



Stellungnahme zur Vorabkontrolle

**„Umgang mit Ereignisberichten – Gerichtshof“
Fall 2013-0786**

Der Gerichtshof hat einen Sicherheitsdienst mit der Erstellung von Ereignisberichten zu allen Unregelmäßigkeiten, Funktionsstörungen, Maßnahmen zur Personenrettung oder Problemen betreffend die Sicherheit oder den Schutz von Personen sowie von beweglichen und unbeweglichen Gütern auf dem Gelände des Gerichtshofs beauftragt. Diese Berichte können personenbezogene Daten enthalten, z. B. betreffend Personen, die Opfer eines Unfalls, eines Brands oder von Unwohlsein waren oder aber bei einem Diebstahl in den Räumlichkeiten des Gerichtshofs überrascht wurden.

Brüssel, den 12. September 2016

1. Verfahren

Am 27. Juni 2013 erhielt der Europäische Datenschutzbeauftragte (nachfolgend „**der EDSB**“) vom Gerichtshof der Europäischen Union (nachfolgend „**der Gerichtshof**“) eine Meldung für eine Vorabkontrolle gemäß Artikel 27 Absatz 2 Buchstabe a der Verordnung (EG) Nr. 45/2001 (nachfolgend „**die Verordnung**“) betreffend den Umgang mit Ereignisberichten.

Der Meldung waren die folgenden Anhänge beigelegt:

- eine Beschreibung der Sicherheitsmaßnahmen;
- das Informationsblatt zur Verarbeitung von personenbezogenen Daten;
- die Bestimmungen des Großherzogtums Luxemburg vom 16. Oktober 1997 über den Schutz der Arbeitnehmer – Standardsicherheitsvorschriften (ITM-ET 32.10) (nachfolgend „**die Bestimmungen ITM-ET**“);
- ein Auszug aus dem Bewachungsvertrag Nr. CJ-03/2010¹.

Zwischen dem Gerichtshof und dem EDSB fand mehrmals Schriftverkehr statt. Am 16. März 2016 wurden dem EDSB zusätzliche Unterlagen² und eine geänderte Meldung übermittelt.

Da es sich um eine *nachträgliche* Vorabkontrolle handelt, findet die Frist von zwei Monaten, in der der EDSB grundsätzlich seine Stellungnahme abgeben muss, keine Anwendung³.

2. Sachverhalt

2010 schloss der Gerichtshof mit einem Sicherheitsdienst einen Vertrag über Dienstleistungen in Bezug auf die allgemeine Sicherheit und den Brandschutz. Die Mitarbeiter des besagten Sicherheitsdienstes sind in diesem Rahmen verpflichtet, **Ereignisberichte** zu allen Unregelmäßigkeiten, Funktionsstörungen, Maßnahmen zur Personenrettung oder Problemen betreffend die Sicherheit oder den Schutz von Personen sowie von beweglichen und unbeweglichen Gütern auf dem Gelände des Gerichtshofs zu erstellen. Diese Berichte werden innerhalb von 24 Stunden per E-Mail an das Referat Sicherheit und Schutz weitergeleitet (das an die Direktion Gebäude des Gerichtshofs angeschlossen ist). Am Morgen eines jeden Werktags wird eine Zusammenfassung der Berichte der letzten 24 Stunden erstellt und per E-Mail an das Referat Sicherheit und Schutz übermittelt. Jedes Jahr werden etwa 1 500 bis 2 000 Ereignisberichte verfasst.

¹ Der Gerichtshof legte nachträglich alle maßgeblichen Bewachungsverträge in Kopie vor: Vertrag Nr. CJ-03/2010 für den Zeitraum vom 16.12.2010 bis zum 15.07.2015 und Vertrag Nr. CJ 12-2014 für den Zeitraum vom 16.07.2015 bis zum 15.07.2020.

² Vorlage für den Ereignisbericht; Vorlage für den zusammenfassenden Bericht; Auszug aus dem Lastenheft für Leistungen des Sicherheitsdienstes.

