Konferenz über die „Sicherheit des E-Government“
Europäisches Parlament, Brüssel, 19. Februar 2013

„Die Rolle der Datenschutzbestimmungen“

Peter Hustinx
Der Europäische Datenschutzbeauftragte

Wie die Einladung zu dieser Konferenz zurecht ausführt, *„zählt das E-Government weltweit zu den Prioritäten unter den Maßnahmen der laufenden Reformen des öffentlichen Sektors, wo der Einsatz von Informations- und Kommunikationstechnologien darauf gerichtet ist, Transaktionen zu digitalisieren, öffentliche Dienstleistungen zu erbringen sowie die Innovation in der öffentlichen Verwaltung zu fördern“*. Daneben zeigt sie auch einige Herausforderungen auf: *„Wie kann ein angemessenes Maß an Sicherheit garantiert werden und wie kann die Privatsphäre der Bürger geschützt werden?“*

Diese Einleitung richtet ihren Fokus auf die Herausforderungen in Bezug auf die Privatsphäre, und zwar insbesondere im Hinblick auf die aktuellen und sehr wahrscheinlich zukünftigen Datenschutzbestimmungen. Dies soll in keiner Art und Weise als eine Begrenzung verstanden werden, sondern als Beitrag, um einige der Herausforderungen zu bewältigen und um die besten Lösungen zu finden.

Es werden nun zuerst kurz einige der wichtigsten Eigenschaften dessen aufgezeigt, was allgemein als „E-Government“ bezeichnet wird (1), sowie die Beziehung zwischen Sicherheit und Privatsphäre (2). Danach werden einige der wichtigsten Punkte der Herausforderungen betreffend die Privatsphäre oder den Datenschutz[1] betrachtet (3) und wie sie durch die Überprüfung des EU-Rechtsrahmens für den Datenschutz beeinflusst werden (4). Dies führt zu einigen Kernbotschaften und Schlussfolgerungen (5).

1. E-Government

Der Begriff „E-Government“ deckt (viel) mehr als nur den – systematischen – Einsatz von IKT für die Erbringung öffentlicher Dienste. Anderenfalls wären die Schwerpunkte dieser Konferenz die Effizienz oder die Kostenvorteile gewesen. *Die derzeitige Reformen des*

[1] Privatsphäre und Datenschutz sind eng miteinander verbunden, stellen jedoch verschiedene rechtliche Konzepte dar. Beide sind im EU-Recht als Grundrechte anerkannt und werden in der Charta der Grundrechte getrennt genannt: Achtung des Privat- und Familienlebens (Artikel 7) und Schutz personenbezogener Daten (Artikel 8). Dieser letztgenannte Schutz findet sich auch im Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union, zusammen mit einer allgemeinen Rechtsgrundlage für die Durchführung der Regelungen des Datenschutzes, die sowohl für die Organe und Einrichtungen der EU als auch für die Mitgliedstaaten gelten, wenn sie Tätigkeiten ausüben, die in den Anwendungsbereich des Unionsrechts fallen. Artikel 16 AEUV ist die Hauptgrundlage für die laufende Überprüfung des EU-Rechtsrahmens für Datenschutz.

Postanschrift: rue Wiertz 60 – B-1047 Brüssel
Dienststelle: Rue Montoyer 30
E-Mail: edps@edps.europa.eu – Website: www.edps.europa.eu
Tel: (32-2) 283 19 00 - Fax: (32-2) 283 19 50

öffentlichen Sektors decken jedoch viele andere Dimensionen ab, die miteinander verbunden sind und wie folgt zusammengefasst werden können:

- Neuzuordnung öffentlicher Aufgaben: Die Verfügbarkeit von IKT ermöglicht nicht nur, sondern verlangt häufig eine neue Konzeption öffentlicher Aufgaben und Dienste, die potenziell verschiedene Dienststellen und Dienststellenstufen betrifft und private Akteure in verschiedenen Funktionen (Front- und Back-Office) einschließt.
- Gemeinsame Infrastruktur: Eine neue Konzeption öffentlicher Aufgaben und Dienste führt häufig zu einer gemeinsamen Infrastruktur für einen multifunktionalen Einsatz oder zur Erbringung geteilter Dienste.
- Online-Dienste: Neue Infrastrukturen erlauben nicht nur, dass Dienste online erbracht werden, sondern auch über öffentliche Dienste und Organisationen, womit mehr oder weniger unabhängige Schnittstellen mit Bürgern (Nutzern, Kunden usw.) geschaffen werden.

