EUROPÄISCHER DATENSCHUTZBEAUFTRAGTER

BERICHT
UMFRAGE 2015

Messung der Einhaltung der Datenschutzvorschriften in Organen und Einrichtungen der EU

21. Januar 2016

INHALTSVERZEICHNIS

I. Vorwort

Der Europäische Datenschutzbeauftragte (EDSB) ist die unabhängige Aufsichtsbehörde, die für die Überwachung und Gewährleistung der Einhaltung der Verordnung (EG) Nr. 45/2001 (Verordnung)[1] zuständig[2] ist, also der für Organe, Einrichtungen, Büros und Agenturen der EU (EU-Einrichtungen) bei der Verarbeitung personenbezogener Daten geltenden Datenschutzvorschriften.

Aufgabe des EDSB ist es, EU-Einrichtungen bei der Erhebung, Verwendung und Speicherung personenbezogener Daten sowohl in ihrem Arbeitsalltag als auch in ihren Kerntätigkeiten dabei zu unterstützen, nicht nur auf die Einhaltung der Vorschriften zu achten, sondern auch in enger Zusammenarbeit mit dem in jeder EU-Einrichtung bestellten behördlichen Datenschutzbeauftragten (DSB) dem Grundsatz der Rechenschaftspflicht[3] Genüge zu tun. EU-Einrichtungen müssen nicht nur die Verordnung einhalten, sondern auch in der Lage sein, dies *nachzuweisen*.

Um in seiner Arbeit noch wirksamer zu werden, und weil er eine noch engere Wechselwirkung mit den von ihm überwachten EU-Einrichtungen anstrebt, nimmt der EDSB alle zwei Jahre eine **allgemeine Bestandsaufnahme** vor, bei der es im Wesentlichen um Aspekte geht, die auf Fortschritte bei der Umsetzung der Verordnung in den EU-Einrichtungen hindeuten. Dieser Bericht ist das Ergebnis der fünften dieser Bestandsaufnahmen; er gründet auf den Antworten, die bis September 2015[4] von **61 EU-Einrichtungen** eingegangen waren.

Im Einklang mit der Durchsetzungsstrategie[5] des EDSB wird dieser Bericht mit der Absicht veröffentlicht, die EU-Einrichtungen zu veranlassen, klarer Rechenschaft über die Einhaltung der Datenschutzvorschriften abzulegen. Der Bericht ist Teil unserer Bemühungen, EU-Einrichtungen darin zu schulen und anzuleiten, wie die Datenschutzvorschriften in der Praxis am besten eingehalten werden können, wobei der Schwerpunkt auf Arten der Verarbeitung liegt, die mit hohen Risiken für natürliche Personen verbunden sind. Der Bericht unterstreicht also **Fortschritte**, die im Vergleich zu früheren Umfragen erzielt wurden, weist aber auch auf **Defizite** hin. Ferner werden die Ergebnisse der **Inspektionsbesuche** ausgewertet, die aufgrund der Ergebnisse der letzten Umfrage in einer Reihe von EU-Einrichtungen stattfanden.

Die eingegangenen Antworten und frühere Inspektionsbesuche haben gezeigt, dass bei der Anwendung der Verordnung nicht nur Zeit und Ressourcen, sondern auch der gute Wille der betreffenden Einrichtung eine Rolle spielen. Der Bericht nimmt also keine Bewertung der individuellen Leistung der in den EU-Einrichtungen jeweils bestellten DSB vor. Vielmehr betrachtet er die Gesamtleistung jeder einzelnen EU-Einrichtung, die für die Wahrung des Rechts natürlicher Personen auf Schutz der Privatsphäre bei der Verarbeitung personenbezogener Daten verantwortlich ist. Bei der Gewährleistung der Einhaltung der Verordnung handelt es sich um einen Prozess, der das **Engagement** und die **Unterstützung** seitens der Hierarchie in allen EU-Einrichtungen erfordert.

---

[1] 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.

[2] Nach Maßgabe von Artikel 41 Absatz 2 der Verordnung.

[3] Siehe die am 2. März 2015 veröffentlichte Strategie 2015-2019 des EDSB, abrufbar auf der Website des EDSB: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Strategy/15-02-26_Strategy_2015_2019_DE.pdf.

[4] Mehrere Einrichtungen und Agenturen haben nach diesem Datum geantwortet. Wo dies möglich war, wurden ihre Antworten noch in diesen Bericht aufgenommen.

[5] Siehe das Strategiepapier des EDSB vom 13. Dezember 2010 „Überwachung und Gewährleistung der Einhaltung der Verordnung (EG) Nr. 45/2001“, S. 8.

Der EDSB wird die Ergebnisse dieser Umfrage bei der Planung weiterer Aufsichts- und Durchsetzungstätigkeiten berücksichtigen. Bei unserer Beaufsichtigung der EU-Einrichtungen setzen wir auf Aufklärung, Überzeugungskraft und Vorbildfunktion und behalten uns unsere Durchsetzungsbefugnisse als letztes Mittel vor. Unsere Aktivitäten werden eine Kombination von **Leitlinien** für EU-Einrichtungen, **Durchsetzungsmaßnahmen** und weiteren Maßnahmen zur Förderung der **Rechenschaftspflicht** sein. So werden auf der Grundlage der Ergebnisse dieser Umfrage insbesondere durch einen augenfälligen Mangel an Engagement eines Organs oder einer Einrichtung ausgelöste Inspektionsbesuche geplant.

II. Zusammenfassung

Diese Umfrage vermittelt einen Gesamtüberblick über die Einhaltung von Datenschutzvorschriften durch EU-Einrichtungen und beleuchtet somit die Rolle des EDSB als unabhängige Aufsichtsbehörde.

Auch wenn die Umfrage ihrer Art nach eher technisch ist und sich auf formale Aspekte konzentriert, liefert sie doch wertvolle Hinweise für die Bewertung von Tendenzen, fördert die Transparenz gegenüber Interessenträgern und fließt in die Entscheidungen des EDSB über seine Aufsichts- und Durchsetzungstätigkeiten ein. Ihre Veröffentlichung findet zu einem Zeitpunkt statt, an dem der EDSB seine Aktivitäten für das Jahr 2016 festlegt.

Ganz allgemein belegen die Ergebnisse kontinuierliche Fortschritte bei der Anwendung der Datenschutzvorschriften in allen EU-Einrichtungen. Die Umfrage bestätigt also einen generell positiven Trend in den höchst heterogenen EU-Einrichtungen, in denen Umfang und Komplexität der Verarbeitungsvorgänge sehr verschieden ausfallen.

Die etablierten und älteren Einrichtungen müssen ihr Hauptaugenmerk nun auf die Wahrung des Erreichten richten, also auf die Pflege korrekter Bestandsverzeichnisse und die Beibehaltung ihrer Meldungsquoten an ihre Datenschutzbeauftragten und den EDSB.

Weniger gut etablierte Einrichtungen haben Boden gutgemacht; mehrere Agenturen haben bei den Meldungen perfekte Werte erreicht. Dort, wo weniger Fortschritte zu beobachten sind, insbesondere bei Meldungen an den EDSB, werden wir mit unserer Unterstützung dafür sorgen, dass der Datenschutz ganz selbstverständlich berücksichtigt wird.

III. Hauptbericht

1. Einleitung

In ihrer Eigenschaft als öffentliche Verwaltungen verarbeiten Einrichtungen der EU personenbezogene Daten sowohl bei ihren Kerntätigkeiten als auch in Wahrnehmung ihrer administrativen Aufgaben.

Es fällt in die Verantwortung der Einrichtungen der EU, bei der Verarbeitung personenbezogener Daten die Grundrechte und Grundfreiheiten natürlicher Personen zu schützen und mit angemessenen und wirksamen Maßnahmen zu gewährleisten, dass den in der Verordnung (EG) Nr. 45/2001 („Verordnung“) festgeschriebenen Grundsätzen und Verpflichtungen nachgekommen wird, und dies auch belegen zu können.

Der Europäische Datenschutzbeauftragten (EDSB) hat die Pflicht und die Aufgabe, zu überwachen und zu gewährleisten, dass die Rechte natürlicher Personen im Einklang mit der Verordnung[6] gewahrt werden.

In seinem Strategiepapier vom Dezember 2010[7] kündigte der EDSB an, dass er *„diese regelmäßigen Umfragen auch künftig fortführen wird, 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“*.

Ende April 2015 begann der EDSB mit seiner fünften Bestandsaufnahme. Diese stellt die Fortführung der seit 2007 alle zwei Jahre vorgenommenen Bestandsaufnahmen dar und ermöglicht somit ein Aufzeigen der Einhaltungstrends im Zeitverlauf.

Die Umfrage deckte ein weites Feld ab, nämlich alle relevanten 61 Einrichtungen der EU, und konzentrierte sich auf Aspekte, die zweckdienliche Hinweise auf die von ihnen erzielten Fortschritte bei der Anwendung der Verordnung geben. Abgesehen von den üblichen Fragen zum Stand des Bestandsverzeichnisses und des Registers umfasste diese Ausgabe der Umfrage zusätzlich Fragen zu Übermittlungen gemäß Artikel 9 der Verordnung, zur Informationssicherheit, zu Maßnahmen zur Gewährleistung der tatsächlichen Löschung personenbezogener Daten nach Ablauf ihrer Aufbewahrungsfrist und zur Einbeziehung des DSB in die Konzeption neuer Verarbeitungsvorgänge.

Der vorliegende Bericht stützt sich auf die Antworten, die von 61 EU-Einrichtungen (einschließlich bestimmter Einrichtungen des früheren zweiten und dritten Pfeilers) auf Schreiben des EDSB mit gezielten Fragen eingingen. Der EDSB erhielt mit Ausnahme von SESAR JU Antworten von allen betroffenen EU-Einrichtungen. Auf dieses Thema geht der EDSB noch separat ein.

Der EDSB wird die Ergebnisse aus dieser Umfrage bei der Planung künftiger Aufsichts- und Durchsetzungsaktionsprogramme berücksichtigen. Diese Programme werden eine Kombination von Leitlinien für EU-Einrichtungen, Durchsetzungsmaßnahmen und weiteren Maßnahmen zur Förderung der Rechenschaftspflicht sein.

Der Bericht ist wie folgt gegliedert: Abschnitt 2 enthält eine vergleichende Analyse der auf unsere Schreiben hin eingegangenen Antworten auf die einzelnen Fragen, wobei jeweils kurz erläutert wird, warum diese Frage relevant war; in Abschnitt 3 werden die Inspektionsbesuche behandelt, die als Folge der Umfrage 2011 begonnen wurden; wo dies

[6] Nach Maßgabe von Artikel 41 Absatz 2 der Verordnung.
[7] Siehe das Strategiepapier des EDSB vom 13. Dezember 2010 „Überwachung und Gewährleistung der Einhaltung der Verordnung (EG) Nr. 45/2001“, S. 8.

möglich ist, werden die vor und nach den Besuchen erreichten Ergebnisse bei der Einhaltung verglichen, um ihre Wirkung zu untersuchen; Abschnitt 5 schließlich enthält Schlussfolgerungen und die Zusammenfassung.

2. Ergebnisse der Umfrage im Vergleich

2.1. Bestandsverzeichnis und Register der Verarbeitungsvorgänge. Stand der Meldungen an den EDSB

*Gemäß Artikel 25 der Verordnung sind dem DSB alle Verarbeitungen personenbezogener Daten zu melden. Gemäß Artikel 26 der Verordnung sind diese in einem **Register** zu erfassen, dessen Mindestinhalt in diesem Artikel festgelegt ist. Verarbeitungen, die gemäß Artikel 27 der Verordnung besondere „Risiken" beinhalten können, müssen dem EDSB ebenfalls vorab gemeldet werden. Auch ein **„Bestandsverzeichnis"** geplanter oder bereits erfolgender, aber noch nicht dem DSB gemeldeter Verarbeitungen stellt für die Einrichtungen ein Planungsinstrument von unschätzbarem Wert dar. Der EDSB empfiehlt, in einem solchen Bestandsverzeichnis zumindest folgende Felder vorzusehen: Bezeichnung der Verarbeitung, Kurzbeschreibung der Verarbeitung (einschließlich Zweckbestimmungen), Meldung gemäß Artikel 25 (erfolgt oder nicht), Meldung gemäß Artikel 27 (erforderlich oder nicht, erfolgt oder nicht), sowie Kontaktperson („in der Praxis" für die Verarbeitung Verantwortlicher).*

Anders als bisher forderte der EDSB keine Kopien des tatsächlichen Bestandsverzeichnisses oder Registers an, sondern nur die relevante *Anzahl* von Verarbeitungsvorgängen, die 1) im Bestandsverzeichnis aufgeführt sind, 2) dem DSB gemeldet und in das Register eingetragen wurden, 3) als unter Artikel 27 fallend identifiziert wurden und 4) bereits gemäß Artikel 27 dem EDSB gemeldet wurden. Wo derartige Angaben noch feiner untergliedert (beispielsweise nach Generaldirektionen) verfügbar waren, wurden die Einrichtungen aufgefordert, diese Zahlen ebenfalls vorzulegen.

Eine **große Mehrheit** der EU-Einrichtungen führt – wie vom EDSB empfohlen – **sowohl ein Bestandsverzeichnis als auch ein Register**. Die EU-Einrichtungen, die kein separates Bestandsverzeichnis führen, fügen dem Register zuweilen einen Abschnitt über zukünftige Verarbeitungsvorgänge hinzu und fassen somit die beiden Dokumente zu einem zusammen (z. B. das EP).

Im Vergleich zur letzten, im Jahr 2013 durchgeführten Umfrage sind die **Meldungsquoten generell gestiegen**. Die nachstehende Tabelle gibt einen Überblick über die Meldungsquoten in der derzeitigen Umfrage sowie über die Änderungen im Vergleich zur Umfrage 2013. Die Spalte „Artikel 25" bezieht sich auf alle Verarbeitungsvorgänge. Dies umfasst auch diejenigen, die dem EDSB gemäß Artikel 27 der Verordnung zusätzlich zu melden sind. Die Spalte „Artikel 27" enthält weitere Angaben zu diesen Verarbeitungsvorgängen.

In einigen Fällen sind die Quoten gesunken. Dies betrifft in der Regel EU-Einrichtungen mit einer hohen Einhaltungsquote in Fällen, in denen Aktualisierungen des Bestandsverzeichnisses dazu geführt haben, dass die DSB auf weitere Verarbeitungsvorgänge aufmerksam wurden. Dies kann zu Schwankungen im Bereich zwischen 90 % und 100 % führen und ist kein Anlass zu Besorgnis. In Anbetracht der Tatsache, dass laufend neue Verarbeitungen entwickelt werden, ist es, besonders für große Einrichtungen, schwierig, für Artikel 25 eine Meldungsquote von 100 % zu erreichen. Für Meldungen gemäß Artikel 27 können sogar ein oder zwei neue, noch nicht gemeldete Verarbeitungsvorgänge zu einem scheinbar merklichen Rückgang bei den Meldungsquoten führen. Der Grund hierfür ist, dass die Zahl derartiger Verarbeitungen je Einrichtung tendenziell recht gering ist[8].

