EUROPEAN DATA PROTECTION SUPERVISOR

Überwachung und Gewährleistung der Einhaltung der Verordnung (EG) Nr. 45/2001

Strategiepapier

Brüssel, 13. Dezember 2010

Postanschrift: Rue Wiertz 60 – 1047 Brüssel, Belgien
Dienststelle: Rue Montoyer 63
E-Mail: edps@edps.europa.eu – Website: www.edps.europa.eu
Tel.: +32 (0)2 283 19 00 – Fax: +32 (0)2 283 19 50

Inhalt

Überwachung und Gewährleistung der Einhaltung der Verordnung (EG) Nr. 45/2001

1. Einleitung

Im vorliegenden Strategiepapier wird ausgeführt, wie der Europäische Datenschutzbeauftragte (EDSB) die Einhaltung der Verordnung (EG) Nr. 45/2001 („die Verordnung“) überwacht, misst und gewährleistet, und es wird erklärt, welcher Natur die verschiedenen Durchsetzungsbefugnisse sind und wann und wie der EDSB sie ausübt. Das Strategiepapier gibt Aufschluss über viele der derzeit laufenden Aktivitäten und Maßnahmen des EDSB in Bezug auf die Überwachung und Gewährleistung der Einhaltung und beschreibt einen umfassenden Rahmen für alle künftigen Arbeiten in diesem Bereich. Dieser Rahmen orientiert sich an den Grundsätzen der Verhältnismäßigkeit, Rechenschaftspflicht und Einheitlichkeit; er soll Transparenz in Bezug darauf herstellen, wie der EDSB mit den bei unseren Aktivitäten (Bearbeitung von Beschwerden, Vorabkontrollen, Überwachung usw.) gewonnenen Informationen umgeht, und Aufschluss über allgemeine Grundsätze im Zusammenhang mit der Frage geben, wie wir diese Informationen aufnehmen und darauf reagieren, sowie, sofern zutreffend, über das Gewicht oder den Stellenwert, den wir solchen Informationen beimessen.

Ziel der Strategie ist es, die freiwillige Einhaltung der Verordnung und bewährte Vorgehensweisen zu fördern, genügend Anreize für die Einhaltung zu schaffen und gegebenenfalls gezielte Maßnahmen zu erleichtern, indem sie

- hervorhebt, wo die Zuständigkeit für die Einhaltung liegt,
- erklärt, wie der EDSB diese Einhaltung fördert, und
- erklärt, was der EDSB im Fall der Nichteinhaltung unternimmt.

Zur Optimierung der Effizienz des bestehenden Rahmens zielt die Strategie darauf ab, Aufschluss über den in der Verordnung verankerten abgestuften Ansatz zur Gewährleistung des Datenschutzes bei den Einrichtungen und Organen der EU zu geben: die Einrichtungen/Organe, die für die Verarbeitung Verantwortlichen, die behördlichen Datenschutzbeauftragten (DSB) und der EDSB tragen alle zur Anwendung und Einhaltung der Verordnung bei. Daher wird mit der Strategie versucht, Nutzen aus diesen Rollen, Aufgaben und zugrunde liegenden Synergien zu ziehen, um zu gewährleisten, dass die Grundsätze des Datenschutzes auch tatsächlich eingehalten werden.

In Bezug auf den Vertrag von Lissabon sind alle Einrichtungen und Organe der EU an die Grundrechte auf den Schutz der Privatsphäre und der personenbezogenen Daten (siehe Artikel 7 und 8 der EU-Charta und Artikel 16 AEUV) gebunden. Dem EDSB obliegt es zu überwachen und sicherzustellen, dass diese Rechte nach Maßgabe der Verordnung (EG) Nr. 45/2001 geachtet werden.

Aus Artikel 1 Absatz 1 der Verordnung wird deutlich, dass es Aufgabe der Einrichtungen und Organe selbst ist, die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere den Schutz ihrer Privatsphäre bei der Verarbeitung personenbezogener Daten zu schützen.

Darüber hinaus ist dem EDSB sehr daran gelegen, dass die Einrichtungen und Organe zur Wahrnehmung dieser Aufgabe proaktiv vorgehen und sich auch den Grundsatz der „Rechenschaftspflicht" (in dem vor kurzem von der Artikel-29-Datenschutzgruppe ausgearbeiteten Sinne)[1] zu eigen machen und damit den Datenschutz in der Praxis fördern. Rechenschaftspflicht setzt voraus, dass die Einrichtungen und Organe sowie die für die Verarbeitung Verantwortlichen, die in ihrem Auftrag tätig sind, angemessene und wirksame Maßnahmen ergreifen, um zu gewährleisten, dass die in der Verordnung genannten Grundsätze und Verpflichtungen eingehalten werden, und um dies gegenüber dem EDSB auf Anfrage nachweisen zu können. Der EDSB wird sich dann auf seine Aufgaben der Überwachung konzentrieren und bei Bedarf für die Einhaltung Sorge tragen.

Bei den Einrichtungen und Organen der EU spielen die behördlichen Datenschutzbeauftragten eine maßgebliche Rolle, wenn es darum geht, erfolgreiche Programme der Rechenschaftspflicht einzuführen; in diesem Zusammenhang begrüßt der EDSB das Dokument des DSB-Netzwerks zu den „Professionellen Standards für Datenschutzbeauftragte der EU-Organe und Einrichtungen im Rahmen der Verordnung (EG) Nr. 45/2001" (Oktober 2010).[2] Der EDSB ist der Auffassung, dass dieses Dokument eine gute Grundlage für eine neue, effizientere Datenschutzregelung mit sinnvollen Strategien, effizienten Umsetzungsmechanismen und geeigneten Versicherungsprogrammen darstellt.

Der EDSB ist der Überzeugung, dass damit ein selektives, gezieltes und risikobasiertes Durchsetzungskonzept mit Schwerpunkt auf denjenigen Einrichtungen oder Organen möglich wird, denen es eindeutig an Engagement mangelt und/oder die bei der Einhaltung der Verordnung nur wenige Erfolge vorzuweisen haben. Dadurch können wiederum unsere begrenzten Ressourcen innerhalb der bestehenden EU-Datenschutzregelung effizient eingesetzt werden.

