Stellungnahme des Europäischen Datenschutzbeauftragten zu einem von der Europäischen Union durch das Siebte Rahmenprogramm (RP7) für Forschung und technologische Entwicklung (FTE) finanzierten Forschungsprojekt – Turbine (TrUsted Revocable Biometric IdeNtitiEs)

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE –

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16,

gestützt auf die Charta der Grundrechte der Europäischen Union, insbesondere auf die Artikel 7 und 8,

gestützt auf die Verordnung (EG) Nr. 45/2001 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, insbesondere auf Artikel 41,

zur Umsetzung seines Strategiepapiers mit dem Titel „Der EDSB und Forschung und technologische Entwicklung in der EU", das mit dem laufenden Siebten Rahmenprogramm sowie mit künftigen FTE-Rahmenprogrammen in Zusammenhang steht –

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. Einführung

1.1 Allgemeines

1. Erstmalig gibt der EDSB eine Stellungnahme ab, mit der er sein Strategiepapier aus dem Jahr 2008 umsetzt, das den Titel „Der EDSB und Forschung und technologische Entwicklung in der EU" trägt und in dem beschrieben wird, welche möglichen Rollen der EDSB in FTE-Projekten im Rahmen des Siebten Rahmenprogramms für Forschung und technologische Entwicklung (RP7), das die Kommission Ende 2006 eingeleitet hat, spielen könnte.[1]

2. Im Anschluss an eine Analyse des EU-Projekts „TrUsted Revocable Biometric IdeNtitiEs" (Turbine), das eine Erforschung des Bereichs „widerrufliche

[1] http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/08-04-28_PP_RTD_DE.pdf.

Postanschrift: Rue Wiertz 60 – 1047 Brüssel, Belgien
Dienststelle: Rue Montoyer 63
E-Mail: edps@edps.europa.eu – Website: www.edps.europa.eu
Tel.: +32 22831900 – Fax: +32 22831950

biometrische Identitäten“ zum Ziel hat, beschloss der EDSB im Jahr 2008, dem Ersuchen des Konsortiums stattzugeben und eine Stellungnahme zu dem EU-Projekt abzugeben.[2] Der EDSB war der Auffassung, dass das Turbine-Konsortium die Bedingungen erfüllt hatte, die gemäß seinem Strategiepapier für einen Beitrag des EDSB gegeben sein müssen. Er begrüßte die große Bedeutung des Projekts für „Datenschutzfragen“ und war der Ansicht, dass es unter die Prioritäten fällt, die er in seinem Jahresbericht festgelegt hatte.

1.2 Das Instrument der Stellungnahme zu Forschung und technologischer Entwicklung in der EU

3. Dieses Strategiepapier stellt die Kriterien, die Projekte für Beiträge des EDSB erfüllen müssen und auf welche Art und Weise der EDSB an diesen Projekten mitwirken könnte, vor. Einer der Beiträge des EDSB zu Forschung und technologischer Entwicklung in der EU besteht in Stellungnahmen zu einzelnen Forschungsprojekten.

4. In dem Strategiepapier des EDSB heißt es: „Ein für ein bestimmtes Projekt gebildetes Konsortium kann den EDSB um Stellungnahme ersuchen. Zwar leistet der EDSB keine Beiträge zu einem Vorschlag für ein Projekt, es kann jedoch in dem Projektvorschlag vorgesehen werden, dass – sofern dieser den Zuschlag erhält – während der Laufzeit des Projekts eine Stellungnahme des EDSB eingeholt wird. In diesem Fall muss der EDSB davon in Kenntnis gesetzt werden und seine Zustimmung dazu geben, dass vor der Vorlage der Antwort auf die Aufforderung zur Einreichung von Vorschlägen eine Bezugnahme auf eine künftige Stellungnahme des EDSB in den Vorschlag aufgenommen wird. Das Konsortium muss in den mit seinem Vorschlag eingereichten Unterlagen deutlich machen, dass der EDSB seine Stellungnahme in seiner Eigenschaft als unabhängige Behörde abgeben wird.“ Die Unabhängigkeit des EDSB im Fall solcher Beiträge wird sowohl im Strategiepapier als auch in allen Schreiben mit den ihn kontaktierenden Interessengruppen des Projekts deutlich hervorgehoben.

1.3 Ziel und Umfang der Stellungnahme

5. Übergeordnetes Ziel des EDSB ist es, mit seinem Beitrag die Anwendung des Grundsatzes des *„eingebauten Datenschutzes“* bei europäischen FTE-Projekten zu fördern, eine striktere Anwendung dieses Grundsatzes zu erreichen und somit die Umsetzung des EU-Rechtsrahmens für den Datenschutz zu erleichtern. Die Stellungnahme geht nicht nur auf die im Forschungsprojekt vorgesehenen technischen Entwicklungen als solche ein, sondern auch auf die im Projekt angewandten Forschungsmethoden und -verfahren.

6. Die Stellungnahme des EDSB soll keine Ergänzung zur Rolle der Gutachter des Projekts oder der zuständigen nationalen Datenschutzbehörden darstellen, sondern ihr Ziel ist es vielmehr, eine fachkundige Meinung zu datenschutzrechtlichen Aspekten eines bestimmten Projekts abzugeben. Infolgedessen prüft der EDSB nicht alle Projektergebnisse, sondern er ersuchte um Einsichtnahme in die Dokumente des Projekts, die seiner Ansicht nach für den Datenschutz von Bedeutung sind.

[2] Siehe: Der Europäische Datenschutzbeauftragte, Jahresbericht 2008, S. 70.

7. Das Konsortium des Projekts stellte dem EDSB alle relevanten Dokumente zur Verfügung, in denen bei den Forschungsarbeiten des Projekts Turbine datenschutzrechtliche Aspekte zum Tragen kommen. Der EDSB führte außerdem mit verschiedenen Vertretern des Konsortiums mehrere Gespräche, um bestimmte Punkte zu klären und bei Bedarf weitere Dokumente zu erhalten. erhielt der EDSB vom Konsortium Anmerkungen zu einem Entwurf seiner Stellungnahme.

