Data Protection Aspects of eCall
Data Protection Aspects of eCall

NOTE

Abstract
This briefing note deals with the data protection aspects of the Commission’s Proposal for a Regulation of the European Parliament and of the Council concerning type-approval requirements for the deployment of the eCall in-vehicle system and amending Directive 2007/46/EC COM(2013) 316 final. It explains why the eCall system entails the processing of personal data. It deals with the data protection issues both for the mandatory 112-based eCall in-vehicle system as well as additional private emergency and added value services offered in parallel or building on the public 112-based eCall.
CONTENTS

LIST OF ABBREVIATIONS 4

EXECUTIVE SUMMARY 5

1. INTRODUCTION 7
   1.1. In-vehicle emergency call (eCall) service – how does it work? 7
   1.2. Initiatives of the European Parliament and the European Commission 7
   1.3. Commission’s Proposal COM(2003) 316 final 8

2. MANDATORY 112-BASED ECALL IN-VEHICLE SYSTEM 9
   2.1. From voluntary to mandatory system 9
   2.2. Risks for privacy and personal data processing 10
   2.3. Personal data – are they really involved? 11
   2.4. Practical implications for the legislature 11
      2.4.1. Scope of the data (Minimum Set of Data) 11
      2.4.2. Constant tracking 13
      2.4.3. Privacy by Design / Privacy Enhancing Technologies 14
      2.4.4. Informational obligations 14
      2.4.5. Other principles of personal data processing 15
   2.5. Actors involved – who should be responsible and for what? 16
      2.5.1. Practical implications for the manufactures 17
      2.5.2. Practical implications for other actors 17
   2.6. Other possible uses of eCall data 17

3. ADDITIONAL EMERGENCY AND/OR ADDED VALUE SERVICES ("PRIVATE" SERVICES) 18
   3.1. Examples of additional emergency/added value services 18
   3.2. General or specific regulation – which approach should apply? 19
   3.3. Other specific issues that may need to be regulated 20

REFERENCES 21
LIST OF ABBREVIATIONS

ABS   Anti-lock Braking System
APS   Acoustic Parking System
BMW   Bayerische Motoren Werke
CEN   European Committee for Standardisation, EN CEN 15772
CNG   Compressed national gas
eCall In-vehicle emergency call
EDPS  European Data Protection Supervisor
e.g.  Exempli gratia (for example)
EU    European Union
GM    General Motors
i.e.  Id est (which means)
IT    Information technology
MNO   Mobile Network Operators
MSD   Minimum Set of Data
PSAP  Public Safety Answering Point
VIN   Vehicle Identification Number
Working Party Article 29 Working Party
EXECUTIVE SUMMARY

The eCall system

This briefing note deals with the data protection aspects of the Commission’s Proposal for a Regulation of the European Parliament and of the Council concerning type-approval requirements for the deployment of the eCall in-vehicle system and amending Directive 2007/46/EC COM(2013) 316 final, hereinafter “Proposal”.

The in-vehicle emergency call (“eCall”) system, which is usually merely ‘dormant’, automatically establishes a 112-based audio channel between the occupants of a car and a Public Safety Answering Point (“PSAP”) in case of an accident. At the same time, the system also generates a Minimum Set of Data (“MSD”) and sends it to the PSAP, which allows an ambulance to be sent to the place of the accident even in the event that voice contact with the occupants of the vehicle is not possible.

The Proposal is part of a set of measures aiming at ensuring mandatory deployment across the EU of the 112-based emergency call (eCall) service by 1 October 2015. The proposal contains rules on privacy and data protection (Article 6 and Recital 13). In particular, it seeks to ensure that any processing of personal data through the eCall in-vehicle system complies with the personal data protection rules contained in Directives 95/46/EC and 2002/58/EC. Recital 8 of the Commission’s Proposal clarifies that the mandatory equipping of vehicles with the 112-based eCall in-vehicle system is “without prejudice to the right of all stakeholders such as car manufacturers and independent operators to offer additional emergency and/or added value services, in parallel with or building on the 112-based eCall in-vehicle system”.