[8] Die durchschnittliche Zahl von Verarbeitungen, die unter Artikel 27 fallen, liegt bei 20; ausgenommen hiervon ist die Kommission, wo sie sich auf mehr als 200 beläuft.

Anhand dieser Richtwerte sollen die Leistungen von EU-Einrichtungen mit denen der anderen Mitglieder ihrer Gruppe verglichen werden. Es wäre allerdings nicht fair, ein seit langem bestehendes Organ wie den Rat oder die Kommission mit einer vor kurzem eingerichteten Agentur zu vergleichen, die noch in Wachstum und Aufbau begriffen ist. Aus diesen Gründen werden Einrichtungen mit anderen verglichen, die im Hinblick auf ihre Datenschutzfunktionen einen ähnlichen Entwicklungsstand erreicht haben; dabei entstanden vier Gruppen (A bis D)[9].

Organ/Einrichtung	**% Meldungen nach Artikel 25**	**% Meldungen nach Artikel 27**	**Quote Artikel 25 im Vergleich zur Umfrage 2013**	**Quote Artikel 27 im Vergleich zur Umfrage 2013**
ERH	100%	90%	+/- 0	- 10
EK	97%	91%	+ 1	- 9
Rat	98%	100%	+ 4	+/- 0
EZB	100%	83%	+/- 0	+/- 0
EuGH	95%	97%	- 2	+4
AdR	100%	100%	+ 2	+/- 0
EWSA	93%	100%	- 6	+ 5
EIB	92%	84%	- 8	-13
EP	91%	92%	- 2	-8
OLAF	94%	100%	- 6	+/- 0
BÜRGERBEAUFTRAGTER	81%	100%	- 19	+/- 0
CDT	72%	93%	- 3	+ 1
Gruppendurchschnitt	**96%**	**93%**	**-3**	**-3**

Tabelle 1: Meldungsquoten für Einrichtungen in Gruppe A

Einrichtungen in Gruppe A weisen im Durchschnitt hohe Meldungsquoten auf, die sich meist um 90 % bewegen. Wie bereits ausgeführt, schränkt ein so hoher Ausgangswert den Raum für Verbesserungen ein, und einige Einrichtungen haben geringere Werte als in der Umfrage 2013 angegeben. Sind solche Schwankungen auf hohem Niveau zu beobachten, ist dies nicht unbedingt Anlass zur Sorge. Sie machen jedoch deutlich, dass das Register ein lebendiges Dokument ist - neue Verarbeitungsvorgänge werden hinzugefügt, ältere mitunter gelöscht, bestehende auf den neuesten Stand gebracht. Und so war auch in mehreren Antworten von Überarbeitungen des Registers die Rede, die häufig aktualisierte Meldungen zur Folge hatten. Das bedeutet, dass die Arbeit nicht beendet ist, wenn ein Register erst einmal aufgebaut worden ist.

Dessen ungeachtet fallen einige der Rückgänge jedoch besonders ins Auge. Der Rückgang bei der Quote der Meldungen gemäß Artikel 27 bei der EIB ist auf die Ermittlung neuer Verarbeitungen zurückzuführen, die einer Vorabkontrolle zu unterziehen sind.

Auch der Bürgerbeauftragte hat weitere meldepflichtige Verarbeitungsvorgänge ermittelt, weshalb es vorübergehend zu einer niedrigeren Quote von Meldungen gemäß Artikel 25 kam.

[9] Siehe Anhang 3 mit Erläuterungen zur Bildung der einzelnen Gruppen.

Organ/Einrichtung	% Meldungen nach Artikel 25	% Meldungen nach Artikel 27	Quote Artikel 25 im Vergleich zur Umfrage 2013	Quote Artikel 27 im Vergleich zur Umfrage 2013
CEDEFOP	98%	100%	+ 8	+ 7
CPVO	87%	86%	- 4	- 4
EASME	100%	100%	+ 10	+ 10
EASA	94%	100%	+ 13	+ 35
EDSB	94%	100%	- 4	+/- 0
EUA	86%	100%	- 9	+/- 0
EFSA	94%	100%	+ 16	+ 16
EIF[10]	34%	47%	-	-
EMCDDA	74%	93%	- 2	+/- 0
EMA	96%	91%	- 4	- 3
EMSA	100%	92%	+ 3	+ 7
ECSEL[11]	15%[12]	100%	-	-
ENISA	92%	100%	+ 3	+/- 0
ETF	100%	100%	+/- 0	+/- 0
EUROFOUND	100%	100%	+ 8	+/- 0
FRA	100%	100%	+ 4	+/- 0
HABM	94%	97%	+ 4	+ 7
OSHA	97%	100%	+ 1	+/- 0
Gruppendurchschnitt	**90%**	**94%**	**+3**	**+5**

Tabelle 2: Meldungsquoten für Einrichtungen in Gruppe B

Einrichtungen der Gruppe B weisen weitgehend eine solide Leistung auf; FRA, Eurofound, EASME und ETF melden sogar hervorragende Ergebnisse. CEDEFOP und OSHA haben die Bestpunktzahl um ein oder zwei Meldungen verfehlt.

Ein besonderes Lob verdient die EASA, die früher in ihrer Gruppe eher am unteren Ende zu finden war. Ihre schlechte Leistung in der Umfrage 2011 hatte einen Inspektionsbesuch im Frühjahr 2012 zur Folge, woraufhin bei der Umfrage 2013 eine deutliche Verbesserung beobachtet werden konnte. Im Bericht über diese Umfrage hieß es, die EASA sei zwar schon weit gekommen, doch bleibe noch Einiges zu tun. Die EASA hat sich angestrengt und gehört jetzt zu den Leistungsfähigen.

Die EUA hat mehrere neue Verarbeitungen ermittelt und wurde außerdem einer Umorganisation unterzogen, weshalb einige Aktualisierungen erforderlich wurden; diese Entwicklungen haben zu einem vorübergehenden Rückgang geführt.

Manche Zahlen lassen sich mit denen der letzten Umfrage nicht einfach vergleichen.

Der EIF wird bei vielen administrativen Verarbeitungen teilweise von der EIB unterstützt. Die Umfrage 2013 erbrachte unter anderem, dass nur wenige der unabhängigen Verarbeitungen des EIF gemeldet worden waren, und dass die überwiegende Zahl der im

[10] EIF-Zahlen können nicht sinnvoll mit der Umfrage 2013 verglichen werden; siehe weiter unten.
[11] ECSEL ist die Nachfolgeeinrichtung von ARTEMIS und ENIAC, die zusammengelegt wurden, weshalb sich die Zahlen nicht einfach mit denen der letzten Umfrage vergleichen lassen.
[12] Siehe weiter unten die Erläuterung auf S. 8.

Register eingetragenen Verarbeitungen eigentlich Meldungen der „EIB-Gruppe“ waren, bei denen sich der EIF auf die EIB stützte. Seitdem hat der EIF mit einer Überprüfung seines Bestandsverzeichnisses und seines Registers begonnen und ist dabei auf eine erhebliche Zahl weiterer Verarbeitungen gestoßen (64 Verarbeitungen im Bestandsverzeichnis aufgeführt, im Vergleich zu 23 EIF-spezifischen Verarbeitungen plus 16 Verarbeitungen der EIB-Gruppe zuvor). Die Zahlen geben den Stand wieder, wie er in der Antwort des EIF auf die Umfrage dargestellt wurde; nach dem Stichtag hat der EIF noch große Fortschritte erzielt (siehe auch weiter unten Abschnitt 3.3). ECSEL ist die Nachfolgeeinrichtung von ARTEMIS und ENIAC, die zusammengelegt wurden, weshalb sich die Zahlen nicht einfach mit denen der letzten Umfrage vergleichen lassen. Zwar hat ECSEL einige Verfahren und Verarbeitungsvorgänge von den Vorgängerorganisationen „geerbt“ (wie die vorabkontrollpflichtigen Verarbeitungen), doch läuft derzeit eine umfassende Überprüfung von Bestandsverzeichnis und Register; nach der Planung von ECSEL hätten alle aktualisierten Meldungen bis Ende September an den DSB gesandt worden sein müssen.

Die Quote der EMCDDA bei den Meldungen gemäß Artikel 25 gehört zu den niedrigsten in dieser Gruppe. Anders als bei einigen anderen Agenturen scheint dies wirklich Ausdruck mangelnder Fortschritte zu sein, da die Zahl der Meldungen stagnierte. Die EMCDDA sollte sich bemühen, diese Lücke zu schließen.

Organ/Einrichtung	**% Meldungen nach Artikel 25**	**% Meldungen nach Artikel 27**	**Quote Artikel 25 im Vergleich zur Umfrage 2013**	**Quote Artikel 27 im Vergleich zur Umfrage 2013**
EACEA	98%	96%	+/- 0	+ 1
CHAFEA	82%	100%	+ 30	+/- 0
ECDC	100%	100%	+ 4	+/- 0
EFCA	96%	100%	+ 17	+/- 0
ERA	92%	93%	+ 6	+ 4
FRONTEX[13]	88%	90%	-	-
GSA[14]	52%	54%	-	-
INEA	91%	100%	+ 22	+ 37
Cleansky 2	100%	100%	+ 7	+/- 0
ECHA	100%	100%	+/- 0	+/- 0
ERCEA	90%	100%	- 8	+ 5
F4E	64%	73%	- 2	- 10
FCH JU	100%	100%	+/- 0	+ 33
IMI	75%	100%	- 25	+/- 0
REA	89%	93%	- 7	+ 11
SESAR	-	-	-	-
Gruppendurchschnitt	**88%**	**93%**	**+3**	**+6**

Tabelle 3: Meldungsquoten für Einrichtungen in Gruppe C

[13] Frontex legte im Rahmen der Umfrage 2013 nur eine Kopie seines Registers, nicht jedoch das Bestandsverzeichnis vor, weshalb kein aussagekräftiger Vergleich angestellt werden kann.

[14] Die GSA antwortete nicht rechtzeitig auf die Umfrage 2013; somit konnte kein aussagekräftiger Vergleich angestellt werden.

Die Gruppe C steht nicht länger hinter der Gruppe B zurück, was beweist, dass der Aufbau von Bestandsverzeichnis und Register zwar mühsam, aber möglich ist. ECHA, FCH-JU, Cleansky und ECDC meldeten perfekte Werte; EACEA und EFCA kamen diesen sehr nahe.

Frontex gab in der Vergangenheit Anlass zur Sorge, weshalb der EDSB Ende 2012 dort einen Inspektionsbesuch abstattete. Auf die Umfrage 2013 hatte der Besuch offensichtlich noch keine großen Auswirkungen. In diesem Jahr hingegen konnte Frontex mit einer beachtlichen Leistung aufwarten. Die Zusammenarbeit mit Frontex hat sich erheblich verbessert; deutlich wurde dies an der Kooperation während eines Inspektionsbesuchs im Jahr 2014 und an einer Umstellung bei den Aktivitäten von Frontex auf mehr Verarbeitungen personenbezogener Daten für operative Zwecke.

Bei der Meldungsquote von F4E gab es einen leichten Rückgang. Hinter den Prozentsätzen verbirgt sich jedoch die Tatsache, dass die absoluten Zahlen im Bestandsverzeichnis und im Register deutlich gestiegen sind - bei Artikel 25 von 21 von 32 erledigten auf 38 von 59 erledigten; bei Artikel 27 von 15 von 18 auf 22 von 30. Die Zahlen sind daher nicht Anzeichen einer Stagnation, sondern eines steilen Anstiegs.

Am Stichtag war die GSA noch immer schlechter gestellt als die anderen Mitglieder ihrer Gruppe (siehe auch weiter unten Abschnitt 3.4), und SESAR gab keine inhaltlichen Antworten auf die Umfrage (siehe weiter unten Abschnitt 2.6).

Organ/Einrichtung	% Meldungen nach Artikel 25	% Meldungen nach Artikel 27	Quote Artikel 25 im Vergleich zur Umfrage 2013	Quote Artikel 27 im Vergleich zur Umfrage 2013
ACER	34%	36%	+ 6	+ 5
GEREK[15]	36%	31%	+ 23	- 2
CEPOL	24%	56%	+ 21	+ 13
EASO	54%	62%	+ 35	+ 37
EBA	100%	29%	+ 86	- 38
EDA	100%	100%	-	-
EAD	80%	47%	+ 48	- 20
EIGE	50%	86%	- 13	+/-0
EIOPA	13%	44%	+/-0	- 14
EIT	28%	38%	+ 13	- 32
ESMA	32%	29%	- 3	- 32
ESRB[16]	siehe EZB	siehe EZB	-	-
EUISS	25%	17%	+ 25	+ 17
eu-LISA	81%	11%	+ 81	+ 11
EUSC	52%	100%	+ 52	+ 100
Gruppendurchschnitt	**53%**	**47%**	**+29**	**+3**

Tabelle 4: Meldungsquoten für Einrichtungen in Gruppe D

Der Gruppe D gehören die zuletzt gegründeten Agenturen und Einrichtungen an; daher sind ihre Meldungsquoten häufig niedriger. Da diese Agenturen häufig noch mit dem Aufbau ihrer Geschäftsprozesse beschäftigt sind, sind tendenziell auch ihre Bestandsverzeichnisse weniger fundiert.

Ein Beispiel hierfür ist die ACER: Zwar stieg die Quote ihrer Meldungen gemäß Artikel 25 nur leicht an, doch verbirgt sich dahinter, dass sich die Zahl der Meldungen im Register fast verdreifacht hat; dieser Aufschwung wurde durch einen ähnlichen Anstieg der Zahl der im Bestandsverzeichnis aufgeführten Verarbeitungen ausgeglichen[17].

Ganz ähnlich ist auch beim EAD der Anstieg der Artikel 25-Meldungen tatsächlich größer, als es die Prozentsätze bei den Meldungen vermuten lassen. 2013 hatte er noch 65 Verarbeitungen in seinem Bestandsverzeichnis aufgeführt; 2015 war diese Zahl auf 118 gestiegen, folgerichtig stieg auch die Meldungsquote an. Der Rückgang bei Artikel 27 ist das Ergebnis eines ähnlichen Wettlaufs nach oben: 15 von 32 Verarbeitungen werden als gemeldet angegeben (2013 waren es 10 von 15), was eine niedrigere Quote zur Folge hat, aber trotzdem einen Gewinn an Kontrolle über seine Verarbeitungen bedeutet.

Die EBA hat sich offensichtlich zunächst auf Artikel 25-Meldungen konzentriert und hier eine beeindruckende Verbesserung vorzuweisen, bedenkt man insbesondere das Wachstum

[15] Das GEREK meldete mehrere weitere Verarbeitungen gemäß Artikel 27, allerdings erst nach dem Stichtag für die Einreichung von Beiträgen zur Umfrage, weshalb sie für die Berechnung hier nicht berücksichtigt werden konnten.
[16] Die Verarbeitungen des ESRB sind in die Dokumentation der EZB integriert; der DSB der EZB ist gleichzeitig der DSB des ESRB.
[17] 2013 meldete die ACER 9 von 32 Artikel 25-Meldungen als erledigt, dieses Mal wurden 31 von 92 als erledigt gemeldet.

des Bestandsverzeichnisses von 35 auf 58 Einträge. Durch die Ermittlung neuer Verarbeitungen traten auch mehr Fälle gemäß Artikel 27 ans Tageslicht, weshalb die Quote bei den Artikel 27-Meldungen erheblich sank (von 4 von 6 auf 5 von 17). Der nächste Schritt wird für die EBA darin bestehen, diese Lücke zu schließen.