1.4 Turbine

8. Turbine (TrUsted Revocable Biometric IdeNtitiEs) ist ein Forschungsprojekt, das von der Europäischen Union durch das Siebte Rahmenprogramm (RP7) für Forschung und technologische Entwicklung finanziert wird (http://www.turbine-project.eu). Angaben der Partner des Projekts Turbine zufolge besteht das allgemeine Projektziel darin,

   - eine innovative Technologie für den Schutz der Privatsphäre zu entwickeln, die eine sichere Erkennung von elektronischen Benutzern (eID) per Fingerabdruck-Biometrie ermöglicht, und

   - zu zeigen, dass diese Technologie aufgrund ihrer Leistung und Sicherheit für den Einsatz in gewerblichen Anwendungen für das elektronische Identitätsmanagement (eIDM) geeignet ist und dem Bürger Nutzen bringt, weil sie einen besseren Schutz der Privatsphäre gewährleistet und das Vertrauen der Nutzer in das elektronische Identitätsmanagement durch die Verwendung von Fingerabdrücken erhöht.

9. Ziel des Projekts ist es, ein datenschutzfreundliches biometrisches Verfahren auf der Basis von Fingerabdrücken zu erarbeiten. Das Hauptaugenmerk des Projekts Turbine lag dabei auf der Entwicklung eines sogenannten Pseudo-Identitäten-Protokolls (PI-Protokoll), das geschützte (biometrische) Templates verwendet. In diesem PI-Protokoll werden biometrische Daten umgewandelt, so dass mehrere biometrische Identitäten erstellt, aber nicht miteinander verkettet werden können. Im Einzelnen bedeutet dies, dass bei dem Verfahren der biometrische Fingerabdruck durch eine verschlüsselte Ableitung des Fingerabdrucks ersetzt wird, die als „biometrische Identität“ bezeichnet wird. Hierzu werden besondere Hash-Funktionen verwendet, die auf Verschlüsselungsalgorithmen basieren. Die Verwendung verschiedener Verschlüsselungsalgorithmen ermöglicht die Erstellung einer entsprechenden Anzahl von biometrischen Identitäten für den gleichen Fingerabdruck.

10. Jede biometrische Identität ist ausschließlich mit der Person verknüpft, deren Fingerabdruck abgenommen wurde, wobei ein bestimmter Algorithmus Anwendung findet. Wenn das oben beschriebene Verfahren in einem biometrischen System angewendet wird, um beispielsweise den Zugang von Personen zu Anlagen zu kontrollieren, können die Personen mittels ihrer biometrischen Identitäten identifiziert werden, ohne dass die biometrischen Rohdaten in Form ihrer Fingerabdrücke aufbewahrt werden müssen. Mit dem PI-Protokoll können biometrische Daten außerdem lokal, beispielsweise auf einem Token, abgelegt werden, wenngleich andere Architekturen möglich bleiben.

11. Ein wichtiges Merkmal des Projekts besteht darin, dass die Turbine-Technologie darauf abzielt, das biometrische Template durch eine verschlüsselte Umwandlung der Fingerabdruckinformationen in einen **nicht umkehrbaren Schlüssel** zu

schützen, der Abgleiche mittels Bit-für-Bit-Vergleichen ermöglicht. Es wird davon ausgegangen, dass die umgewandelten biometrischen Daten irreversibel sind, also nicht zu den biometrischen Mustern und ursprünglichen Templates zurückführen. Um das Vertrauen der Nutzer zu erhöhen, wird dieser Schlüssel darüber hinaus **widerruflich** sein, d. h. ein neuer unabhängiger Schlüssel kann erzeugt werden, damit biometrische Identitäten neu ausgestellt werden können.

12. Nach Ansicht des EDSB sind diese beiden Merkmale (die erwartete Unumkehrbarkeit (Irreversibilität) des Schlüssels und die Widerrufbarkeit des Schlüssels) der Technologie die beiden Säulen des Projekts Turbine. Aus datenschutzrechtlicher Sicht sind diese beiden Aspekte für den EDSB von besonders großem Interesse und werden im Folgenden eingehender erörtert. Zunächst folgt jedoch eine Analyse der biometrischen Daten, die im Zusammenhang mit dem Projekt Turbine verarbeitet werden.

2. Rechtliche Prüfung

2.1 Biometrische Daten

13. Der EDSB hat wiederholt betont, dass bei der Einführung und Verarbeitung biometrischer Daten konsistente und nachdrückliche Schutzmaßnahmen unerlässlich sind. Aufgrund der besonderen Natur biometrischer Daten ist ihre Einführung mit speziellen Risiken verbunden, die es zu mindern gilt. Diese besonderen Merkmale biometrischer Daten sind der Grund für das Interesse des EDSB am Projekt Turbine und für die spezielle Zielsetzung des Projekts.

14. Der EDSB stellt fest, dass die rechtlichen Aspekte im Zusammenhang mit dem Einsatz der Biometrie von den Projektpartnern sehr ernst genommen wurden.

15. In der Tat wurden die rechtlichen Bedenken und Auflagen im Zusammenhang mit der Verarbeitung biometrischer Daten seit Projektbeginn berücksichtigt. Die rechtlichen Bedenken werden in verschiedenen Dokumenten vorgebracht, insbesondere im Arbeitspapier über Biometrie der Artikel-29-Datenschutzgruppe[3] sowie in Stellungnahmen, wie denen des EDSB zum großangelegten Einsatz der Biometrie in der EU[4].

16. Dem EDSB wurde ein ausführliches Dokument mit den rechtlichen Auflagen, in die funktionale und technische Anforderungen einfließen, vorgelegt, das während der ersten Monate des Projekts erarbeitet und beim Beratungsausschuss des Projekts zur weiteren Kommentierung und Ergänzung eingereicht worden war.[5] Für den EDSB zeigt dies das Engagement der Projektpartner, den eingebauten Datenschutz bereits zu einem frühen Zeitpunkt in die Laufzeit des Projekts zu integrieren.

[3] Artikel-29-Datenschutzgruppe, *Arbeitspapier über Biometrie*, WP 80, 1. August 2003.

[4] Beispielsweise die Stellungnahme des EDSB vom 19. Oktober 2005 zu drei Vorschlägen betreffend das Schengener Informationssystem der zweiten Generation (SIS II) und die Stellungnahme des EDSB vom 23. März 2005 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen Mitgliedstaaten über Visa für den kurzfristigen Aufenthalt.

[5] Siehe Turbine, Ergebnis D.1.1.1.

2.1.1 Verarbeitung biometrischer Daten

17. Im Rahmen des Projekts Turbine werden vor allem biometrische Daten verarbeitet. Daher ist es unabdingbar, ihren Status zu bestimmen.