³ Der EDSB übermittelte dem DSB am 18. Dezember 2013 mehrere Fragen und am 16. Oktober 2015 einen Hinweis und einen Entwurf der Darlegung des Sachverhalts. Der DSB antwortete am 16. November 2015. Der Entwurf der Stellungnahme wurde am 16. Juni 2016 an den DSB des Gerichtshofs versandt. Der Gerichtshof teilte seine Anmerkungen am 5. August 2016 mit.

2.1. Rechtsgrundlage und Rechtmäßigkeit der Verarbeitung

Laut dem Gerichtshof hat die Verarbeitung die folgenden **Rechtsgrundlagen**:

- Artikel 26 der Bestimmungen ITM-ET (ITM = luxemburgische Gewerbeaufsicht); diese Vorschrift betrifft die Sicherheitseinrichtungen (Vorrichtungen für Brandschutz und Überwachung der Luft, Gasmelder usw.) und die Pflicht zur Führung von Aufzeichnungen zu den Kontrollen, denen diese Einrichtungen unterzogen werden;
- Artikel 4.2 des Lastenhefts für Leistungen des Sicherheitsdienstes „GS4 Security Services“; diese Vorschrift verpflichtet den Sicherheitsdienst, (i) ein System zur elektronischen Verwaltung und Überwachung der Ereignisberichte zu nutzen und (ii) dem Gerichtshof alle von diesem angeforderten Tätigkeitsberichte vorzulegen.

Die ursprüngliche Meldung bezog sich außerdem auf den „*Leitplan zur allgemeinen Sicherung des Gebäudekomplexes des Gerichtshofs der EU*“. Dieses Dokument wird in der aktualisierten Meldung nicht mehr erwähnt⁴.

Die **Rechtmäßigkeit** der Verarbeitung basiert auf Artikel 5 Buchstabe a und Artikel 10 Absatz 2 Buchstabe b der Verordnung.

2.2. Betroffene Personen

Betroffen sind Personen, die in einen Unfall in den Gebäuden oder der unmittelbaren Umgebung des Gerichtshofs verwickelt sind, und zwar unabhängig davon, ob es sich um Mitarbeiter des Gerichtshofs handelt oder nicht.

2.3. Datenkategorien

Die **Ereignisberichte** können die folgenden personenbezogenen Daten enthalten:

- persönliche Angaben der in den Unfall verwickelten Personen (Name und Vorname, Telefon- und Faxnummer, E-Mail-Adresse);
- Informationen aus den Ausweisdokumenten dieser Personen (Reisepass, Führerschein usw.);
- Angaben zur Art des Zwischenfalls (Unfall, Diebstahl, Personenrettung, Gesundheitszustand des Opfers, Verdacht auf eine Straftat usw.);
- Fahrzeugkennzeichen;
- Ort, Datum, Uhrzeit und Ursache des Zwischenfalls;
- festgestellte Schäden und vorläufige Maßnahmen.

Neben den Ereignisberichten erstellt der Sicherheitsdienst am Morgen eines jeden Werktags eine **Zusammenfassung** der Berichte der letzten 24 Stunden und ordnet diese dabei nach fünf Kategorien:

- technische Störungen;
- Zwischenfälle in Bezug auf den Brandschutz;
- Sicherheitsprobleme;
- Maßnahmen zur Personenrettung;
- Sonstiges.

⁴ Siehe die E-Mail des DSB des Gerichtshofs vom 16. März 2016.

Diese Zusammenfassung besteht aus einer Tabelle, in der die Zahl der Zwischenfälle je Kategorie, der Gegenstand und die Nummer eines jeden Berichts sowie eventuelle Anmerkungen angegeben sind.

2.4. Empfänger der Daten

Die Ereignisberichte und die Berichtszusammenfassungen werden auf elektronischem Weg (E-Mail) im PDF-Format übermittelt.

Die **Empfänger** dieser Daten sind:

- die Beamten und Mitarbeiter des Referats Sicherheit und Schutz des Gerichtshofs⁵;
- der Leiter der Direktion Gebäude;
- die für die Sicherheit verantwortlichen Mitarbeiter des Sicherheitsdienstes;
- die luxemburgischen Verwaltungs- und Strafbehörden, damit diese ihre Befugnisse im Rahmen der Strafverfolgung ausüben können (Empfänger gemäß den nationalen Gesetzen, die in Anwendung der Richtlinie 95/46/EG verabschiedet wurden). Das Referat Sicherheit und Schutz kann die Berichte entsprechend der Tragweite des jeweiligen Zwischenfalls an diese Behörden weiterleiten.

