbürger.
    - Junge Menschen, die wenig Interesse an diesen Fragen haben, da sie so sehr an neue Technologien gewohnt sind. Wir müssen so bald wie möglich im Bereich der Bildung und Aufklärung aktiv werden.

30. **Kommunikation als wirkungsvolles Hebelwerkzeug.** Es ist wichtig und dringlich, dass unsere Datenschutzbehörden bessere Handlungsmittel erhalten und Anerkennung auf internationaler Ebene zugesichert bekommen. Öffentliches Vertrauen und Unterstützung sind unerlässlich. Datenschutz muss konkreter gemacht werden. Nur Organisationen, die kommunizieren – normalerweise über die Medien und auf eine Art und Weise, die für die Öffentlichkeit insgesamt **bedeutungsvoll, zugänglich und relevant** ist – werden die Macht erhalten, die erforderlich ist, um die öffentliche Meinung zu beeinflussen, und somit von den Staaten und der internationalen Gemeinde gehört und ernst genommen zu werden. Nur wenn diese Bedingung erfüllt wird, können die Datenschutzbehörden unverzichtbare Handlungsmittel erhalten.

31. Das bedeutet, dass wir in allen unseren Behörden professionelle Kommunikationspartner einsetzen, und dass die vermittelten Botschaften in allen Datenschutzbehörden möglichst einheitlich sind.

## B – Eine interessante Kommunikationsbotschaft könnte im Aufzeigen einer Parallele zwischen dem Schutz der persönlichen Freiheiten und dem Schutz der Umwelt liegen

32. Was die Umwelt anbelangt, so werden wir nicht ungestraft davonkommen. Auf die gleiche Weise müssen wir im Bereich des Datenschutzes bei jeder unkontrollierten technologischen Entwicklung und jedem Gesetz, das ohne klare Vision der potenziellen Risiken erlassen wird, höchste Vorsicht walten lassen. In einem solchen Fall besteht die Gefahr, dass unser „Kapital“ in Form von Freiheit und Identität reduziert oder sogar zunichte gemacht wird. Auch kann es nicht wiedergewonnen werden, und zwar genau deshalb, weil technologische Innovation irreversibel ist.

33. Möglicherweise sind Datenschutz und der Schutz der Privatsphäre genauso kostbar wie die Luft, die wir atmen. Beide sind unsichtbar, aber ihr Verlust ist gleichermaßen mit katastrophalen Folgen verbunden.

## V – PROGRAMM ANSCHLIESSENDER AKTIVITÄTEN

34. Die Besprechung dieser Initiative bei der geschlossenen Sitzung der Internationalen Konferenz der Datenschutzbeauftragten in London sollte als erster Schritt in Richtung eines wachsenden Konsenses gesehen werden – eines Konsenses über die Notwendigkeit zur Ausarbeitung von Mitteln für bessere Kommunikation und effektiveren Datenschutz.

35. Datenschutzbehörden, die diese Initiative unterstützen, verpflichten sich zur Weiterentwicklung von und übernehmen ggf. die Verantwortung für eine Reihe von Aktivitäten, die bei der nächsten Konferenz in Montreal vorgestellt und weiter verfolgt werden, z. B.:
    - Workshop zu strategischen Themen: Bedingungen, um Datenschutzbehörden effektiver zu machen; mögliche Entwicklung von „Prinzipien einer guten Überwachung“ beim Datenschutz; Informationen zu Best Practice (Datenschutzbeauftragte und strategische Mitarbeiter); Überlegungen hinsichtlich der Entwicklung einer internationalen Konvention
    - Workshop zum Thema Kommunikation: Verfügbares Expertenwissen im Bereich der Datenschutzkommunikation (z. B. Kampagnen, Meinungsforschung); Entwicklung einer gemeinsamen Botschaft und wirksamer Hilfsmittel für deren Verbreitung (professionelle Kommunikationspartner)
    - Workshop zum Thema Durchsetzung: Verfügbares Expertenwissen im Bereich Überwachung und Gewährleistung der Vorschriftenbefolgung; wirksame Mechanismen zur Inspektion (z. B. Audits) und Intervention (Datenschutzbeauftragte und Personal von Durchsetzungsbehörden)
    - Workshop zur internen Organisation: Jüngste Erfahrungen mit organisatorischen Veränderungen; Projekte zur Verbesserung von Effizienz und Effektivität (Datenschutzbeauftragte und organisatorisches Personal)
    - Alle sonstigen Aktivitäten, die für diese Initiative als relevant erachtet werden