18. Der Artikel-29-Arbeitsgruppe zufolge[6] können biometrische Daten „als biologische Eigenschaften, physiologische Merkmale, Gesichtszüge oder reproduzierbare Handlungen definiert werden, wobei diese Merkmale und/oder Handlungen für die betreffende Person spezifisch und messbar sind, auch wenn die in der Praxis angewandten Modelle für ihre technische Messung in gewissem Umfang auf Wahrscheinlichkeiten beruhen. Typische Beispiele für biometrische Daten sind Fingerabdrücke, Augennetzhaut, Gesichtsform, Stimme, aber auch Handgeometrie, Venenstruktur oder auch spezielle Fähigkeiten oder sonstige Verhaltensmerkmale (z. B. handgeschriebene Unterschrift, Tastenanschlag, charakteristische Gangart oder Sprechweise usw.)."

19. Des Weiteren hat die Artikel-29-Arbeitsgruppe auf Folgendes hingewiesen: „Eine Besonderheit biometrischer Daten besteht darin, dass sie sowohl als *inhaltliche Information* über eine bestimmte Person („Titius hat diesen Fingerabdruck") als auch als ein Element zur Herstellung einer Verbindung zwischen einer Information und der Person angesehen werden können („Dieser Gegenstand wurde von einer Person mit diesem Fingerabdruck berührt. Dieser Fingerabdruck passt zu Titius; deswegen wurde dieser Gegenstand von Titius berührt."). Insofern können sie als „Kennzeichen" dienen. Aufgrund ihrer einzigartigen Verbindung mit einer bestimmten Person können biometrische Daten zur *Identifizierung* dieser Person verwendet werden."

20. Im Fall des Projekts Turbine verwendet das vorgeschlagene biometrische System ein Verfahren, bei dem biometrische Daten (Fingerabdrücke) „pseudonymisiert" werden, indem sie durch verschlüsselte unumkehrbare Derivate (biometrische Identitäten) ersetzt werden, die durch Einweg-Verschlüsselungstechniken unter Anwendung von Hash-Funktionen erzeugt werden. Da davon ausgegangen wird, dass es aufgrund der technischen Mittel zur Erzeugung der biometrischen Identitäten nicht möglich ist, die biometrischen Rohdaten anhand der biometrischen Identitäten abzurufen, kann eine biometrische Identität nicht als Inhalt der Information angesehen werden, die eine Person im oben beschriebenen Sinn charakterisiert. Die Verwendung einer biometrischen Identität anstelle der biometrischen Rohdaten in Form eines Fingerabdrucks stellt daher einen besseren Schutz der Person dar, weil es aus technischer Sicht als unmöglich erachtet wird, die Fingerabdruckinformationen direkt aus der vom Projekt Turbine vorgeschlagenen biometrischen Identität zu extrahieren. Aufgrund der Tatsache, dass nach wie vor der direkte Bezug der biometrischen Identität zu einer bestimmten Person besteht (da nur der Fingerabdruck derselben Person unter Verwendung des gleichen Verschlüsselungsalgorithmus wiederholt zur Erzeugung der gleichen biometrischen Identität führen kann), wäre die Identifizierung der Person anhand der biometrischen Identität jedoch auf die gleiche Weise möglich wie bei biometrischen Rohdaten. Auch wenn die biometrische Identität allein nicht zur Offenlegung personenbezogener Daten führen könnte, wäre die Identifizierung der Person im Rahmen des biometrischen Systems (z. B. während der Zugangskontrolle) in Kombination mit anderen personenbezogenen Daten, die für die gleiche Person im

[6] Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", WP 136, S. 8.

System gespeichert werden (z. B. die vollständige Angabe des Namens), also dennoch möglich. In diesem Sinn sind biometrische Identitäten, wie sie gemäß dem Projekt Turbine erzeugt und verwendet werden, ebenfalls als personenbezogene Daten anzusehen.[7]

21. Wie wiederholt in Stellungnahmen, die biometrische Daten behandeln, geäußert, ist der der EDSB der Ansicht, dass die Verarbeitung bestimmter biometrischer Daten, die über das einfache Speichern von Fotografien hinausgeht, besondere Risiken für die Rechte und Freiheiten der betroffenen Personen beinhaltet, was sie daher (auf der Grundlage von Artikel 27 Absatz 1 der Verordnung (EG) Nr. 45/2001) der Vorabkontrolle unterwirft. Diese Auffassung gründet sich vor allem auf den Abgleich, der mit gewissen Risiken verbunden ist, und auf den Charakter der biometrischen Daten, da diese Art von Daten bestimmte inhärente Merkmale aufweist. Beispielsweise ändern biometrische Daten die Beziehung zwischen Körper und Identität unwiderruflich, weil durch sie die Merkmale des menschlichen Körpers „maschinenlesbar“ und zum Gegenstand weiterer Verwendung werden. Neben dem äußerst speziellen Charakter der Daten können auch andere Risiken unerwartete und/oder unerwünschte Folgen für die betroffenen Personen haben, beispielsweise die Möglichkeiten der Verknüpfung und der Stand der technischen Instrumente. Eine solche Verarbeitung biometrischer Daten erfordert daher besondere Maßnahmen, die nachfolgend untersucht werden.

2.1.2 Die Merkmale des Projekts Turbine

22. Im Alltag können die Identität und die personenbezogenen Daten einer Person kompromittiert werden. Aus diesem Grund müssen sie unbedingt geschützt werden. Dies gilt auch für biometrische Daten. Da eine Person jedoch nur über eine begrenzte Anzahl von Iris und Fingern verfügt, kompromittiert ein Identitätsdiebstahl solcher Daten die zugehörigen biometrischen Referenzen und macht sie für die künftige Nutzung unbrauchbar. Biometrische Daten sind eng mit den betroffenen Personen verbunden, und eine Kompromittierung dieser Daten würde die Unantastbarkeit der Personen gefährden und sie verwundbar machen. Daher müssen die Qualität der verarbeiteten Daten und deren Sicherheit unbedingt gewährleistet werden.

23. Das Projekt Turbine tritt dafür ein, dass die biometrischen Daten, die verarbeitet und in einen biometrischen Schlüssel umgewandelt werden, zwei besondere Merkmale aufweisen sollen.

Unumkehrbarkeit des Schlüssels

24. Im Rahmen des Projekts Turbine wird der Fingerabdruck als Träger der Identität, der den Zugang zu den personenbezogenen Daten einer Person ermöglicht, in einen aus einer Binärzeichenfolge bestehenden Schlüssel umgewandelt, der als nicht umkehrbar[8] angesehen wird, das heißt, es wird davon ausgegangen, dass die Binärzeichenfolge keinen Bezug zum ursprünglichen Fingerabdruck aufweist. Damit können einer Person mehrere Identitäten oder Pseudo-Identitäten zugewiesen

[7] Siehe die Begründung im Beschluss der griechischen Datenschutzbehörde Nr. 31/2010.