Das EASO ist eine Beispiel für eine Agentur, die die Leistung stetig verbessert und sich vom unterdurchschnittlichen Bereich in ihrer Gruppe auf eine Position leicht über dem Mittel des Feldes bewegt hat.

Das EIT weist einige Verbesserungen bei Artikel 25 auf, muss aber bei Artikel 27-Meldungen einen Rückgang hinnehmen, weil neue meldepflichtige Verarbeitungen ermittelt wurden.

eu-LISA, deren ständiger DSB erst im Frühjahr 2014 bestellt wurde, hat bei Artikel 25-Meldungen sehr große Fortschritte vermelden können, nachdem sie in der Umfrage 2013 bei Null gestartet war. Bei den Artikel 27-Meldungen liegt sie jedoch zurück und sollte sich bemühen, diese Lücke zu schließen.

Mehrere Agenturen in dieser Gruppe, die nach Auskunft in den bisherigen Umfragen nur langsam in Gang gekommen waren, haben unterdessen Unterstützung vom EDSB in Form von Besuchen oder abgeordneten Mitarbeitern erhalten, die der Einhaltung der Verordnung Schub verleihen sollten:

An das EUSC wurde im Herbst 2014 ein Mitarbeiter des EDSB abgeordnet, woraufhin es seinen Rückstand bei Artikel 27-Meldungen aufholen konnte; bei Artikel 25 bewegt es sich in die richtige Richtung.

EIGE wurde schon nach der Umfrage 2011 für einen Inspektionsbesuch vorgemerkt, der dann im Frühjahr 2013 erfolgte. Diese Maßnahme schlug sich bereits in der Umfrage 2013 nieder, bei der die Agentur ein für ihr Alter respektables Ergebnis erzielte. Der Schwung scheint jedoch inzwischen erlahmt zu sein, und EIGE sollte sich nicht auf seinen Lorbeeren ausruhen, sondern weiter an der Verbesserung ihrer Compliance arbeiten.

EIOPA befindet sich ähnlich wie ACER und EAD im Aufwind; die Zahl der Einträge im Bestandsverzeichnis hat sich von 2013 auf 2015 fast verdoppelt (70 statt 40). Die gesunkene Quote bei den Artikel 27-Meldungen ist darauf zurückzuführen, dass mehrere künftige Verarbeitungen im Bestandsverzeichnis bereits für eine Vorabkontrolle vorgemerkt sind.

Das EUISS bestellte seinen ersten DSB nach der Umfrage 2013. Im Herbst 2014 fand ein Beratungsbesuch auf Mitarbeiterebene statt. Es sind zwar Fortschritte zu verzeichnen, doch sollte das EUISS seine Compliance-Aktivitäten intensivieren. Hierfür ist vor allem erforderlich, dass die einzelnen Geschäftsbereiche ihre Artikel 25-Meldungen an den DSB weiterreichen, damit gegebenenfalls das Vorabkontrollverfahren eingeleitet werden kann.

Im Frühjahr 2013 fand ein Treffen zwischen dem Exekutivdirektor der ESMA und dem EDSB statt; im Sommer 2015 erfolgte dann ein Beratungsbesuch. Der bemerkenswerte Rückgang bei den Artikel 27-Meldungen ist auf die Ermittlung zahlreicher weiterer Verarbeitungen zurückzuführen, die darunter fallen.

2.2. Datenübermittlungen im Zeitraum 2013-2014 an Empfänger, die keinen einzelstaatlichen Vorschriften zur Umsetzung der Richtlinie 95/46/EG unterliegen

Klingt bekannt? Bereits **2013** (Umfrage 2013)[18] hat der EDSB EU-Einrichtungen um Informationen über Übermittlungen personenbezogener Daten an Empfänger gebeten, die keinen einzelstaatlichen Rechtsvorschriften zur Umsetzung der Richtlinie 95/46/EG unterworfen sind. Der EDSB bat seinerzeit ganz offen um Informationen zu solchen Übermittlungen, um sich einen allgemeinen Überblick zu verschaffen und auch im Hinblick auf das Abfassen von Leitlinien.

Im Jahr 2013 gaben von insgesamt 62 Organen und Einrichtungen der EU 35 an, sie würden derartige Übermittlungen überhaupt nicht vornehmen; 17 weitere gaben an, es gebe keine strukturellen Übermittlungen, jedoch könne es in konkreten Einzelfällen zu solchen Übermittlungen kommen. Vor diesem Hintergrund kam der EDSB zu dem Schluss (Umfrage 2013, S. 21): **„Übermittlungen gemäß Artikel 9 als Teil der Kerntätigkeiten von EU-Einrichtungen sind selten“**.

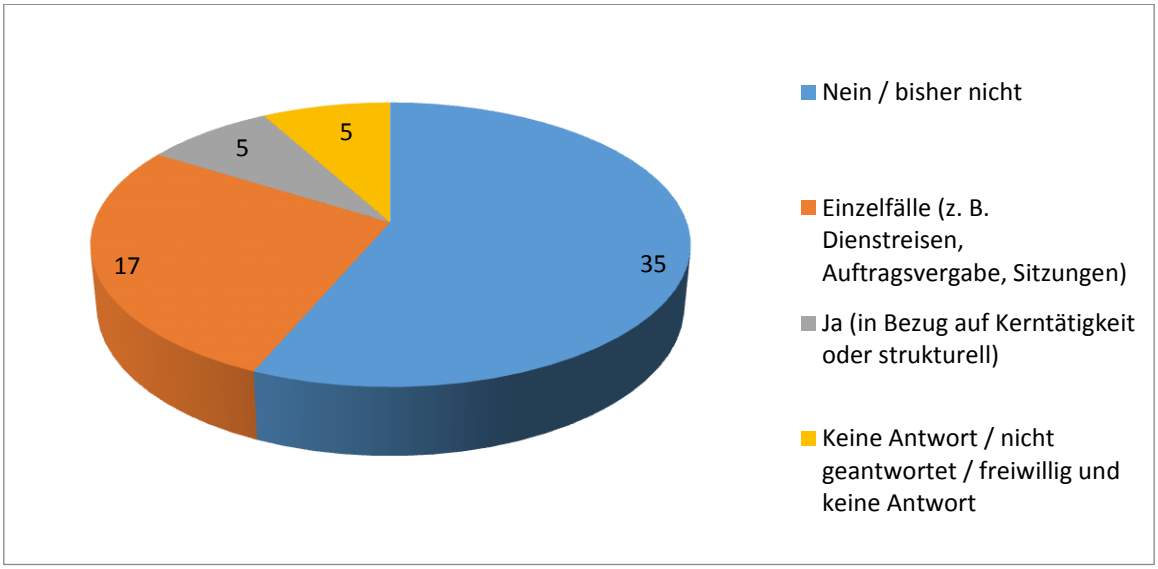

Abbildung 1 Überblick über Übermittlungen gemäß Artikel 9 (Umfrage 2013)

Was hat sich also geändert? Im Juli 2014 **veröffentlichte der EDSB ein Positionspapier** zur „Übermittlung personenbezogener Daten an Drittländer und internationale Organisationen durch Organe und Einrichtungen der EU“[19] Vor diesem Hintergrund fragte der EDSB im Rahmen **dieser Umfrage** nach Übermittlungen personenbezogener Daten gemäß Artikel 9 in den Jahren 2013 und/oder 2014. Die Frage bejahten nur 18 von insgesamt 61 Einrichtungen. Übermittlungen gemäß Artikel 9 als Teil der Kerntätigkeiten von EU-Einrichtungen sind also nach wie vor selten[20]. Weil diese Übermittlungen jedoch mit **erhöhten Risiken** einhergehen, fragten wir in dieser Umfrage nach **näheren Einzelheiten**.

[18] Siehe https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Inquiries/2014/14-01-24_survey_report_DE.pdf.

[19] https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Papers/14-07-14_transfer_third_countries_DE.pdf

[20] Der vergleichsweise Rückgang gegenüber den Zahlen aus der Umfrage 2013 lässt sich durch die Begrenzung auf einen bestimmten Zeitraum erklären (so gab z. B. der EuGH an, dass bei bestimmten Verarbeitungsvorgängen solche Übermittlungen grundsätzlich vorgesehen sind, dass aber 2013 und 2014 keine solche Übermittlung stattgefunden hatte).

Verschiedene Arten von Übermittlungen gemäß Artikel 9: Hatten in diesem Zeitraum Übermittlungen stattgefunden, sollten die EU-Einrichtungen getrennt Übermittlungen angeben, die gemäß Artikel 9 Absatz 2 (Angemessenheitsbeurteilung), Artikel 9 Absatz 6 oder Artikel 9 Absatz 7 (Ausnahmen) oder gemäß Artikel 9 an Empfänger vorgenommen worden waren, die ihren Sitz in EWR-Ländern haben, deren Tätigkeit aber von der Anwendung der Richtlinie 95/46/EG ausgenommen ist (z. B. an Justizbehörden).

Artikel 9 der Verordnung *regelt im Wesentlichen Übermittlungen in Drittländer und an internationale Organisationen. Da Übermittlungen an Dritte zwangsweise einen gewissen Verlust der Kontrolle über personenbezogene Daten mit sich bringen, ist es wichtig, dass die Empfänger angemessen strengen Datenschutzvorschriften unterliegen. Für Übermittlungen innerhalb von oder zwischen EU-Einrichtungen und auch für Übermittlungen an die meisten Empfänger in der EU stellt dies kein Problem dar. Bei Übermittlungen an andere Dritte kann dies zu einem Problem werden, da deren Datenschutzstandards häufig schwächer als der EU-Standard sind. Aus diesem Grund ist Artikel 9, der derartige Übermittlungen regelt, restriktiver als die Vorschriften für Übermittlungen innerhalb der EU. Dies spiegelt das* ***erhöhte Risiko wider, das mit solchen Übermittlungen verbunden*** *ist.*

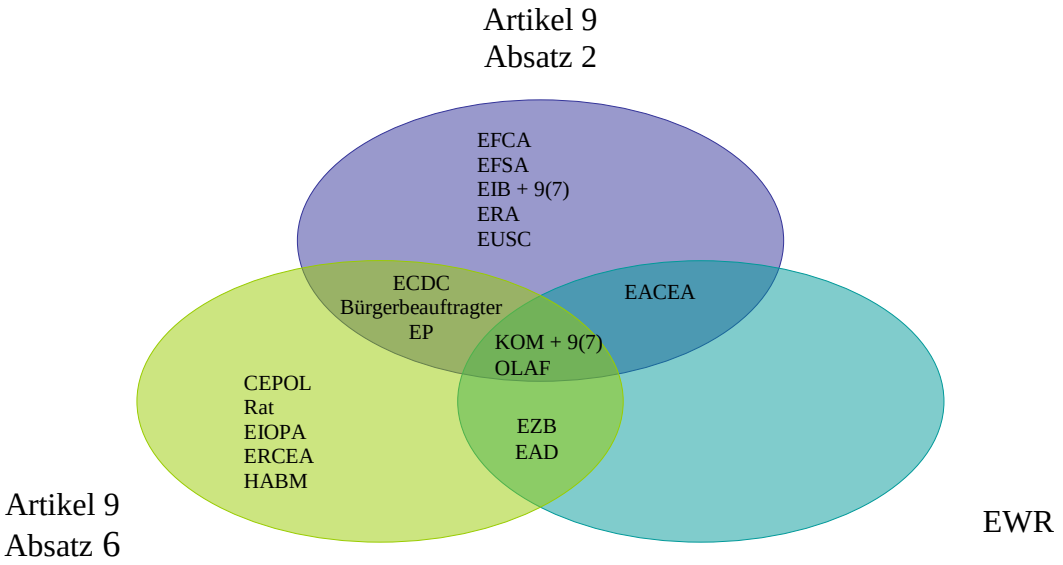

Abbildung 2: Überblick über Übermittlungen gemäß Artikel 9 (Umfrage 2015)

Andere Einrichtungen wiesen darauf hin, dass sie bestimmte Übermittlungen gemäß Artikel 9 nicht *als von ihnen veranlasst* betrachten (z. B. der EDSB für diejenigen, die von Drittanbietern für deren eigene Zwecke vorgenommen werden, oder CEDEFOP-Mitarbeiter für die Bereitstellung ihrer eigenen personenbezogenen Daten an Veranstalter von Sitzungen / Konferenzen / Veranstaltungen in Drittländern).

Von den 18 Einrichtungen[21], die für diesen Zeitraum Übermittlungen gemäß Artikel 9 angaben, unterstrichen drei (EFSA, EuGH und Bürgerbeauftragter) ausdrücklich die **Nutzung sozialer Medien**: Twitter[22], YouTube, LinkedIn und Flickr-Seiten (EFSA) sowie Google+ (Bürgerbeauftragter).

- Nähere Angaben zu Übermittlungen gemäß Artikel 9 wurden in einer Tabelle abgefragt, und zwar zu der Verarbeitungstätigkeit (wie in der Artikel 25-Meldung erwähnt), dem Empfänger, der Grundlage (z. B. Angemessenheitsbeurteilung durch den für die Verarbeitung Verantwortlichen), dem Bereich (z. B. Strafverfolgung), dem „Wie" der Übermittlung (z. B. Übermittlung der Daten per Post, per E-Mail, durch Zugriff auf eine Datenbank usw.), den Kategorien personenbezogener Daten sowie der Häufigkeit solcher Übermittlungen.
- Darüber hinaus wollte der EDSB etwas über etwaige besondere Schwierigkeiten im Zusammenhang mit den oben genannten Tätigkeiten und nach Möglichkeit zu deren Ursachen erfahren.
- Schließlich wollte der EDSB wissen, ob ein internes System zur Überwachung und Registrierung von Übermittlungen gemäß Artikel 9 besteht.

Zu **Übermittlungen gemäß Artikel 9 Absatz 2** gaben 11 Einrichtungen[23] für den Zeitraum 2013 und/oder 2014 Übermittlungen sehr unterschiedlicher Kategorien personenbezogener Daten in einer Vielzahl von Bereichen und mit unterschiedlicher Häufigkeit an (diese Angaben dürften keine weiteren Schlussfolgerungen über den einzelnen Verarbeitungsvorgang hinaus zulassen). So nannte beispielsweise die EACEA solche Übermittlungen zum Zweck der Vergabe und Durchführung von Zuschüssen im Bereich Bildung, die EFCA im Zusammenhang mit der Übermittlung von Inspektionsberichten über Fischereifahrzeuge, die EIB zur versicherungsmathematischen Berechnung von Ruhegehaltsansprüchen der Mitarbeiter (ähnlich für die Verwaltung von Ruhegehältern: EUSC).

Zu den Empfängern gehören internationale Organisationen (z. B. OECD für die EIB, WHO, FAO und OECD für die EFSA), aber auch regionale und nationale Behörden und benannte Kontaktstellen (z. B. GD EAC und EACEA für Programme der allgemeinen/beruflichen Bildung, Verkehrsbehörden für die ERA oder Zollbehörden für die GD TAXUD).

