



Stellungnahme zu einer vom Datenschutzbeauftragten der Europäischen Investitionsbank empfangenen Meldung zur Vorabkontrolle im Hinblick auf die Aufzeichnung von Telefonzentralen- und Sicherheitsraum-Telefongesprächen

1. Verfahren

Am 15. März 2013 erhielt der Europäische Datenschutzbeauftragte (**EDSB**) eine Meldung zur Vorabkontrolle im Hinblick auf die Verarbeitung personenbezogener Daten in Bezug auf die „Aufzeichnung von Telefonzentralen- und Sicherheitsraum-Telefongesprächen“ vom Datenschutzbeauftragten (**DSB**) der Europäischen Investitionsbank (**EIB**) sowie dazugehörige Dokumente.

Am 21. März 2013 und 5. April wurden Fragen gestellt, welche die EIB am 17. April 2013 beantwortete, wobei sie zudem weitere Dokumente vorlegte. Der Entwurf der Stellungnahme wurde zwecks Kommentierung am 7. Juni 2013 an den DSB übersandt; am 19. Juni 2013 bestätigte der DSB, dass es keine Kommentare gebe.

2. Sachverhalt

Wenn die EIB zu dem Schluss kommt, dass ihre Bedrohungsstufe „gelb“¹ oder höher ist, kann die EIB beschließen, ein- und ausgehende Anrufe von der und zur Telefonzentrale sowie von den und zu den Sicherheitsräumen aufzuzeichnen. Diese Entscheidung wird vom Krisenausschuss² auf Empfehlung des Sicherheitsbeauftragten der EIB getroffen. Sie wird wöchentlich einer Überprüfung unterzogen. Die Aufzeichnung wird sobald wie möglich durch einen förmlichen Beschluss des Krisenausschusses deaktiviert.

Wenn das Verfahren initiiert wird, werden Anrufe wie folgt aufgezeichnet:

- während der Bürozeiten bei der Telefonzentrale eingehende Anrufe werden aufgezeichnet, bis sie an ihren Endempfänger weitervermittelt worden sind;
- außerhalb der Bürozeiten werden bei der Telefonzentrale eingehende Anrufe zu Sicherheitsräumen weitergeschaltet und aufgezeichnet, bis sie zu ihrem Endempfänger weitervermittelt worden sind;

¹ Die möglichen Stufen lauten wie folgt:

- a) weiß - Normalzustand, keine besonderen Bedrohungen ermittelt;
- b) gelb - Reaktion auf Spannungen oder eine bedrohliche Stimmung, Vorbereitung auf anormale Situationen;
- c) orange - Bedrohung wurde angekündigt oder beobachtet;
- d) rot - spezifische Hinweise auf eine sehr wahrscheinlich unmittelbar bevorstehende Terrordrohung sind eingegangen.

Im Verlauf der Jahre 2011 und 2012 war die Bedrohungsstufe stets „weiß“.

² Tagt unter dem Vorsitz des Direktors mit Generalvollmacht für Information und Gestaltung des Arbeitsumfeldes; der Generalsekretär und die betroffenen Direktoren mit Generalvollmacht sind Mitglieder des Ausschusses.

- ausgehende Anrufe, die direkt von der Telefonzentrale und den Sicherheitsräumen aus gewählt werden (bei letztgenannten nur außerhalb der Bürozeiten) werden in ihrer Gesamtheit aufgezeichnet.

Außerdem werden Uhrzeit, Datum und Länge der Anrufe sowie die Telefonnummern (falls verfügbar) gespeichert. Bei eingehenden Anrufen werden die Anrufer nicht darauf hingewiesen, dass ihr Anruf aufgezeichnet werden könnte.

Audioaufzeichnungen von Anrufen und die damit verbundenen Daten werden 30 Tage lang gespeichert; danach werden sie automatisch gelöscht, außer wenn eine Untersuchung läuft, die eine längere Speicherung rechtfertigt. Für derartige Untersuchungen gibt es eine Funktion im Telefonsystem, die das Exportieren von Aufzeichnungen ermöglicht.