2. Überwachung der Einhaltung

Dem EDSB steht eine ganze Reihe von Instrumenten und Mechanismen für die Wahrnehmung seiner Aufgabe der Überwachung der Einhaltung zur Verfügung. Einige leiten sich unmittelbar aus den Bestimmungen der Verordnung ab, während andere wiederum das Ergebnis einer unterschiedlichen Gesetzgebung sind oder einfach der bewährten Praxis entsprechen. Anhand der aus all diesen Instrumenten und Mechanismen

[1] Stellungnahme 3/2010 zum Grundsatz der Rechenschaftspflicht (WP 173), angenommen am 13. Juli 2010, abrufbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_de.pdf

[2] Abrufbar unter http://www.edps.europa.eu/EDPSWEB/edps/Supervision/DPOnetwork

abgeleiteten Hinweise werden Informationen zu einzelnen Einrichtungen oder Organen zusammengetragen, die ihrerseits dabei helfen, fundierte Entscheidungen über formale Durchsetzungsmaßnahmen zu treffen.

2.1. Instrumente des EDSB zur Gewährleistung der Einhaltung

2.1.1. Sensibilisierung

Der EDSB wird nach Maßgabe von Artikel 46 Buchstabe d und Artikel 47 Absatz 1 Buchstabe b der Verordnung auch weiterhin Zeit und Mittel in die Bereitstellung von Beratung, Handlungsempfehlungen und Schulungen (sowohl allgemein als auch maßgeschneidert) zu Datenschutzfragen investieren, die in seinen Aufgabenbereich fallen. Er wird diese Handlungsempfehlungen bei Bedarf auf geeignete Art und Weise veröffentlichen bzw. bekannt machen. Er möchte damit nicht nur die Einhaltung, sondern auch die Übernahme bewährter Verfahren bei den Einrichtungen und Organen der EU fördern.

Im Zusammenhang mit dieser Strategie erwartet der EDSB, dass die angebotene Beratung oder die Schulungsangebote von den entsprechenden Einrichtungen oder Organen umgesetzt werden, und er erwartet, dass die für die Verarbeitung Verantwortlichen und insbesondere die behördlichen Datenschutzbeauftragten eine entscheidende und angemessene Rolle im Einklang mit ihren Aufgaben im Sinne der Verordnung spielen (siehe Artikel 24 Absatz 1 Buchstabe a und c über behördliche Datenschutzbeauftragte). Er wird daher entsprechende Erkenntnisse und Anhaltspunkte, die bei der Wahrnehmung seiner Pflichten gewonnen bzw. zusammengetragen wurden, bei der Prüfung potenzieller Durchsetzungsmaßnahmen berücksichtigen und die Nachfrage nach und die Inanspruchnahme der angebotenen Schulungen und Beratungsangebote bzw. Handlungsempfehlungen überwachen, damit er diesbezüglich Entscheidungen in voller Kenntnis der Sachlage treffen kann.

Derzeit erstellt der EDSB Handlungsempfehlungen zu bestimmen Themen in Form von Themenpapieren, damit bei den Agenturen horizontale Stellungnahmen zu den üblichen Verwaltungsverfahren angenommen werden können. Diese sollen dann als EDSB-Standards für Einrichtungen dienen. Die Arbeit in diesem Bereich kann in Form von Workshops und interaktiven Seminaren weiterentwickelt werden, bei denen der EDSB unsere Position und Erfahrung in einem bestimmten Bereich vorstellt.

2.1.2. Vorabkontrollen

Aufgrund von Artikel 27 der Verordnung ist der EDSB befugt, Verarbeitungen, die besondere Risiken für die Rechte und Freiheiten der betroffenen Personen beinhalten können, vorab zu kontrollieren. Darüber hinaus werden mit diesem Artikel auch die behördlichen Datenschutzbeauftragten beauftragt, dem EDSB diese Vorabkontrollen zu melden. Die Stellungnahme, die sich aus einer Vorabkontrolle ergibt, ist wiederum dem für die Verarbeitung

Verantwortlichen zu melden, der auf Verlangen zur Änderung der Verarbeitung oder aufgrund des Risikopotenzials zu einer Durchsetzungsmaßnahme verpflichtet ist.

Als der EDSB seine Tätigkeit aufnahm, hatte er zunächst einen Rückstand an Fällen von Ex-post-Vorabkontrollen in Bezug auf Verarbeitungen abzuarbeiten, die bereits vorhanden waren. 2004 forderte der EDSB die Einrichtungen/Organe auf, ein Bestandsverzeichnis der Fälle zu erstellen, die potenziell einer Vorabkontrolle unterzogen werden mussten. In Bezug auf Ex-post-Vorabkontrollen wählte er einen thematischen Ansatz; er legte Schwerpunktthemen (medizinische Daten, Mitarbeitergespräche, fachspezifische Daten, soziale Dienste) fest und verlangte bei diesen Themen eine Meldung. Nach dieser Anfangsphase bat der EDSB die Einrichtungen, alle Meldungen über bereits vorhandene Verarbeitungen vorzulegen. Derzeit ist die Lage so, dass dem EDSB die überwiegende Mehrheit der Ex-post-Vorabkontrollen bei EU-Einrichtungen gemeldet wurde.

