



01609/06/DE
WP 125

Arbeitsdokument: Eingriffe in den Datenschutz im Rahmen der Initiative eCall

Angenommen am

26. September 2006

Diese Arbeitsgruppe wurde gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzt. Sie ist ein unabhängiges europäisches Beratungsgremium in Datenschutzfragen. Ihre Aufgaben werden in Artikel 30 der Richtlinie 95/46/EG sowie in Artikel 15 der Richtlinie 2002/58/EG beschrieben.

Die Sekretariatsgeschäfte werden wahrgenommen durch das Direktorat C (Ziviljustiz, Grundrechte und Unionsbürgerschaft) der Europäischen Kommission, Generaldirektion Justiz, Freiheit und Sicherheit, B-1049 Brüssel, Belgien, Büro LX-46 01/43.

Website: http://ec.europa.eu/justice_home/fsj/privacy/index_de.htm

DIE GRUPPE FÜR DEN SCHUTZ NATÜRLICHER PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN,
eingesetzt durch Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995¹,

gestützt auf Artikel 29 und Artikel 30 Absatz 1 Buchstabe c und Absatz 3 jener Richtlinie,

gemäß ihrer Geschäftsordnung, insbesondere auf Artikel 12 und 14

HAT FOLGENDES ARBEITSDOKUMENT ANGENOMMEN:

1. EINFÜHRUNG

Ziel dieses Arbeitsdokuments ist die Darlegung datenschutzrechtlicher Bedenken im Zusammenhang mit der geplanten Einführung eines harmonisierten, europaweiten bordeigenen Notrufdienstes („eCall“), der auf der einheitlichen europäischen Notrufnummer 112 aufbaut².

Eine der Initiativen der Europäischen Kommission war die Errichtung des eSafety-Forums der Privatwirtschaft/des öffentlichen Sektors zur Verbesserung der Straßenverkehrssicherheit durch den Einsatz moderner Informations- und Kommunikationstechnologien. Das eCall-System wurde zu einer der höchsten Prioritäten erklärt, und es wurde eine eCall-Fördergruppe (eCall Driving Group) eingesetzt, an der alle wichtigen Akteure beteiligt sind³. Die eCall-Fördergruppe hat Empfehlungen ausgearbeitet, die einen Fahrplan für die Einführung umfassen, der die Verwirklichung des eCall-Systems in allen Mitgliedstaaten erleichtern und dazu beitragen soll, dass das System ab dem 1. September 2010 eine für alle Neufahrzeuge verfügbare Standardoption sein wird⁴.

Die eCall Fördergruppe hat eine Absichtserklärung über die eCall-Einführung vorgelegt. Durch diese Absichtserklärung soll vor allem sichergestellt werden, dass eCall später auch in allen EU-Mitgliedstaaten funktionieren wird. Die Absichtserklärung bindet alle Beteiligten bei der Einführung des eCall-Systems auf der Grundlage gemeinsam verabschiedeter Spezifikationen für Architektur und Schnittstellen sowie die zu übermittelnden Mindestdaten (Minimum Set of Data, MSD). Die Absichtserklärung wurde im August 2004 von der Europäischen Kommission, von der ACEA im Namen der Automobilindustrie und von der branchenübergreifenden Partnerschaft ERTICO unterzeichnet. Sie hat heute über 60 Unterzeichner, darunter sieben EU-Mitgliedstaaten⁵, die Schweiz und Norwegen.

¹ ABl. L 281 vom 23.11.1995, S. 31, abrufbar unter: http://ec.europa.eu/justice_home/fsj/privacy/

² Mitteilung der Kommission: Zweite eSafety-Mitteilung: Verbreitung des eCall-Systems unter den Bürgern (KOM(2005) 431, abrufbar unter: http://europa.eu/information_society/activities/esafety/index_en.html

³ Mitteilung der Kommission: Informations- und Kommunikationstechnologien für sichere und intelligente Fahrzeuge, KOM(2003) 542 endg. vom 15.9.2003

⁴ Die Empfehlung der eCall Driving Group, einschließlich aller Anhänge, ist über die folgende Website abrufbar: http://www.esafetysupport.org/en/ecall_toolbox/driving_group_ecall.