Laut EIB werden die Aufzeichnungen nur benutzt, um gegebenenfalls vorkommende Terrordrohungen, insbesondere telefonisch übermittelte Drohungen, zu analysieren. Nur der Sicherheitsbeauftragte (oder sein Stellvertreter) kann die (einmalig gültigen) Zugangscodes von der IT-Abteilung erhalten, die das Telefonsystem der EIB verwaltet. Gewonnene Daten können dann an den Krisenausschuss und nach dessen Einwilligung sowie nach Unterrichtung des DSB an die Polizeidienststellen in Luxemburg übermittelt werden.

Betroffene Personen werden mit Hilfe einer Informationsmitteilung informiert, die sowohl im Intranet der EIB als auch auf der Website der EIB veröffentlicht wird. Die Informationsmitteilung informiert die betroffenen Personen darüber, dass „aus Gründen besonderer Gefahren für die Sicherheit“ Anrufe ohne Ertönen eines Warnsignals gegebenenfalls aufgezeichnet werden können, und enthält die Telefonnummern des FM Service Desk und des Sicherheitsbeauftragten, der für weitere Auskünfte kontaktiert werden kann.

Wenn die betroffenen Personen Auskunft über ihre personenbezogenen Daten erhalten möchten, können sie nach Genehmigung seitens des Sicherheitsbeauftragten, der vor seiner Entscheidung den DSB konsultieren sollte, Auskunft über diese Daten erhalten. Betroffene Personen haben das Recht, die Aufzeichnungen (zu Nachweiszwecken) zu sperren und löschen zu lassen, sollten sie rechtswidrig sein. Diesbezüglich können – wie in Artikel 20 der Verordnung 45/2001 (die Verordnung) festgelegt – Einschränkungen gelten.

Der für die Verarbeitung Verantwortliche ist die EIB, während die mit der Verarbeitung beauftragte Stelle die Verwaltungseinheit „Sicherheit und Dienstleistungen“ in der Abteilung „Gebäude und Logistik“ der Direktion „Information und Gestaltung des Arbeitsumfeldes“ ist.

3. Rechtliche Prüfung

3.1. Vorabkontrolle

Die Verarbeitung der Daten stellt eine Verarbeitung personenbezogener Daten dar und wird von einer Einrichtung der Europäischen Union bei der Ausübung von Tätigkeiten durchgeführt, für die Unionsrecht gilt. Die Verarbeitung der Daten ist automatisiert. Daher findet die Verordnung Nr. 45/2001 Anwendung.

Artikel 27 Absatz 1 der Verordnung (EG) Nr. 45/2001 sieht für sämtliche „Verarbeitungen, die aufgrund ihres Charakters, ihrer Tragweite oder ihrer Zweckbestimmungen besondere Risiken für die Rechte und Freiheiten der betroffenen Personen beinhalten können“, eine

Vorabkontrolle durch den EDSB vor. Artikel 27 Absatz 2 der Verordnung enthält eine nicht erschöpfende Aufzählung von Datenverarbeitungsvorgängen, die solche Risiken beinhalten können.

Die Verarbeitung personenbezogener Daten, die mit dem elektronischen Kommunikationsverkehr zusammenhängen, impliziert besondere Risiken; das gesamte Kapitel IV der Verordnung befasst sich mit dem Schutz personenbezogener Daten in diesem Kontext. Artikel 36 legt den allgemeinen Grundsatz der Vertraulichkeit des Kommunikationsverkehrs fest.