In der Mehrheit der Fälle ist die Grundlage für eine solche Übermittlung eine Angemessenheitsbeurteilung durch den für die Verarbeitung Verantwortlichen (z. B. GD AGRI für die Überwachung von Informationen über den Bio-Landbau). Andere Möglichkeiten sind z. B. eine Angemessenheitsentscheidung der Europäischen Kommission (z. B. GD RTD für Vorschlagsbewertung und Zuschussverwaltung) oder das Safe Harbor-Abkommen zwischen der EU und den Vereinigten Staaten.

[21] Die Kommission hatte ihre Angaben weiter untergliedert: 14 von 41 Generaldirektionen hatten in diesen Zeitraum Übermittlungen gemäß Artikel 9 vorgenommen. Die EMSA führte aus: „Wenn die EMSA überhaupt Daten an Akteure außerhalb der EU übermitteln würde, was in der Regel über ein Reisebüro geschähe, handelte es sich dabei nur um Daten, die für die Buchung von Reisedienstleistungen (Transport und Hotel) für Dienstreisen von EMSA-Mitarbeitern erforderlich wären. In der Realität ist eine Anwendung von Artikel 9 jedoch nicht gerechtfertigt".

[22] Siehe https://secure.edps.europa.eu/EDPSWEB/edps/cache/off/EDPS/Legal_notice/Twitter_policy zur Twitter-Strategie des EDSB. Weitere Hilfestellung sollte mit der Veröffentlichung der Leitlinien des EDSB für elektronische Kommunikation verfügbar sein.

[23] Die Kommission vermeldete, dass sieben von 41 Generaldirektionen in diesen Zeitraum Übermittlungen gemäß Artikel 9 Absatz 2 vorgenommen hatten.

12 Einrichtungen[24] gaben für 2013 und/oder 2014 **Übermittlungen gemäß Artikel 9 Absatz 6** an; auch hier ging es um äußerst verschiedene Kategorien personenbezogener Daten in einer Vielzahl von Bereichen.

Zu den Hauptempfängern gehören Reisebüros (CEPOL, EZB, EIOPA[25]); Visa-Agenturen/Konsulate (EZB, EIOPA); verschiedene regionale und internationale Organisationen (z. B. im Bereich der Fischereibewirtschaftung für GD MARE oder WHO für GD SANTE und ECDC) und Zollbehörden für GD TAXUD.

In ihren Antworten zur Rechtsgrundlage erwähnten die Einrichtungen fast alle in Artikel 9 Absatz 6 aufgeführten Möglichkeiten:

- Artikel 9 Absatz 6 Buchstabe a wird von der GD ESTAT für die Registrierung von Teilnehmern an einem Video-Wettbewerb und von der GD TAXUD für den Zugang zu einem Team-Arbeitsbereich im Zusammenhang mit der Teilnahme an den Fiscalis- und Zoll-Programmen genannt;
- Artikel 9 Absatz 6 Buchstabe c wird für die Verwaltung lokaler Mitarbeiter in EU-Delegationen und für Übermittlungen an Sozialversicherungs- und Steuerverwaltungen durch den EAD zitiert;
- Artikel 9 Absatz 6 Buchstabe d dient der GD MARE als Grundlage bei der Meldung von Fischereifahrzeugen und der GD JUST für ihr Schnellwarnsystem für gefährliche Non-Food-Erzeugnisse;
- Artikel 9 Absatz 6 Buchstaben d und e werden vom Rat für Dienstreisen in Drittländer und von der GD SANTE für ihr Frühwarn- und Reaktionssystem herangezogen.

Übermittlungen gemäß Artikel 9 Absatz 7 erfolgen an Bestimmungsorte, die kein angemessenes Schutzniveau gewährleisten, für die aber der für die Verarbeitung Verantwortliche ausreichende Garantien bietet[26]. Derartige Übermittlungen kommen nur selten vor: lediglich zwei GD der Kommission (GD SANTE und GD TAXUD) und die EIB haben solche Übermittlungen identifiziert (auch wenn für die EIB noch keine tatsächlich stattgefunden hat).

Lediglich vier Einrichtungen (EACEA, EZB, EAD und OLAF) gaben an, Übermittlungen personenbezogener Daten gemäß Artikel 9 an Empfänger vorgenommen zu haben, die ihren Sitz in **EWR-Ländern** haben, aber Tätigkeiten nachgehen, die von der Anwendung der Richtlinie 95/46/EG ausgenommen sind (z. B. an Polizei- oder Justizbehörden[27]).

***

[24] Die Kommission vermeldete, dass neun von 41 Generaldirektionen in diesen Zeitraum Übermittlungen gemäß Artikel 9 Absatz 6 vorgenommen hatten.

[25] Die EMSA führte aus: „Wenn die EMSA überhaupt Daten an Akteure außerhalb der EU übermitteln würde, was in der Regel über ein Reisebüro geschähe, handelte es sich dabei nur um Daten, die für die Buchung von Reisedienstleistungen (Transport und Hotel) für Dienstreisen von EMSA-Mitarbeitern erforderlich wären. In der Realität ist eine Anwendung von Artikel 9 jedoch nicht gerechtfertigt".

[26] Siehe Positionspapier, S. 14, Abschnitt 6. Siehe Positionspapier, S. 21f., Abschnitt 6.3 zu der Pflicht zur Einbeziehung des DSB in den Analyseprozess vor der Annahme angemessener Maßnahmen sowie zu den drei Szenarien für eine Ex ante-Einbeziehung des EDSB.

[27] Siehe Positionspapier, S. 22f., Abschnitt 7. Dort heißt es: „Diese Ausschlüsse waren vor der Annahme des Vertrags von Lissabon erforderlich, stehen jedoch jetzt grundsätzlich nicht mit dessen Artikel 16 sowie mit Artikel 8 der Charta der Grundrechte der Europäischen Union im Einklang".

Gar keine Probleme? In Anbetracht der gemeldeten Häufigkeit und mitunter Komplexität der oben geschilderten Aktivitäten überrascht es, dass nur die EIB angab, **auf Schwierigkeiten gestoßen** zu sein, und in dem Zusammenhang festhielt, es sei schwierig, die **Angemessenheit von Drittländern** festzustellen. Der EDSB hat in seinem Positionspapier (S. 13, Abschnitt 5.2) Folgendes eingeräumt: „In der Praxis wird es jedoch für den für die Verarbeitung Verantwortlichen nicht immer möglich sein, bezüglich eines Drittlands oder einer internationalen Organisation die Angemessenheit vollständig zu beurteilen. In derartigen Fällen sollte der für die Verarbeitung Verantwortliche davon ausgehen, dass das Schutzniveau nicht angemessen ist und **andere Optionen in Erwägung ziehen**."

Für den Fall, dass der für die Verarbeitung Verantwortliche dessen ungeachtet beschließt, eine **Angemessenheitsbeurteilung**[28] vorzunehmen, führt der EDSB im Positionspapier (S. 13f., Abschnitte 5.2 und 5.3) aus: „Mit Blick auf den Grundsatz der Rechenschaftspflicht sollte der für die Verarbeitung Verantwortliche, soweit dies relevant ist, die **Schritte sorgfältig dokumentieren, mit denen er Angemessenheit gewährleistet**, und eine entsprechende Risikobewertung durchführen." Außerdem gilt: „Jede von dem für die Verarbeitung Verantwortlichen vorgenommene Analyse sollte (...) dem EDSB auf Verlangen vorgelegt werden".

Ferner heißt es in dem Positionspapier des EDSB (S. 14, Abschnitt 5.3): „Vor dem Hintergrund der Leitlinie zu Konsultationen im Bereich Aufsicht und Durchsetzung sollte der **DSB** des Organs oder der Einrichtung der EU stets konsultiert und in die Analyse einbezogen werden. Darüber hinaus sind die für die Verarbeitung Verantwortlichen aufgefordert, den **EDSB** zu konsultieren, wenn die Angelegenheit a) eine gewisse Neuheit oder Komplexität aufweist (bezüglich der der DSB oder das Organ echte Zweifel hegen), oder b) sich eindeutig auf die Rechte der betroffenen Person auswirkt (aufgrund der mit der Verarbeitung verbundenen Risiken usw.)".

***

Auf die Frage nach dem Vorhandensein eines **internen Überwachungs- und Registrierungssystems** für Übermittlungen gemäß Artikel 9 bestätigten nur sechs Einrichtungen die Existenz eines solchen Systems. Eine Einrichtung kündigte die baldige Schaffung eines solchen Systems an, während eine weitere größere Einrichtung die Zentralisierung ihres/ihrer bestehenden Systems/Systeme plant.

Die Tatsache, dass nur rund ein Viertel aller Einrichtungen, die Übermittlungen gemäß Artikel 9 vornehmen, über ein internes Überwachungs- und Registrierungssystem verfügen, ist besorgniserregend. Im Positionspapier (S. 9, Abschnitt 3.4) merkt der EDSB zu einem solchen System an: „Auf diese Weise lässt sich die interne Verwaltung internationaler Übermittlungen unterstützen und die Rechenschaftspflicht und die Einhaltung der Verordnung wirksam gewährleisten". Folglich hat der EDSB die Einrichtung eines solchen Systems als bewährte Vorgehensweise empfohlen und Folgendes unterstrichen: „Es sollte nicht nur Übermittlungen nach Feststellung der Angemessenheit erfassen, sondern auch, was noch wichtiger wäre, Übermittlungen aufgrund von Ausnahmen (Artikel 9 Absätze 6 und 7)".

Der EDSB empfiehlt daher den Einrichtungen, ein internes System zur Registrierung von Übermittlungen gemäß Artikel 9 zu schaffen, um **wirksam Rechenschaft und Einhaltung der Verordnung** zu gewährleisten.

[28] Siehe S. 10-12, Abschnitt 4.2 des Positionspapiers zum Begriff der „Angemessenheit".

Abbildung 3: Überblick über die Antworten zu Übermittlungen (Umfrage 2015)

Q1 **Übermittlungen gemäß Art. 9**		*Q2* **Art. 9 Abs. 2**	*Q3* **Art. 9 Abs. 6**	*Q4* **Art. 9 Abs. 7**	*Q5* **EWR**	*Q7* **Überwachungs- / Registrierungssystem**
CEPOL			CEPOL			
KOM (nach GD[29])		KOM (7 GD)	KOM (9 GD)	KOM		KOM (2 GD)
Rat			Rat	(2 GD)		
EACEA		EACEA			EACEA	
EZB			EZB		EZB	
ECDC		ECDC	ECDC			ECDC
EAD			EAD		EAD	
EFCA		EFCA				EFCA
EFSA		EFSA				
EIB		EIB				EIB („bald“)
EIOPA			EIOPA	EIB		EIOPA
EP		EP	EP			
ERA		ERA				
ERCEA			ERCEA			ERCEA
EUSC		EUSC				
HABM			HABM			
OLAF		OLAF	OLAF		OLAF	OLAF
Bürgerbeauftragter		Bürgerbeauftragter	Bürgerbeauftragter			
18		11	12	2	4	6

Das „Wie“ der Übermittlung. Die meisten Übermittlungen erfolgen auf drei Wegen: per Post (Brief, manchmal eingeschrieben, oder *„note verbale“*; 8 Fälle), per E-Mail (in einigen Fällen verschlüsselt; 11 Fälle) oder durch Gewährung des Zugangs zu einer bestimmten Datenbank (sieben Fälle) oder durch eine Kombination dieser Kanäle (fünf Fälle). Weitere Möglichkeiten sind Übermittlungen per Fax, ein Web-Formblatt, per Telefon oder persönliche Übergabe.

2.3. Informationssicherheit

Der EDSB wollte Folgendes erfahren:

- Gibt es ein eigenes Verfahren für das Management Ihrer Informationssicherheit?
- Werden für Datenverarbeitungsvorgänge Risikobewertungen vorgenommen? Wenn ja, wollte der EDSB wissen, für welchen Anteil (%) der Datenverarbeitungsvorgänge in den beiden letzten Jahren Risikobewertungen erfolgten.
- Verfügt die Einrichtung über eine allgemeine Sicherheitsstrategie[30]? Wenn ja: Enthält diese allgemeine Sicherheitsstrategie auch einen Abschnitt über Informationssicherheit?
- Gibt es ein förmliches Verfahren für den Umgang mit Sicherheitszwischenfällen?
- Werden dem DSB Sicherheitszwischenfälle gemeldet, bei denen es um personenbezogene Daten geht?

[29] AGRI, EAC, GROW, HR, MARE, RTD, TAXUD für Art. 9 Abs. 2; EMPL, ESTAT, JUST, MARE, NEAR, PMO, SANTE, TAXUD, TRADE für Art. 9 Abs. 6.
[30] Diese Frage bezog sich nicht auf anwendungsspezifische Sicherheitsstrategien.

Mit Ausnahme von acht Einrichtungen gaben alle an, über ein eigenes Verfahren für das Management ihrer Informationssicherheit zu verfügen. Zwei Einrichtungen planen die Einrichtung eines Verfahrens im weiteren Verlauf des Jahres 2015. Zwei Einrichtungen erwähnten ausdrücklich die ISO-Zertifizierung (ECHA / ISO 9001) oder Durchführung (GSA (GNSS); ISO 27001) in diesem Zusammenhang.

19 Einrichtungen gaben in ihrer Antwort an, keine oder zumindest nicht regelmäßig Risikobewertungen für ihre Datenverarbeitungsvorgänge vorzunehmen, wobei eine Einrichtung darauf hinwies, eine solche Vorgehensweise sei „in einer Einrichtung mit begrenzten Ressourcen nicht realistisch“. Die Mehrheit der Einrichtungen (38) bestätigte hingegen ausdrücklich, für ihre Datenverarbeitungsvorgänge Risikobewertungen durchzuführen. Von dieser Mehrheit machten 18 Einrichtungen Angaben zum Prozentsatz der Verarbeitungen, bei denen eine solche Bewertung vorgenommen wird; die Bandbreite reichte von „unerheblich“ bis 100 % (letzteres bei acht Einrichtungen), was bedeutet, das in Einrichtungen, die Risikobewertungen durchführen und Prozentsätze vorlegen, im Durchschnitt zwei Drittel (66,4 %) ihrer Datenverarbeitungen einer Risikobewertung unterzogen wurden.

16 Einrichtungen gaben an, nicht über eine allgemeine Sicherheitsstrategie zu verfügen, und zwei Einrichtungen erwähnten ihre Absicht, eine solche im weiteren Verlauf des Jahres 2015 auszuarbeiten. In den meisten Fällen enthalten diese allgemeinen Sicherheitsstrategien einen Abschnitt über Informationssicherheit. Eine Einrichtung merkte an, zwar keine allgemeine Sicherheitsstrategie, aber eine IKT-Sicherheitsstrategie zu haben.

45 Einrichtungen bestätigten die Existenz eines förmlichen Verfahrens für den Umgang mit Sicherheitszwischenfällen (13 bekräftigten ausdrücklich, nicht über ein solches Verfahren zu verfügen), zwei weitere erwähnten, ein solches Verfahren sei derzeit in der Erarbeitung.