⁵ Finnland, Schweden, Griechenland, Italien, Litauen, Slowenien und Zypern

Kürzlich verabschiedete das Europäische Parlament mit sehr großer Mehrheit eine Entschließung zur Unterstützung der Einführung des eCall-Systems⁶, in der die Mitgliedstaaten dringend zur Unterzeichnung der Absichtserklärung aufgerufen werden.

Die Artikel 29-Datenschutzgruppe erkennt zwar die sozioökonomischen Vorteile an, die die breite Einführung des eCall-Dienstes für die Bürger mit sich bringen könnte, weist jedoch darauf hin, dass der eCall-Dienst zu Eingriffen in den Datenschutz führen wird, die hervorgehoben und in angemessener Weise behandelt werden müssen.

In Anbetracht der ihr durch Artikel 30 Absatz 1 Buchstabe a der Datenschutzrichtlinie übertragenen Aufgaben und um auf die datenschutzrechtlichen Fragen, die in Verbindung mit der beabsichtigten Einführung des eCall-Systems aufgeworfen werden, zu antworten, erachtet es die Artikel 29-Datenschutzgruppe daher für nötig, die derzeitige Situation zu analysieren und das vorliegende Arbeitsdokument diesem Fragenkomplex zu widmen.

2. PRINZIP DES ECALL-SYSTEMS

Die vorgeschlagene eCall-Architektur basiert auf einer quasi-simultanen Sprach-Daten-Verbindung von einem eCall-Generator zu einer primären Notrufabfragestelle („PSAP“, Public Safety Answering Point). Bei der „PSAP“ handelt es sich entweder um eine Behörde oder um einen privaten Diensteanbieter, der der Kontrolle einer Behörde untersteht.

Der eCall-Generator initiiert einen eCall-Notruf, der im Falle eines Unfalls automatisch durch Fahrzeugsensoren oder manuell durch die Fahrzeuginsassen ausgelöst wird, und überträgt den eCall-Notruf an die nächstgelegene PSAP.

Der eCall-Notruf besteht aus zwei Elementen: einem auf der Notrufnummer 112 basierenden, rein sprachlichen (Audio) Telefonanruf und einem Mindestdatensatz (Minimum Set of Data, MSD). Der über das Mobilfunknetz übertragene eCall-Notruf (Daten und Sprache) wird durch den Mobilfunknetzbetreiber (mobile network operator, MNO) als 112-Notruf erkannt. Basierend auf dem Verfahren für die Bearbeitung von 112-Notrufen ergänzt der MNO den Anruf um die Anruferidentifizierung (caller line identification, CLI), und fügt, gemäß der Universaldienstrichtlinie⁷ und der Empfehlung zu E112⁸, den nächstgelegenen Standort hinzu.

Nach dieser Bearbeitung übermittelt der Telekommunikationsnetzbetreiber die 112-Sprachnachricht zusammen mit der CLI, dem nächstgelegenen Mobilfunkstandort und den eCall-Mindestdaten (MSD) an die entsprechende PSAP. Dann überträgt die PSAP eine Bestätigung an den eCall-Generator, in der angegeben wird, dass die Mindestdaten ordnungsgemäß empfangen wurden.

⁶ Bericht über Straßenverkehrssicherheit: Verbreitung des eCall-Systems unter den Bürgern. Berichterstatter: Gary Titley (A6-0072/2006)

⁷ Richtlinie 2002/22/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten. ABl. L 108 vom 24.4.2002, S. 51

⁸ Empfehlung 2003/558/EG der Kommission vom 25. Juli 2003 zur Übermittlung von Angaben zum Anruferstandort in elektronischen Kommunikationsnetzen an um Standortangaben erweiterte Notrufdienste. ABl. L 189, S. 49.

Es ist hervorzuheben, dass bei dem vorgeschlagenen eCall-Dienst keine ununterbrochene Lokalisierung des bordeigenen Systems durch einen Dritten erfolgen wird, da das System nicht permanent mit den Mobilkommunikationsnetzen verbunden sein wird, sondern nur im Falle seiner Aktivierung bei einem Unfall oder einer manuellen Aktivierung durch die Fahrzeuginsassen.