In Sonderfällen können die Daten auch an andere Empfänger übermittelt werden⁶.

2.5. Informationen für die betroffenen Personen

Mitarbeiter des Gerichtshofs: ein Informationsblatt⁷ und die Meldung zur Verarbeitung sind im Intranet des Gerichtshofs verfügbar.

Andere Personen: das Informationsblatt ist auf der Website des Gerichtshofs nicht verfügbar⁸. Bei den Sicherheitsmitarbeitern am Empfang kann eine Papierversion des Informationsblatts öffentlich eingesehen werden.

⁵ Die in der ursprünglichen Meldung erwähnte Abteilung Gebäude und Sicherheit des Gerichtshofs wurde inzwischen abgeschafft. Das Referat Sicherheit und Schutz ist von nun an direkt an die Direktion Gebäude angeschlossen.

⁶ - an den Präsidenten und den Kanzler des Gerichtshofs sowie die diese unterstützenden Beamten im Rahmen ihrer jeweiligen Zuständigkeiten gemäß Artikel 20 Absatz 4 der Verfahrensordnung des Gerichtshofs;

- an den Gerichtshof, das Gericht und/oder das Gericht für den öffentlichen Dienst oder einen nationalen Richter sowie die Anwälte und Bevollmächtigten der Parteien im Fall eines Rechtsstreits;
- an die für die Prüfung von Beschwerden zuständige Instanz des Gerichtshofs, des Gerichts oder des EUGöD, den Präsidenten und den Kanzler des betroffenen Gerichts sowie den Rechtsberater für Verwaltungsangelegenheiten im Fall einer Beschwerde gemäß Artikel 90 Absatz 2 des Beamtenstatuts;
- an das OLAF im Fall einer Untersuchung in Anwendung der Verordnung (EU, Euratom) Nr. 883/2013 und des Beschlusses des Gerichtshofs vom 12. Juli 2011 über die Bedingungen und Modalitäten der internen Untersuchungen zur Bekämpfung von Betrug, Korruption und sonstigen rechtswidrigen Handlungen zum Nachteil der Interessen der Europäischen Union;
- an den internen Prüfer im Rahmen seiner Aufgaben gemäß Artikel 98 und 99 der Verordnung (EU, Euratom) Nr. 966/2012 über die Haushaltsordnung;
- an den EDSB gemäß Artikel 47 Absatz 2 der Verordnung;
- an den DSB des Gerichtshofs gemäß Punkt 4 des Anhangs der Verordnung;
- an den Europäischen Bürgerbeauftragten im Rahmen von Artikel 228 AEUV.

⁷ Im Anhang zur Meldung.

⁸ Erläuterung des DSB in einer E-Mail vom 5. August 2016.

2.6. Speicherung, Sicherheitsmaßnahmen und Dauer der Datenaufbewahrung

[...]

Die **Aufbewahrungsdauer** der Berichte beträgt 10 Jahre und einen Tag. Laut dem für die Verarbeitung Verantwortlichen basiert diese Dauer, die nicht aus einer gesetzlichen Verpflichtung resultiert, auf einer allgemeinen Gepflogenheit im Großherzogtum Luxemburg für den Umgang mit sicherheitsrelevanten Aufzeichnungen⁹.

Eine Archivierung in Papierform ist nicht vorgesehen.

3. Rechtliche Prüfung

3.1. Vorabkontrolle

Die Verarbeitung der personenbezogenen Daten erfolgt durch eine Einrichtung der Europäischen Union mithilfe teilweise automatisierter Verfahren. Die Verordnung findet somit Anwendung. Diese Verarbeitungstätigkeit unterliegt einer Vorabkontrolle durch den EDSB, denn sie beinhaltet besondere Risiken im Zusammenhang mit der Verarbeitung von Daten über Gesundheit und Verdächtigungen zu Straftaten (Artikel 27 Absatz 2 Buchstabe a der Verordnung)¹⁰.