Artikel 27 sieht nur wenig Spielraum für einen selektiven Ansatz bei Vorabkontrollen vor, doch hat der EDSB den Geltungsbereich dieses Artikels anhand von Artikel 27 Absatz 3 (der die Möglichkeit einer Konsultation des EDSB vorsieht, falls Zweifel hinsichtlich der Notwendigkeit einer Vorabkontrolle bestehen) eingeschränkt. So hat der EDSB beispielsweise festgelegt, dass die Verarbeitung personenbezogener Daten in Bezug auf den Einsatz von Mobiltelefonen durch Mitarbeiter der EACI, die sich auf Dienstreise begeben, keiner Vorabkontrolle unterzogen werden musste, da der Zweck der Verarbeitung darin bestand, Rechnungen von über 50,-- EUR zu prüfen, und nicht, persönliche Aspekte in Bezug auf die Mitarbeiter zu bewerten. In einem anderen Fall entschied der EDSB, dass die Verarbeitung personenbezogener Daten im Hinblick auf die Gewährung von Erziehungszulagen für Mitarbeiter der EBBD nicht vorab kontrolliert werden musste, da damit *per se* nicht versucht werden sollte, Personen von einem Recht, einer Leistung oder einem Vertrag auszuschließen.

Die Weiterverfolgung der bei einer Vorabkontrolle abgegebenen Stellungnahmen ist ein entscheidender Bestandteil der Durchsetzungsstrategie des EDSB. Der EDSB schließt Stellungnahmen bei Vorabkontrollen normalerweise mit der Erklärung ab, dass die Verarbeitung nicht gegen die Verordnung (EG) Nr. 45/2001 verstößt, sofern bestimmte Empfehlungen umgesetzt werden. Werden diese Empfehlungen nicht umgesetzt und nicht mit entsprechenden Nachweisen belegt, muss sich die Einrichtung dessen bewusst sein, dass sie eine formale Durchsetzungsmaßnahme riskiert. Der EDSB wird seinerseits klare, prägnante Empfehlungen abgeben und Fristen vorgeben, und er wird deren Einhaltung konsequent und gründlich überprüfen.

Vorabkontrollen sind eine Möglichkeit, um mit Einrichtungen/Organen einen vorbeugenden Dialog in Form von Zusammenkünften oder öffentlichen Anhörungen einzurichten mit dem Ziel, eine positive und proaktive Datenschutzkultur zu fördern.

Mithilfe der Vorabkontrollen kann sich der EDSB aber auch einen Einblick in die Tätigkeiten der Einrichtungen und Organe der EU verschaffen, wichtige Datenschutzprobleme ermitteln und ein EDSB-Präzedenzrecht entwickeln. Dank der bei der Anwendung der Verordnung gewonnenen Erfahrungen konnte der EDSB Know-how erwerben und Einrichtungen und Organen thematische allgemeine Leitlinien vorlegen.

Die Leitlinien des EDSB zur Videoüberwachung vom 17. März 2010[3] sollten im Hinblick auf die Vorlage von Handlungsempfehlungen für Einrichtungen und Organe als auch auf die Überprüfung, bei der der Schwerpunkt auf die Rechenschaftspflicht verlagert wird, als Pilotfall gesehen werden. Wenn sich ein Organ an die Empfehlungen des EDSB hält, besteht im Grunde kein Bedarf an Vorabkontrollen. Doch auch hier gilt: wenn eine Einrichtung oder ein Organ die Leitlinien missachtet, die festgelegten Fristen nicht einhält oder die damit verbundenen Empfehlungen nicht umsetzt, steigt das Risiko einer formalen Durchsetzungsmaßnahme.

2.1.3. Konsultationen

Mit Artikel 28 Absatz 1 und Artikel 46 Buchstabe d der Verordnung wird den Einrichtungen und Organen der EU die Aufgabe zugewiesen, den EDSB über die Erstellung interner Vorschriften und die Einführung von Verwaltungsverfahren für die Verarbeitung personenbezogener Daten zu unterrichten und zu konsultieren.

In Artikel 28 Absatz 1 heißt es, dass die Organe und Einrichtungen den EDSB über die Ausarbeitung verwaltungsrechtlicher Maßnahmen wie Durchführungsbestimmungen zur Verordnung oder zum behördlichen Datenschutzbeauftragten (Artikel 24 Absatz 8) sowie von allgemeinen internen Verwaltungsvorschriften für die Verarbeitung personenbezogener Daten (z. B. Nutzung von E-Mail, elektronische Überwachung, Archivierung usw.) unterrichten müssen. Der EDSB wird gegebenenfalls die geplanten Maßnahmen bewerten und Empfehlungen abgeben, die von der Einrichtung umgesetzt werden sollten. Der EDSB geht davon aus, dass er über die diesbezüglich erzielten Fortschritte auf dem Laufenden gehalten wird, und er wird diese zur Gewährleistung der Einhaltung weiterverfolgen.

In Artikel 46 Buchstabe d wird die beratende Funktion des EDSB im weiteren Sinne so beschrieben, dass sie sich auf *„alle Fragen, die die Verarbeitung personenbezogener Daten betreffen“* bezieht, und es wird hinzugefügt, dass der EDSB beratend tätig werden kann, *„bevor [die Organe und Einrichtungen] interne Vorschriften für den Schutz der Grundrechte und Grundfreiheiten von Personen bei der Verarbeitung personenbezogener Daten ausarbeiten“*.

Auch wenn sich Artikel 46 Buchstabe d mit Artikel 28 Absatz 1 überschneidet, wird der Geltungsbereich auf „alle“ anderen Fragen ausgeweitet; dies ist die Grundlage für eine Beratung in Fällen, in denen es um spezifische

[3] Zu finden unter http://www.edps.europa.eu/EDPSWEB/edps/Supervision/Guidelines

Verarbeitungen oder abstrakte Fragen zur Auslegung der Verordnung geht (beispielsweise, wie das Auskunftsrecht in bestimmten Fällen, in denen praktische Schwierigkeiten auftreten, umzusetzen ist, wie Artikel 9 auszulegen und anzuwenden ist usw.). Wenn die Konsultationen auf hypothetischen Fällen beruhen oder sich mit Auslegungsfragen befassen, ist die Weiterbearbeitung beschränkt, lässt sich jedoch nicht ganz ausschließen.