Zweck der Verarbeitung ist die Aufzeichnung des Inhalts von Anrufen, die damit als Verarbeitungsvorgang gilt, der besondere Risiken für die Rechte und Freiheiten der betroffenen Personen beinhalten kann.³

Die Meldung erwähnt auch die Verarbeitung von Daten, die „Sicherungsmaßnahmen“ betreffen, die eine der besonderen Datenkategorien darstellen, die Vorabkontrollen auslösen (Artikel 27 Absatz 2 Buchstabe a). Insbesondere nennt sie die Tatsache, dass die zu erfassenden Daten zur Beurteilung von Terrordrohungen dienen sollen, als Grund für die Vorlage des Verarbeitungsvorgangs zur Vorabkontrolle. Es ist darauf hinzuweisen, dass „Sicherungsmaßnahmen“, wie sie in Artikel 10 Absatz 5 der Verordnung definiert werden, Maßnahmen wie etwa der vorbeugende Gewahrsam oder das Einfrieren von Vermögenswerten oder ähnliche Maßnahmen sind; nicht jede Erfassung von Daten für Sicherheitszwecke fällt unter Artikel 10 Absatz 5. Es versteht sich von selbst, dass bei der überwiegenden Mehrzahl der Anrufer keinerlei Verbindung zu derartigen weiteren Maßnahmen besteht.

Auch wenn Artikel 27 Absatz 2 Buchstabe a hier nicht anzuwenden ist, ist der Verarbeitungsvorgang einer Vorabkontrolle gemäß Artikel 27 Absatz 1, wie oben beschrieben, zu unterziehen.

Da die Vorabkontrolle dazu dienen soll, Situationen zu behandeln, die bestimmte Risiken beinhalten können, sollte die Stellungnahme des EDSB vor Beginn des Verarbeitungsvorgangs abgegeben werden.

In diesem Fall wurde der EDSB über einen vorhergehenden Verarbeitungsvorgang informiert, der stärker eingreift als der vorgelegte Verarbeitungsvorgang. Der EDSB ersuchte die EIB dringend, den Verarbeitungsvorgang unverzüglich bis spätestens zum 15. März 2013 zu melden. Die vorgelegte Meldung weist bedeutende Änderungen gegenüber dem vorhergehenden Verarbeitungsvorgang auf.

Die Meldung des DSB ging am 15. März 2013 ein. Gemäß Artikel 27 Absatz 4 ist diese Stellungnahme innerhalb von zwei Monaten abzugeben. Wenn der EDSB von dem für die Verarbeitung Verantwortlichen weitere Auskünfte wünscht, kann diese Frist ausgesetzt werden, bis er die gewünschten Antworten erhält. Dieser Fall wurde vom 21. März 2013 bis zum 17. April 2013 und vom 7. Juni 2013 bis zum 19. Juni 2013 ausgesetzt; insgesamt wurde die Frist also um 39 Tage ausgesetzt. Der EDSB hat seine Stellungnahme also bis zum 24. Juni 2013 abzugeben.

³ Siehe z. B. folgende Stellungnahmen des EDSB zu Vorabkontrollen: „Enregistrement de la ligne réservée aux appels relatifs aux urgences et à la sécurité à Bruxelles (n° 88888)“ vom 22. Mai 2006; „Aufzeichnung von Notrufen bei der GFS in Ispra“ vom 13. Oktober 2008; „Enregistrement de la ligne réservée aux appels au dispatching technique relatifs aux interventions dans les immeubles de la CE à Bruxelles (n° 55555)“ vom 19. November 2008.

3.2. Rechtmäßigkeit der Verarbeitung

Personenbezogene Daten dürfen nur dann verarbeitet werden, wenn Gründe gemäß Artikel 5 der Verordnung vorliegen. Artikel 5 Buchstabe a erwähnt Verarbeitungen, die „für die Wahrnehmung einer Aufgabe erforderlich“ sind, „die aufgrund der Verträge zur Gründung der Europäischen Gemeinschaften oder anderer aufgrund dieser Verträge erlassener Rechtsakte ausgeführt“ werden. Erwägungsgrund 27 der Verordnung stellt klar, dass die „Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft zur Wahrnehmung einer Aufgabe im öffentlichen Interesse [...] die Verarbeitung personenbezogener Daten“ einschließt, „die für die Verwaltung und das Funktionieren dieser Organe und Einrichtungen erforderlich ist“.