[8] Im Sinne des Projekts bezieht sich Unumkehrbarkeit auf die Schwierigkeit, aus der geschützten Referenz mehr Informationen als das Ergebnis des jeweiligen Abgleichs abzuleiten (andere Informationen könnten beispielsweise die ursprünglichen biometrischen Daten oder medizinische Daten umfassen).

werden, die mit verschiedenen persönlichen Informationen verknüpft werden können, beispielsweise mit Gesundheits-, Finanz- und Rechtsinformationen. Die Verwendung eines nicht umkehrbaren Schlüssels zur Erzeugung erneuerbarer Templates scheint die Ermittlung der ursprünglichen biometrischen Referenzdaten (anhand dieses Schlüssels) daher unmöglich zu machen.

25. Da die Umkehrbarkeit unterbunden wird, werden die biometrischen Referenzdaten, die von Natur aus mit der Person verknüpft sind, besser geschützt und können nicht mehr kompromittiert werden. Das Merkmal der Unumkehrbarkeit wird aus Sicht des Datenschutzes und der Sicherheit im Sinne der Datenschutzgrundsätze begrüßt, die in der Verordnung (EG) Nr. 45/2001 zum Ausdruck gebracht werden. Beispielsweise sieht Artikel 4 Absatz 1 Buchstabe b dieser Verordnung vor, dass personenbezogene Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen. Das System macht die biometrischen Darstellungen unumkehrbar und verhindert damit, dass die biometrischen Daten für einen anderen Zweck verwendet werden als ursprünglich vorgesehen. Es gewährleistet außerdem, dass die biometrischen Daten selbst nicht länger als nötig aufbewahrt werden, da sie durch den aus einer Binärzeichenfolge bestehenden Schlüssel ersetzt werden.

26. Gemäß Artikel 4 Absatz 1 Buchstabe c dürfen personenbezogene Daten außerdem nur „den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sein und nicht darüber hinausgehen“. Da die Binärzeichenfolge der Daten die biometrischen Referenzdaten ersetzt, kann davon ausgegangen werden, dass nur notwendige personenbezogene Daten verarbeitet werden. Dieses System verhindert die Verarbeitung weiterer Daten, die in der biometrischen Referenz enthalten sind.

27. Aus sicherheitstechnischer Sicht (auf die Artikel 21 und 22 der Verordnung (EG) Nr. 45/2001 eingehen) bedeutet die Unumkehrbarkeit des Schlüssels, dass die ursprünglichen biometrischen Daten durch größere Sicherheit geschützt sind, da sie keinen Bezug zum Schlüssel aufweisen. Dieser Sicherheitsaspekt wird durch das Merkmal der Widerrufbarkeit des Schlüssels noch verstärkt.

Widerrufbarkeit des Schlüssels

28. Das Projekt Turbine beschreibt ein Verfahren, bei dem die Pseudo-Identitäten widerrufen werden können. Dank dieser Lösung stehen der betroffenen Person alternative Möglichkeiten der Authentifizierung für die Dienste zur Verfügung, wenn die Pseudo-Identitäten widerrufen werden müssen.

29. Im Rahmen des Projekts Turbine wird der Standpunkt vertreten, dass sich das Risiko kompromittierter biometrischer Referenzen für bestimmte Arten von Angriffen mindern lässt, indem Methoden bereitgestellt werden, mit denen sich Templates erneuern lassen. Wenn mehrere unterschiedliche Templates aus den gleichen Referenzdaten extrahiert werden können, kann das Template selbst erneuert werden, wenn es Gegenstand eines Identitätsdiebstahls ist. Damit kann das kompromittierte Template widerrufen werden.

30. Ein biometrisches Merkmal kann nicht geändert werden. Jede Person besitzt ganz bestimmte Finger und Augen, und diese biometrischen Daten können nicht „erneuert“ werden. Daher besteht die Gefahr, dass biometrische Daten, die kompromittiert sind, für immer kompromittiert bleiben. Auf der Grundlage dieser

Gefahr bietet ein widerrufliches Template für diese biometrischen Daten verschiedene Vorteile.

31. Durch die Verwendung eines widerruflichen Schlüssels kann die biometrische Darstellung eines Fingerabdrucks, aus der der ursprüngliche Fingerabdruck nicht reproduziert werden kann (Unumkehrbarkeit), gelöscht und neu ausgestellt werden.

32. Durch Widerrufen eines kompromittierten Templates gewährleistet das System, dass das Template nicht weiter verwendet werden kann, weil das System es nicht mehr als gültiges Template erkennen würde. Die Weiterverwendung eines kompromittierten Templates wäre nicht mit dem ursprünglichen Zweck vereinbar (Artikel 4 Absatz 1 Buchstabe b der Verordnung (EG) Nr. 45/2001).

33. Darüber hinaus gewährleistet die Widerrufbarkeit des Templates, dass die Daten sachlich richtig und auf den neuesten Stand gebracht sind (Artikel 4 Absatz 1 Buchstabe d der Verordnung (EG) Nr. 45/2001). Wenn die Daten sachlich nicht mehr richtig (kompromittiert usw.) sind, können die Daten auf den neuesten Stand gebracht werden, weil es möglich ist, das auf biometrischen Daten basierende Template zu widerrufen und zu erneuern.

2.1.3 Bewährte Praktiken für die Forschung im Bereich biometrischer Daten

34. Informationen des Turbine-Konsortiums zufolge wurden rechtliche Aspekte des Identitätsmanagements (IDM) und rechtliche Aspekte der Verwendung biometrischer Daten analysiert. In diesem Zusammenhang wurden zehn „bewährte Praktiken“ für den Einsatz biometrischer Daten in Identitätsmanagementsystemen untersucht und entwickelt.[9] Das Ergebnis der vorgeschlagenen „bewährten Praktiken“ wurde dem EDSB ebenfalls vorgelegt. Es basiert einerseits auf Stellungnahmen der Datenschutzbehörden, des EDSB und der Artikel-29-Datenschutzgruppe sowie andererseits auf den neuen Methoden, die im Rahmen des Projekts Turbine untersucht, getestet und umgesetzt wurden. Die vorgeschlagenen Leitlinien wurden außerdem dem Beratungsausschuss des Konsortiums vorgelegt und mit dessen Mitgliedern erörtert. Der EDSB ist der Meinung, dass diese Dokumente die Absicht des Projektkonsortiums belegen, seine Forschungsarbeiten auf einer soliden rechtlichen Grundlage durchzuführen.