3.2. Rechtsgrundlage und Rechtmäßigkeit

Die Umstände und Zwecke von Ereignisberichten können sehr verschieden sein:

- die technische Sicherheit der Einrichtungen (einschließlich des Brandschutzes) und infolgedessen auch indirekt die Sicherheit von Personen;
- die Sicherheit von Personen (die Mitarbeiter des Gerichtshofs sein können, aber nicht müssen) ohne Bezug auf die Einrichtungen (Diebstahl usw.);
- die Gesundheit von Personen (die Mitarbeiter des Gerichtshofs sein können, aber nicht müssen) ohne Bezug auf die Einrichtungen (Unwohlsein, Unfall).

a. Rechtsgrundlage

Der Gerichtshof erwähnt als Basis der Verarbeitung zwei Rechtsgrundlagen:

- Artikel 26 der Bestimmungen ITM-ET;
- Artikel 4.2 des Lastenhefts für Leistungen des Sicherheitsdienstes „GS4 Security Services“¹¹.

⁹ Gemäß Artikel 26 der Bestimmungen ITM-ET müssen diese Aufzeichnungen zur Verfügung der Kontrollorgane – d. h. der luxemburgischen Gewerbeaufsicht – gehalten werden. Eine bestimmte Aufbewahrungsdauer ist hingegen nicht vorgesehen.

¹⁰ Gemäß Artikel 27 der Verordnung werden Verarbeitungen, die aufgrund ihres Charakters, ihrer Tragweite oder ihrer Zweckbestimmungen besondere Risiken für die Rechte und Freiheiten der betroffenen Personen beinhalten können, vom EDSB vorab kontrolliert. In Artikel 27 Absatz 2 der Verordnung sind die Verarbeitungen aufgeführt, die solche Risiken beinhalten können, und zwar insbesondere unter Buchstabe a Verarbeitungen von Daten, die Verdächtigungen, Straftaten, strafrechtliche Verurteilungen oder Sicherungsmaßnahmen betreffen. Verarbeitungen, die diese Daten nur ausnahmsweise oder punktuell betreffen, unterliegen hingegen keiner Vorabkontrolle. Angesichts der Angaben des Gerichtshofs scheint dies vorliegend nicht der Fall zu sein; die Verarbeitung unterliegt folglich der Vorabkontrolle.

¹¹ Siehe die Zusammenfassung des Sachverhalts in Abschnitt 2.1.

Die Bestimmungen ITM-ET stellen angesichts ihres Anwendungsbereichs¹² nur in Bezug auf die Berichte zur Sicherheit der Einrichtungen eine Rechtsgrundlage für die Verarbeitung dar. Das Lastenheft ist keine Rechtsgrundlage für die Verarbeitung (Erstellung von Berichten) an sich, sondern nur für die Untervergabe dieser Tätigkeit an den Sicherheitsdienst.

Der Gerichtshof muss folglich einen internen Beschluss fassen, der die Erstellung von Berichten für die verschiedenen vorstehend beschriebenen Zwecke vorsieht.

b. Rechtmäßigkeit

In Bezug auf die **Ereignisberichte zur technischen Sicherheit** der Einrichtungen **und zum Brandschutz** kann die Verarbeitung gemäß Artikel 5 Buchstabe a (im Lichte von Erwägung 27 der Verordnung) als rechtmäßig angesehen werden.

Die Datenverarbeitungen im Rahmen der **Ereignisberichte zur Gesundheit** (z. B. Unwohlsein eines Mitarbeiters oder eines Dritten) und der Berichte **zu Sicherheitsproblemen ohne Bezug auf die Einrichtungen** (Diebstahl und andere Vergehen in den Gebäuden und ihrer unmittelbaren Umgebung) sind gemäß denselben Bestimmungen unter dem Vorbehalt rechtmäßig, dass der Gerichtshof einen internen Beschluss fasst, in dem die Erstellung solcher Berichte vorgesehen ist (siehe vorstehend Punkt a).

