



DER EUROPÄISCHE  
DATENSCHUTZBEAUFTRAGTE

# EDSB Newsletter

Nr. 40 | Dezember 2013

## IN DIESER AUSGABE

### SCHLAGLICHTER

- 1 Privatsphäre und Datenschutz können das Verbrauchervertrauen in die digitale Gesellschaft wiederherstellen
- 1 TEN-T EA: Hinweisgeber müssen geschützt werden

### AUFSICHT

- 2 Leitlinien über Urlaub und Gleitzeit: Meldungen zu Datenverarbeitungsvorgängen
- 2 *Ex-post*-Vorabkontrollen: Abbau von Altfällen
- 2 Einrichtung der Investigative Data Consultation Platform

### BERATUNG

- 3 Garantien für das eCall-System sind dringend vonnöten
- 3 PNR-Abkommen zwischen der EU und Kanada: kein Abflug ohne Verbesserungen des Datenschutzes
- 3 Kontrolle der Datenschutzrisiken bei der elektronischen Rechnungsstellung
- 3 Die Besteuerung sollte nicht auf Kosten von Datenschutz und Transparenz gehen

### IT POLICY

- 4 Risikobeurteilung und Sicherheitsmaßnahmen bei EU-Einrichtungen
- 4 Gedanken zur Sicherheit: Internetdesigner wehren sich gegen Überwachung
- 4 LinkedIn *Intro*: Vorsicht bei der Verbindung!

### VERANSTALTUNGEN

- 5 Sitzung der DSB

### VORTRÄGE UND VERÖFFENTLICHUNGEN

### BEHÖRDLICHE DATENSCHUTZBEAUFTRAGTE

## SCHLAGLICHTER

### Privatsphäre und Datenschutz können das Verbrauchervertrauen in die digitale Gesellschaft wiederherstellen

Der Vorschlag der Europäischen Kommission zur Vereinheitlichung von Telekommunikationsdienstleistungen in der EU wird die Freiheit des Internets unangemessen einschränken, so der Europäische Datenschutzbeauftragte (EDSB).

**Eine Überwachung und Einschränkung der Aktivitäten von Nutzern im Internet darf nur geschehen, um einen gezielten,**

**spezifischen und legitimen Zweck zu erreichen. Die breit angelegte Überwachung und Einschränkung von Kommunikation über das Internet in diesem Vorschlag widerspricht dem EU-Datenschutzrecht und der Charta der Grundrechte der Europäischen Union. Ein solcher Eingriff in die Rechte auf Datenschutz, Vertraulich-**

**keit der Kommunikation und Privatsphäre wird wenig dazu beitragen, das Verbrauchervertrauen in den Markt für elektronische Kommunikation in Europa wiederherzustellen.**

Peter Hustinx, EDSB

[Stellungnahme des EDSB](#)

[Pressemitteilung des EDSB](#)

### TEN-T EA: Hinweisgeber müssen geschützt werden



European  
Commission

Trans-European  
Transport Network  
Executive Agency

Nach Maßgabe des Statuts der Beamten der Organe und Einrichtungen der EU sind Beamte, die Kenntnis von Sachverhalten erhalten, die rechtswidrige Handlungen, einschließlich Betrug oder Korruption, vermuten lassen, verpflichtet, ihre Vorgesetzten zu unterrichten. Damit Mitarbeiter mutmaßliche rechtswidrige Handlungen sicher und vertraulich melden können, haben die Organe und Einrichtungen der EU ein Verfahren zum Schutz von Hinweisgebern eingerichtet. In unserer Stellungnahme vom 28. Oktober 2013 haben wir einen von der Exekutivagentur für das trans-europäische Verkehrsnetz (TEN-T

EA) ausgearbeiteten Entwurf für ein solches Verfahren vor dessen Annahme analysiert und folgende Empfehlungen abgegeben:

- unnütze und irrelevante Angaben von Hinweisgebern sollten nicht länger als erforderlich aufbewahrt werden;
- personenbezogene Daten, die verarbeitet werden, sollten auf solche Daten beschränkt werden, die zur Überprüfung der Behauptungen unbedingt erforderlich sind;
- die vertrauliche Behandlung der Identität von Hinweisgebern sollte automatisch und nicht nur auf Antrag gewahrt werden; und

- der Grundsatz der Vertraulichkeit sollte im weiten Wortsinne und umfassend und nicht nur in Bezug auf beschuldigte Personen angewandt werden.