Die Mindestdaten (Minimum Set of Data, MSD)⁹ bestehen aus Folgendem: (i) Zeitpunkt des Unfalls, (ii) genauer Standort einschließlich Fahrtrichtung, (iii) Fahrzeugkennung, (iv) eCall-Kennzeichner zur Angabe der Schwere des Unfalls (zumindest die Angabe, ob der eCall-Notruf manuell oder automatisch ausgelöst wurde), (v) Angaben über einen möglichen Diensteanbieter.

Die in den Mindestdaten vorgesehenen optionalen Daten zum Unfallstatus werden derzeit noch erörtert. Die in diesem optionalen Feld enthaltenen Angaben (d. h. Kraftstoffsorte, die das Fahrzeug verwendet), sollten den Datenschutzverordnungen entsprechen. Insbesondere sollte dabei das Verhältnismäßigkeitsprinzip beachtet werden: Es sollten nur diejenigen Daten aufgenommen werden, die für eine angemessene Bearbeitung des Notfalls notwendig sind.

Die vorgeschlagene eCall-Architektur trägt der Möglichkeit Rechnung, dass der Effekt des eCall-Systems weiter verstärkt werden könnte, wenn von einem Diensteanbieter, basierend auf zusätzlichen Daten – den sogenannten erweiterten Daten (Full Set of Data, FSD) – zusätzliche fahrzeug- und personenbezogene Daten übermittelt werden.

3. DAS eCALL-SYSTEM AUS DATENSCHUTZRECHTLICHER PERSPEKTIVE UND RECHTLICHE ARGUMENTATION

3.1. *Obligatorische oder freiwillige Basis*

Die Europäische Kommission hat vorläufig ein selbstregulatorisches Konzept zusammen mit den Mitgliedstaaten und der Privatwirtschaft gewählt, aber sollte die eCall-Einführung nicht gemäß dem vereinbarten Fahrplan vorankommen, kann sie weitere Maßnahmen in Betracht ziehen, darunter auch regulatorische Maßnahmen.

Auch wenn die Artikel 29-Datenschutzgruppe die sozioökonomischen Vorteile und den Wert für die öffentliche Sicherheit, die die breite Einführung des eCall-Dienstes mit sich bringen könnte, anerkennt, gibt es nichtsdestoweniger diverse datenschutzrechtliche Bedenken, die in diesem Kontext angesprochen werden müssen.

Bevor die Eingriffe in den Datenschutz näher beleuchtet werden, hat die Artikel 29-Datenschutzgruppe zwei Alternativen für die Einführung des eCall-Systems in ihre Überlegungen einbezogen, die zuallererst betrachtet und dann weiter analysiert werden sollten:

- Alternative (1) Das eCall-System ist auf freiwilliger Basis wählbar, oder
- Alternative (2) Das eCall-System ist ein obligatorischer Dienst.

⁹ Siehe Mindestdaten-Beschreibung in den abschließenden Empfehlungen der eCall Driving Group, Abschnitt 4.2.2.4 (MSD description, eCall DG Final recommendations, section 4.2.2.4)

Zu Alternative (1)

Erfolgt die Einführung des eCall-Systems auf freiwilliger Basis als eine Art von fortschrittlichem Dienst zur Unterstützung der Straßenverkehrssicherheit, muss eine einfache Möglichkeit für die Aktivierung/Deaktivierung des Systems eingeführt werden.

In diesem Fall ist das System *de facto* in das Fahrzeug eingebettet, und seine Aktivierung sollte freiwillig sein¹⁰. Der Benutzer, der nicht notwendigerweise der Fahrzeughalter ist, wird jederzeit die Möglichkeit haben, das System ein- oder auszuschalten, und zwar ohne technische oder finanzielle Beschränkungen. Diese Wahlmöglichkeit könnte beispielsweise durch den Einbau eines eigenen und problemlos zu betätigenden Knopfes/Schalters realisiert werden, in ähnlicher Weise, wie dies für den Beifahrer-Airbag gelöst ist.