Die verschiedenen vorstehend genannten Berichtsarten können Daten über Gesundheit und Verdächtigungen zu Straftaten enthalten, einschließlich der Berichte zur Sicherheit der Einrichtungen¹³. Die Rechtmäßigkeit der Verarbeitung dieser Datenkategorien resultiert aus Artikel 10 Absatz 2 Buchstabe a (für Personen, die keine Mitarbeiter des Gerichtshofs sind – falls eine gültige Einverständniserklärung abgegeben wurde) und b (für Mitarbeiter des Gerichtshofs) sowie Artikel 10 Absatz 5 der Verordnung. Um jedoch die Rechtmäßigkeit der Verarbeitung insbesondere in Bezug auf diejenigen Personen zu bekräftigen, die nicht zum Personal des Gerichtshofs gehören, sollte im oben genannten Beschluss ausdrücklich vorgesehen sein, dass solche Daten in den Berichten enthalten sein können.

Dieselben Regeln gelten insoweit für die Zusammenfassungen der Berichte, als diese personenbezogene Daten enthalten.

Im Übrigen ist es – wie nachfolgend in Abschnitt 3.3 erwähnt – angebracht, **die Sammlung** von personenbezogenen Daten (insbesondere der in Artikel 10 der Verordnung genannten Daten) im größtmöglichen Maß zu **beschränken**.

Empfehlung

1. Es sollte ein interner Beschluss gefasst werden, der im Hinblick auf die verschiedenen oben genannten Berichtstypen die Erstellung von Ereignisberichten vorsieht und in diesem Rahmen die Verarbeitung der in Artikel 10 der Verordnung erwähnten besonderen Datenkategorien erlaubt.
2. Im Fall der Sammlung von Daten zur Gesundheit von Personen, die keine Mitarbeiter des Gerichtshofs sind, sollte darauf geachtet werden, dass gemäß Artikel 10 Absatz 2

¹² Siehe Artikel 1 – Zweck und Geltungsbereich.

¹³ z. B. Personen, die infolge einer Störung an den Einrichtungen verletzt wurden, Personen, die der Sabotage einer Einrichtung verdächtigt werden.

Buchstabe a der Verordnung die Zustimmung dieser Personen zur Verarbeitung ihrer Daten eingeholt wird; außerdem sollte der Sicherheitsdienst in dieser Hinsicht entsprechende Anweisungen erhalten.

3.3. Datenqualität

Gemäß Artikel 4 Absatz 1 Buchstabe c der Verordnung müssen bzw. dürfen die verarbeiteten Daten „den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sein und nicht darüber hinausgehen“. Laut der Meldung und dem Informationsblatt sowie in Anbetracht des Formats des Ereignisberichts ist es möglich, dass die Sicherheitsmitarbeiter eine große Zahl von Daten sammeln. Es obliegt dem Referat Sicherheit und Schutz, den Auftragsverarbeiter darauf hinzuweisen, dass er nur Daten erheben darf, die im Hinblick auf die Zwecke ihrer Verarbeitung angemessen und erheblich sind und keinesfalls über diese Zwecke hinausgehen, nämlich die Erstellung von Berichten, anhand derer der Gerichtshof ggf. die gebotenen Sicherheits- und Schutzmaßnahmen ergreifen kann. So scheint die Sammlung von Daten zur Gesundheit der betroffenen Personen in den meisten Fällen für die Erreichung dieses Ziels nicht notwendig zu sein.

Empfehlung

3. Der Sicherheitsdienst sollte auf den Grundsatz der Minimierung des erhobenen Datenvolumens – insbesondere in Bezug auf Gesundheitsdaten – hingewiesen werden.

3.4. Auftragsverarbeiter

Wenn eine Datenverarbeitung gemäß Artikel 23 der Verordnung im Auftrag des für die Verarbeitung Verantwortlichen durch einen Auftragsverarbeiter erfolgt, so bedarf es dafür zwischen dem Auftragsverarbeiter und dem für die Verarbeitung Verantwortlichen eines entsprechenden Vertrags oder Rechtsakts. In diesem Vertrag muss vorgesehen sein, dass der Auftragsverarbeiter (in Bezug auf die Datenverarbeitung) auf Weisung des für die Verarbeitung Verantwortlichen handelt. Der Auftragsverarbeiter muss die Einhaltung der Verpflichtungen in Bezug auf Vertraulichkeit und Sicherheit gewährleisten, die im vorliegenden Fall in den geltenden nationalen Rechtsvorschriften zur Umsetzung von Artikel 17 der Richtlinie 95/46/EG festgelegt sind.