Der größte Teil der derzeitigen Reformen des öffentlichen Sektors ist *national orientiert*, auch wenn Erfahrungen mit ähnlichen Projekten in anderen Ländern geteilt werden. Die Anzahl grenzübergreifender Systeme (wie das Binnenmarkt-Informationssytem) ist noch sehr begrenzt.

2. Sicherheit und Privatsphäre

Es besteht kein Zweifel darüber, dass eine IKT-Infrastruktur für E-Government-Dienste ein sehr hohes und stabiles Sicherheitsniveau erfordert, um die Verfügbarkeit, Integrität und Vertraulichkeit auf einer kontinuierlichen Basis garantieren zu können. Dies gilt um so mehr im Hinblick auf die Risiken und potenziellen Auswirkungen von Cyber-Angriffen. In diesem Kontext ist es deshalb durchaus möglich dass für die Bereitstellung einer angemessenen Sicherheit eindeutig eine mehrstufige Infrastruktur gefordert werden muss.

„Sicherheit" und „Privatsphäre" dürfen jedoch nicht verwechselt werden, so wie „Privatsphäre und Datenschutz" nicht als eine Unterkategorie der Sicherheit behandelt werden dürfen.[2] Diese sollten besser als unterschiedliche und sich nur zum Teil überlagernde Begriffe angesehen werden. Kurz gesagt: Eine gute Sicherheit bedeutet nicht notwendigerweise eine gute Privatsphäre und einen guten Datenschutz, aber eine gute Privatsphäre und ein guter Datenschutz erfordern immer eine gute Sicherheit.[3]

Dies kann auch anders formuliert werden: Wenn Sicherheitsmaßnahmen notwendig sind, um gegen die „*unberechtigte* Weitergabe oder den *unberechtigten* Zugang" oder gegen „jede andere Form der *unrechtmäßigen* Verarbeitung" zu schützen[4], so geht es bei der Privatsphäre und dem Datenschutz mehr darum, ob eine bestimmte Weitergabe oder ein bestimmter Zugang einer anderen Form der Verarbeitung *berechtigt* oder *rechtmäßig* sein soll. Zu den

---

[2] Der Begriff „Datenschutz" stammt aus Deutschland und wird seit den 1980er Jahren breiter verwendet. Er zielt jedoch nicht auf den Schutz der Daten als solche ab, sondern auf den Schutz der Privatpersonen gegen ein zweckwidriges Erheben und Verwenden ihrer personenbezogenen Daten. Artikel 1 der aktuellen Datenschutzrichtlinie 95/46/EG lautet: *„Die Mitgliedstaaten gewährleisten (...) den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten."*

[3] Artikel 16 und 17 der Richtlinie 95/46/EG behandeln die „Vertraulichkeit" und die „Sicherheit der Verarbeitung".

[4] Artikel 17 Absatz 1 der Richtlinie 95/46/EG: *„Die Mitgliedstaaten sehen vor, dass der für die Verarbeitung Verantwortliche die geeigneten technischen und organisatorischen Maßnahmen durchführen muss, die für den Schutz gegen die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang – insbesondere wenn im Rahmen der Verarbeitung Daten in einem Netz übertragen werden – und gegen jede andere Form der unrechtmäßigen Verarbeitung personenbezogener Daten erforderlich sind.* (...)".

Sicherheitsmaßnahmen gehören auch bestimmte Rechte für die betroffenen Personen sowie bestimmte Regelungen über institutionelle Überwachungen.[5]

3. Herausforderungen betreffend die Privatsphäre oder den Datenschutz

Ein kurzer Überblick über die derzeitigen Datenschutzbestimmungen für E-Government zeigt die folgenden Hauptbereiche auf.