*Gemäß Artikel 22 Absatz 1 der Verordnung, in dem es um den Stand der Technik und die Kosten der Durchführung geht, hat der für die Verarbeitung Verantwortliche geeignete technische und organisatorische **Maßnahmen** zu treffen, **damit ein Schutzniveau gewährleistet ist**, **das den** von der Verarbeitung ausgehenden **Risiken** und der Art der zu schützenden personenbezogenen Daten **angemessen ist**.*

Solche Maßnahmen sind insbesondere zu treffen, um einer unbefugten Weitergabe oder einem unbefugten Zugang, einer zufälligen oder unrechtmäßigen Vernichtung oder einem zufälligen Verlust, einer Veränderung sowie jeder anderen Form der unrechtmäßigen Verarbeitung vorzubeugen.

REA: „...für die gesamte Forschungsfamilie steht ein Online-Tool zur Verfügung, und bei einem Sicherheitsverstoß, bei dem es um personenbezogene Daten geht, (...) muss der für die Verarbeitung Verantwortliche dieses Formular für die Bekanntmachung eines Verstoßes gegen die Datenschutzvorschriften verwenden ...“

Lediglich sechs Einrichtungen gaben an, ihr DSB erhalte bei einem Informationssicherheitszwischenfall im Zusammenhang mit personenbezogenen Daten keine Meldung[31]; eine merkte an, es gäbe trotz wiederholter Audit-Empfehlungen zu diesem Thema keine solche Meldung. Für eine Einrichtung war eine solche Meldung eher mit den primären Aufgaben des DSB als IT-Beauftragtem und weniger mit seiner Rolle als DSB verknüpft.

[31] Für eine Einrichtung soll die Meldepflicht in ein derzeit in der Erarbeitung befindliches förmliches Verfahren aufgenommen werden.

Mehrere Einrichtungen wiesen auf die rein hypothetische Natur solcher Meldungen an den DSB hin, da es keine Zwischenfälle dieser Art gegeben habe.

Bürgerbeauftragter: „Es gibt zwar kein Standardverfahren für Verletzungen des Schutzes personenbezogener Daten, doch war es bisher so, dass bei einem Datensicherheitszwischenfall dem DSB offiziell Meldung erstattet wurde. So musste insbesondere der für die Verarbeitung Verantwortliche dem DSB einen Bericht über den Zwischenfall vorlegen. Der Bericht enthielt folgende Informationen: a) eine chronologische Schilderung der Ereignisse, die zur nicht genehmigten Übermittlung der personenbezogenen Daten führten; b) Angaben zu Umfang und Art der übermittelten personenbezogenen Daten und zur Zahl der betroffenen Personen; c) die Maßnahme zur Abmilderung möglicher nachteiliger Wirkungen der Verletzung des Schutzes personenbezogener Daten; d) die Maßnahme zur Unterrichtung der von dem Zwischenfall Betroffenen oder die Gründe, diese Unterrichtung zu unterlassen; und e) die Maßnahmen, mit denen in Zukunft eine Wiederholung des Zwischenfalls verhindert werden soll.“

Alles in allem haben die EU-Einrichtungen verstanden, dass Informationssicherheit als Prozess zu managen ist, dass also Informationssicherheit nichts ist, das ein für allemal erreicht wird, sondern das laufend überwacht und immer wieder bewertet werden muss. Allerdings scheinen Risikobewertungen noch nicht überall ihren Platz in den Informationssicherheitsverfahren der EU-Einrichtungen gefunden zu haben (Risikobewertungen sind ein wichtiges Instrument für den Umgang mit Unwägbarkeiten im Sicherheitsmanagement in einer Organisation[32]). Dies wirft die Frage auf, wie EU-Einrichtungen über den Einsatz von Ressourcen und entsprechende Bemühungen um eine bessere Informationssicherheit entscheiden.

Das Management von Sicherheitszwischenfällen[33] scheint überdies meist formell in den EU-Einrichtungen abgehandelt zu werden, häufig unter Einbeziehung des DSB, wenn personenbezogene Daten betroffen sind. Dieser Ansatz gewährleistet eine angemessene, den potenziellen Auswirkungen der Verletzungen auf die betroffenen Personen gerecht werdende Behandlung von Verletzungen des Schutzes personenbezogener Daten.

2.4. Gewährleistung der wirksamen Löschung personenbezogener Daten

Der EDSB stellte Fragen

- zum Vorhandensein einer **schriftlichen Strategie** für die wirksame Löschung personenbezogener Daten nach Ablauf der Aufbewahrungsfrist;
- zum Vorhandensein eines **Standardverfahrens** für die wirksame Löschung personenbezogener Daten nach Ablauf der Aufbewahrungsfrist;
- zum Vorhandensein **automatisierter Verfahren** zur Unterstützung der Löschung in allen Ihren Systemen;
- zu Maßnahmen, mit denen die **Löschung in Sicherheitskopien** (sofern vorhanden) gewährleistet wird.

[32] Siehe ISO 27001, ISO 27005, BSI Standard 100-3, NIST special publication 800-300, EBIOS, Octave Allegro, MAGERIT.
[33] Siehe ISO 27035, NIST 800-61r2.

Von 61 Einrichtungen gaben 38 an, sie verfügten über eine **schriftliche Strategie für die wirksame Löschung** personenbezogener Daten. Eine Einrichtung merkte an, sie sei dabei, eine solche Strategie zu erarbeiten. Manche Erklärungen deuten allerdings darauf hin, dass dieser Selbsteinschätzung eine eher großzügige Auslegung des Begriffs „Strategie“ zugrunde liegt, denn eine ganze Reihe von Einrichtungen betrachtet schon die Festlegung einer Aufbewahrungsfrist „pro Verarbeitungsvorgang“ im Register des DSB als Beweis für eine schriftliche Strategie. Zwei Einrichtungen sprachen von der Erarbeitung einer schriftlichen Strategie als einem „künftigen“ oder „laufenden“ Projekt, und in einer Einrichtung bedarf eine solche Strategie „noch der Billigung“.

Der EDSB hatte um eine Kurzbeschreibung der allgemeinen Strategie oder einer **Beschreibung** ausgewählter Teile gebeten, sofern die Strategie sich zu jedem Verarbeitungsvorgang oder zu ausgewählten Verarbeitungsvorgängen äußert. Die meisten Einrichtungen antworteten hierauf mit verarbeitungsspezifischen Beispielen, wie unter anderem folgenden:

EFCA: „Zu Verarbeitungsvorgängen im HR-Bereich: ... Die HR-Archive sind in acht Unterkategorien von Akten mit Mitarbeiterdaten unterteilt. Die allgemeine Aufbewahrungsstrategie ist in den Meldungen an das Datenschutzregister der EFCA niedergelegt. Daher wurde eine zusammenfassende Tabelle mit Aufbewahrungsfristen für HR-Akten extrahiert. Die HR-Roadmap sieht eine jährliche Überarbeitung und ein Follow-up von HR-Aktivitäten vor. Dadurch wird einmal pro Jahr eine Überprüfung der Archive und Aufbewahrungsfristen und die Einleitung der Vernichtung von Akten ausgelöst“.

*In Artikel 4 Absatz 1 Buchstabe e der Verordnung heißt es, dass personenbezogene Daten **so lange**, **wie es** für die Erreichung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, **erforderlich ist**, in einer Form gespeichert werden, die die Identifizierung der betroffenen Person ermöglicht. Gemäß Artikel 4 Absatz 2 der Verordnung hat der für die Verarbeitung Verantwortliche für die Erfüllung dieser Verpflichtung zu sorgen.*

EUISS: „Die Regeln für Praktika besagen, dass nach Abschluss des Praktikantenprogramms nur einige wenige Daten (Nachname, Vorname) vom Dokumentations- und Forschungsbeauftragten zusammen mit einem Bericht über die Tätigkeit des Praktikanten zu Archivierungs- und Aufzeichnungszwecken (z. B. für Empfehlungsschreiben) aufbewahrt werden“.

Auf die Frage nach einem **Standardverfahren** für die wirksame Löschung personenbezogener Daten nach Ablauf der Aufbewahrungsfrist antworteten 26 Einrichtungen, sie hätten ein solches Verfahren. Zwei weitere gaben an, die Einrichtung eines solchen Standardverfahrens sei für sie ein „künftiges“ oder „laufendes“ Projekt. Eine Einrichtung erwähnte, ein Standardverfahren gebe es „nur für einige Verarbeitungsvorgänge“.

ECHA: „Die ECHA verfügt über ein Verfahren für die Kontrolle von Dokumenten und Aufzeichnungen ... Es enthält strenge Grundsätze für die Aufbewahrung von Dokumenten. Die einzelnen Aufbewahrungsfristen für alle in der Agentur identifizierten Aufzeichnungen sind in einem anderen formellen Dokument erfasst, dem ECHA Records Retention Schedule. Der Anhang zum Verfahren für die Kontrolle von Dokumenten und Aufzeichnungen enthält detaillierte und praktische Anweisungen zur Vernichtung bzw. Löschung von Dokumenten auf Papier und in elektronischer Form nach Ablauf der Aufbewahrungs- bzw. Speicherfrist.

Lediglich 11 Einrichtungen behaupten, **automatisierte Verfahren zur Unterstützung der Löschung** in allen bestehenden Systemen zu haben (11 Einrichtungen verfügen nicht über derartige Systeme und haben daher geantwortet „Entfällt“). Fünf weitere gaben an, die Einrichtung solcher automatisierten Verfahren sei für sie ein „künftiges“ oder „laufendes“ Projekt. In den Beispielen geht es häufig um CCTV-Filmmaterial (fünf Einrichtungen).

Im Hinblick auf die **Löschung von Daten in Sicherheitskopien** erwähnten 42 Einrichtungen, sie sorgten für die Löschung von Sicherheitskopien, doch schilderten die meisten nur kurz oder gar nicht, *wie* sie die Löschung tatsächlich vornehmen.

2.5. Ihr Datenschutzbeauftragter und Sie

Klingt bekannt? In der **Umfrage 2013** hatten wir Angaben dazu erbeten, wie DSB in die Gestaltung neuer Verarbeitungen personenbezogener Daten einbezogen werden und hatten in dem Zusammenhang Bezug auf gegebenenfalls vorhandene Governance-Dokumente (vor allem für IT) oder einfache Beschreibungen eingeführter bewährter Vorgehensweisen genommen, seien sie nun formalisiert oder nicht.

Da diese **Frage absichtlich sehr offen formuliert worden war**, fielen auch die Antworten sehr vielfältig aus, waren aber doch ein umfassender Beleg dafür, dass sich viele EU-Einrichtungen der Notwendigkeit bewusst sind, sich von Anfang an Gedanken über den Datenschutz zu machen und ihren DSB einzubeziehen. Wir stellten allerdings fest, dass die EU-Einrichtungen dies auf unterschiedliche Art und Weise gewährleisten.

Was hat sich also geändert? Aufbauend auf den bisherigen Ergebnissen hat der EDSB für die Ausgabe **2015** der Umfrage **gezieltere Fragen** gestellt. In einem eigenen Abschnitt, bei dem der EDSB ausdrücklich darum gebeten hatte, die Beantwortung *nicht* dem DSB zu überlassen, forderte er Informationen darüber an, ob die Aufgaben des DSB in seiner Arbeitsplatzbeschreibung aufgeführt sind, ob die Wahrnehmung der Aufgaben des DSB in seine Leistungsbeurteilung einfließt und wie der DSB in die Konzeption neuer Verarbeitungsvorgänge einbezogen wird.

Die Bedeutung des Datenschutzbeauftragten (DSB) als Partner sowohl für die für die Verarbeitung Verantwortlichen in den EU-Einrichtungen als auch für den EDSB kann gar nicht genug betont werden. ***DSB spielen eine Schlüsselrolle bei der Gewährleistung der Einhaltung der Verordnung.*** *Sie sind für Bedienstete in den EU-Einrichtungen der erste Ansprechpartner, wenn es darum geht, sie über ihre Rechte und Pflichten zu beraten und eine Datenschutzkultur entstehen zu lassen. Darüber hinaus sind sie auch die wichtigste Verbindungsstelle für den EDSB. Intern können DSB bewährte Vorgehensweisen in ihren EU-Einrichtungen verbreiten, als Drehscheibe für Wissen agieren, die Verarbeitung Verantwortliche beraten und Probleme aufzeigen. Die frühzeitige Einbeziehung des DSB in die Konzeption neuer Verarbeitungsvorgänge stellt eine gute Möglichkeit dar, eingebauten Datenschutz zu gewährleisten.*

Wie in der **Strategie des EDSB** unterstrichen[34], setzen wir auf eine enge Zusammenarbeit mit den Datenschutzbeauftragten, um EU-Einrichtungen dabei zu unterstützen, von einem allein auf der Einhaltung der Vorschriften beruhenden Ansatz zu einem Ansatz überzugehen, der sich auch auf Rechenschaftspflicht gründet.

Einbeziehung des DSB: In verschiedenen Antworten auf die Umfrage 2013 wurde erwähnt, dass die DSB nicht (früh) genug beteiligt werden oder dass Konsultationen zu allgemein gehalten sind. In ihren Antworten auf die Umfrage 2015 **geben *alle* Einrichtungen an, dass der DSB in die Konzeption neuer Verarbeitungsvorgänge einbezogen wird**, auch wenn die meisten Einrichtungen nicht genau beschrieben, *wie* der DSB beteiligt wird, sondern die Frage einfach nur mit Ja beantworteten[35]. Zwei Einrichtungen erwähnen eine verstärkte Einbeziehung ihrer DSB. Mehrere Einrichtungen

[34] https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Strategy/15-07-30_Strategy_2015_2019_Update_EN.pdf, S. 20.

[35] So heißt es z. B. beim EUSC: „Alle neuen Verarbeitungsvorgänge müssen vom DSB daraufhin geprüft werden, ob sie den Vorschriften Genüge tun“.

nutzten allerdings **einschränkende Formulierungen**, die von „kann konsultiert werden“ über „gelegentlich“, „gegebenenfalls“, „falls erforderlich“ bis zu „bei Bedarf“ /„ad hoc“ / „fallweise“ reichen.