Dieser Pflicht wird durch die mit dem Auftragsverarbeiter geschlossenen Verträge Genüge getan¹⁴. [...]

3.5. Informationspflicht gegenüber den betroffenen Personen

Artikel 11 und 12 der Verordnung definieren die Modalitäten, gemäß denen die betroffenen Personen zu informieren sind, um ihnen gegenüber eine transparente und faire Datenverarbeitung zu gewährleisten.

Was die **Empfänger der Daten** betrifft, so werden in der Meldung und im Informationsblatt zahlreiche potenzielle Empfänger genannt, u. a. der Europäische Bürgerbeauftragte und der EDSB. Zur Information weist der EDSB darauf hin, dass Behörden, die personenbezogene Daten im Rahmen eines einzelnen Untersuchungsauftrags erhalten, nicht als „Empfänger“ im

¹⁴ Artikel 16.2 des Vertrags vom 16. November 2010 und Artikel II.6.1 des Vertrags vom 1. Juli 2015.

Sinne von Artikel 2 Buchstabe g der Verordnung gelten und im Informationsblatt nicht als solche genannt werden müssen.

Was die **Rechtsgrundlage der Verarbeitung** betrifft, so muss diese gemäß Empfehlung Nr. 1 geändert werden.

Empfehlung

5. Die Meldung und das Informationsblatt sollten gemäß Empfehlung Nr. 1 hinsichtlich der Rechtsgrundlage der Verarbeitung ergänzt werden.
6. Das Informationsblatt sollte auf der Website des Gerichtshofs veröffentlicht werden.

3.6. Dauer der Datenaufbewahrung

Gemäß Artikel 4 Absatz 1 Buchstabe e der Verordnung dürfen personenbezogene Daten nur *„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“*.

Die in der Meldung genannte Aufbewahrungsdauer beträgt 10 Jahre. Der Gerichtshof bezieht sich in dieser Hinsicht laut eigener Aussage auf eine allgemeine Gepflogenheit im Großherzogtum Luxemburg für den Umgang mit sicherheitsrelevanten Aufzeichnungen.

Diese besonders lange Aufbewahrungszeit, die keine gesetzliche Grundlage hat und angewandt wird, ohne im Hinblick auf die Art des Berichts, die Schwere des Zwischenfalls und die Reaktion auf den Bericht einen Unterschied zu machen, ist unverhältnismäßig und entspricht nicht den Vorgaben von Artikel 4 Absatz 1 Buchstabe e der Verordnung.

Auch wenn es angesichts einer allgemeinen Gepflogenheit im Großherzogtum Luxemburg gerechtfertigt sein mag, Ereignisberichte zur Sicherheit der Einrichtungen 10 Jahre lang aufzubewahren, so scheint diese Dauer doch nicht angemessen zu sein, wenn man z. B. an einen Ereignisbericht denkt, der sich auf den Zusammenstoß von zwei Fahrzeugen auf einem Parkplatz des Gerichtshofs bezieht, der nur zu einem geringfügigen Sachschaden geführt hat, oder aber einen Bericht zu einem leichten Unwohlsein eines Besuchers des Gerichtshofs.

Die Dauer der Aufbewahrung der Berichte und der Berichtszusammenfassungen sollte vom Gerichtshof neu bewertet werden.

Empfehlung

7. Die Dauer der Aufbewahrung der Berichte und der Berichtszusammenfassungen sollte insbesondere unter Berücksichtigung der Art der Berichte und der Reaktion auf diese Berichte neu bewertet werden.

* *
*

Vorbehaltlich der Hinweise und Empfehlungen in der vorliegenden Stellungnahme scheint die Datenverarbeitung durch den Gerichtshof im Rahmen des Umgangs mit Ereignisberichten der Verordnung zu entsprechen.

Der EDSB bittet den Gerichtshof, ihm innerhalb von **vier Monaten** mitzuteilen, welche Maßnahmen ergriffen werden, um den Empfehlungen der vorliegenden Stellungnahme zu folgen.

Brüssel, den 12. September 2016

Wojciech RAFAŁ WIEWIÓROWSKI