Anwendungsbereich

Die nationalen Rechtsvorschriften in Anwendung der Richtlinie 95/46/EG gelten für die Verarbeitung „personenbezogener Daten" im privaten oder öffentlichen Sektor, das heißt, für *„alle Informationen über eine bestimmte oder bestimmbare natürliche Person*".[6] Obwohl diese Rechtsvorschriften in Übereinstimmung mit der Richtlinie denselben Grundkonzepten und Grundsätzen folgen, tendieren sie in vielen wichtigen Einzelheiten zu leichten Unterschieden. Jedes einzelstaatliche Recht gilt für alle Verarbeitungen *„die im Rahmen der Tätigkeiten einer Niederlassung ausgeführt werden, die der für die Verarbeitung Verantwortliche"* im Hoheitsgebiet dieses Mitgliedstaats besitzt.[7] Grundsätzlich bedeutet dies, dass E-Government in einem bestimmten Mitgliedstaat durch die Rechtsvorschriften dieses Mitgliedstaats gedeckt ist. Dabei handelt es sich normalerweise um das allgemeine Datenschutzgesetz dieses Staates, eventuell in Verbindung mit einem besonderen Gesetz.

Verantwortung

Die Verantwortung für die Einhaltung der Datenschutzanforderungen liegt bei dem „für die Verarbeitung Verantwortlichen". Dabei handelt es sich um *„die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet"*.[8] Im öffentlichen Sektor ist dies normalerweise die öffentliche Stelle, die rechtlich für die Erbringung des Dienstes zuständig ist. Im E-Government können jedoch zunehmend auch andere private oder öffentliche Akteure beteiligt werden. Dies kann zu verschiedenen Vereinbarungen für die gemeinsame Kontrolle führen. Dabei können aber die Natur und der Zweck dieser Vereinbarungen problematisch sein.

Der für die Verarbeitung Verantwortliche muss vom „Auftragsverarbeiter" sorgfältig unterschieden werden. Als Auftragsverarbeiter gilt *„die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet*".[9] Die Auftragsverarbeiter haben konkrete Pflichten, vor allem in Bezug auf die Vertraulichkeit und Sicherheit der Verarbeitung, aber das Hauptaugenmerk liegt auf den für die Verarbeitung Verantwortlichen. Diese Terminologie schließt dabei nicht andere Auftragsverarbeiter und Unterauftragsverarbeiter aus. Jedoch verbleibt die Notwendigkeit, die allgemeine Verantwortung des für die Verarbeitung Verantwortlichen sicherzustellen.

---

[5] Artikel 8 der Charta der Grundrechte lautet:
1. Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten. 2. Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken. 3. Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

[6] Artikel 2 Buchstabe a) und Artikel 3 der Richtlinie 95/46/EG

[7] Artikel 4 der Richtlinie 95/46/EG

[8] Artikel 2 Buchstabe d) der Richtlinie 95/46/EG

[9] Artikel 2 Buchstabe e) der Richtlinie 95/46/EG

Rechtmäßige Verarbeitung

Die materiellen Prinzipien des Datenschutzes enthalten in Bezug auf die rechtmäßige Verarbeitung eine Reihe von Schlüsselvoraussetzungen. Für die Datenqualität[10] bestehen die Schlüsselvoraussetzungen darin, dass die personenbezogenen Daten

(a) nach Treu und Glauben und auf rechtmäßige Weise verarbeitet werden;

(b) für festgelegte eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden (...);

(c) den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen;

(d) sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sind (...);

(e) nicht länger, als es für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist, in einer Form aufbewahrt werden, die die Identifizierung der betroffenen Personen ermöglicht. (...).

Personenbezogene Daten dürfen nur verarbeitet werden, wenn die folgenden und in diesem Kontext wichtigsten Schlüsselvoraussetzungen für die Rechtmäßigkeit[11] erfüllt sind:

(a) Die betroffene Person hat ohne jeden Zweifel ihre Einwilligung gegeben; oder

(b) (...)