Rat: „Bei Verarbeitungsvorgängen, die nicht die Entwicklung neuer IT-Systeme zur Folge haben, wird der DSB in der Regel in einer frühen Phase konsultiert, damit sichergestellt ist, dass die geplante Verarbeitung auch den Datenschutzvorschriften entspricht. Zu den häufiger auftretenden Fragen gehören Qualität der Daten, Empfänger, Sicherheitsmaßnahmen, Datenaufbewahrungsfristen und Information betroffener Personen.
Bei der Entwicklung neuer IT-Systeme arbeitet der DSB eng mit DGA CIS (IT-Abteilung) zusammen, um die Einbeziehung des DSB in den allerersten Phasen der Planung eines neuen IT-Tools zu verbessern und zu dokumentieren. Damit soll die Identifizierung von Risiken für den Datenschutz und die Einführung von datenschutzfreundlichen Technologien zur Minderung dieser Risiken gefördert werden. Mit Hilfe einer Muster-Datenschutzfolgenabschätzung wird ermittelt, ob Bedarf an solchen Technologien besteht und ob sie angemessen sind; mit ihr können sich der Projektmanager und der DSB einen Überblick über die betroffenen personenbezogenen Daten und über die Hauptrisiken verschaffen, die die Verarbeitung mit sich bringt.
Darüber hinaus nimmt der DSB an Sitzungen des HR/IT-Ausschusses teil, also des Ausschusses, der für die Planung, Billigung und Verwaltung aller IT-Systeme und Anwendungen für HR und die Verwaltung des Generalsekretariats des Rates zuständig ist.“

EIOPA:
„- Zweiwöchentliche Sitzungen mit dem für die Verarbeitung Verantwortlichen (also dem Exekutivdirektor);
- monatliche Sitzungen mit der mittleren Führungsebene der Corporate Support Unit (also Referatsleiter, Leiter des IT-Teams und Leiter des Beschaffungsteams);
- monatliche Sitzung mit der mittleren Führungsebene des HR-Teams (also dessen Teamleiter);
- Einbeziehung in Business Plan Requests;
der Erlass/die Überarbeitung von Standardarbeitsanweisungen (wie Strategie und Verfahren) umfasst eine rechtliche Kontrolle durch den DSB;
- Einsetzung von Datenschutzkoordinatoren in jedem EIOPA-Team und regelmäßige Sitzungen mit ihnen;
- regelmäßige allgemeine Fortbildungen zum Thema Datenschutz für alle Mitarbeiter bieten ein gutes Forum für den Informationsaustausch.
Die Tatsache, dass der DSB seine Aufgaben nicht in Vollzeit wahrnimmt und beim Rechtsteam angesiedelt ist, gilt als Vorteil, da der DSB auf diese Weise über anstehende neue Verarbeitungsvorgänge auf dem Laufenden gehalten wird.“

EP: „... Der DSB ist von der Grundkonzeption und Gestaltung seines Tätigkeitsbereichs her stets in die Abfassung und Überprüfung aller neuen internen Beschlüsse einbezogen, bei denen es um personenbezogene Daten geht ... Der DSB ist regelmäßig auch in neue IT-Projekte eingebunden ... Darüber hinaus ist der DSB dank regelmäßiger Sitzungen mit der Führungsebene und den DSK stets über neue Verarbeitungen informiert. Schließlich finden zwei- oder dreimal pro Jahr Fortbildungsveranstaltungen für die Mitarbeiter statt, die in den verschiedenen GD am intensivsten mit Datenschutzfragen befasst sind“.

Um das Thema noch aus dem **Blickwinkel eines weiteren Akteurs** zu beleuchten, hat der **EDSB die DSB anonym befragt**, von denen (bei einer Beteiligung von rund 50 %) lediglich etwas mehr als die Hälfte aussagte, sie würde angemessen konsultiert (17 „Ja“, 15 „Nein“). Insgesamt stuften sie ihre Zufriedenheit mit ihrer Konsultation bei 6,4 ein (auf einer Skala von 0 („praktisch nie konsultiert“) bis 10 („immer konsultiert“)). Die Kommentare waren teils positiv („regelmäßig in Geschäftsentscheidungen aller Art einbezogen“; „gute Zusammenarbeit zwischen DSB und Geschäftsbereichen, hohes Datenschutzbewusstsein“; „deutliche Verbesserung in den letzten anderthalb Jahren“), teils weniger positiv („Konsultation ist kohärent und regelmäßig, erfolgt aber zu spät im Prozess, ist mehr Brandbekämpfung als eingebauter Datenschutz“); gelegentlich wurde angedeutet, dass der DSB vorsätzlich ausgeschlossen oder zumindest so lange absichtlich im Dunkeln gelassen wird, bis bestimmte Entscheidungen nicht mehr rückgängig gemacht werden können, und dass auf diese Weise das Konzept des eingebauten Datenschutzes nicht wirklich umgesetzt

werden kann. In den meisten Anmerkungen hieß es, man werde zu spät im Prozess zu Verarbeitungsvorgängen konsultiert bzw. *entdecke* sie zu spät.

In den Anmerkungen der Einrichtungen zur **Art der Einbeziehung** des DSB wurden im Wesentlichen dreierlei Formen genannt, nämlich Einbeziehung im Wege eines festgelegten und strukturierten Verfahrens (sechs Einrichtungen), durch Teilnahme des DSB an Arbeitsgruppen, Lenkungsausschüssen oder Managementsitzungen (13 Fälle, insbesondere IT-Lenkungsausschüsse = fünf), und durch Aufnahme der Konsultation des DSB als obligatorischen Schritt in Vorlagen für Projektmanagement oder Kontrollkästchen auf Laufzetteln (vier Einrichtungen).

Damit werden Ergebnisse der Umfrage 2013 bestätigt, bei der der EDSB auf regelmäßige Sitzungen mit den einschlägigen Abteilungen (HR, IT, ...) und auf die Aufnahme eines „Datenschutz-Checks" in Vorlagen für Projektmanagement als besonders wertvolle Instrumente für die Gewährleistung der ordnungsgemäßen Einbeziehung des DSB gestoßen war. Die Antworten bestätigten ferner, dass die Verfahren umso formalisierter sind, je größer die Einrichtung ist. Auch dieses Mal erwähnten einige Einrichtungen die anderen Aufgaben des DSB, die dafür sorgten, dass er immer auf dem neuesten Wissensstand ist (z. B. Aufgaben im IT-Bereich oder als Rechtsberater des Direktors). Dies galt vor allem in kleineren Agenturen.

Der EDSB erinnert an dieser Stelle erneut daran, dass diese Vorgehensweise für kleine oder gerade eingerichtete Agenturen passend sein mag, dass aber **für größere Organisationen ein stärker formalisiertes Konsultationsverfahren angebracht sein dürfte**.

EMA: „...Im Verfahren ist vorgesehen, den Datenschutzbeauftragten offiziell in Kenntnis zu setzen, wenn von den zuständigen Diensten eine neue Strategie vorgeschlagen wird. ... Darüber hinaus finden vierteljährlich bilaterale Gespräche zwischen dem DSB und dem Verwaltungsdirektor statt, bei denen sowohl Fragen der Anwendung der aktuellen Strategie erörtert werden als auch die Gestaltung künftiger Strategien/Aktivitäten besprochen wird".

ERCEA: „Der DSB der ERCEA ist Mitglied des IT-Lenkungsausschusses. Die Weisungen der ERCEA für die Vorbereitung und Validierung interner Verfahren (ICS8) sehen ausdrücklich vor, dass die für Geschäftsprozesse Verantwortlichen vor Beginn der Validierung eines internen Verfahrens den DSB frühzeitig zu konsultieren haben. Darüber hinaus muss der DSB zu allen Verfahrensentwürfen oder -änderungen gehört werden, bei denen es um die Verarbeitung personenbezogener Daten geht (VISA erforderlich im ARES Laufzettel) ..."

HABM: „... enge Beziehung aufgrund unserer internen Vorschriften zur Durchführung der Verordnung (EG) Nr. 45/2001, denen zufolge die jeweiligen für die Verarbeitung Verantwortlichen verpflichtet sind, dem DSB vorab alle Verarbeitungen personenbezogener Daten sowie erhebliche Änderungen an bestehenden Verarbeitungen zu melden. Insbesondere in jedem internen Vermerk an den Präsidenten des Amtes gibt es ein von der entsprechenden Hauptabteilung auszufüllendes Feld betreffend die „Konsultation des DSB". Dies ist der Konsultation des DSB bei allen Projekten und Aktivitäten des Amtes förderlich, bedeutet für die Leitung des Amtes aber auch Gewissheit darüber, dass Datenschutzfragen vor der Übermittlung des Vorschlags an den Präsidenten angemessen berücksichtigt wurden. Der DSB ist ferner Mitglied des Informationssicherheitsforums. Aufgabe des Forums ist es, die Sicherheit der Verarbeitung personenbezogener und anderer Daten im HABM im Einklang mit ISO 27001 zu gewährleisten. ...".

Rat: „Mit Hilfe einer Muster-Datenschutzfolgenabschätzung wird ermittelt, ob Bedarf an solchen Technologien besteht und ob sie angemessen sind; mit ihr können sich der Projektmanager und der DSB einen Überblick über die betroffenen personenbezogenen Daten und über die Hauptrisiken verschaffen, die die Verarbeitung mit sich bringt."

Der „eingebaute Datenschutz“ hat sich bewährt. Er hilft dabei, Probleme schon früh im Entwurfsprozess auszumachen - und damit z. B. kostspielige Umgestaltungen von Software in späteren Phasen zu vermeiden[36] - und die Datenschutzkultur zu einem festen Bestandteil des Entwicklungszyklus zu machen. **Die frühzeitige Einbeziehung des DSB in die Konzeption neuer Verarbeitungsvorgänge stellt eine gute Möglichkeit dar, eingebauten Datenschutz zu gewährleisten.**

***

Für die meisten DSB gilt, dass ihre Aufgaben Teil ihrer **Arbeitsplatzbeschreibung** sind. Dies trifft nur bei sechs Einrichtungen (EDA, EMSA, ERCEA, Eurofound, INEA, OSHA) nicht zu. Zwei Einrichtungen (ERCEA, INEA) erwähnten, das bestehende System von *Arbeitsplatzbeschreibungen* sei zu allgemein und könne die Besonderheiten des DSB nicht abdecken, doch seien diese Besonderheiten (einschließlich Teilzeittätigkeit als DSB) in den *Zielen* des DSB niedergelegt.

Die überwiegende Mehrheit von Einrichtungen bestätigt, dass die Wahrnehmung der Aufgaben des DSB in seine **Leistungsbeurteilung** einfließt; lediglich auf vier Einrichtungen (EuGH, EDA, EMSA, Bürgerbeauftragter) trifft dies nicht zu. Eine Einrichtung äußert Bedenken bezüglich der Unabhängigkeit des DSB, sollte dessen Leistung beurteilt werden. Vor diesem Hintergrund hat der EDSB 2005 in seinem **Positionspapier zur Rolle der behördlichen Datenschutzbeauftragten**[37] klargestellt, dass ein DSB zwar keine Weisungen entgegennimmt, aber trotzdem einer Leistungsbeurteilung unterzogen werden kann. Im Sinne der Unabhängigkeit des DSB sollte jedoch „der **„DSB nur seiner Anstellungsbehörde und nicht einem direkten Vorgesetzten berichten“**[38].

Die 2010 vom Netz der Datenschutzbeauftragten der Organe und Einrichtungen der EU herausgegebenen **Beruflichen Standards für Datenschutzbeauftragte**[39] bieten in dieser Frage weitere Orientierung, insbesondere für **Teilzeit-DSB**:

- Auf S. 6 dieses Dokuments heißt es: „Ein DSB, der einem direkten Dienstvorgesetzten (Direktor oder Referatsleiter) Bericht erstattet, fühlt sich möglicherweise gedrängt, zu kooperieren und reibungslos mit der Leitung der Behörde und anderen Kollegen auszukommen, da sich eine strenge Wahrnehmung seiner Aufgaben als DSB nachteilig auf seine Laufbahn auswirken könnte. Nimmt ein DSB seine Aufgaben ordnungsgemäß wahr, bedeutet dies oft, dass er seine Meinung entschlossen und nachdrücklich auch gegenüber für die Verarbeitung Verantwortlichen vertreten muss, die in der Organisation einen höheren Rang einnehmen, was bestenfalls als „bürokratisch“ oder schlechtestenfalls als unangenehme „Quertreiberei“ wahrgenommen werden kann. Der DSB muss also Druck und Schwierigkeiten standhalten können, die in dieser Position unvermeidbar

[36] Eine Einrichtung wies ausdrücklich auf dieses Problem hin und merkte an, es bestehe weniger für Systeme im HR-Bereich, da nunmehr der DSB regelmäßig an Sitzungen des HR/IT-Lenkungsausschusses teilnehme.
[37] Positionspapier zur Rolle der behördlichen Datenschutzbeauftragten für die Gewährleistung einer wirksamen Einhaltung der Verordnung (EG) Nr. 45/2001, siehe https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PositionP/05-11-28_DPO_paper_EN.pdf.
[38] Positionspapier zur Rolle der behördlichen Datenschutzbeauftragten für die Gewährleistung einer wirksamen Einhaltung der Verordnung (EG) Nr. 45/2001, S. 8.
[39] Berufliche Standards für Datenschutzbeauftragte der Organe und Einrichtungen der EU, die nach der Verordnung (EG) Nr. 45/2001 arbeiten; veröffentlicht vom Netz der Datenschutzbeauftragten der Organe und Einrichtungen der EU, siehe http://ec.europa.eu/dataprotectionofficer/docs/dpo_standards_en.pdf .

sind. Um diesen Druck zu mindern, sollte der DSB dem Leiter der Verwaltung des Organs oder der Einrichtung berichten und von ihm beurteilt werden. Dies gilt insbesondere für Teilzeit-DSB, die bezüglich ihrer Pflichten als DSB direkt der Anstellungsbehörde berichten und von ihr beurteilt werden sollten, bezüglich ihrer sonstigen Aufgaben hingegen ihrem Dienstvorgesetzten berichten und von ihm beurteilt werden sollten."

- Auf S. 7 des Dokuments heißt es unter anderem: „... Bei der Beurteilung der Leistung eines DSB sollte der Beurteilende sorgfältig darauf achten, den DSB nicht für unpopuläre Meinungen zu tadeln oder Datenschutzanforderungen als Verwaltungsaufwand zu betrachten. Bei Teilzeit-DSB sollte die Wahrnehmung der DSB-Pflichten gleiches Gewicht haben wie die Wahrnehmung der anderen Aufgaben. Sofern in den Durchführungsbestimmungen des Organs/der Einrichtung vorgesehen, sollte dem EDSB Gelegenheit gegeben werden, sich zur Leistung des DSB zu äußern".

Die von Einrichtungen in ihren Antworten auf die Umfrage 2015 genannten Beispiele machen deutlich, dass derartige Empfehlungen allmählich in die Beurteilung vieler DSB eingeflossen sind:

CdT: „Die Leistungsbeurteilung des DSB erfolgt mit zwei Beurteilungsverfahren, zum einen durch den Direktor (der nur die Wahrnehmung der DSB-Aufgaben beurteilt) und zum anderen durch den Dienstvorgesetzten."

Cedefop (Teilzeit-DSB): „... werden zwei getrennte und unterschiedliche Leistungsbeurteilungen von zwei verschiedenen Beurteilenden vorgenommen, die sich mit der Rolle als DSB bzw. mit der anderen Funktion befassen."

EBA: „Die Beurteilung erfolgt durch eine mittlere Führungskraft des DSB, wobei sich auch der Exekutivdirektor zu den Pflichten der Person als DSB äußert."

ECDC: „Der Wahrnehmung der DSB-Pflichten wird gleiches Gewicht beigemessen wie der Wahrnehmung der anderen Aufgaben. Da der DSB direkt dem Direktor Bericht erstattet, erfolgt die Beurteilung der Wahrnehmung der DSB-Aufgaben durch den Direktor. Diese Regeln wurden intern offiziell festgelegt."

EMA: „... der beurteilende unmittelbare Vorgesetzte ... berät sich mit dem Verwaltungsdirektor bezüglich der Leistungen des DSB und nimmt vor Fertigstellung des Berichts seinen Beitrag / seine Kommentare entgegen".