Dieser Standpunkt basiert auf der Tatsache, dass eines der zentralen Kriterien für die Zulässigkeit der Verarbeitung von Daten Artikel 7 Buchstabe a der Datenschutzrichtlinie ist, der besagt, dass die Verarbeitung von Daten erfolgen darf, wenn die betroffene Person ohne jeden Zweifel ihre Einwilligung zu der Verarbeitung gegeben hat. Eine solche Einwilligung muss „ohne Zwang“ gegeben worden sein und sollte der betroffenen Person auch die Möglichkeit geben, die Einwilligung zu widerrufen. Es ist hervorzuheben, dass die Einwilligung nicht als „ohne Zwang gegeben“ zu betrachten ist, wenn die betroffene Person im Rahmen eines Vertrages mit nicht verhandelbaren Klauseln (wie es üblicherweise bei Fahrzeugverkaufsverträgen der Fall ist) eine diesbezügliche Klausel zu akzeptieren hat.

Darüber hinaus betrachtet die Artikel 29-Datenschutzgruppe Situationen als rechtswidrig, in denen beispielsweise durch Kraftfahrzeugversicherungen oder Autovermietungen dahingehend Druck ausgeübt wird, das eCall-Instrument aktiviert zu lassen. Eine ähnliche Verpflichtung könnte Angestellten auferlegt werden, die Firmenwagen benutzen, wobei eine Einwilligung zur Verwendung des eCall-Systems direkt oder indirekt erzwungen werden könnte.

Die Artikel 29-Datenschutzgruppe möchte betonen, dass Benutzer mögliche Eingriffe in den Datenschutz befürchten und sich gegen den Einsatz des Systems entscheiden könnten, wenn das eCall-System nicht kostenlos und ohne zusätzlichen Aufwand jederzeit und auf der Stelle aktiviert oder speziell deaktiviert werden kann. Da dies auch ein Sprungbrett für die geplante weit verbreitete Einführung des eCall-Systems sein kann, muss auch unter diesem Aspekt eine problemlose und kostenlose Deaktivierung eingeführt werden.

Obwohl die Datenverarbeitung in vielen Fällen ein lebenswichtiges Interesse der betroffenen Person darstellen mag und dann die eCall-Einführung durch Artikel 7 Buchstaben c, d und e der Datenschutzrichtlinie gestützt werden mag, wird dies nicht in jedem Fall so sein. Beispielsweise kann es Fälle geben, in denen sich ein Unfall ereignet und das eCall-System automatisch ausgelöst wird, aber keine Notwendigkeit für den Einsatz der Rettungsdienste besteht.

¹⁰ Dies bedeutet nicht, dass der Dienst nicht automatisch eingeschaltet werden kann, wenn der Motor gestartet wird, sondern dass der Benutzer in der Lage sein sollte, den Dienst jederzeit zu deaktivieren/aktivieren.

Auf der Grundlage der bisher verfügbaren Informationen über die Konfiguration des eCall-Systems geht die Datenschutzgruppe davon aus, dass es möglich sein wird, eine Standortbestimmung des betreffenden Fahrzeugs vorzunehmen, ohne dass dieses jedoch permanent lokalisiert wird – das heißt, das System wird nur dann bei dem Kommunikationsnetzwerk angemeldet, wenn sich ein Unfall ereignet oder das System manuell ausgelöst wird. Die Datenschutzgruppe begrüßt dieses Merkmal und möchte betonen, dass im Hinblick auf die mögliche Aktivierung von eCall-Geräten eine permanente Verbindung derartiger Geräte mit den Kommunikationsnetzen und damit eine permanente Lokalisierbarkeit der Fahrzeuge unter dem Aspekt des Datenschutzes nicht akzeptabel wäre. Dies bedeutet, dass es akzeptabel sein könnte, die drei zuletzt von GPS/Galileo-Systemen (sofern an Bord des Fahrzeugs verfügbar und an das eCall-Gerät angeschlossen) erfassten Fahrzeugstandorte im Speicher des eCall-Geräts zu speichern, ohne dass Daten übertragen werden, sofern kein auslösender Faktor (d. h. Unfall oder manuelle Aktivierung) vorliegt. In einem derartigen Fall müsste der Umfang der erhobenen Daten eindeutig begrenzt werden und jede weiter gehende Nutzung der Informationen – das heißt, für andere Zwecke als die Gewährleistung der Straßenverkehrssicherheit – verhindert werden.