Der EDSB begrüßt jede proaktive Konsultation seitens einer Einrichtung oder eines Organs und wird diese als positiven Schritt auf dem Weg zur Einhaltung einstufen. Er erwartet jedoch von den betroffenen Organen/Einrichtungen, dass sie entsprechend Verantwortung übernehmen, um Änderungen vorzunehmen oder um die Ratschläge oder Empfehlungen, die sich aus diesen Konsultationen ergeben, umzusetzen; falls dies nicht der Fall ist, kann er eine formale Durchsetzungsmaßnahme nicht ausschließen.

2.1.4. Bearbeitung von Beschwerden

Artikel 33 der Verordnung bietet Mitarbeitern von Organen/Einrichtungen der EU die Möglichkeit, beim EDSB Beschwerde wegen angeblicher Verletzungen der Bestimmungen dieser Verordnung über die Verarbeitung personenbezogener Daten einzureichen. Nach Maßgabe von Artikel 46 Buchstabe a und b muss der EDSB solche Beschwerden gegebenenfalls prüfen oder untersuchen. Für eine Untersuchung von Beschwerden durch den EDSB ist es insbesondere erforderlich, dass die behördlichen Datenschutzbeauftragten und die für die Verarbeitung Verantwortlichen zusammenarbeiten, es werden jedoch auch andere Bedienstete der betreffenden Einrichtung bzw. des betreffenden Organs in die Untersuchung eines bestimmten Falls einbezogen, sofern dies erforderlich ist.

Beschwerden und die sich daraus ergebenden Untersuchungen sind aus Sicht der Überwachung der Einhaltung wichtige Informationsquellen. Der EDSB wird diese Informationen auch weiterhin auswerten, um entscheiden zu können, ob sich daraus größere Einhaltungsprobleme ergeben oder ob diese Informationen auf eine mangelhafte Einhaltung bzw. auf eine Nichteinhaltung hinweisen, die sich bei seinen Überwachungstätigkeiten im weiteren Sinne ergeben. Anschließend entscheidet er, ob weitere Schritte, etwa eine Kontrolle oder eine formale Durchsetzungsmaßnahme, angebracht sind.

Der EDSB hat eine Beschwerdestrategie erlassen, wonach er bei der Bearbeitung von Beschwerden selektiv vorgehen kann. Die entsprechenden Kriterien sind im internen Handbuch „Beschwerden“ beschrieben; demzufolge ist zunächst zu klären, ob, und dann, wie eine Beschwerde zu bearbeiten ist. Diese Kriterien werden mit zunehmender Erfahrung weiter verfeinert, doch die Hauptbestandteile der Strategie wurden bereits veröffentlicht[4], damit potenzielle Beschwerdeführer die Vorgehensweise des EDSB nachvollziehen können und damit der EDSB besser mit ihren Erwartungen umgehen kann.

[4] Zu finden unter http://www.edps.europa.eu/EDPSWEB/edps/Supervision/Complaints

Der EDSB zieht darüber hinaus in Betracht, Handlungsempfehlungen für Einrichtungen und für die Öffentlichkeit vorzulegen, wonach es im Allgemeinen für beide Parteien bewährte Praxis wäre zu versuchen, die Angelegenheit bilateral über ein Verfahren der internen Prüfung zu klären, auch wenn direkt beim EDSB Beschwerde eingereicht werden kann. Wichtig ist, dass dies voraussetzt, dass dem behördlichen Datenschutzbeauftragten die entsprechenden Ressourcen zur Verfügung gestellt werden, damit er Beschwerden bearbeiten kann. Die nach Artikel 24 Absatz 8 der Verordnung zu erlassenden Durchführungsbestimmungen sehen solche Befugnisse in einer Reihe von Organen und Einrichtungen vor. Darüber hinaus wird diese Vorgehensweise im Papier des DSB-Netzwerks zu den „Standesregeln für behördliche Datenschutzbeauftragte“ befürwortet[5] und trägt damit zu den Zielen bei, die Rechenschaftspflicht der für die Verarbeitung Verantwortlichen zu verstärken und die Verantwortung für die Einhaltung auf die Einrichtungen/Agenturen selbst abzuwälzen.

2.1.5. Gezielte Überwachung und Berichterstattung

Der EDSB führt eine gezielte Überwachung auf der Grundlage der bei allen seinen Überwachungstätigkeiten zusammengetragenen Kenntnisse, Erkenntnisse und Hinweise durch, um Themen oder besondere Einrichtungen/Organe zu ermitteln, die einer gezielteren Aufmerksamkeit bedürfen. Dies umfasst normalerweise Untersuchungen des Schriftverkehrs in Bezug auf bestimmte Arten der Datenverarbeitung bei allen oder einigen Einrichtungen oder Organen, kann jedoch bei Bedarf auch einen Kontrollbesuch vor Ort bedeuten – etwa dann, wenn eine Einrichtung bzw. ein Organ wiederholt nicht geantwortet hat oder die Bestimmungen der Verordnung nicht ausreichend beachtet. Solche Maßnahmen führen normalerweise zu einer vereinbarten Reihe von Empfehlungen und Fristen, häufig in Form eines Leitfadens.

Die Nichtumsetzung dieser Empfehlungen und/oder die Nichteinhaltung der damit verbundenen Fristen können Maßnahmen formellerer Natur nach sich ziehen. Der EDSB erwartet und verlangt im Rahmen dieses Prozesses, dass ihn die Leiter der Einrichtungen, die für die Verarbeitung Verantwortlichen und natürlich die behördlichen Datenschutzbeauftragten im Einklang mit den Artikeln 47 Absatz 2 Buchstabe a und 24 Absatz 1 Buchstabe b der Verordnung unterstützen und mit ihm zusammenarbeiten.

2.1.6. Allgemeine Überwachung und Berichterstattung

Bislang hat der EDSB zweimal versucht, die allgemeine Einhaltung der Verordnung zu messen, indem er die Leiter von Einrichtungen und Agenturen angeschrieben und sie um eine schriftliche Rückmeldung zu bestimmten

[5] Siehe Abschnitt 3.7 der „Professionellen Standards für Datenschutzbeauftragte der EU-Organe und Einrichtungen im Rahmen der Verordnung (EG) Nr. 45/2001“.