Wir haben es begrüßt, wie das Verfahren zur Meldung von Missständen auf die Informationen hinweist, die für den Anwendungsbereich des Verfahrens relevant bzw. irrelevant sind, zugleich jedoch die Bedeutung der Einführung strengerer Einschränkungen sowie der Vertraulichkeit der Daten zum Schutz von Hinweisgebern unterstrichen. Die TEN-T EA hat das Verfahren entsprechend unseren Kommentaren finalisiert.

[Stellungnahme des EDSB](#)

## Leitlinien über Urlaub und Gleitzeit: Meldungen zu Datenverarbeitungsvorgängen

Im Dezember 2012 haben wir Leitlinien über Urlaub und Gleitzeit vorgelegt. In ihnen hat der EDSB die Organe und Einrichtungen der EU aufgefordert, Verarbeitungsvorgänge zu melden, die noch nicht analysiert wurden, um eine sachgerechte Umsetzung der datenschutzrechtlichen Anforderungen im Rahmen von Verarbeitungsvorgängen in Zusammenhang mit Urlaub und Gleitzeit zu gewährleisten. Seitdem sind bei uns 47 Meldungen zu einer ganzen Reihe von Verarbeitungsvorgängen eingegangen. Darauf haben wir mit Kurzstellungsmaßnahmen

reagiert, die sich auf die Bereiche beschränken, in denen die Verarbeitungsvorgänge von den bereits vorliegenden Leitlinien abweichen.

Unsere Analyse dieser Meldungen hat ergeben, dass das Hauptanliegen bei allen Verarbeitungen die Dauer der Vorratsspeicherung der erhobenen Daten ist. Ein weiteres Problem betraf die Datenschutzklausel, die von Personalverantwortlichen unterzeichnet werden muss. Diese Klausel bezieht sich speziell auf die Verarbeitung von Gesundheitsdaten, und wir haben darauf bestanden, dass

die betreffenden Mitarbeiter eine Geheimhaltungserklärung unterzeichnen. Außerdem haben wir darauf verwiesen, wie wichtig es ist, Mitarbeitern und ihren Familienangehörigen einschlägige Informationen zu den Vorgängen an die Hand zu geben, falls dabei auch ihre personenbezogenen Daten verarbeitet werden.

Wir haben, von wenigen Ausnahmen abgesehen, auf alle Meldungen geantwortet, die wir auf unserer Website bereits veröffentlicht haben bzw. derzeit veröffentlichen.

*Leitlinien des EDSB*



## Ex-post-Vorabkontrollen - Abbau von Altfällen

Ex-post-Vorabkontrollen umfassen sowohl Vorgänge, bereits angelaufen sind, als auch Verarbeitungsvorgänge, die vor dem 17. Januar 2004 (Ernennung des ersten EDSB und des stellvertretenden EDSB) bzw. vor Inkrafttreten der [Verordnung](#) angelaufen sind. Als der EDSB sein Amt antrat, gab es einen Nachholbedarf bei Ex-post-Vorabkontrollen. Da die Organe und Einrichtungen der EU jetzt

genügend Zeit für die Meldung ihrer vorhandenen Verarbeitungsvorgänge hatten, haben wir sie gebeten, dafür Sorge zu tragen, dass uns alle noch ausstehenden Verarbeitungsvorgänge bis Ende Juni 2013 gemeldet werden. Für bestimmte Aktivitäten, die von den erst vor kurzem errichteten Organen wahrgenommen wurden und die unmöglich im Vorfeld gemeldet werden konnten, etwa

bei Einstellungsverfahren, wurde eine Ausnahme gemacht. Infolge dieser Frist gingen zwischen Anfang Juni 2012 und Ende Juli 2013 180 Meldungen bei uns ein. Im Jahr 2013 wurde in 29 Fällen befunden, dass keine Vorabkontrolle erforderlich war, im Unterschied zu den acht Fällen, die 2012 unnötigerweise vorgelegt wurden.