Zu Alternative (2)

Soll der eCall-Dienst obligatorisch sein, wäre das System *de facto* in das Fahrzeug eingebettet, und seine Aktivierung wäre obligatorisch. Diese Alternative müsste jedoch durch eine entsprechende Verordnung mit EU-weiter Geltung durchgesetzt werden. Eine derartige Verordnung müsste im Hinblick auf den Datenschutz ordnungsgemäß begründet werden.

Sollte das eCall-System ein obligatorisches Instrument sein, müssten alle Einschränkungen der Datenschutzrechte bei der Anwendung der in der Datenschutzrichtlinie festgelegten Grundsätze, beispielsweise unter anderem der Grundsatz der Verhältnismäßigkeit, in der Rechtsvorschrift klar dargelegt werden. In das eCall-System sollten Technologien zur Stärkung des Datenschutzes eingebettet werden, um eCall-Anwendern den gewünschten Schutz zu bieten. Auch Sicherungssysteme zur Verhinderung von Überwachung und Missbrauch müssen entwickelt und integriert werden. Dies wird entsprechend auch für das Szenario unter Alternative 1 gelten. Nationale Datenschutzbehörden sollten konsultiert werden, um Empfehlungen hinsichtlich der bestmöglichen Verfahren einzuholen.

Zusammenfassung: Ist das eCall-System optional, muss eine benutzerfreundliche Lösung eingeführt werden, bei der durch Einführung der technischen Möglichkeit, das eCall-System von Fall zu Fall aus- oder einzuschalten, die Selbstbestimmung der Kraftfahrzeugbenutzer berücksichtigt wird, was beispielsweise durch elektronische Schalter, Chipkarten oder sonstige Geräte, die die willentliche Aktivierung des eCall-Geräts und auf Wunsch die Übermittlung von über die Mindestdaten hinausgehenden Daten ermöglichen, geschehen kann. Ist das eCall-System obligatorisch, müssen in einer entsprechenden Rechtsvorschrift Bestimmungen festgelegt werden, wobei die Grundsätze des Datenschutzes zu beachten sind.

In beiden oben genannten Fällen wird die Artikel 29-Datenschutzgruppe die Sensibilisierung unterstützen, wobei sie den Schwerpunkt auf Eingriffe in den Datenschutz legen wird. Nationale Datenschutzbehörden werden im Rahmen der Artikel 29-Datenschutzgruppe zur weiteren Sensibilisierung für das eCall-System beitragen, wobei der Schwerpunkt auf Datenschutzfragen wie der transparenten und rechtmäßigen Verarbeitung der über das eCall-System erhobenen Daten liegen wird.

Die Artikel 29-Datenschutzgruppe gibt dem freiwilligen Konzept für die Einführung des eCall-Dienstes den Vorzug. Falls die obligatorische Alternative eingeführt wird, muss ein geeignetes Sicherungssystem hinsichtlich des Datenschutzes eingeführt werden.

3.2. *Zwei Ausbaustufen der Dienste*

Unabhängig davon, ob das eCall-System obligatorisch oder optional wäre, sieht die eCall-Initiative die Möglichkeit eines erweiterten Systems vor, das die Erbringung von Mehrwertdiensten durch die Diensteanbieter umfasst. In diesem Fall wird es die beiden folgenden Ausbaustufen der Dienste geben:

(1) Der erste beabsichtigte Dienst bewirkt die Auslösung der Übermittlung der in den Mindestdaten enthaltenen Angaben an die entsprechende Notrufabfragestelle, nämlich Fahrzeugstandort, Unfallzeitpunkt, Fahrzeugkennung und eCall-Status (zumindest die Angabe, ob der eCall-Notruf manuell oder automatisch ausgelöst wurde), was die Feststellung der Schwere des Unfalls ermöglichen wird.

Dieser „Basisdienst“ ist der von der Europäischen Kommission befürwortete Dienst.