In bestimmten Situationen mit einem hohen Bedrohungs- und Krisenpotenzial könnte es notwendig sein, zusätzliche Vorsichtsmaßnahmen zu treffen, um den ordnungsgemäßen Betrieb der EIB sicherzustellen. Die wesentlichen Merkmale der Verarbeitung sind in einem internen Dokument niedergelegt, das vom Vorstand der EIB genehmigt wurde. Dieses Dokument legt die Verarbeitungszwecke sowie die Kriterien für die Aktivierung der Aufzeichnung fest. Es macht keine Angaben zu den Aufbewahrungsfristen oder zu möglichen Empfängern außerhalb der EIB.

Aufgrund der Tatsache, dass die Aufzeichnung von Anrufen eine eingreifende Handlung ist, sollten die Regeln klar auf einer Rechtsgrundlage formuliert werden. Insbesondere das Ausmaß, die Zuständigkeiten der verschiedenen Beteiligten, die Aufbewahrungsfristen und die Empfänger (alle im Einklang mit der Empfehlung in dieser Stellungnahme modifiziert) sollten klar festgelegt werden. Das als Rechtsgrundlage vorgelegte Dokument behandelt alle diese Aspekte nicht und sollte geändert werden.

Empfehlung: eine klare und vollständige Rechtsgrundlage für die Aufzeichnung dieser Anrufe heranziehen.

3.3. Qualität der Daten

Artikel 4 Absatz 1 Buchstabe c der Verordnung legt den Grundsatz fest, dass die Daten den Zwecken entsprechen müssen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sein müssen und nicht darüber hinausgehen dürfen.

Zweck der Verarbeitung ist die Analyse gegebenenfalls vorkommender Terrordrohungen, insbesondere von telefonisch eingehenden Drohungen, die ausdrücklich in der Meldung erwähnt wurden.

Da die überwiegende Mehrzahl der ein- und ausgehenden Anrufe nicht relevant für diesen Zweck ist, wäre eine Aufzeichnung sämtlicher Anrufe eindeutig unverhältnismäßig. Der gewählte Ansatz, d. h., nur Anrufe aufzuzeichnen, wenn die Bedrohungsstufe „gelb“ oder höher ist, und der Krisenausschuss hat formal beschlossen, so vorzugehen, erlaubt die Beschränkung des Eingriffs in den Verarbeitungsprozess und der unnötigen Verarbeitung personenbezogener Daten. Dies ist ein wichtiger Schritt weg von der früheren Praxis, bei der diese Anrufe immer aufgezeichnet wurden.

Die Meldung nimmt ausdrücklich Bezug auf telefonisch eingehende Terrordrohungen, die logischerweise eher bei ein- als bei ausgehenden Anrufen angenommen werden können.⁴ Aus diesem Grund könnte die Unterscheidung zwischen ein- und ausgehenden Anrufen dazu dienen, die Erfassung und Speicherung personenbezogener Daten noch stärker zu vermeiden.

Empfehlung: evaluieren, ob das Verarbeitungsziel auch erreichbar ist, wenn nur eingehende Anrufe aufgezeichnet werden.

3.4. Aufbewahrung von Daten

Die Aufzeichnungen ein- und ausgehender Anrufe werden 30 Tage lang gespeichert, wenn das System aktiviert ist. Der für diese Frist angegebene Zweck ist die Analyse möglicher Terrordrohungen.

Artikel 4 der Verordnung beinhaltet den Grundsatz, dass personenbezogene Daten nur so lange gespeichert werden sollen, wie es für die Erreichung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist.

Um zu beurteilen, ob diese Aufbewahrungsfrist angemessen ist, kann ein Vergleich mit den Fristen für andere Sicherheitsmaßnahmen nützlich sein. Für die Videoüberwachung (CCTV) in den Gebäuden der Organe und Einrichtungen der Europäischen Union empfiehlt der EDSB eine maximale Aufbewahrungsfrist von 7 Tagen (außer wenn eine Untersuchung eingeleitet wird).⁵ Im vorliegenden Fall scheint diese Frist genügend Zeit zu lassen, um zu beurteilen, ob aufgezeichnete Drohungen an die Polizeidienststellen in Luxemburg weitergeleitet werden sollten.