Im Rahmen des Projekts Turbine wurden die folgenden bewährten Praktiken ermittelt:

- Nutzung der biometrischen Daten grundsätzlich nur zum Zweck des Abgleichs;
- standardmäßige Kontrolle des Nutzers über seine biometrischen Daten;
- mehrere Identitäten und Pseudonymität;
- Widerrufbarkeit biometrischer Identitäten und deren erneute Ausstellung;
- Prüfung der Authentifizierungsdaten und/oder Identitätsprüfung;
- Löschung der Muster und ursprünglichen Templates;
- Einsatz von Technologien zum Schutz der Privatsphäre;
- Transparenz und Informationspflicht gegenüber den betroffenen Personen;
- Festlegung der Ausweichverfahren und des Verfahrens für das Einlegen von Rechtsmitteln gegen eine Vergleichsentscheidung;
- bewährte Praktiken für die Organisation (insbesondere für die Phase der

[9] Siehe Turbine, Ergebnis 1.4.3. („Turbine Best Practices“).

Erfassung biometrischer Daten), die Sicherheit und die Zertifizierung des biometrischen Identitätsmanagementsystems.

35. Im Oktober schlug der EDSB die Erarbeitung eines grundlegenden, allgemeinen Anforderungskatalogs vor, der die besonderen Merkmale biometrischer Daten berücksichtigt. Dieser Katalog sollte auf alle Arten von Systemen anwendbar sein, die mit der Biometrie arbeiten. Es handelt sich um die folgenden allgemeinen Anforderungen:

    - Gezielte Folgenabschätzung: Diese Anforderung gewinnt angesichts der jüngsten Entwicklungen der Strategien hinsichtlich einer Datenschutzfolgenabschätzung, die sowohl von der Artikel-29-Datenschutzgruppe als auch vom EDSB dargelegt werden, an Bedeutung.

    - Schwerpunkt auf dem Erfassungsprozess: Die Erfassung biometrischer Daten ist ein wichtiger Schritt im allgemeinen Prozess der biometrischen Identifizierung. Es müssen alle Vorkehrungen getroffen werden, damit in der Erfassungsphase tatsächlich die Mehrheit der Personen erfasst wird. Darüber hinaus muss bei der Erfassung die Höhe der Falschrückweisungsrate (FRR) und der Falschakzeptanzrate (FAR) berücksichtigt werden. Außerdem sollten Ausweichverfahren zur Verfügung stehen, wenn der Erfassungsprozess nicht erfolgreich absolviert werden kann.

    - Ausweichverfahren: Leicht verfügbare Ausweichverfahren sollten eingeführt werden, um die Würde der Personen, die falsch identifiziert werden könnten, zu wahren und zu vermeiden, dass sie unter den Mängeln des Systems zu leiden haben.

    - Festlegung des Grads der Genauigkeit: Im Zusammenhang mit den Ausweichverfahren müssen der Grad der Genauigkeit des Systems sowie insbesondere die Falschrückweisungsrate und die Falschakzeptanzrate entsprechend der Genauigkeit des Systems genau definiert und im Hinblick auf die Personen, die das System nutzen, laufend überwacht werden. Der erforderliche Bedarf an Ausweichverfahren richtet sich nach der Höhe dieser beiden Raten.

36. Der EDSB teilt die Ansicht, dass die Entwicklung der oben genannten bewährten Praktiken hilfreich ist, um geeignete Maßnahmen für ein biometrisches Identitätsmanagementsystem einzuführen, das mit dem Rechtsrahmen der EU im Einklang steht. Mit einer solchen Checkliste könnten in der Tat datenschutzfreundlichere Systeme entwickelt werden, wenn die bewährten Praktiken von Anfang an berücksichtigt werden. Nach Gesprächen mit den Projektpartnern hat der EDSB erkannt, dass dieser Aspekt in die Forschungsarbeiten des Projekts eingeflossen ist, da bereits zu Projektbeginn konkrete Ziele hinsichtlich der Genauigkeit festgelegt wurden, wenngleich der Grad der Genauigkeit in der Liste der bewährten Praktiken nicht im engeren Sinne erwähnt wird. Darüber hinaus wurde der Grad der Genauigkeit im Rahmen der Forschungsarbeiten getestet, überprüft und sogar dahin gehend verbessert, als vorgesehen ist, dass solche konkreten Genauigkeitsgrade in einem biometrischen System, das in einer Betriebsumgebung eingesetzt wird, festgelegt werden.

37. Der EDSB merkt jedoch an, dass die im Rahmen des Projekts Turbine erarbeitete Liste der bewährten Praktiken offenbar nicht zwingend vorschreibt, dass der von einem biometrischen System erwartete konkrete Grad der Genauigkeit festgelegt werden muss. Der EDSB hält dies aber für überaus wichtig. Daher sollte ein solcher Grad der Genauigkeit frühzeitig im System definiert und regelmäßig überprüft werden. Aus diesem Grund sollte er nicht nur angewandt werden, sondern auch ein wesentlicher Bestandteil der bewährten Praktiken darstellen.

2.1.4 Die Nutzung proprietärer und öffentlich zugänglicher biometrischer Datenbanken

38. Die Turbine-Partner führten Leistungstests durch, um die im Rahmen des Projekts entwickelten Algorithmen zu testen und zu bewerten. Für Test- und Bewertungszwecke beschlossen die Turbine-Partner zu Beginn des Projekts (in der Beschreibung der Tätigkeit), die Tests an proprietären Datenbanken und an öffentlich zugänglichen biometrischen Fingerabdruckdatenbanken vorzunehmen.

Proprietäre Datenbanken

39. Der EDSB hat festgestellt, dass einige der Projektpartner ihre eigenen Unternehmensdatenbanken[10] verwendet haben und außerdem eine norwegische proprietäre Datenbank herangezogen wurde.

40. Das Projektkonsortium wies nach, dass gewährleistet ist, dass diese proprietären biometrischen Datenbanken die nationalen Datenschutzvorschriften der Länder einhielten, in denen die Tätigkeiten stattfinden und in denen die Partner niedergelassen sind.