(2) Die zweite Ausbaustufe des Dienstes liegt darin, dass zu den in den Mindestdaten enthaltenen, ausgetauschten „Basisangaben“ zusätzliche Angaben hinzukommen, die im Besitz eines Dritten sind – beispielsweise Versicherungsgesellschaften, Kraftfahrzeug-Callcenter, Gesundheitsdienste, Rechtsanwälte, Automobilclubs usw. Werden erweiterte Daten (full set of data, FSD) übertragen, ist ein Vertrag zwischen dem Fahrzeughalter und dem Diensteanbieter erforderlich.

In diesem Szenario würde der Benutzer dem Diensteanbieter den Empfang der zusätzlichen Daten im Zusammenhang mit dem Unfall oder den Fahrzeuginsassen gestatten, damit dieser beispielsweise Unterstützung durch eine Versicherungsgesellschaft oder einen Automobilclub oder sprachliche Unterstützung gewähren kann. Dieser erweiterte Dienst wird den Erwartungen zufolge durch die Marktkräfte entwickelt werden.

Grundsätzlich spricht nichts gegen eine derartige Regelung. Die diesbezüglichen Fragen sind jedoch komplexer und erfordern eine eingehendere Würdigung. Insbesondere die Vorschriften zur Datensicherheit müssen strikt befolgt werden, insbesondere weil es sich bei einigen der zu verarbeitenden Daten um sensible Daten handelt. Für die Erweiterung der Basisfunktionalitäten des eCall-Systems, das heißt, die Übersendung erweiterter Daten (Full Set of Data, FSD) an einen privaten Diensteanbieter zusätzlich zu den Mindestdaten (Minimum Set of Data, MSD), ist eine detaillierte Definition erforderlich. Diese Dienste sollten in vollem Umfang den einschlägigen Verordnungen zum Datenschutz entsprechen.

Die Artikel 29-Datenschutzgruppe möchte erneut auf die Grundprinzipien hinweisen, die durch Drittanbieter zu berücksichtigen sind:

- (i) Die Datenschutzgruppe möchte betonen, dass es sich bei den erweiterten Daten nicht um einen „*a priori*“-Datensatz handeln wird, da diese Daten vielmehr das Ergebnis der vertraglichen Vereinbarungen zwischen dem Fahrzeughalter/-nutzer (abhängig von der Durchführung der FSD-Erweiterung) und den einzelnen Diensteanbietern (Versicherungsgesellschaften, Automobilclubs, Gesundheitsdienste usw.) sein werden. Daher müssen die Zwecke, für die die erweiterten Daten und die einzelnen Elemente der erweiterten Daten verwendet werden dürfen, in den einzelnen Verträgen eindeutig festgelegt werden. In den Verträgen sollte auch eindeutig festgelegt werden, dass es sich bei dem Drittdiensteanbieter um den Verantwortlichen für die relevanten Daten handelt, der allen sowohl gemäß der Datenschutzrichtlinie als auch gemäß einzelstaatlichen Rechtsvorschriften geltenden datenschutzrechtlichen Verpflichtungen für Datenverantwortliche unterliegt.
- (ii) Es dürfen nur Daten übertragen werden, die für die spezifischen Zwecke „notwendig“ und „relevant“ sind, das heißt, es muss sichergestellt werden, dass jeder Drittdiensteanbieter nur diejenigen Daten erhält, die für die Zwecke des jeweiligen Vertrags benötigt werden. Unter dem Aspekt des Datenschutzes ist eine „en-bloc“-Übertragung der erweiterten Daten naheliegenderweise nicht zulässig. Es werden voraussichtlich geeignete technische Vorkehrungen nötig sein, damit das eCall-System nur diejenigen Daten auswählt, die für die einzelnen Diensteanbieter relevant sind. In diesem Kontext wird auch abgewogen werden müssen, ob die relevanten Angaben in allen Fällen übertragen werden sollen – wie oben dargelegt, kann es Fälle geben, in denen sich ein Unfall ereignet und das System ausgelöst wird, aber keine Notwendigkeit für den Einsatz von Rettungsdiensten besteht.
- (iii) Die in den erweiterten Daten enthaltenen Angaben sollten von der Automobilindustrie und den Beteiligten eindeutig festgelegt werden, und Fahrzeughalter müssen in geeigneter Weise über die Funktionsweise und den Betrieb des Systems unterrichtet werden. Diese Unterrichtung sollte auch die Folgen umfassen, die es hat, wenn sich der Halter entschließt, seine Einwilligung zur Übertragung der erweiterten Daten oder eines Teils der erweiterten Daten zu widerrufen; dabei ist zu wiederholen, dass der Widerruf dieser Einwilligung nicht gegen die Interessen des Fahrzeughalters gerichtet sein sollte.
- (iv) Sollten die erweiterten Daten medizinische oder andere sensible Daten umfassen, wird beim Umgang mit dem Datensatz besonders sorgsam vorgegangen werden müssen. Neben der ausdrücklichen Einwilligung des Fahrzeughalters erfordert die Verarbeitung dieser Daten spezifische Sicherheitsvorkehrungen, die in manchen Fällen in einzelstaatlichen Rechtsvorschriften im Einzelnen festgelegt sind.
- (v) Die Bestimmungen betreffend die Weiterübermittlung der Daten sind zu befolgen, insbesondere in Fällen, in denen ein Drittdiensteanbieter seine Verarbeitungen (zum Teil) an Organisationen mit Sitz in Drittländern outsourct; als hilfreiche Leitlinien mögen die Überlegungen in Dokument WP74¹¹ dienen.