## Einrichtung der Investigative Data Consultation Platform

Die Investigative Data Consultation Platform (IDCP) ist eine Projektdatenbank, die den Austausch von Informationen über Ermittlungen zur Betrugsbekämpfung zwischen dem OLAF und seinen internationalen Partnerbehörden fördern soll. Sobald sie funktionsfähig ist, wird die IDCP den Nutzern die Möglichkeit bieten zu überprüfen, ob in den Dateien der Partner bestimmte Informationen enthalten sind, etwa die Namen von Personen, gegen die ermittelt wird, Telefonnummern, Anschriften usw.

In unserer Stellungnahme haben wir eine Reihe von Empfehlungen abgegeben, u. a.:

- die Gewährleistung vorschriftsgemäßer Zugangsrechte für betroffene Personen;

- die Verkürzung der Speicherfrist für die Vorratsdatenspeicherung; und
- die Gewährleistung der Datenqualität.

Da die Aktivitäten der IDCP strukturelle Übertragungen personenbezogener Daten gemäß Artikel 9 der [Verordnung](#) (EG) Nr. 45/2001 zur Folge haben, kann das System ohne eine separate Genehmigung durch den EDSB gemäß Artikel 9 Absatz 7 der Verordnung nicht in Betrieb gehen. Daher wird die IDCP erst aktiviert werden, wenn der EDSB eine solche Genehmigung erteilt.

*Stellungnahme des EDSB*



## Garantien für das eCall-System sind dringend vonnöten

Das 112-eCall-System ist eine Initiative, mit der Autofahrern rasche Hilfe bei Zusammenstößen oder Unfällen innerhalb der Europäischen Union bereitgestellt werden soll. In unserer Stellungnahme vom 29. Oktober 2013 zum *Vorschlag der Kommission für eine Verordnung über Anforderungen für die Typengenehmigung zur Einführung des eCall-Systems* haben wir auf das potenzielle Eindringen des Systems

in die Privatsphäre hingewiesen. Zwar haben wir es begrüßt, dass in der Verordnung Bestimmungen zu wesentlichen Datenschutzgarantien enthalten ist, doch haben wir auch nachdrücklich die Aufnahme zusätzlicher Garantien verlangt. Ab dem 1. Oktober 2015 müssen alle neuen Fahrzeuge mit eCall-Systemen ausgerüstet werden. Von dieser breit angelegten Einführung wird erwartet, dass die

Funktionen der eCall-Technologieplattform (Ortungs-, Verarbeitungs- und Kommunikationsmodule) *kommerziell genutzt* werden (etwa moderne Versicherungen, Ortung gestohlener Fahrzeuge, elektronische Mautsysteme (eTolling)). Da dies mit Datenschutzrisiken verbunden ist, haben wir auf die Notwendigkeit entsprechender Datenschutzgarantien verwiesen.

[Stellungnahme des EDSB](#)



## Kontrolle der Datenschutzrisiken bei der elektronischen Rechnungsstellung

In der gesamten Europäischen Union verlangen Stellen, die öffentliche Ausschreibungen durchführen, zunehmend, dass die Rechnungsstellung elektronisch erfolgen soll. Die Normen und Standards zu Inhalt, Format, Layout, technischen Anforderungen und anderen Aspekten der Rechnungsstellung unterscheiden sich jedoch von Mitgliedstaat zu Mitgliedstaat erheblich. *Der Vorschlag der Kommission für eine Richtlinie über die elektronische Rechnungsstellung bei öffentlichen Aufträgen* zielt darauf ab, die Nutzung der elektronischen Rechnungsstellung zu fördern und die Interoperabilität zwischen den Mitgliedstaaten zu verbessern. In unserer Stellungnahme vom 11. November 2013 zu diesem