Fragen gebeten hat. Der EDSB wird diese regelmäßigen „Umfragen“ auch künftig fortführen, um sicherzugehen, dass er über ein repräsentatives Bild von der Einhaltung der Datenschutzvorschriften bei den Organen/Einrichtungen der EU verfügt, und um angemessene interne Ziele festzusetzen, um seine Ergebnisse umsetzen zu können.

Darüber hinaus wird der EDSB auf der Grundlage der bei ihm eingegangenen Antworten und Hinweise allen Einrichtungen/Agenturen individuelle Stellungnahmen vorlegen und im Fall der Nichteinhaltung einschlägige präskriptive Ziele festlegen. Mithilfe der Rückmeldungen kann er aber gegebenenfalls auch Einrichtungen/Organe für Kontrollbesuche auswählen. Falls die Ziele nicht erfüllt werden, werden normalerweise verbindliche Entscheidungen einschließlich einer Berichtspflicht getroffen. Im Fall einer fortdauernden Nichteinhaltung der Verordnung wird mit hoher Wahrscheinlichkeit eine formale Durchsetzungsmaßnahme (siehe unten) ausgelöst.

Ferner ist zu beachten, dass manche Einrichtungen im Rahmen ihrer Durchführungsbestimmungen ihre Datenschutzbeauftragten dazu verpflichten, Tätigkeitsberichte zu erstellen. Diese Berichte enthalten häufig Hinweise darauf, inwieweit die Verordnung in der Einrichtung eingehalten wird, und sind daher ganz eindeutig im Interesse des EDSB. Der EDSB würde es daher begrüßen, Kopien dieser Berichte[6] zu bekommen, würde jedoch natürlich mit den darin beschriebenen Problemen kooperativ und informell umgehen, um die Einrichtungen nicht generell von dieser Vorgehensweise abzubringen. Werden jedoch die Einrichtung die sich daraus ergebenden Empfehlungen oder Ratschläge des EDSB nicht befolgt, kann eine formale Durchsetzungsmaßnahme nicht ausgeschlossen werden.

2.1.7. Kontrollen

In den Artikeln 41 Absatz 2, 46 Buchstabe c und 47 Absatz 2 der Verordnung sind breit gefasste Befugnisse verankert, einschließlich der Befugnis, Kontrollen durchzuführen, die den EDSB in die Lage versetzen, seine Funktion als Kontrollbehörde wahrzunehmen.

Derzeit wird eine spezifische Kontrollstrategie ausgearbeitet. Doch in Anbetracht des für Kontrollen erforderlichen erheblichen Zeit- und Ressourcenaufwands ist dem EDSB sehr an einer selektiven Vorgehensweise gelegen, was die Inanspruchnahme dieser Ressourcen betrifft, die auf zwei allgemeine Arten von Kontrollen (allgemeine und thematische Kontrollen) beschränkt ist und durch Hinweise und Sachverhalte ausgelöst wird, die mithilfe der anderen, in diesem Kapitel beschriebenen Werkzeuge zusammengetragen werden.

[6] In Abschnitt 4.1 der „Professionellen Standards für Datenschutzbeauftragte der EU-Organe und Einrichtungen im Rahmen der Verordnung (EG) Nr. 45/2001“ wird die Übermittlung einer Kopie dieser Berichte an den EDSB empfohlen.

Bei den üblichen Kontrollen soll untersucht und gewährleistet werden, dass die Entscheidungen des EDSB, die er im Rahmen der bei den Vorabkontrollen abgegebenen Stellungnahmen oder von Beschwerden trifft, eingehalten werden, sowie ganz allgemein auch die Verordnung in allen Fällen, in denen sich bei regelmäßigen Überwachungen ernst zu nehmende Hinweise darauf ergeben haben, dass der Einhaltungsmechanismus blockiert ist. Sie sind daher als die letzte Stufe vor einer formalen Durchsetzungsmaßnahme zu werten.

Der EDSB führt darüber hinaus auch thematische Kontrollen durch; dabei geht er so vor, dass er in einem bestimmten Bereich bzw. zu einem bestimmten Thema beratend tätig wird und Fristen festlegt, innerhalb derer von den Einrichtungen und Agenturen erwartet wird, dass sie die Datenschutzregelungen und die Empfehlungen in seinen Handlungsempfehlungen einhalten. Sollten sie diese Fristen nicht einhalten oder die geforderten Regelungen bzw. Empfehlungen nicht umsetzen, ist die Wahrscheinlichkeit, dass eine formale Durchsetzungsmaßnahme ergriffen wird, größer.

Kontrollen sind von Natur aus maßgeschneidert und werden aufgrund besonderer Anforderungen und Ziele strukturiert. Der EDSB wird jedoch sehr wahrscheinlich die Leiter und führenden Mitarbeiter der Einrichtung bzw. des Organs, die zuständigen für die Verarbeitung Verantwortlichen, die Datenschutzbeauftragten[7] und andere wichtige Mitarbeiter in den Prozess mit einbinden wollen, und diese werden sich bereit erklären, mit ihm zusammenzuarbeiten.

2.2. Externe Instrumente zur Überwachung der Einhaltung

Datenschutz-Folgenabschätzungen, Meldungen von Sicherheitsverletzungen und interne Berichte über die Einhaltung der Datenschutzvorschriften sind Mechanismen, die von Einrichtungen und Organen der EU selbst genutzt werden können, um die Einhaltung ihrer Verpflichtungen im Bereich Datenschutz zu gewährleisten, aber auch ihre Bereitschaft zur Umsetzung der „Rechenschaftspflicht“ bzw. deren Anwendung nachzuweisen. Zwar sind diese noch nicht alle in gesetzlichen Verpflichtungen verankert, doch sollten sie als wichtige Instrumente in dem Umfeld, in dem der EDSB tätig ist, sowie als wichtige Indikatoren der Kultur und als Informationsquellen zum Nachweis der Einhaltung gesehen werden. Dort, wo sie wichtig und angebracht sind, wird ihre Nutzung auch vom EDSB gefördert, beispielsweise durch die Herausgabe von Handlungsempfehlungen.