Empfehlung: die Aufbewahrungsfrist auf 7 Tage reduzieren oder rechtfertigen, warum eine längere Frist erforderlich ist.

3.5. Übermittlungen von Daten

Aufgezeichnete Anrufe können an den Krisenausschuss übermittelt werden und nach dessen Einwilligung sowie nach Unterrichtung des DSB an die Polizeidienststellen in Luxemburg.

Übermittlungen werden durch Artikel 7, 8 und 9 der Verordnung geregelt – je nachdem, ob der Empfänger ein Organ oder eine Einrichtung der Europäischen Union ist (Artikel 7), den nationalen Rechtsvorschriften zur Umsetzung der Richtlinie 95/46/EG unterworfen ist (Artikel 8) oder besagter Richtlinie nicht unterworfen ist (Artikel 9).

Für Übermittlungen an den Krisenausschuss gilt Artikel 7. Die Norm für eine diesem Artikel unterworfenen Übermittlung verlangt, dass die Daten „für die rechtmäßige Erfüllung der Aufgaben erforderlich sind, die in den Zuständigkeitsbereich des Empfängers fallen“ (Artikel 7 Absatz 1). Der Empfänger darf die Daten ausschließlich für die Zwecke verwenden, für die sie übermittelt wurden. Der Krisenausschuss ist für die Sicherstellung der Kontinuität des Geschäftsbetriebs der EIB in Krisensituationen zuständig; Informationen über Bedrohungen sind wichtig, um diese Entscheidungen treffen zu können; derartige Übermittlungen erfolgen im Einklang mit Artikel 7.

⁴ Zudem wäre in jedem Fall bei ausgehenden Anrufen die gewählte Nummer bekannt.

⁵ Die Leitlinien sind auf der Website des EDSB verfügbar.

Für Übermittlungen an die Polizeidienststellen in Luxemburg gilt Artikel 8. Selbst wenn die Richtlinie 95/46/EG selbst nicht für die Tätigkeit der Polizei gilt, finden ihre Umsetzungsvorschriften in Luxemburg auch in diesem Sektor Anwendung. Artikel 3 des Luxemburger Datenschutzgesetzes („Gesetz vom 2. August 2002 zum Schutz personenbezogener Daten bei der Datenverarbeitung“ in seiner aktuellen Fassung, eigene Hervorhebung) besagt:

"Artikel 3. Anwendungsbereich

(1) Dieses Gesetz gilt für:

[...]

- die Verarbeitung von Daten bezüglich der öffentlichen Sicherheit, der Verteidigung, der Ermittlung und Verfolgung von Straftaten oder der Staatssicherheit, auch in Verbindung mit bedeutenden wirtschaftlichen oder finanziellen Interessen des Staates, unbeschadet der spezifischen nationalen oder internationalen Bestimmungen in diesen Bereichen.

(2) Dieses Gesetz gilt für:

(a) die Verarbeitung durch einen auf dem luxemburgischen Staatsgebiet niedergelassenen für die Verarbeitung Verantwortlichen; [...]"⁶

Für den Fall, dass Aufzeichnungen Belege für Terrordrohungen enthalten, könnten Übermittlungen an die Polizeidienststellen von Luxemburg dem Artikel 8 Buchstabe a unterworfen sein, da die Übermittlung erforderlich ist, damit die Polizei ihre Aufgaben in Ausübung ihrer amtlichen Autorität wahrnimmt, d. h., die Untersuchung von Straftaten wie etwa Terrordrohungen. Da es zu derartigen Übermittlungen wahrscheinlich auf Initiative der EIB kommen wird, müsste diese von Fall zu Fall bei jeder Übermittlung beurteilen, ob derartige Übermittlungen erforderlich sind. Laut der Meldung trifft der Krisenausschuss die Entscheidung, ob die Daten weitergeleitet werden sollen oder nicht. Es sollte sichergestellt werden, dass der Krisenausschuss jedes Vorkommnis von Fall zu Fall entscheidet. Die Beurteilung sollte in einem Übermittlungsregister dokumentiert werden.