Vorschlag haben wir auf die erhöhten Risiken für Privatsphäre und Datenschutz bei der papierlosen und maschinenlesbaren Bereitstellung von Rechnungsdaten verwiesen. Wir haben diesen Schritt auf dem Weg zu einer papierlosen elektronischen Rechnungsstellung zwar begrüßt, zugleich jedoch darauf hingewiesen, dass Fragen wie etwa die unzulässige Nutzung personenbezogener Daten für die automatische Profilerstellung oder die Data Mining unbedingt Beachtung geschenkt werden muss. Solche Verwendungsmöglichkeiten sind kaum mit den Datenschutzrechten vereinbar bzw. würden weitere Garantien erforderlich machen.

[Stellungnahme des EDSB](#)



## PNR-Abkommen zwischen der EU und Kanada: kein Abflug ohne Verbesserungen des Datenschutzes

Die *Vorschläge für Beschlüsse des Rates über das Abkommen zwischen Kanada und der EU über die Übermittlung und Verarbeitung von Fluggastdatensätzen*

(*Passenger Name Records – PNR*) werfen Fragen zur Notwendigkeit und Verhältnismäßigkeit auf. In unserer Stellungnahme vom 30. September 2013 haben wir

die Notwendigkeit und den Umfang von PNR-Registern und der massenhaften Übertragung von PNR-Daten erneut in Frage gestellt. Ebenso haben wir die Rechtsgrundlage für das Abkommen hinterfragt und unserer Besorgnis Ausdruck verliehen, dass

es für Unionsbürger offenbar keine unabhängige Möglichkeit gibt, Rechtsbehelf einzulegen. Wir haben Empfehlungen zu mehreren Themen abgegeben wie z. B.:

- den Ausschluss der Verarbeitung sensibler Daten;
- eine kürzere und angemessene Dauer für die Vorratsdatenspeicherung;
- eine beschränkte Zahl von PNR-Datenkategorien, die verarbeitet werden; und
- die ausdrückliche Erwähnung der unabhängigen Behörde als Aufsichtsbehörde.

[Stellungnahme des EDSB](#)



## Die Besteuerung sollte nicht auf Kosten von Datenschutz und Transparenz gehen

Die Kommission plant eine Änderung ihrer *Richtlinie bezüglich der Verpflichtung zum automatischen Austausch von Informationen im Bereich der Besteuerung* mit dem Ziel, den Geltungsbereich dieser Richtlinie auf weitere Kategorien von Daten wie z. B. Dividenden, Veräußerungsgewinne, sonstige Finanzerträge und Kontensalden zu erweitern. Mit dieser Erweiterung soll ein Beitrag zur Gleichbehandlung verschiedener Arten von Vermögensgegenständen geleistet werden. In unserem Schreiben an die Kommission haben wir empfohlen, dass die Art der betroffenen personenbezogenen Daten und die Zwecke des

Austauschs dieser Daten genauer definiert werden sollen. Außerdem haben wir unserer Besorgnis darüber Ausdruck verliehen, dass sowohl in der derzeit gültigen Richtlinie als auch in dem neuen Richtlinienvorschlag keine Bestimmungen darüber enthalten sind, wie der Grundsatz der Transparenz praktisch umgesetzt werden soll. Wir haben den Gesetzgeber dringend dazu aufgefordert, in diesem neuen Vorschlag auch Fragen wie z. B. die Definition der Arten der betroffenen personenbezogenen Daten, der Transparenz, der Erforderlichkeit und der Verhältnismäßigkeit zu prüfen.