Dort, wo solche Initiativen freiwillig ergriffen wurden, wird der EDSB dementsprechend auch konstruktiv und unterstützend bei allen dabei ermittelten Fragen der Einhaltung der Vorgaben vorgehen und nur dann schwerwiegendere und formellere Maßnahmen ergreifen, wenn eine solche Zusammenarbeit nicht gegeben ist.

[7] Die Rolle der behördlichen Datenschutzbeauftragten bei den vom EDSB durchgeführten Kontrollen wird in der Kontrollstrategie des EDSB näher ausgeführt.

Zwei weitere Instrumente, die die Effizienz der Tätigkeiten des EDSB zur Überwachung der Einhaltung steigern könnten, sind Audits und Risikobewertungen, wobei diese allerdings erst noch entwickelt werden müssen.

2.2.1. Datenschutz-Folgenabschätzungen (PIAs)

Der EDSB soll Einrichtungen und Agenturen dazu anhalten, Datenschutz-Folgenabschätzungen in Bezug auf neue Verarbeitungen von personenbezogenen Daten durchzuführen. Der EDSB prüft daher die Erstellung von Handlungsempfehlungen zu dieser Frage, entweder, um anzugeben, ob wir erwarten, dass solche PIAs standardmäßig durchgeführt werden sollten, oder, indem die Art der Daten oder der Verarbeitung genau beschrieben wird, für die wir eine solche PIA erwarten würden. Ein alternativer Ansatz zugunsten dieses Werkzeugs zur Überprüfung der Einhaltung bestünde darin, dass der EDSB zunächst die Frage prüft, ob eine PIA erforderlich ist, und wenn ja, diese Maßnahme der Einrichtung auferlegt.

PIAs sind sehr wichtig, denn sie bieten Einrichtungen und Organen die Möglichkeit, sich einen besseren Einblick in wichtige Risiken für die Privatsphäre und in Möglichkeiten zu verschaffen, diese Risiken zu bewältigen. Sie können aber auch zu Meldungen und möglicherweise Vorabkontrollen, Empfehlungen und zu einer Weiterverfolgung führen.

2.2.2. Meldungen von Sicherheitsverletzungen

Der EDSB soll Einrichtungen aber auch dazu anhalten, interne Verfahren bei Verstößen gegen die Sicherheitsvorschriften (im Einklang mit der Datenschutzrichtlinie für elektronische Kommunikation und der entsprechenden Praxis auf nationaler Ebene) einzuführen, die Meldungen durch den für die Verarbeitung Verantwortlichen an den behördlichen Datenschutzbeauftragten und/oder den EDSB vorsehen. Die Durchführungsbestimmungen der Kommission zur Sicherheit (Meldung an den behördlichen Datenschutzbeauftragten) sollte als ein erster Schritt in diese Richtung gesehen werden.

Die Antwort des EDSB auf solche Meldungen hängt natürlich von mehreren Faktoren ab, einschließlich vom Ausmaß des Verstoßes, von Art und Umfang der betroffenen Daten, von der Zahl der Betroffenen, dem Standort der Empfänger usw. Die Antwort des EDSB richtet sich aber auch nach dem Unterschied zwischen gemeldeten Verstößen im Rahmen von Selbstauskünften und solchen, von denen er über Beschwerden, die Presse oder andere Medien Kenntnis erlangt.

2.2.3 Interne Berichte über die Einhaltung der Datenschutzvorschriften

Der EDSB sollte die Herausgabe von Handlungsempfehlungen in Erwägung ziehen, mit denen Einrichtungen und Organe der EU dazu angehalten werden, interne Berichte über die Einhaltung der Datenschutzvorschriften zu erstellen. Diese sind nicht nur ein nützliches Überwachungsinstrument, sondern helfen auch dabei, die Verantwortung für die Überwachung der Einhaltung auf die Einrichtungen selbst abzuwälzen und auf diese Weise die Rechenschaftspflicht zu fördern. Der EDSB könnte für Einrichtungen und Organe Anreize schaffen, um sich proaktiv zu einer solchen Berichterstattung zu verpflichten, indem beispielsweise geeignete Ausnahmeregelungen von unseren allgemeinen Erhebungen zu Überwachungszwecken ermöglicht werden.

2.2.4. Audits

Der EDSB könnte die Zusammenarbeit mit Auditdiensten prüfen, damit Fragen der Einhaltung von Vorschriften, die Teil ihrer Arbeit sind, vom EDSB auf angemessene Art und Weise überwacht werden können. Dies erfordert zweifellos eine Art Absichtserklärung, in der Rollen, Aufgaben und Verfahren klar festgelegt werden. Die Einrichtungen und Organe müssten außerdem darauf aufmerksam gemacht werden, dass ein solcher Informationsaustausch gegebenenfalls stattfindet.

2.2.5. Risikobewertungen

Zur Förderung einer selektiven, risikobasierte Vorgehensweise und eines effizienteren und stärker zielgerichteten Arbeitsprogramms könnte der EDSB versuchen, Kriterien aufzustellen und regelmäßige Bestandsaufnahmen (etwa halbjährlich) vorzunehmen, um zu ermitteln, welche Bereiche und Themen besonderer Aufmerksamkeit und Beachtung bedürfen.

3. Durchsetzung

3.1. Einführung und Hintergrund

Die Befugnisse des EDSB zur Durchsetzung sind in Artikel 47 der Verordnung dargelegt. Ihr Anwendungsbereich ist relativ breit, denn sie reichen von der Beratung bis hin zu Verwarnungen und Verboten der Verarbeitung. Die vorliegende Strategie soll Klarheit und Einheitlichkeit in die Ausübung dieser Befugnisse bringen.