Empfehlung: von Fall zu Fall bei jeder Übermittlung überprüfen, ob Übermittlungen an die Polizeidienststellen in Luxemburg erforderlich sind, und diese Beurteilung in einem Übermittlungsregister dokumentieren.

3.6. Recht auf Auskunft und Berichtigung

Betroffene Personen haben das Recht, Auskunft über ihre Daten zu erhalten und unrichtige Daten berichtigen zu lassen (Artikel 13 und 14 der Verordnung). Diese Rechte können entsprechend Artikel 20 eingeschränkt werden; so erlaubt Artikel 20 Absatz 1 Buchstabe a beispielsweise Einschränkungen, wenn diese zur Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten erforderlich sind.

Laut der Meldung „können betroffene Personen Auskunft über die betreffenden Gesprächsaufzeichnungen nach Einwilligung des Sicherheitsbeauftragten der Bank erhalten, der zuvor den DSB konsultieren sollte“.

In Einschränkung dieser allgemeinen Regel sollte Artikel 20 im engeren Sinne seines Wortlautes gelesen werden. Daher sollte allgemein Auskunft erteilt werden, außer wenn

⁶ Abgerufen von der Website der Nationalen Kommission für den Datenschutz des Großherzogtums Luxemburg: http://www.cnpd.public.lu/de/legislation/droit-lux/doc_loi02082002mod_de.pdf.

spezifische Gründe vorliegen, die die Anwendung einer Ausnahme in einem besonderen Fall rechtfertigen. Der Wortlaut „nach Einwilligung des Sicherheitsbeauftragten der Bank“ ist in diesem Lichte zu lesen.

3.7. Informationspflicht gegenüber betroffenen Personen

Gemäß Artikel 11 und 12 der Verordnung ist an betroffene Personen ein Mindestkatalog an Informationen zu übermitteln, sofern ihnen diese noch nicht vorliegen. Artikel 11 betrifft Situationen, in denen die Daten bei der betroffenen Person erhoben werden, z. B. in Antragsformularen. Artikel 12 betrifft Situationen, in denen die Daten nicht bei der betroffenen Person erhoben werden, d. h., es gibt keine direkte Interaktion zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen, und die betroffene Person weiß nicht notwendigerweise, dass ihre Daten erfasst werden (z. B. Videüberwachung, frühes Stadium interner Untersuchungen). Die gemeinsamen Elemente dieses Katalogs sind die Identität des für die Verarbeitung Verantwortlichen; die Zwecke des Verarbeitungsvorgangs, für den die Daten bestimmt sind; die Empfänger oder Kategorien von Empfängern; das Bestehen von Auskunfts- und Berichtigungsrechten bezüglich der sie betreffenden Daten; weitere Informationen, die erforderlich sind, um eine Verarbeitung nach Treu und Glauben zu gewährleisten (z. B. die Rechtsgrundlage des Verarbeitungsvorgangs, für den die Daten bestimmt sind, die zeitliche Begrenzung der Speicherung der Daten, das Recht, sich jederzeit an den Europäischen Datenschutzbeauftragten zu wenden). Einschränkungen sind entsprechend Artikel 20 der Verordnung möglich.

Die in der Meldung enthaltene Mitteilung, die auf der Website der EIB veröffentlicht werden soll, nennt lediglich den Zweck des Verarbeitungsvorgangs, die allgemeinen Kategorien der betreffenden Daten sowie Kontaktdaten, um weitere Auskünfte zu erhalten.

Unabhängig von der Frage, ob Artikel 11 oder Artikel 12 für die vorliegende Situation gilt, ist diese Information nicht ausreichend.⁷

Zu beachten ist auch, dass dies – obwohl diese Informationsmitteilung theoretisch für alle betroffenen Personen verfügbar wäre – nicht ausreichend ist, um eine angemessene Information sicherzustellen. Außer wenn eine der Ausnahmen entsprechend Artikel 20 der Verordnung ordnungsgemäß Anwendung finden kann (z. B. Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten), sollte die EIB bei eingehenden Anrufen eine automatische Ansage abspielen, während die Anrufer darauf warten, dass ein Mitarbeiter der Telefonzentrale den Anruf entgegennimmt. Diese Ansage sollte grundlegende Informationen zu einer möglichen Aufzeichnung sowie zu deren Zwecken enthalten.⁸ Sie müsste nur dann abgespielt werden, wenn die Aufzeichnung aktiv ist.