[Anmerkungen des EDSB](#)





## Risikobeurteilung und Sicherheitsmaßnahmen bei EU-Einrichtungen

Die aktuellen Enthüllungen über Überwachungs- und Spionagetätigkeiten von Nachrichtendiensten in Mitgliedstaaten und Drittländern legen den Schluss nahe, dass die elektronische Kommunikation von Einrichtungen und Delegationen der EU ein Ziel war. Es gibt weiterhin Befürchtungen, dass einige Sicherheits- und Verschlüsselungswerkzeuge auf dem Markt absichtlich geschwächt wurden, um die Überwachung zu vereinfachen.

Angesichts dieser Bedenken möchte der EDSB überprüfen, ob die EU-Einrichtungen die Risikobeurteilung in Bezug auf ihre Datenschutzmaßnahmen nach wie vor für sachgemäß und die derzeitigen Sicherheitsmaßnahmen für angemessen erachten. Zu diesem Zweck treffen wir uns mit dem Europäischen Parlament, der Kommission und dem Rat, um mehr über ihre Reaktion auf die Enthüllungen sowie über die nächsten Schritte zu erfahren.



## Gedanken zur Sicherheit: Internetdesigner wehren sich gegen Überwachung

Die Internet Engineering Task Force (IETF), die Einrichtung, die die Standards konzipiert, nach denen das Internet funktioniert, ist vom 3. bis 8. November 2013 in Vancouver zusammengekommen, um Möglichkeiten zur Verbesserung des Stands der Technik bei der Internetsicherheit zu erarbeiten. Anfang September erschien in *The Guardian* ein

*Artikel* von Bruce Schneier, einem bekannten Kryptographen, Sicherheitsexperten und Buchautor, der Internettechniker aufforderte, tätig zu werden und diese Zusammenkunft dem Thema der allgegenwärtigen Überwachung zu widmen. Offenkundig hatten auch die Internettechniker von der allgegenwärtigen Überwachung genug. Nach den Enthül-

lungen dieses Sommers in Bezug auf die NSA gelangte die IETF, die der Botschaft von Bruce Schneier Gehör geschenkt hatte, zu dem Schluss, dass die allgegenwärtige Überwachung als ein technischer Angriff gewertet werden musste, und stimmte einer Erweiterung der IETF-Standards zu. Dies ist nur einer von vielen Schritten, die in der Internetgemeinde im weiteren

Sinne eingeleitet wurden, um massive technische Gegenmaßnahmen gegen diese Art von Überwachung zu ergreifen. Doch ist die Entwicklung und Veröffentlichung angemessener technischer Spezifikationen nur der erste Schritt, denn diese müssen umgesetzt und anschließend flächendeckend angewandt werden, wenn die Privatsphäre im Internet tatsäch-

lich besser geschützt werden soll. Dies dürfte Zeit kosten und erfordert auch die Beteiligung anderer Interessengruppen.

Mehr darüber:

[„Leading Engineers Agree to Upgrade Standards to Improve Internet Privacy and Security“](#)

[„Pervasive Monitoring is an Attack“](#)



### LinkedIn *Intro*: Vorsicht bei der Verbindung!

Die professionelle Website des sozialen Netzwerks LinkedIn hat *Intro* eingeführt, eine neue Anwendung für iOS-Apple-Produkte. Bei dieser Anwendung, mit der Nutzer in ihren Mailanwendungen auf ihrem iPhone oder iPad LinkedIn-Profil einsehen können, werden die E-Mails der Nutzer über LinkedIn-Server umgeleitet. Dort werden Metadaten zum LinkedIn-Profil in die E-Mails eingefügt, die *Intro*-Nutzer erhalten, und das Unternehmen gewährt sich im Wesentlichen selbst Zugang

zu allen E-Mails. Der EDSB zeigt sich besorgt über die Risiken, die diese Anwendung für die Privatsphäre mit sich bringt, da die E-Mails von *Intro*-Nutzern preisgegeben werden; daher empfehlen wir Ihnen dringend, die App nicht auf Ihrem Apple-Gerät zu installieren.

Sie können mehr über die Anwendung *Intro* von LinkedIn in zwei Sicherheitsblogs einer Sicherheitsgruppe (Drittpartei) erfahren, wenn Sie [hier](#) und [hier](#) klicken.