In Anbetracht der Tatsache, dass nach Auskunft aller Einrichtungen die DSB in die Konzeption neuer Verarbeitungsvorgänge eingebunden sind, **fordert der EDSB alle Einrichtungen auf, dafür zu sorgen, dass die Arbeit des DSB bei der Leistungsbeurteilung des DSB gewürdigt wird.**

Die DSB wiederum fordert der EDSB auf, ihre eigenen gemeinsamen Grundsätze für gute Aufsicht (Anforderungen, Jahresarbeitsprogramm, Jahresbericht usw.) zu entwickeln, anhand derer ihre Leistung bei der Arbeit gemessen werden kann[40].

2.6. Einrichtungen, die nicht auf die Umfrage geantwortet haben

Bis zum Zeitpunkt der Annahme dieses Textes hatte nur eine Einrichtung, nämlich SESAR JU, keine inhaltlichen Antworten auf die Umfrage vorgelegt.

[40] Siehe ferner das Positionspapier zur Rolle der behördlichen Datenschutzbeauftragten für die Gewährleistung einer wirksamen Einhaltung der Verordnung (EG) Nr. 45/2001, S. 8.

Das SESAR JU gab „mangelnde Kapazitäten“ aufgrund der unvorhergesehenen Notwendigkeit der Bestellung eines amtierenden DSB an.

Fakt ist jedoch nach wie vor, dass die Verordnung einzuhalten ist. Wie in der Einleitung dargelegt, werden die Ergebnisse dieser Umfrage in die Planung von Durchsetzungsmaßnahmen für 2016 einfließen. Wenn EU-Einrichtungen nicht rechtzeitig antworten, kann dies Anlass zur Sorge sein.

3. Folgemaßnahmen der letzten Umfrage: Inspektionsbesuche

3.1. Allgemeine Anmerkungen

Im Nachgang zur letzten Umfrage hat der EDSB – abgesehen vom allgemeinen Follow-up und einigen Sonderfällen – fünf Einrichtungen besucht, die während der Umfrage 2013 besonders aufgefallen waren.

Seinerzeit war eine Inspektion im eigentlichen Sinne für diese Einrichtungen nicht geplant, weil sie die Verordnung (EG) Nr. 45/2001 generell nur in geringem Maße einhielten. Es wäre schwierig gewesen, die „Realität" von noch nicht gemeldeten Verarbeitungsvorgängen oder nicht vorhandenen Instrumenten für die Einhaltung (Bestandsverzeichnis, Register) „zu prüfen", weil es keine Erwartungsgrundlage für die Prüfung gegeben hätte.

> ***Inspektionsbesuche**: Ein Besuch ist ein Instrument zur Förderung der Einhaltung der Rechtsvorschriften, dessen Zweck darin besteht, das Engagement der Führungsebene eines Organs oder einer Agentur für die Einhaltung der Verordnung zu verbessern. Die Entscheidung zu einem Besuch wird in der Regel bei unzureichender Einhaltung der Datenschutzbestimmungen, bei mangelnder Kommunikation oder auch mit dem Ziel der Sensibilisierung getroffen. Grundlage dieser Entscheidung sind die Informationen, die der EDSB im Zuge der Überwachung der Einhaltung der Vorschriften, beispielsweise im Rahmen einer allgemeinen Umfrage, erhoben hat. Zunächst findet ein Vor-Ort-Besuch des EDSB oder seines Stellvertreters statt, gefolgt von einem Schriftverkehr über einen spezifischen Plan für das weitere Vorgehen, der zwischen dem EDSB und der besuchten Einrichtung vereinbart wird.*

Diese Inspektionsbesuche dienen dazu, das Engagement des oberen und mittleren Managements zu sichern. Dieser „Top-down"-Ansatz soll die Beteiligung seitens des Managements sicherstellen. Die Erfahrung hat gezeigt, dass ein wirksamer Datenschutz nicht nur von Ressourcen, sondern auch vom guten Willen der Organisation abhängt. Kurzum: Bei diesen Besuchen handelt es sich um **„höfliche Besuche, aber nicht um Höflichkeitsbesuche".** Das Instrument derartiger Inspektionsbesuche wurde seitdem in Artikel 36 der Geschäftsordnung des EDSB kodifiziert[41].

Um der Einhaltung der Verordnung einen Schub zu geben, nutzte der EDSB die Besuche, um in Absprache mit der Hierarchie der betreffenden Einrichtung einen genauen Fahrplan aufzustellen. In den Fahrplänen waren genaue Ziele und Fristen vorgegeben: Erstellung eines Bestandsverzeichnisses, Fortschritte bei der Zahl der Meldungen nach Artikel 25 und 27, Meldung gezielter Verfahren, zu denen der EDSB Leitlinien[42] herausgegeben hat, und andere die besuchte Einrichtung betreffende Fragen (z. B. Gewährleistung einer langfristigen Bestellung eines DSB, Unterweisung der Bediensteten in Datenschutzangelegenheiten usw.).

Um die Wirkung solcher Besuche zu messen, wurde wie schon in der Vergangenheit die Zahl der Meldungen bei der Umfrage 2013 mit der bei der jetzigen Umfrage verglichen.

Name	**Ergebnisse in der Umfrage 2015**		**Ergebnisse in der Umfrage 2013**		**Änderung der Quote**	
	Artikel 25	**Artikel 27**	**Artikel 25**	**Artikel 27**	**Artikel 25**	**Artikel 27**
EIGE	50%	86%	**63%**	**86%**	**-13**	**+/- 0**

[41] http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32013D0504(03)&from=DE.
[42] https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/Guidelines.

EIF	34%	47%	**Nicht vergleichbar**		-	-
GSA (GNSS)	52%	54%	**Nicht vergleichbar**			
EUSC	52%	100%	**Keine Antwort**			
EUISS	25%	17%	**0%**	**0%**	**+25**	**+17**

Abbildung 4: Entwicklung der Meldequoten bei besuchten Agenturen

Die obige Tabelle zeigt die Prozentsätze für Meldungen gemäß Artikel 25 und Artikel 27 in den Jahren 2013 und 2015 für jede der besuchten Einrichtungen und die Änderungen bei den Prozentpunkten. Sie bestätigt, dass sich Besuche eindeutig positiv auf die Einhaltung der Verordnung auswirken. Die nachstehenden Abschnitte geben zusätzliche Informationen zu den einzelnen Besuchen und den danach festgestellten Verbesserungen.

3.2. EIGE

Das Europäische Institut für Gleichstellungsfragen (EIGE) in Vilnius nahm seine Tätigkeit offiziell im Sommer 2010 auf. Auf unsere Umfrage 2011 antwortete das EIGE mit Verspätung, und bis Anfang 2013 hatte es noch keine einzige Vorabkontrollmeldung eingereicht. Aus diesem Grund stattete der stellvertretende Datenschutzbeauftragte dem EIGE im Mai 2013 einen Besuch ab. Bei dem halbtägigen Besuch traf er mit Vertretern der Leitung des EIGE, den für die Verarbeitung verantwortlichen Mitarbeitern sowie dem Datenschutzbeauftragten und dessen Stellvertreter zusammen. Im Anschluss an den Besuch einigten sich das EIGE und der EDSB auf einen Plan, mit dem die uneingeschränkte Einhaltung der Datenschutzbestimmungen erreicht werden soll. Für eine Agentur ihres Alters zeigte die EIGE in der Umfrage 2013 gute Leistungen und hatte auch an den anderen im Fahrplan aufgeführten Punkten gearbeitet. Allerdings ist die Quote der Meldungen gemäß Artikel 25 seit der Umfrage 2013 gesunken, was ein Hinweis darauf sein könnte, dass die anfänglichen Anstrengungen nicht fortgesetzt wurden.

3.3. EIF

Der Europäische Investitionsfonds (EIF) ist eine öffentlich-private Partnerschaft zwischen der EIB, der Europäischen Kommission und verschiedenen Finanzinstitutionen mit Sitz in Luxemburg als Anteilseignern. Sein Kerngeschäft besteht darin, für KMU Risikofinanzierung bereitzustellen. Die Entscheidung, dem EIF einen Besuch abzustatten, ging auf eine erneute Prüfung der jeweiligen Rollen von EIF und EIB bei der Datenverarbeitung zurück, die nicht ganz klar waren, und auf die daraus folgenden niedrigen Meldungsquoten in der Umfrage 2013 für Verarbeitungsvorgänge, die der EIF alleine (unabhängig von der EIB) durchführt. Im Verlauf des Besuches wurden mehrere Bereiche ermittelt, in denen die Verordnung nicht eingehalten wird, z. B. betreffend die Klarheit des Bestandsverzeichnisses und den Mangel an Meldungen sowohl gemäß Artikel 25 als auch gemäß Artikel 27 der Verordnung. Der EIF verpflichtete sich zu Maßnahmen im Rahmen eines gemeinsam vereinbarten Fahrplans, mit denen die Einhaltung der Verordnung erreicht werden soll. In der Zwischenzeit hat er das Bestandsverzeichnis vervollständigt, das Artikel 25-Register auf den neuesten Stand gebracht und beim EDSB eine Reihe von Meldungen gemäß Artikel 27 eingereicht. Die Zahlen in Abschnitt 2.1 geben den Stand zum Zeitpunkt der Antworten des EIF auf die Umfrage wieder; seitdem hat der EIF seinen Rückstand aufgearbeitet und ist auf dem besten Weg, den Fahrplan vollständig abzuarbeiten.

3.4. EUSC (EU SatCen) und GSA (Agentur für das Europäische GNSS)

Auch das Satellitenzentrum der EU (EU SatCen) und die Agentur für das Europäische GNSS (GSA) waren auf der Grundlage der Umfrage 2013 für einen Besuch ausgewählt worden; Anlass waren Probleme bei der Kommunikation. Da keine der beiden Agenturen bis zu der von uns gesetzten Frist ausreichende Nachweise für eine zufriedenstellende Einhaltung der Verordnung vorgelegt hatte, beschlossen wir diese Besuche auf Arbeitsebene, bei denen über Themen von Humanressourcenmanagement bis IT-Sicherheit und über die Aufgaben verschiedener Akteure innerhalb der Organisation im Bereich Datenschutz gesprochen werden sollte. In ihrem Rahmen fanden von Sachbearbeitern des EDSB geleitete Kurse und Fragestunden statt, mit denen der Agentur praktische Hilfestellung geboten und Mitarbeiter und Management darüber aufgeklärt werden sollten, wie sie Datenschutzgrundsätze am besten in ihr Arbeitsumfeld integrieren können. Beide Agenturen brachten sich engagiert in die Kontakte mit uns ein und sagten zu, ihre Einhaltung der Datenschutzgrundsätze zu verbessern, so dass bis zur Umfrage 2015 eine umfassende Einhaltung gewährleistet ist. Die Zusammenarbeit mit der GSA hat sich zwar verbessert, doch lag zum Stichtag für diese Umfrage die Zahl der Meldungen für eine Agentur ihres Alters nach wie vor unter dem Durchschnitt. Bis zum Datum der Veröffentlichung dieses Berichts wurden jedoch mehrere neue Artikel 27-Meldungen eingereicht. An das EU SatCen wurde im November 2014 ein Mitarbeiter des EDSB abgeordnet; im Anschluss daran fand im Dezember 2014 eine Sitzung auf Direktorenebene statt. Seitdem wurden alle Artikel 27-Meldungen eingereicht und konnten fast alle Fälle abgeschlossen werden. Bei IT-spezifischen Meldungen soll bei Bedarf eine enge Zusammenarbeit mit dem EDSB erfolgen.

3.5. EUISS

Das Institut der Europäischen Union für Sicherheitsstudien (EUISS) wurde aufgrund seiner Leistung in der Umfrage 2013 für einen Besuch ausgewählt. Das EUISS, eine Agentur des ehemaligen zweiten Pfeilers, aktualisierte seine Rechtsgrundlage Anfang 2014. Aus praktischen Erwägungen wurde der Besuch in eine Sitzung des Direktors des EUISS und des stellvertretenden Datenschutzbeauftragten im Juni 2014 und einen Besuch beim EUISS in Paris auf Mitarbeiterebene im Oktober 2014 unterteilt. In dem Gespräch zwischen Direktor und stellvertretendem Datenschutzbeauftragten verpflichtete sich das EUISS zu einer besseren Einhaltung der Verordnung. Während des Besuchs in Paris fanden Gespräche zwischen Mitarbeitern des EDSB und dem neu ernannten Leiter der Verwaltung des EUISS, dem DSB und zuständigen Mitarbeitern statt und es wurde eine Schulung zu Datenschutzgrundsätzen abgehalten. Überprüft wird die bessere Einhaltung der Verordnung anhand der vorliegenden Umfrage 2015. Das EUISS hat zwar damit begonnen, an seiner Einhaltung der Verordnung zu arbeiten, doch erfolgen noch immer nicht genügend Meldungen, selbst für eine Agentur, in der der Datenschutzbeauftragte erst seit kurzem vertreten ist (der erste DSB des EUISS wurde erst nach der Umfrage 2013 ernannt). Insbesondere für die Geschäftseinheiten bleibt noch viel zu tun, damit sie ihren Meldepflichten beim DSB nachkommen.

3.6. Auswertung des Besuchsprogramms

Wie schon bei der vorherigen Umfrage zeigen auch hier die Ergebnisse, dass sich Inspektionsbesuche als wirksames Instrument bei der Verbesserung der Einhaltung erwiesen haben, denn sie führen bei den meisten der besuchten Einrichtungen zur Informationsgewinnung, sensibilisieren die Führungsebene und ermöglichen Einigungen über konkrete Ziele und Fristen. Das Programm wird somit in den kommenden Jahren fortgesetzt.

Die Ergebnisse der gegenwärtigen Umfrage werden erneut eine wichtige Rolle bei der Entscheidung spielen, welche EU-Einrichtungen in der Zukunft besucht werden sollen.

Die meisten Besuche haben zu einer besseren Einhaltung geführt; falls ein Besuch allerdings keine positiven Veränderungen bewirkt, müssen weitere Follow-up-Maßnahmen in Betracht gezogen werden. In solchen Fällen kann der EDSB beschließen, eine Inspektion durchzuführen oder auf die in Artikel 47 Absatz 1 der Verordnung vorgesehenen Durchsetzungsbefugnisse zurückzugreifen[43].

[43] Siehe das Strategiepapier des EDSB „Inspektionsbesuche durch den EDSB“ (https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Inquiries/2013/13-11-04_EDPS_Inspection_Policy_EN.pdf), p. 5.

4. Schlussfolgerung und geplantes Follow-up

Insgesamt bestätigen die Ergebnisse der Umfrage aus diesem Jahr stete Fortschritte im Hinblick auf die vollständige Umsetzung der Verordnung in den EU-Einrichtungen.

Für die etablierten und älteren Organe und Einrichtungen hat sich bei den Antworten nicht viel geändert - die Meldungsquoten sind hoch, und die Funktion des DSB ist gefestigt. Nun besteht die Aufgabe für diese EU-Einrichtungen darin, die Bestandsverzeichnisse und Register zu pflegen. In manchen Fällen sind die Meldungsquoten aufgrund neuer Verarbeitungsvorgänge, die gerade eingerichtet werden, leicht gesunken. Dies ist an sich kein Grund zur Beunruhigung, zeigt jedoch, dass eine gute Pflege der Bestandsverzeichnisse und Register konstanter Aufmerksamkeit bedarf und keine einmalige Aufgabe ist. Diese EU-Einrichtungen haben nun die Aufgabe, den Datenschutz in allen ihren Bereichen durchzusetzen und ihn ganz selbstverständlich werden zu lassen.