Die Informationsmitteilung sollte so erweitert werden, dass sie alle in Artikel 11 der Verordnung genannten Informationen enthält.

Während für die allgemeine Öffentlichkeit eine auf der Website der EIB veröffentlichte allgemeine Mitteilung zur Privatsphäre und eine Ansage für eingehende Anrufe ausreichend

⁷ In vergleichbaren früheren Fällen ist der EDSB davon ausgegangen, dass Artikel 11 Anwendung findet, wenn die Aufzeichnung angekündigt wird (siehe in den Fußnoten 3 und 8 angegebene Stellungnahmen).

⁸ Dies würde eingeführten Praktiken für andere Verfahren entsprechen, die die Aufzeichnung von Anrufen implizieren, siehe z. B. Stellungnahme des EDSB zur Vorabkontrolle: „Enregistrement de la ligne réservée aux appels au dispatching technique relatifs aux interventions dans les immeubles de la CE à Bruxelles (n° 55555)“ vom 19. November 2008.

wäre, sollte das in der Telefonzentrale und den Sicherheitsräumen arbeitende Personal eine gezieltere Information erhalten, da sie stärker betroffen sind. Dies könnte geschehen, indem die Mitteilung zusätzlich per E-Mail an die betroffenen Mitarbeiter versandt oder auf andere Weise sichergestellt wird, dass das Personal davon Kenntnis erhält.

Empfehlungen: Außer wenn eine der Ausnahmen gemäß Artikel 20 der Verordnung ordnungsgemäß Anwendung finden kann, sollte bei eingehenden Anrufen eine kurze automatische Ansage abgespielt werden, die die Anrufer über die Verarbeitung informiert. Diese Informationsmitteilung sollte so erweitert werden, dass sie die in Artikel 11 vorgeschriebenen Informationen enthält. Das in der Telefonzentrale und in den Sicherheitsräumen arbeitende Personal sollte gezieltere Informationen erhalten.

3.8. Sicherungsmaßnahmen

[...]

4. Schlussfolgerung:

Es besteht keine Veranlassung anzunehmen, dass gegen Bestimmungen der Verordnung 45/2001 verstoßen wird, sofern die in dieser Stellungnahme gegebenen Empfehlungen umfassend berücksichtigt werden.

An die gegebenen Empfehlungen sei nachstehend nochmals erinnert:

- eine klare und vollständige Rechtsgrundlage für die Aufzeichnung dieser Anrufe formulieren;
- evaluieren, ob das Verarbeitungsziel auch erreichbar ist, wenn nur eingehende Anrufe aufgezeichnet werden;
- von Fall zu Fall bei jeder Übermittlung überprüfen, ob Übermittlungen an die Polizeidienststellen in Luxemburg erforderlich sind, und diese Beurteilung in einem Übermittlungsregister dokumentieren;
- die Aufbewahrungsfrist auf 7 Tage reduzieren oder rechtfertigen, warum eine längere Frist erforderlich ist;
- die Informationsmitteilung so erweitern, dass sie die gemäß Artikel 11 vorgeschriebenen Informationen enthält;
- dem in der Telefonzentrale und in den Sicherheitsräumen arbeitenden Personal gezieltere Informationen geben;
- außer wenn eine der Ausnahmen gemäß Artikel 20 der Verordnung ordnungsgemäß Anwendung finden kann, sollte bei eingehenden Anrufen eine kurze automatische Ansage abgespielt werden, die die Anrufer über die Verarbeitung informiert.

Geschehen zu Brüssel, am 20. Juni 2013

(unterzeichnet)

Giovanni Buttarelli
Stellvertretender Europäischer Datenschutzbeauftragter