(c) die Verarbeitung ist für die Erfüllung einer rechtlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt; oder

(d) (...)

(e) die Verarbeitung ist erforderlich für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt und dem für die Verarbeitung Verantwortlichen oder dem Dritten, dem die Daten übermittelt werden, übertragen wurde; oder

(f) (...).

Die Einhaltung dieser Bedingungen erfordert eine sorgfältige und rechtzeitige Analyse aller wichtigen Einzelheiten, insbesondere der *Zweckbestimmung,* der *zulässigen Verwendung* und des *Bedarfs an personenbezogenen Daten* in ihren verschiedenen Verarbeitungsstadien. Die Sicherstellung der Einhaltung dieser Bedingungen obliegt dem für die Verarbeitung Verantwortlichen.[12]

Interessanterweise verlangen die zuvor genannten Bestimmungen für die Sicherheit der Verarbeitungen die Durchführung von *„geeigneten technischen und organisatorischen Maßnahmen (...), die für den Schutz (...) gegen jede Form der unrechtmäßigen Verarbeitung personenbezogener Daten erforderlich sind. Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei ihrer Durchführung entstehenden Kosten ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.“*[13] Dies setzt einen hohen Standard für die meisten maßgeblichen E-Government Projekte.

Rechte der betroffenen Personen

Der für die Verarbeitung Verantwortliche muss auch Verfahren für die Ausübung bestimmter besonderer Rechte der betroffenen Person vorsehen. Hierzu zählen neben den geeigneten Informationen, die den betroffenen Personen bei Erhebung ihrer Daten zur Gewährleistung einer transparenten Verarbeitung mitgeteilt werden müssen, das Recht auf Auskunft,

[10] Artikel 6 Absatz 1 der Richtlinie 95/46/EG
[11] Artikel 7 der Richtlinie 95/46/EG
[12] Artikel 5 Absatz 2 der Richtlinie 95/46/EG
[13] Artikel 17 Absatz 1 der Richtlinie 95/46/EG

Berichtigung und Löschung sowie das Widerspruchsrecht in Bezug auf die Verarbeitung, die alle nur mit einige ziemlich enge Ausnahmen anwendbar sind.[14]

Kontrolle

Die Entwicklung des E-Government unterliegt in allen Mitgliedstaaten nicht nur einer Überwachung und ihrer eventuellen Durchführung seitens unabhängiger Kontrollstellen. Bei wichtigen Projekten kann es in verschiedenen Phasen auch zu einer vorherigen Beteiligung kommen. Dazu gehört eventuell eine vorherige Anhörung über besondere Rechtsvorschriften, die bestimmte Maßnahmen des E-Government einführen.[15]

4. Überprüfung des EU-Rechtsrahmens

Die Europäische Kommission legte im Januar 2012 einen Vorschlag für eine Datenschutz-Grundverordnung[16] vor, die die Richtlinie 95/46/EG ersetzen soll. Dieser Vorschlag wird derzeit im Europäischen Parlamente und im Rat diskutiert. Folgende Aspekte erscheinen die wichtigsten für das E-Government zu sein.

Anwendungsbereich

Die vorgeschlagene Verordnung wird unmittelbar in allen Mitgliedstaaten gelten und die derzeitigen einzelstaatlichen Rechtsvorschriften ersetzen, wobei eine gewisse Flexibilität für nationale Besonderheiten bleibt. Der Grad der Flexibilität im öffentlichen Sektor bildet einen bedeutenden Diskussionspunkt, vor allem im Rat. Grundsätzlich wird die Verordnung jedoch ein einziges Regelungswerk liefern, das in allen Mitgliedstaaten gilt. Unter seinen Anwendungsbereich würden auch in Drittländern niedergelassene und auf dem europäischen Markt tätige Akteure fallen.[17] Dies würde zu einer bedeutenden Auswirkung auf die Leistung von Cloud-Dienste führen.