¹¹ http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp74_de.pdf

4. ANDERE FRAGEN IM ZUSAMMENHANG MIT DEM eCALL-SYSTEM

Generell gibt es auch Bedenken im Zusammenhang mit der Erstellung von Datenbanken durch Telekommunikationsbetreiber, mit den Fristen für die Speicherung von erhobenen Daten sowie mit Fragen im Zusammenhang mit der Sicherheit der gespeicherten Daten.

4.1. Datenbanken

Weitere datenschutzrechtliche Bedenken ergeben sich in Verbindung mit den Datenbanken, die angelegt werden, um die fälschliche Verwendung/den Missbrauch des Systems zur Verknüpfung der Identität des Fahrzeughalters und der SIM-Karte des eCall-Systems zu verhindern, deren Hauptzweck die Suche nach Personen wäre, die das System missbrauchen, beispielsweise Autofahrer, die sich verfahren haben usw.

Im Falle der fälschlichen Verwendung/des Missbrauchs des Systems, die/der zu Nachteilen für die Notrufabfragestellen führen könnte (d. h. ein System setzt mehrere eCall-Notrufe ohne triftigen Grund ab), sollten die Notrufabfragestellen ein Verfahren zur Rückverfolgung des Systems, von dem die fälschliche Verwendung ausgeht, festlegen. In einem derartigen Fall können die beiden folgenden Verfahren in Betracht gezogen werden: (i) von den Mobilfunknetzbetreibern die Identifizierung des Eigentümers des Geräts zu verlangen (über die in der SIM-Datenbank gespeicherten Angaben), wie im Falle der 112-Notrufe, oder (ii) die Identifizierung der Behörde, welche die Fahrgestellnummern kontrolliert, zu verlangen.

Zu den Hauptbedenken der Artikel 29-Datenschutzgruppe gehört die potenzielle Gefahr, dass ein weiterer Dritter zu verschiedenen Zwecken Zugang zu diesen Datenbanken haben könnte. Daher möchte die Artikel 29-Datenschutzgruppe betonen, dass jede Sekundärnutzung von Daten, zum Beispiel für verkehrsbezogene Vollzugsverfahren, unzulässig sein sollte, da sie im Widerspruch zu den Grundsätzen der Datenschutzrichtlinie stehen würde.

4.2. Sicherheitsfragen

Eine weitere Gruppe von Bedenken wird durch Sicherheitsfragen aufgeworfen, deren Gegenstand die Frage ist, ob das eCall-System ausreichend gegen unbefugten Zugriff geschützt ist. Um ein zuverlässiges System einzuführen und den unbefugten Zugriff diverser Dritter auf die im eCall-System enthaltenen personenbezogenen Daten zu vermeiden, muss innerhalb des bordeigenen Systems und im Transportprotokoll ein hinreichendes Schutzniveau gewährleistet werden¹².