Der EDSB hat unter Berücksichtigung des interinstitutionellen Rahmens, in dem er tätig ist, bis dato zur Rechtsdurchsetzung noch keinen repressiven Ansatz verfolgt, sondern es vorgezogen, Empfehlungen auszusprechen und die Einhaltung der Vorschriften anzuregen, anstatt den für die Verarbeitung Verantwortlichen abzumahnen oder rechtsverbindliche Anordnungen zu erteilen. Doch nach einer fünfjährigen Tätigkeit ist es höchste Zeit, eine Änderung der Vorgehensweise zu signalisieren.

Der EDSB wird zwar nach wie vor die Einhaltung der Vorschriften sowie bewährte Verfahren auf informelle und kooperative Art und Weise fördern, jetzt jedoch einen proaktiven und ganzheitlichen Ansatz bei formalen Maßnahmen in Fällen ernstlicher, vorsätzlicher oder wiederholt auftretender Probleme oder aber dann wählen, wenn sein Rat nicht befolgt wurde. Wir sind uns dessen bewusst, dass dann, wenn in Fällen, in denen uns Nachweise der Nichteinhaltung vorliegen, nicht gehandelt wird, eine Kollision mit unseren Zielen der Rechenschaftspflicht und Einheitlichkeit vorliegt, was die Autorität des EDSB zu untergraben droht.

Wie bereits an anderer Stelle in dieser Strategie ausgeführt, wird der EDSB, wenn es darum geht zu entscheiden, ob er eine formale Durchsetzungsmaßname einleiten soll oder nicht, alle Nachweise, Belege und Sachverhalte, die er bei seinen gesamten Kontrolltätigkeiten zusammengetragen hat, sorgfältig prüfen. Diese Informationen helfen ihm nicht nur bei der Entscheidung, ob er eine Durchsetzungsmaßnahme einleiten soll oder nicht, sondern auch, wenn es darum geht zu entscheiden, welche Art von Maßnahme ergriffen werden soll.

3.2. Arten und Definition von Durchsetzungsmaßnahmen

Es gibt verschiedene Arten von Durchsetzungsmaßnahmen, die dem EDSB zur Verfügung stehen. Er wird eingedenk der Ergebnisse, die damit erzielt werden können, sowie des möglichen Abschreckungseffekts bzw. der erzieherischen Nebenwirkung für die Einrichtung bzw. das Organ sowie für andere Einrichtungen und Organe die effizienteste Maßnahme auswählen. Im Zusammenhang mit dieser Strategie wird eine formale Durchsetzungsmaßnahme im Sinne der Artikel 47 Absatz 1 Buchstabe c bis h der Verordnung definiert, wonach der EDSB folgende Befugnisse besitzt. Er kann

- anordnen, dass Anträge auf Ausübung bestimmter Rechte in Bezug auf Daten bewilligt werden, wenn derartige Anträge unter Verstoß gegen die Artikel 13 bis 19 abgelehnt wurden;

- den für die Verarbeitung Verantwortlichen ermahnen oder verwarnen;

- die Berichtigung, Sperrung, Löschung oder Vernichtung aller Daten, die unter Verletzung der Bestimmungen für die Verarbeitung personenbezogener Daten verarbeitet wurden, und die Meldung solcher Maßnahmen an Dritte, denen die Daten mitgeteilt wurden, anordnen;

- die Verarbeitung vorübergehend oder endgültig verbieten;

- das betroffene Organ oder die betroffene Einrichtung der Gemeinschaft und, falls erforderlich, das Europäische Parlament, den Rat und die Kommission mit der Angelegenheit befassen;

- (zu den entsprechenden Bedingungen) den Gerichtshof der Europäischen Gemeinschaften anrufen.

Auch wenn diese Befugnisse in der Praxis eher selten ausgeübt werden, hat der EDSB die Absicht, einen stärker proaktiv ausgelegten und robusteren Ansatz zu wählen, um sie in Zukunft auszuüben. In Abschnitt 3.4 werden zur Veranschaulichung einige Beispielszenarien vorgestellt.

3.3. Auslöser von Durchsetzungsmaßnahmen

Der EDSB wählt einen selektiven und angemessenen Ansatz, wenn er Durchsetzungsmaßnahmen einleitet und betreibt, der mit seinen beschränkten Ressourcen in Einklang steht. Wie bereits ausgeführt, ist der interinstitutionelle Rahmen einem auf Zusammenarbeit beruhenden Ansatz zugunsten von Maßnahmen auf der Grundlage von Artikel 47 Absatz 1 Buchstabe b (der sich auf den für die Verarbeitung Verantwortlichen und auf Vorschläge zur Behebung eines Verstoßes bezieht) förderlich. Daher wird eine formale Maßnahme in den meisten Fällen dadurch ausgelöst, dass Bedenken bezüglich eines erheblichen tatsächlich entstandenen oder potenziellen Schadens infolge der Nichteinhaltung der Datenschutzgrundsätze oder der wiederholten, ernsthaften oder vorsätzlichen Nichtbefolgung der Empfehlungen des EDSB vorliegen.

Eine Durchsetzungsmaßnahme wird normalerweise zunächst ausgelöst durch

- Fragen, die im Rahmen der bei uns eingereichten Beschwerden aufgeworfen werden;

- Bedenken, die sich durch unsere Kontroll- und/oder Überwachungstätigkeiten ergeben;

- Fragen, die durch unsere Konsultationen sichtbar werden.

Wenn es darum geht zu entscheiden, ob Maßnahmen ergriffen werden sollen oder nicht, welche Art von Maßnahme sowie deren Ausmaß, werden wir folgende Kriterien prüfen:

- Ist eine Maßnahme erforderlich, um eine wichtige Rechtsfrage oder einen wichtigen Grundsatz zu klären?

- Ist eine Maßnahme dadurch gerechtfertigt, dass die Wahrscheinlichkeit besteht, dass sich ein Verstoß nachhaltig negativ auswirken wird oder dass sich dieser Verstoß wiederholt, falls die Maßnahme nicht ergriffen wird?