41. Beispielsweise wurden die folgenden Maßnahmen für den Betrieb der norwegischen Datenbank ergriffen:

- Freiwillige Teilnehmer wurden mündlich und schriftlich darüber informiert, dass biometrische Muster („Rohdaten“) erhoben und in einer Datenbank für Forschungszwecke gespeichert würden.
- Wenn die freiwilligen Teilnehmer dem zustimmten, *willigten sie schriftlich ein* und stellten ihre Fingerabdruckbilder für Lehr-, Forschungs- und Testzwecke zur Verfügung. Die Formulare mit der schriftlichen Einwilligung werden von der norwegischen Universität (Partner des Projekts) aufbewahrt, die auch für die Datenverarbeitung verantwortlich ist.
- Den betroffenen Personen wurde ein jederzeit gültiges Widerspruchsrecht eingeräumt.
- Die Datenschutzbehörde in Norwegen wurde im Januar 2008 vor Projektbeginn über die Datenerhebung („Meldeskjema“) informiert und Vorschriften. eingehalten.

[10] Des Weiteren wurde angegeben, dass es sich um allgemeine Forschungsdatenbanken der betreffenden Unternehmen in Frankreich bzw. Schweden gehandelt habe. In Schweden gewährleistet und überwacht der Datenschutzbeauftragte des Unternehmens, dessen Name der schwedischen Datenschutzbehörde bekannt ist, dass die biometrischen Daten auf rechtmäßige Weise und ordnungsgemäß verarbeitet werden. In Frankreich wurden die Bedingungen für die Nutzung biometrischer Datenbanken für Forschungszwecke mit der französischen Datenschutzbehörde (CNIL) erörtert, um eine Berechtigung für alle proprietären Datenbanken entsprechend dem französischen Recht einzuholen. Im Juli 2010 erließ die CNIL einen diesbezüglichen Beschluss („Délibération 2010-336“).

- Organisatorische und technische Sicherheitsmaßnahmen wurden ergriffen, um die biometrischen Daten zu sichern und zu schützen. Beispielsweise werden die Daten auf Rechnern gespeichert, die durch Benutzername und Kennwort geschützt sind und in abschließbaren Räumen stehen. Außerdem sind die Rechner weder mit dem Internet noch mit einem anderen Netzwerk verbunden.
- Die Daten dieser Datenbank werden ausschließlich vom Gjøvik University College (GUC) gespeichert. Der Zugriff auf diese Daten ist auf berechtigte Personen des GUC beschränkt, die diese Daten für Forschungszwecke nutzen müssen. Die Tests wurden in Norwegen durchgeführt.
- Die Daten werden weder Dritten noch Projektpartnern übermittelt.

42. Angesichts der verschiedenen Maßnahmen, die im Zusammenhang mit proprietären Datenbanken umgesetzt wurden, nimmt der EDSB zur Kenntnis, dass die Turbine-Partner Datenschutzanforderungen eingeführt haben, die den aktuellen nationalen Datenschutzvorschriften in den Ländern, in denen die betreffenden Datenbanken genutzt werden, entsprechen.

Öffentlich zugängliche Datenbanken

43. Einige der Partner führten Tests durch, die auf öffentlich zugänglichen Biometriedatenbanken basierten. Eine dieser Datenbanken war in Italien entwickelt worden und wurde von verschiedenen Projektpartnern genutzt.

44. Der EDSB untersuchte die ausschließliche Nutzung für Test- und Forschungszwecke von *öffentlich zugänglichen biometrischen Datenbanken*, die von Dritten stammten.

45. Wie oben erläutert, ist der EDSB der Ansicht, dass das Vorhandensein bestimmter biometrischer Daten, die über Fotografien hinausgehen, und die Methode des Abgleichs besondere Risiken für die Rechte und Freiheiten der betroffenen Personen beinhalten.

46. Ausgehend von dieser Begründung sollten die biometrischen Daten als personenbezogene Daten eingestuft werden, da sie zur Identifizierung von Personen verwendet werden können, und die einschlägigen nationalen Rechtsvorschriften sollten Anwendung finden. Nach Ansicht einiger nationaler Datenschutzbehörden und des EDSB[11] unterliegen solche Biometriedatenbanken einem Meldeverfahren.

47. Im Fall von Italien beispielsweise hat der EDSB den Eindruck, dass die verschiedenen Formen der Verarbeitung biometrischer Daten der italienischen Datenschutzbehörde (*Garante*) gemeldet werden müssen. Des Weiteren können die Erhebung und Verarbeitung biometrischer Daten zum Zwecke des Aufbaus einer biometrischen Datenbank aufgrund der besonderen Natur der biometrischen Daten bestimmte Risiken für die Rechte und Freiheiten der betroffenen Personen beinhalten. Für das Projekt müsste daher geprüft werden, ob die dem Konsortium bereitgestellten biometrischen Daten im Einklang mit dem jeweiligen nationalen Rechtsrahmen erhoben wurden und ob die zuständige Datenschutzbehörde eine Stellungnahme oder Genehmigung bezüglich der Rechtmäßigkeit der Datenbank abgegeben bzw. ausgestellt hat.

[11] Der EDSB fordert von den europäischen Organen und Einrichtungen, dass sie biometrische Datenbanken zum Zwecke einer Vorabkontrolle melden.

48. Aus dem Informationsaustausch zwischen dem EDSB und dem Projektkonsortium geht hervor, dass im Rahmen des Projekts zwischen dem Land, in dem die öffentlich zugängliche Datenbank von einem für die Verarbeitung Verantwortlichen eingerichtet wurde, und den Ländern, in denen die Daten aus der Datenbank von den Projektpartnern genutzt wurden, unterschieden wurde.

49. Das Projektkonsortium gab an, dass es die Rechtmäßigkeit der Verarbeitungsvorgänge in den Ländern, in denen die Datenbank von den Turbine-Partnern weiter genutzt wurde, überprüft habe, indem es die Verarbeitungsvorgänge den nationalen Datenschutzbehörden gemeldet habe. Der EDSB konnte jedoch nicht eindeutig ermitteln, ob das Konsortium auch für die öffentlich zugängliche Datenbank in Italien eine solche Überprüfung vorgenommen hat. In einem solchen Fall sollte das Konsortium von der Stelle, die die Daten bereitstellt, den Nachweis fordern, dass die Daten unter Einhaltung der nationalen Datenschutzvorschriften zur Umsetzung der Datenschutzrichtlinie erhoben wurden. Daher kann der EDSB nicht beurteilen, ob das Konsortium ausreichende Garantien erhalten hat, dass diese Datenbank rechtlich betrachtet den nationalen Vorschriften des Landes entspricht, in dem der für die Verarbeitung Verantwortliche niedergelassen ist.