Die Ergebnisse in Gruppe B sind ähnlich. Bei Artikel 27-Meldungen haben die Einrichtungen zu denen in Gruppe A aufschließen können; bei Artikel 25 bestehen noch kleine Lücken. Auch Agenturen wie die EASA, die etwas hinterherhinkten, haben an Boden gewonnen. Mehrere Agenturen haben perfekte Ergebnisse gemeldet, einige haben dieses Ziel um nur wenige Meldungen verfehlt.

Die Gruppe C weist nunmehr durchschnittliche Meldungsquoten auf, die besser sind als die der Gruppe B in der Umfrage 2013, und hat in dieser Umfrage fast zu dieser Gruppe aufgeschlossen. Die INEA kann hier ebenso wie Frontex als Erfolgsgeschichte bezeichnet werden, denn beide haben sich vom Sorgenkind zu Agenturen im soliden Mittelfeld entwickelt.

Dass die Gruppe D geringere Quoten aufweist, ist verständlich. Allerdings scheint sich nach den beachtlichen Verbesserungen zwischen den Umfragen 2011 und 2013 der Fortschritt ein wenig verlangsamt zu haben, insbesondere bei den Artikel 27-Meldungen. Der EDSB wird Unterstützung und Begleitung bieten, wo dies für eine ordnungsgemäße Durchführung der Verordnung erforderlich ist.

Diese Umfrage ist nicht nur als Bestandsaufnahme zur Durchführung der Verordnung gedacht. Sie fließt auch in die Entscheidungen des EDSB bezüglich seiner Aufsichts- und Durchsetzungstätigkeiten ein.

Bei Betrachtung der Umfrageergebnisse wird deutlich, dass eine Reihe von Einrichtungen mit der Einhaltung der Verordnung noch Probleme zu haben scheint.

Neben solchen Besuchen kann der EDSB auch weitere Durchsetzungsmaßnahmen erwägen und auf seine Befugnisse gemäß der Verordnung zurückgreifen.

IV. Anhang 1 - Methode

Wie ihre Vorgängerinnen wurde auch diese Umfrage auf Dokumentenbasis durchgeführt, d. h., es wurden bei EU-Einrichtungen schriftliche Informationen abgefragt. Die Fragenliste wurde den EU-Einrichtungen im April 2015 übersandt; Erinnerungsschreiben wurden auf Arbeitsebene im Juni 2015 verschickt. Die Antworten gingen im Juni und Juli 2015 ein. Im Dezember 2015 wurden die EU-Einrichtungen zum Berichtsentwurf konsultiert.

Die EU-Einrichtungen wurden gebeten, Informationen zu folgenden Aspekten vorzulegen:

1. **Bestandsverzeichnis und Register**[44]: die Zahl von Verarbeitungsvorgängen, die 1) im Bestandsverzeichnis aufgeführt sind, 2) dem DSB gemeldet und in das Register eingetragen wurden, 3) als unter Artikel 27 fallend identifiziert wurden und 4) dem EDSB bereits gemäß Artikel 27[45] gemeldet wurden;

2. **Übermittlungen personenbezogener Daten gemäß Artikel 9** in den Jahren 2013 und/oder 2014:
   - Übermittlungen gemäß Artikel 9 Absatz 2, Artikel 9 Absatz 6 oder Artikel 9 Absatz 7 und Übermittlungen gemäß Artikel 9 an Empfänger, die ihren Sitz in EWR-Ländern haben, deren Tätigkeit aber von der Anwendung der Richtlinie 95/46/EG ausgenommen ist;
   - nähere Angaben zu dem Verarbeitungsvorgang (wie in der Artikel 25-Meldung erwähnt), dem Empfänger, der Grundlage, dem Bereich (z. B. Strafverfolgung), dem „Wie“ der Übermittlung, den Kategorien personenbezogener Daten sowie der Häufigkeit solcher Übermittlungen;
   - besondere Schwierigkeiten, die bei den genannten Tätigkeiten aufgetreten sind;
   - Vorhandensein eines internen Systems für die Überwachung und Registrierung von Übermittlungen gemäß Artikel 9;

3. **Informationssicherheit**: 1) Vorhandensein eines Verfahrens speziell für Informationssicherheit, 2) Durchführung von Risikobewertungen, 3) Vorhandensein einer allgemeinen Sicherheitsstrategie[46], 4) Vorhandensein eines förmlichen Verfahrens für den Umgang mit Sicherheitszwischenfällen und 5) Meldung an den DSB bei einem Informationssicherheitszwischenfall im Zusammenhang mit personenbezogenen Daten.

4. **Gewährleistung der wirksamen Löschung personenbezogener Daten**: 1) Vorhandensein einer schriftlichen Strategie und eines Standardverfahrens für die wirksame Löschung personenbezogener Daten nach Ablauf der Aufbewahrungsfrist, 2) Existenz automatisierter Verfahren zur Unterstützung der Löschung in allen Systemen, 3) Maßnahmen, mit denen die Löschung in Sicherheitskopien (sofern vorhanden) gewährleistet wird.

5. **Ihr Datenschutzbeauftragter und Sie**: In einem eigenen Abschnitt, bei dem der EDSB ausdrücklich darum gebeten hatte, die Beantwortung *nicht* dem DSB zu überlassen, forderte der EDSB Informationen darüber an, ob die Aufgaben des DSB

[44] Anders als bei früheren Umfragen verlangte der EDSB keine Kopien der tatsächlichen Bestandsverzeichnisse oder Register.
[45] Wo derartige Angaben noch feiner untergliedert (beispielsweise nach Generaldirektionen des Organs oder der Einrichtung) verfügbar sind, wurden die EU-Einrichtungen aufgefordert, diese Zahlen ebenfalls vorzulegen.
[46] Diese Frage bezog sich nicht auf anwendungsspezifische Sicherheitsstrategien.

in seiner Arbeitsplatzbeschreibung aufgeführt sind, ob die Wahrnehmung der Aufgaben des DSB in seine Leistungsbeurteilung einfließt, und wie der DSB in die Konzeption neuer Verarbeitungsvorgänge einbezogen wird.

Einen Überblick über die Antworten auf die Fragen 1 und 2 bietet eine vergleichende Tabelle (siehe weiter unten Abschnitt **Error! Reference source not found.** oben). Die Fragen 2 bis 5, die sich nicht leicht für eine quantitative Analyse anbieten, werden im Hauptteil dieses Berichts einer qualitativen Analyse unterzogen.

V. Anhang 2: Einige methodologische Einschränkungen

I. Eine Einrichtung, die nicht alle Verfahren identifiziert, bei denen es zur Verarbeitung personenbezogener Daten kommt, kann ein anscheinend besseres Einhaltungsergebnis aufweisen, als dies tatsächlich der Fall ist.

II. Bestandsverzeichnisse können bereits Verfahren mit Verarbeitungen enthalten, die von der Einrichtung identifiziert, jedoch noch nicht voll entwickelt wurden. Das Verfahren kann natürlich nicht vor seiner vollständigen Festlegung gemeldet werden. In der Berechnung taucht es jedoch als nicht gemeldete Verarbeitung auf und senkt damit das Maß der Einhaltung der Verordnung.

III. Eine Einrichtung kann in ihrem Bestandsverzeichnis eine künftige risikobehaftete Verarbeitung aufführen; da das zu dieser Verarbeitung gehörende Verfahren noch nicht ausreichend weit entwickelt ist, kann es nicht nach Artikel 27 gemeldet werden. In der Berechnung taucht dies als nicht gemeldete Verarbeitung auf und senkt damit das Maß der Einhaltung der Verordnung.

IV. Umgekehrt kann bei Einrichtungen, die viele weitere Verarbeitungsvorgänge identifizieren, die Meldungsquote sinken, selbst wenn sie sich um die Meldungen sehr bemühen. Dieser „Wettlauf nach oben“ wird dort erwähnt, wo er beobachtet wird.

V. Auch die Aktualisierung von Meldungen kann zu einem vorübergehenden Sinken der Meldungsquoten führen. Stellte der EDSB bei Meldungen gemäß Artikel 25 einen solchen Rückgang fest, forderte er Erläuterungen an; häufig handelt es sich um geringfügige Änderungen (so wird z. B. ein neuer Referatsleiter als Kontaktperson angegeben), weshalb sie als erledigt gezählt wurden, um nicht Einrichtungen zu bestrafen, die sich bemüht hatten, ihre Register auf dem neuesten Stand zu halten. Meldungen gemäß Artikel 27, bei denen Änderungen eine Aktualisierung oder gänzlich neue Meldungen an den EDSB erfordern, wurden als nicht erledigt erfasst. Wenn dies geschah, wird es im Bericht erwähnt.

VI. Der EDSB kann die Prüfung einer Meldung aussetzen, wenn zu eben diesem Verfahren gerade EDSB-Leitlinien ausgearbeitet werden. In der Berechnung taucht es jedoch als nicht gemeldete Verarbeitung auf und senkt damit das Maß der Einhaltung der Verordnung. Werden dem EDSB solche Verarbeitungen gemeldet, bevor die Leitlinien veröffentlicht werden, werden sie als gemeldet gezählt und es wird lediglich ihre Prüfung ausgesetzt.

VI. Anhang 3 - Gruppen von EU-Einrichtungen

Gruppe A (12): Organe und Einrichtungen, die vor 2004 gegründet wurden und vor der Einsetzung des EDSB bereits einen DSB bestellt hatten:
Europäische Kommission, Ausschuss der Regionen, Rat, Europäischer Rechnungshof, Europäische Zentralbank, Europäischer Gerichtshof, Europäischer Wirtschafts- und Sozialausschuss, Europäische Investitionsbank, Europäisches Parlament, OLAF, Europäischer Bürgerbeauftragter, Übersetzungszentrum für die Einrichtungen der Europäischen Union.

Gruppe B (17): Einrichtungen, die bis einschließlich 2004 gegründet wurden (oder bis dahin ihre Tätigkeit aufnahmen), einen DSB jedoch erst später bestellten:
CEDEFOP, CPVO, EASME, EASA, EDSB, EUA, EFSA, EIF, EMCDDA, EMA, EMSA, ENISA, ETF, EUROFOUND, FRA, HABM, EU-OSHA.

Gruppe C (18): Einrichtungen, die nach 2004, aber vor 2011 gegründet wurden (oder in diesem Zeitraum ihre Tätigkeit aufnahmen):
EFCA, EACEA, Chafea, ECDC, ECSEL (als Nachfolger von ARTEMIS und ENIAC), ERA, FRONTEX, GSA, INEA, Clean Sky JU, ECHA, ERCEA, F4E, FCH JU, IMI JU, REA, SESAR.

Gruppe D (15): Einrichtungen, die 2011 oder danach gegründet wurden (oder ihre Tätigkeit aufnahmen), sowie frühere Einrichtungen des zweiten und dritten Pfeilers:
ACER, GEREK, EASO, EBA, EIOPA, EIGE, EIT, ESMA, ESRB, EAD, eu-LISA, CEPOL, EDA, EUISS, EUSC.

VII. Anhang 4: Liste der Abkürzungen der Einrichtungen

ACER	Agentur für die Zusammenarbeit der Energieregulierungsbehörden
AdR	Ausschuss der Regionen
CdT	Übersetzungszentrum für die Einrichtungen der Europäischen Union
Cedefop	Europäisches Zentrum für die Förderung der Berufsbildung
CEPOL	Europäische Polizeiakademie
Chafea	Exekutivagentur für Verbraucher, Gesundheit und Lebensmittel
Clean Sky JU	Gemeinsames Unternehmen Clean Sky
CPVO	Gemeinschaftliches Sortenamt
EACEA	Exekutivagentur Bildung, Audiovisuelles und Kultur
EAD	Europäischer Auswärtiger Dienst
EASA	Europäische Agentur für Flugsicherheit
EASME	Exekutivagentur für kleine und mittlere Unternehmen
EASO	Europäisches Unterstützungsbüro für Asylfragen
EBA	Europäische Bankenaufsichtsbehörde
ECDC	Europäisches Zentrum für die Prävention und die Kontrolle von Krankheiten
ECHA	Europäische Chemikalienagentur
ECSEL JU	Gemeinsames Unternehmen ECSEL
EDA	Europäische Verteidigungsagentur
EDSB	Europäischer Datenschutzbeauftragter
EFCA	Europäische Fischereiaufsichtsagentur
EFSA	Europäische Behörde für Lebensmittelsicherheit
EIB	Europäische Investitionsbank
EIF	Europäischer Investitionsfonds
EIGE	Europäisches Institut für Gleichstellungsfragen
EIOPA	Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung
EIT	Europäisches Innovations- und Technologieinstitut
EK	Europäische Kommission
EMA	Europäische Arzneimittelagentur
EMCDDA	Europäische Beobachtungsstelle für Drogen und Drogensucht
EMSA	Europäische Agentur für die Sicherheit des Seeverkehrs
ENISA	Europäische Agentur für Netz- und Informationssicherheit
EP	Europäisches Parlament
ERA	Europäische Eisenbahnagentur
ERCEA	Exekutivagentur des Europäischen Forschungsrates
ERH	Europäischer Rechnungshof
ESRB	Europäischer Ausschuss für Systemrisiken
ESMA	Europäische Wertpapier- und Marktaufsichtsbehörde
ETF	Europäische Stiftung für Berufsbildung
EUA	Europäische Umweltagentur
EuGH	Gerichtshof der Europäischen Union
EUISS	Institut der Europäischen Union für Sicherheitsstudien
eu-LISA	Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts
EU-OSHA	Europäische Agentur für Sicherheit und Gesundheitsschutz am Arbeitsplatz
EUROFOUND	Europäische Stiftung zur Verbesserung der Lebens- und Arbeitsbedingungen
EUSC	Satellitenzentrum der Europäischen Union
EWSA	Europäischer Wirtschafts- und Sozialausschuss
EZB	Europäische Zentralbank
FCH-JU	Gemeinsames Unternehmen Brennstoffzellen und Wasserstoff
F4E	Fusion For Energy
FRA	Agentur der Europäischen Union für Grundrechte
Frontex	Europäische Agentur für die operative Zusammenarbeit an den Außengrenzen der Mitgliedstaaten der Europäischen Union
GEREK	Gremium Europäischer Regulierungsstellen für elektronische Kommunikation
GSA (GNSS)	Agentur für das Europäische GNSS
IMI JU	Gemeinsames Unternehmen zur Umsetzung der gemeinsamen Technologieinitiative für innovative Arzneimittel
INEA	Exekutivagentur für Innovation und Netze
HABM	Harmonisierungsamt für den Binnenmarkt (Marken, Muster und Modelle)
OLAF	Europäisches Amt für Betrugsbekämpfung
Ombudsman	Europäischer Bürgerbeauftragter
Rat	Rat der Europäischen Union
REA	Exekutivagentur für die Forschung
SESAR JU	Gemeinsames Unternehmen SESAR