- Ist die Praxis der Einrichtung oder des Organs für eine bestimmte Tätigkeit insofern repräsentativ, als sie die Notwendigkeit begründet, ein Beispiel zu statuieren?

- Ist die Nichteinhaltung der Handlungsempfehlungen des EDSB (Positionspapier, Leitlinien, Empfehlungen usw.) durch eine Einrichtung oder ein Organ ein Grund für eine Durchsetzungsmaßnahme?

- Deuten die Einstellung und das Verhalten der Einrichtung, des Organs oder des behördlichen Datenschutzbeauftragten sowohl in Bezug auf den jeweiligen Fall als auch allgemein in Bezug auf Fragen der Einhaltung der Vorschriften auf eine vorsätzliche, wenig hilfreiche oder unkooperative Vorgehensweise hin?

- Reicht das Maß des öffentlichen Interesses an der Frage aus, um eine Durchsetzungsmaßnahme zu begründen?

- Ist die Ergreifung konkreter Durchsetzungsmaßnahmen aufgrund der erforderlichen Ressourcen und aufgrund dessen, dass von mehreren Seiten Bedarf an diesen Ressourcen angemeldet wird, gerechtfertigt?

- Welche Risiken für den Ruf und die Glaubwürdigkeit des EDSB bestehen, falls die Maßnahme ergriffen bzw. nicht ergriffen wird?

- Wäre es angemessener oder effizienter, wenn die Maßnahme auf andere Art und Weise oder von anderen Organen (z. B. vom Europäischen Bürgerbeauftragten oder vor Gericht) ergriffen würde?

3.4. Beispiele für Durchsetzungsmaßnahmen

Nachstehend folgen ein paar Beispiele für die Verhaltensweisen, die mit hoher oder geringer Wahrscheinlichkeit dazu führen, dass der EDSB seine formalen Durchsetzungsbefugnisse ausübt. Immer dann, wenn eine Maßnahme wahrscheinlich ist, sind auch die potenziellen Ergebnisse angegeben. Die Beispiele dienen der Veranschaulichung; sie sind weder erschöpfend noch verbindlich.

3.4.1. Die Maßnahme ist wahrscheinlich (insbesondere nach einer Verwarnung)

- Die Verweigerung des Zugangs des Betroffenen, wenn angenommen werden kann, dass wichtige Informationen vorgehalten werden, kann zu der Anordnung führen, dass Zugang gewährt werden muss;

- die wiederholte Unterlassung, dem EDSB zu antworten oder seine Empfehlungen in Bezug auf Verarbeitungen umzusetzen, kann zu einer Verwarnung des für die Verarbeitung Verantwortlichen führen. Dies könnte mit einem Schreiben an den betroffenen Direktor (oder hochrangigen Beamten) und/oder mit der Bekanntmachung der Unterlassung und einer Erwähnung im Jahresbericht des EDSB verbunden sein;

- die Erhebung und Speicherung von ausführlichen oder sensiblen personenbezogenen Daten über einen sehr viel längeren Zeitraum als notwendig oder für nicht näher bestimmte Zwecke (insbesondere dann, wenn sie sich auf die Berufsaussichten ausüben) könnten zu einer Anordnung führen, die Daten zu löschen oder zu vernichten;

- unbeantwortete Fragen oder Zweifel hinsichtlich der Rechtmäßigkeit der Verarbeitung können dazu führen, dass der EDSB die Verarbeitung vorübergehend oder endgültig verbietet;

- eine vorsätzliche unbefugte Weitergabe von oder der unbefugte Zugriff auf personenbezogene Daten kann dazu führen, dass das Europäische Parlament, der Rat, die Kommission oder unter bestimmten Umständen sogar der Gerichtshof mit der Angelegenheit befasst werden, die anschließend bekannt gemacht wird.

3.4.2. Die Maßnahme ist unwahrscheinlich

- die „zufällige“ Nichteinhaltung der Bestimmungen der Verordnung, die eingestanden wird und auf die unverzüglich eine wirksame Abhilfemaßnahme folgt;

- eine Nichteinhaltung, durch die in den Datenschutz nicht besonders eingegriffen wird und die keinen größeren Schaden verursacht hat, es sei denn, es werden dadurch Probleme in größerem Umfang aufgeworfen;

- eine Nichteinhaltung, bei der Druck anderer Art, wie Negativwerbung und Rufschädigung, schneller und effizienter wirkt als eine formale Durchsetzungsmaßnahme des EDSB.

4. Transparenz und Öffentlichkeit.

Der EDSB ist der Auffassung, dass Transparenz in Bezug auf seine Tätigkeiten sowohl für seine Interessengruppen als auch im Hinblick auf eine verantwortungsvolle Verwaltung wichtig ist. Er stellt daher wichtige Informationen in seine Website ein und nimmt sie in seinen Jahresbericht auf. Außerdem gibt er Pressemitteilungen heraus, in denen er auf wichtige Maßnahmen, Entscheidungen und Stellungnahmen sowie auf wichtige aktuelle Themen im Bereich Datenschutz aufmerksam macht.

Im Hinblick auf seine Tätigkeiten im Bereich der Durchsetzung veröffentlicht der EDSB normalerweise Informationen, wenn er das Parlament, den Rat, die Kommission oder den Europäischen Gerichtshof offiziell mit Angelegenheiten befasst. Darüber hinaus prüft er fallweise, ob es angemessen oder von Vorteil ist, Informationen zu den anderen, in Abschnitt 3.2 beschriebenen Durchsetzungsmaßnahmen über geeignete Medien zu veröffentlichen.

Falls der EDSB beabsichtigt, nähere Angaben oder Zusammenfassungen seiner formalen Durchsetzungsmaßnahmen zu veröffentlichen oder bekannt zu machen, teilt er dies der entsprechenden Einrichtung oder dem entsprechenden Organ im Vorfeld mit, damit diese die Möglichkeit bekommen, eine öffentliche Antwort in Erwägung zu ziehen und vorzubereiten, falls sie dies für angemessen erachten.