[Leitfaden zum Deinstallieren von Intro](#), [LinkedIn FAQs](#) und [Datenschutzzerklärung](#).





# VERANSTALTUNGEN

## Sitzung der DSB

Vom 20. bis 22. November 2013 fand in Brüssel die 34. halbjährliche Sitzung behördlichen Datenschutzbeauftragten (DSB) der EU-Organe und Einrichtungen statt, die erstmals vom EDSB ausgerichtet wurde. Schwerpunktthema waren die Entwicklungen des Datenschutzes auf europäischer und internationaler Ebene, wobei die Reform des EU-Datenschutzrechts und die Rolle der DSB im Mittelpunkt standen. Der Direktor der Direktion C „Grundrechte und Unionsbürgerschaft“ der GD

Justiz der Kommission, Herr Paul Nemitz, hielt einen Vortrag für das Netzwerk der DSB. Außerdem fand ein Workshop zum Thema Datenschutz und Transparenz statt, der Anlass für eine ausführliche und ergiebige Diskussion war. Der EDSB berichtete der Gruppe den aktuellen Sachstand in vielen seiner Tätigkeitsbereiche, einschließlich Vorabkontrollverfahren, Leitlinien, erste Rückmeldungen zu unserer allgemeinen Umfrage Erhebung 2013 und Informationen Dritter bei Beschwerden. Die Sitzung

war aber auch ein nützliches Diskussionsforum über unsere zukünftigen Leitlinien zu Interessenkonflikten, an der viele DSB begeistert teilnahmen.

Alle DSB waren bereit, ihre wertvollen Ansichten und ihre Erfahrungen aus erster Hand in Datenschutzfragen auszutauschen. Dies hat zweifellos zu dem positiven Feedback und zum Erfolg der Sitzung beigetragen.



## VORTRÄGE UND VERÖFFENTLICHUNGEN

- Rede ([pdf](#)) von Giovanni Buttarelli in Budapest, „Data Protection in the Judiciary: The Challenges for Modern Management“ (24. Oktober 2013)



## BEHÖRDLICHE DATENSCHUTZBEAUFTRAGTE

### Aktuelle Ernennungen:

- Herr Gabriele Borla, Europäische Verteidigungsagentur (EDA)
- Herr Nikolaos Chatzimichalakis, Institut der Europäischen Union für Sicherheitsstudien (EUISS)
- Herr Andrej Gras, Europäische Agentur für die operative Zusammenarbeit an den Außengrenzen der Mitgliedstaaten der Europäischen Union (FRONTEX)
- Herr Luca Zampaglione, ad interim, eu-LISA



*Best wishes*

*Meilleurs vœux*

*Frohes Fest*



## Über diesen Newsletter

Dieser Newsletter wird vom Europäischen Datenschutzbeauftragten herausgegeben – einer unabhängigen Behörde der EU, die im Jahr 2004 errichtet wurde und folgende Aufgaben hat:

- Überwachung der Verarbeitung personenbezogener Daten durch die EU-Verwaltung;
- Beratung zu Rechtsvorschriften im Bereich des Datenschutzes;
- Zusammenarbeit mit vergleichbaren Behörden, um einen kohärenten Datenschutz sicherzustellen.

Sie können diesen Newsletter über unsere Website abonnieren / abbestellen.

### KONTAKT

www.edps.europa.eu  
Tel: +32 (0)2 2831900  
Fax: +32 (0)2 2831950  
NewsletterEDPS@edps.europa.eu

### POSTANSCHRIFT

EDSB  
Rue Wiertz 60 – MTS Gebäude  
B-1047 Brüssel  
BELGIEN

### DIENSTSTELLE

Rue Montoyer 30  
B-1000 Brüssel  
BELGIEN

🐦 Folgen Sie uns auf Twitter:  
@EU\_EDPS

© Fotos: iStockphoto/EDSB und Europäische Union.

**EDSB – Der europäische Hüter des Datenschutzes**