Verantwortung

Die vorgeschlagene Verordnung sieht eine erweiterte Verantwortung der für die Verarbeitung Verantwortlichen sowie einige neue Pflichten für die Auftragsverarbeiter vor.[18] Im Allgemeinen müssen die für die Verarbeitung Verantwortlichen geeignete Maßnahmen treffen, um die Einhaltung der Verordnung sicherzustellen, und sie müssen dies auch nachweisen können. Dies umfasst auch eine Reihe konkreter Pflichten, wie die Einführung geeigneter Maßnahmen für den „Datenschutz durch Technik“ und den „Datenschutz durch datenschutzfreundliche Voreinstellungen“. Dazu kommt die Notwendigkeit, „Datenschutz-Folgeabschätzungen“ durchzuführen. Beide Pflichten erscheinen für das E-Government maßgeblich. Dies unterstreicht die Notwendigkeit einer eindeutigen Identifikation des für die Verarbeitung Verantwortlichen sowie sehr starke Vereinbarungen für die gegebenenfalls geteilten Kontrollen.

Rechtmäßige Verarbeitung

Die Schlüsselvoraussetzungen für die rechtmäßige Verarbeitung werden in ihrer heutigen Form weiter bestehen, jedoch möglicherweise aufgrund der Notwendigkeit der zulässigen Weiterverarbeitung einigen flexiblen Regelungen unterworfen sein.[19] Da es sich aber um ein Schlüsselelement des Datenschutzes handelt, wie es auch die EU-Charta der Grundrechte hervorhebt, wird der Grad der Flexibilität begrenzt sein.

---

[14] Artikel 10 bis 14 der Richtlinie 95/46/EG
[15] Artikel 18 bis 21 und Artikel 28 der Richtlinie 95/46/EG
[16] KOM (2012) 11 endgültig
[17] Artikel 3 der vorgeschlagenen Verordnung
[18] Artikel 22 bis 34 der vorgeschlagenen Verordnung
[19] Artikel 5 und Artikel 6 der vorgeschlagenen Verordnung

Rechte der betroffenen Personen
Die Anforderungen für die Transparenz wurden erweitert und alle bestehenden Rechte verstärkt.[20] Dabei wurden neue Elemente wie das „Recht auf Vergessenwerden“ und das „Recht auf Datenportabilität“ aufgenommen, was in einem gewissen Umfang auch im öffentlichen Sektor relevant ist. Die Verantwortung des für die Verarbeitung Verantwortlichen wird daneben zu der Notwendigkeit führen, Mechanismen und Verfahren für die Ausübung der Rechte der betroffenen Person einzurichten. Dies wird daher ein wesentlicher Teil der Entwicklung des E-Government werden.

Kontrolle
Die Aufsichtsbehörden werden weitaus bedeutendere Befugnisse besitzen.[21] Diese werden auch beinhalten, hohe Geldstrafen für Verletzungen der vorgeschlagenen Verordnung auferlegen sowie besondere Maßnahmen ergreifen zu können, wenn allgemeine Pflichten nicht erfüllt werden. Außerdem werden Maßnahmen vorgesehen, um die Zusammenarbeit und die Einheitlichkeit der Ergebnisse in der gesamten EU sicherzustellen.[22]

5. Schlussfolgerungen
Ziel der Überprüfung des EU-Rechtsrahmens ist, die Datenschutzbestimmungen zu stärken, sie in der Praxis effektiver zu gestalten und eine bessere Einheitlichkeit innerhalb der EU sicherzustellen. Ein einziges Regelwerk wird grenzübergreifende Projekte vereinfachen, jedoch auch die Hürden für das E-Government erhöhen.

Die Verantwortung für die Bereitstellung von E-Government-Diensten wird eine sehr klare Aufgabenzuteilung und solide Regelungen über Transparenz und Rechenschaftspflichten erfordern, was den Datenschutz durch Technik, Folgenabschätzungen und regelmäßige Kontrollen der Leistung in der Praxis einschließt.

[20] Artikel 11 bis 21 der vorgeschlagenen Verordnung
[21] Artikel 46 bis 54 und Artikel 79 der vorgeschlagenen Verordnung
[22] Artikel 55 bis 63 der vorgeschlagenen Verordnung