2.2. Protokoll der sicheren Zugangskontrolle

50. Aus den bereitgestellten Informationen geht hervor, dass das vom Projekt Turbine vorgeschlagene Protokoll der sicheren Zugangskontrolle darauf abzielt, die Eigenschaften des Match-on-Card-Verfahrens, die sowohl für hohe Genauigkeit als auch für einen hohen Schutz der Privatsphäre stehen, zu einer Lösung zu erweitern, die das Identifizierungsverfahren unterstützt.

51. Zu klären ist noch die Frage, ob die lokale Speicherung der biometrischen Daten auf einer sicheren Hardware (Terminal) ohne die Notwendigkeit eines Tokens und die Verarbeitung dieser Daten die Sicherheitsanforderungen sowie die Anforderungen in Bezug auf den Schutz der Privatsphäre und den Datenschutz bei der Nutzung biometrischer Daten erfüllen. In diesem Zusammenhang sollte eine kontextuelle Analyse der Situation selbst erfolgen, die auf einer Untersuchung der zuständigen nationalen Datenschutzbehörde basiert.

52. Grundsätzlich bevorzugt der EDSB die Verwendung einer „Eins-zu-eins“-Suchmethode, bei der die Identifizierungsstelle die biometrischen Daten der Person mit einem eindeutigen (auf die Identität bezogenen) Template vergleichen würde. Eine solche Suchmethode führt zu genaueren Ergebnissen.

53. Der EDSB zieht im Allgemeinen Systeme vor, die die biometrischen Templates auf Mikrochips und nicht in zentralen Datenbanken speichern, es sei denn, die Speicherung in einer zentralen Datenbank ist aufgrund bestimmter Bedingungen erforderlich. Die Speicherung auf Mikrochips ist insofern die datenschutzfreundlichere Variante, als das Template auf einem Datenträger (z. B. einem Ausweis mit Mikrochip) gespeichert wird, der sich im Besitz der betroffenen Person befindet. Auf diese Weise hat die betroffene Person selbst die direkte Kontrolle und ist für ihr Template verantwortlich. Keine andere Person hat Zugang zu ihrem Template oder ist in dessen Besitz. Außerdem birgt die Speicherung in zentralen Datenbanken das Risiko so genannter „Phishing Expeditions“ und vereinfacht den Zugang zur Datenbank für andere Zwecke als den, für den die

Datenbank entwickelt wurde. In den meisten Fällen lässt sich dieses Risiko ohne Beeinträchtigung des Sicherheitsniveaus durch ein dezentrales System vermeiden.

54. Nach Auffassung des EDSB sollten Sicherheitsmaßnahmen nicht nur gegen Bedrohungen von außen ergriffen werden, sondern auch gegen Handlungen der Nutzer selbst, insbesondere bei Einsatz eines dezentralen Systems. Die Turbine-Partner gaben an, dass die im Rahmen des Projekts durchgeführte Sicherheitsanalyse interne Angreifer, darunter registrierte Nutzer, einschließt. Darüber hinaus wurden die Projektlösungen so ausgelegt, dass sie mit allen klassischen, technischen und organisatorischen Sicherheitsmaßnahmen, einschließlich Maßnahmen gegen Angriffe von internen Nutzern, in eine Systemarchitektur eingebunden werden können. Der EDSB begrüßt diesen Ansatz zur Wahrung der Datenintegrität.

2.3 Demonstrationssysteme

55. Der EDSB untersuchte, auf welche Weise das Projekt Turbine die Forschungsarbeiten in realistischen Szenarien durchführte. Angaben in den bereitgestellten Dokumenten zufolge wurden zwei Dokumentationssysteme entwickelt: ein System mit zwei Szenarien am Flughafen Thessaloniki (Griechenland) und ein weiteres System in einer Modellapotheke in Deutschland.

56. Die beiden Demonstrationssysteme sollen die im Rahmen des Projekts Turbine entwickelte Technologie veranschaulichen. Für den EDSB war es erfreulich festzustellen, dass die Turbine-Partner bereits zu Beginn der Entwicklung der Demonstrationssysteme den Kontakt mit den zuständigen nationalen Datenschutzbehörden gesucht und die betreffenden Dokumente eingereicht haben. Der EDSB vermittelte als Teil seiner möglichen Tätigkeiten in Bezug auf sein Strategiepapier ebenfalls Kontakte mit den zuständigen Datenschutzbehörden.

2.3.1 Das griechische Demonstrationssystem

57. Bei dem griechischen Demonstrationssystem geht es um die Einrichtung eines Pilotsystems für die biometrische Zugangskontrolle in kritischen Infrastrukturen des „Makedonia Airport“, dem internationalen Flughafen von Thessaloniki. Die Einrichtung des Zugangskontrollsystems im Rahmen des Projekts Turbine erfolgte durch den für die Verarbeitung Verantwortlichen (ein Unternehmen für allgemeine Luftfahrtanwendungen) in Zusammenarbeit mit anderen europäischen Partnern und wurde von der Europäischen Union finanziert. Dem EDSB wurden Dokumente vorgelegt, welche die im Demonstrationssystem angewandten Verfahren und Maßnahmen beschreiben.

58. Der EDSB erhielt außerdem ausführliche Informationen darüber, unter welchen Bedingungen die Zugangskontrolle mit Hilfe der Turbine-Technologie am Flughafen von Thessaloniki eingeführt wurde. Vor allem wurde die Zugangskontrolle nur an Orten eingerichtet, deren Zugang besondere Sicherheitsmaßnahmen erfordert. Außerdem war die Zahl der freiwilligen Teilnehmer begrenzt.

59. Die griechische Datenschutzbehörde erhielt entsprechend dem griechischen Recht eine Meldung bezüglich der Einrichtung dieses Systems und gab daraufhin eine Stellungnahme ab. Sie entschied, dass die Einrichtung des biometrischen Systems ausschließlich zum Zweck der wissenschaftlichen Forschung nicht gegen die

griechischen Datenschutzvorschriften verstößt, und genehmigte die Verarbeitung der Daten für das Demonstrationssystem. Die griechische Datenschutzbehörde knüpfte ihre Entscheidung jedoch an einige Bedingungen: Das Demonstrationssystem durfte wie gemeldet in Betrieb genommen werden, allerdings wurde die Erhebung und Speicherung der ursprünglichen biometrischen Muster (Rohdaten) zum Zweck zusätzlicher Leistungstests untersagt.

60. Der EDSB begrüßte die Entwicklung eines sicheren und datenschutzfreundlichen Erfassungsverfahrens, bei dem die Personen, die an diesem Verfahren beteiligt waren und das Verfahren durchführten, umfassend informiert, geschult und unterstützt wurden, um eine hochwertige und sichere Erhebung der biometrischen Daten für weitere Referenzzwecke zu gewährleisten.