¹² Den Erwartungen zufolge werden Originalgerätehersteller im Automobilbereich ein hinreichendes Schutzniveau für die im bordeigenen System gespeicherten Daten gewährleisten. Andererseits wird davon ausgegangen, dass das von ETSI genormte Übertragungsprotokoll ein hinreichendes Schutzniveau bieten wird.

4.3. *Verhältnismäßigkeit*

Bei der Verwendung des eCall-Systems werden Mindestdaten (Minimum Set of Data, MSD) für die Bearbeitung des Notrufs weitergeleitet. Die Artikel 29-Datenschutzgruppe ist der Ansicht, dass Mindestdaten, die die vollständige Fahrgestellnummer umfassen (wie derzeit angegeben), in Bezug auf den eindeutig festgelegten Zweck unangemessen sein könnten.

Die Artikel 29-Datenschutzgruppe hat Bedenken wegen der Möglichkeit, dass die Einführung des eCall-Dienstes angesichts des gegenwärtig betriebenen Notrufsystems, das in den Mitgliedstaaten gut funktioniert, möglicherweise nicht in allen Fällen notwendig sein wird. Dieses Argument erscheint wichtig, da es die Frage der Verhältnismäßigkeit aufwirft, das heißt, ob die Einführung eines auf der Geolokalisierung basierenden Notrufsystems in Ländern, in denen bereits jetzt ein Notrufsystem gut funktioniert, verhältnismäßig ist?

4.4. *Art des für die Datenverarbeitung Verantwortlichen*

Der für die Datenverarbeitung Verantwortliche wird im Falle des eCall-Systems die Notrufabfragestelle (Public Safety Answering Point, PSAP) sein, die für die Speicherung, die Verarbeitung und den Schutz personenbezogener Daten Protokolle festlegen sollte, die den für andere Notrufsysteme eingeführten Protokollen ähneln. Die Mobilfunknetzbetreiber werden die Mindestdaten in transparenter Weise übermitteln, und sie sollten sicherstellen, dass die eCall-Daten nicht länger gespeichert werden, als es zur Gewährleistung ihrer ordnungsgemäßen Übertragung an die entsprechende Notrufabfragestelle nötig ist. Danach sollten die Mindestdaten gelöscht werden.

In Bezug auf die Anruferidentifizierung und die Übertragung von Lokalisierungsangaben an die Notrufabfragestellen müssten ähnliche Protokolle festgelegt werden, wie sie für die Bearbeitung von E112-Notrufen (um Standortangaben erweiterte Notrufe) gemäß der Universaldienstrichtlinie und der Empfehlung der Kommission zur Übermittlung von Angaben zum Anruferstandort in elektronischen Kommunikationsnetzen an um Standortangaben erweiterte Notrufdienste verwendet werden.

4.5. *Speicherfrist*

Die Artikel 29-Datenschutzgruppe möchte betonen, dass für die verschiedenen Parteien in der eCall-Dienstleistungskette angemessene Speicherfristen für eCall-Daten festgelegt werden sollten. Die einzelstaatlichen Behörden werden die Festlegung und Einhaltung der Fristen überwachen.

5. SCHLUSSFOLGERUNGEN

Auch wenn die Artikel 29-Datenschutzgruppe Bedenken im Zusammenhang mit dem eCall-System hat, gibt sie dem Konzept der freiwilligen Einführung des eCall-Dienstes den Vorzug und empfiehlt dieses.

Aus datenschutzrechtlicher Perspektive ist ein automatisch durch ein Gerät oder manuell ausgelöster und über Mobilfunknetze übertragener Notruf, der zur geografischen Standortbestimmung des Notfalls führt, grundsätzlich zulässig, sofern es diesbezüglich eine spezifische Rechtsgrundlage gibt und hinreichende Vorkehrungen im Bereich des Datenschutzes getroffen werden. Allerdings müssen stets die Zwecke des Notrufsystems und die Relevanz der zu verarbeitenden Daten berücksichtigt werden, insbesondere in Fällen, in denen die Verarbeitung die so genannten erweiterten Daten (Full Set of Data, FSD) umfasst.

Brüssel, den 26. September 2006

Für die Arbeitsgruppe
Der stellvertretende Vorsitzende
Jose Luis Piñar Mañas