61. Der EDSB stellte weiterhin fest, dass Präsentationen ausgearbeitet und Schulungen durchgeführt wurden, in denen die Bedeutung des Datenschutzes während der Erfassungsphase betont wurde. Sachverständige der Turbine-Partner führten während der tatsächlichen Erfassung der Daten weitere Schulungen durch. Darüber hinaus wurden die Einwilligungs- und Informationsformulare bereitgestellt und mehrere Wochen vor Beginn der Erfassung mit möglichen freiwilligen Teilnehmern besprochen.

62. Derartige Verfahren tragen dazu bei, dass die Grundsätze des Datenschutzes während der gesamten Laufzeit des Projekts allgemein umgesetzt werden. Das Projekt gewährleistet eine hohe Datenqualität, indem sichergestellt wird, dass die Personen die richtigen Informationen erhalten und die während der Erfassungsphase verarbeiteten Daten präzise sind.

63. Wenn es um die Erfassung biometrischer Daten geht, prüft der EDSB außerdem immer, ob Ausweichverfahren vorhanden sind. Im griechischen Demonstrationssystem wurde das Ausweichverfahren dadurch gewährleistet, dass die bestehenden Maßnahmen für die Zugangskontrolle nicht durch die Turbine-Lösung ersetzt wurden, sondern parallel dazu verwendet wurden. Auf diese Weise konnten die Teilnehmer bei einem Versagen des Turbine-Demonstrationssystems auf die bestehenden Zugangskontrollen ausweichen.

2.3.2 Das deutsche Demonstrationssystem (GADM)

64. In Bezug auf das deutsche Demonstrationssystem wurde deutlich gemacht, dass das GADM-System gemäß deutschem Recht[12] nicht gemeldet werden musste, wenn die verantwortliche Stelle einen Beauftragten für den Datenschutz bestellt, was der Fall war. Daher wurde der Beauftragte für den Datenschutz bei Sagem Orga von der verantwortlichen Stelle ordnungsgemäß in Kenntnis gesetzt, damit er die Informationen gemäß den gesetzlichen Bestimmungen speichert. Hinsichtlich des GADM-Demonstrationssystems wurde der Beauftragte für den Datenschutz bei Sagem Orga darauf hingewiesen, dass er die Bestimmungen bezüglich des Inhalts der Meldepflicht in § 4e des Bundesdatenschutzgesetzes einzuhalten habe. Er wurde darüber informiert, welche Angaben laut dem deutschen Gesetz erforderlich sind, unter anderem der Name der verantwortlichen Stelle, die Namen der mit der Datenverarbeitung beauftragten Personen, die für den Zugang zu den Daten berechtigten Personen und die Zweckbestimmungen. Für die freiwilligen

[12] § 4d Absatz 2 des Bundesdatenschutzgesetzes und § 4f – siehe auch § 4d Absatz 3 bezüglich der Einwilligung als Grundlage für das Entfallen der Meldepflicht.

Teilnehmer wurde ein Einwilligungsformular vorbereitet, aus dem eindeutig hervorgeht, welche Daten für welche Zwecke durch das Demonstrationssystem verarbeitet werden. Die freiwilligen Teilnehmer wurden außerdem über ihre Rechte ordnungsgemäß informiert.

65. Auch bei diesem Demonstrationssystem war vorgesehen, dass die mit der Erfassung beauftragten Personen über die Notwendigkeit einer sicheren und datenschutzfreundlichen (transparenten) Erfassung aufgeklärt und entsprechend geschult wurden. Des Weiteren wurde darauf hingewiesen, dass die mit der GADM-Erfassung beauftragten Personen über Fachkunde im Bereich der Verarbeitung biometrischer Daten verfügen und sich der Bedeutung qualitativ hochwertiger Referenzdaten bewusst sind.

2.3.3 Zusammenfassung

66. Der EDSB kommt zu dem Schluss, dass das Projektkonsortium beim Betrieb der beiden Demonstrationssysteme den Grundsatz des eingebauten Datenschutzes auf eine Weise umgesetzt hat, die die Bewertung durch die zuständigen Datenschutzbehörden vereinfacht.

3. Schlussfolgerungen

67. Der EDSB begrüßt das Projekt, weil es deutlich macht, dass die Einbindung des Grundsatzes des „eingebauten Datenschutzes“ in die Forschung eine wirksame Maßnahme ist, um Lösungen zu gewährleisten, die die gesetzlichen Datenschutzanforderungen erfüllen. „Eingebauter Datenschutz“ bezieht sich nicht nur auf das Konzept und die technischen Lösungen von IKT-Systemen, sondern erstreckt sich auf die verschiedenen Schritte beim Aufbau des Projekts und dessen organisatorische Vorgehensweisen. Der letztgenannte Aspekt lässt sich erreichen, indem die Einhaltung der Rechtsvorschriften sichergestellt wird, die erforderlichen Datenschutzgrundsätze umgesetzt werden sowie Verfahren und Schulungsmaßnahmen eingeführt werden, die gewährleisten, dass alle betroffenen Parteien die richtigen Informationen und Schulungen erhalten. Darüber hinaus bieten die Demonstrationssysteme die Möglichkeit zu testen, welche Vorteile die Umsetzung dieses Grundsatzes in der Praxis mit sich bringt.

68. Die Entwicklung bewährter Praktiken im Zusammenhang mit der Verwendung biometrischer Daten sollte gefördert werden, um sicherzustellen, dass die Forschung in Zukunft auf einem soliden Datenschutzansatz basiert.

69. Die Umsetzung der beiden Merkmale der Unumkehrbarkeit und der Widerrufbarkeit der biometrischen Identifizierung trägt maßgeblich dazu bei, weil sie Lösungen gewährleisten, die die gesetzlichen Datenschutzanforderungen erfüllen.

70. Der EDSB empfiehlt die Berücksichtigung der folgenden Anmerkungen:

- Bei der Auflistung der bewährten Praktiken sollte berücksichtigt werden, dass ein präzises Maß an Genauigkeit zu etablieren und regelmäßig zu überprüfen ist.

- Auch wenn die Durchführung der Forschungsarbeiten unter Einhaltung strenger rechtlicher Bedingungen erfolgt, sollte das Projektkonsortium von den Stellen, die die biometrischen Daten bereitstellen, Nachweise über die vollständige Einhaltung der jeweiligen nationalen Datenschutzvorschriften fordern.

Brüssel, den 1. Februar 2011

Giovanni BUTTARELLI
Stellvertretender Europäischer Datenschutzbeauftragter