This briefing note explains why the functioning of the mandatory (even “dormant”) in-vehicle eCall system may entail the processing of personal data and deals with the data protection issues arising from this under two distinct aspects:

1. Mandatory 112-Based eCall in-vehicle system

What practical implications does the provision on compliance of any personal data processing through the mandatory 112-based eCall in-vehicle system with the EU data protection rules have for the legislator, and what implications would it have on the obligations of the manufacturers, the national type-approval authorities and eCall users?

2. Additional private emergency and added value services

What implications, if any, does Recital 8, and indeed, possible provision of private emergency and other added value services in parallel or building on the public 112-based eCall, have on data protection and privacy aspects of eCall?

Implications for the mandatory 112-based eCall in-vehicle system

The scope of the automatically generated and transferred Minimum Set of Data (“MSD”) would need to be expressly regulated in the Proposal. In defining the scope of the MSN, the principles of proportionality and minimisation should be observed, pursuant to which only data which is necessary to achieve the intended purpose, i.e. the proper handling of emergency calls, should be processed.

The Proposal must be further clarified to ensure that the prohibition of constant tracking does not affect proper operation of the eCall system, since tracking is used to determine the direction of driving. In particular, the possibility of storing several (e.g. three) last locations of the vehicle should be sufficient.
A general obligation of equipping the in-vehicle eCall system with privacy enhancing technologies should be introduced.

The wording of Article 6 (3) of the Proposal should be modified to ensure that the duty to provide certain information covers not only information “about the processing of data”, but broader information on the rules governing the operation of the eCall system, in particular with respect to privacy and personal data protection.

The Proposal should define the periods of retention of the data processed in the eCall system.

The PSAPs should be qualified as controllers of personal data processed under the mandatory eCall in-vehicle system. Due to the specificities of the eCall system, some responsibilities should also be borne by other actors. The Proposal correctly requires in Article 6 (3) that responsibility for conveying the basic information to the user shall be borne by the manufacturer.

**Additional private emergency and added value services**

Due to the potentially significant impact on the privacy of the vehicle users, providing additional emergency services, as well as added value services, should be - with regard to the obligation to prevent surveillance and misuse as well as to take Privacy by Design / Privacy Enhancing Technologies into account - subject to the same rules which apply to mandatory (public) emergency services.

It is advisable that the Proposal specifies which information is to be given to the data subject when data is being collected in the context of private services in a more detailed manner than in Article 6 (3) (i) of the Proposal and in Article 10 of Directive 95/46/EC.

Aside from the abovementioned general issues, it nevertheless remains doubtful whether the additional emergency services and added value services require more detailed regulation than the mandatory “public” eCall services. It must be pointed out that the basis for data processing (i.e. basically the consent of interested persons or an appropriate agreement as indicated in Article 7 of Directive 95/46/EC) is fundamentally different. Since the rules of data processing in the context of additional services are governed by the general provisions, it does not therefore seem particularly necessary to define issues such as the scope of the data, the legal basis of data processing for purposes connected with providing additional emergency/added value services, rights of vehicles users to deactivation of additional emergency/added value services or data retention periods.

The prohibition of permanent tracking, which is applicable to the mandatory eCall system, but not to private added value services, poses both legal and technical problems. If this prohibition were expanded to private added value services, this would be contrary to market expectations, as well as to expectations of many vehicle users who probably would be willing to agree to such tracking. However, accepting the possibility of permanent tracking for purposes connected with added value services raises the question of the effectiveness of the prohibition of permanent tracking with regard to the eCall system’s normal functioning mode. It is more of a technical than a legal problem whether it is possible to allow, within the same system, permanent tracking for the purposes of added value services but effectively implement and monitor the prohibition of permanent tracking for all other purposes. The committee should reassure itself that this problem can be solved.
1. INTRODUCTION

1.1. In-vehicle emergency call (eCall) service – how does it work?

The purpose of the in-vehicle emergency call ("eCall") system is to establish a 112-based audio channel between the occupants of the vehicle and a Public Safety Answering Point ("PSAP"). The eCall generator installed inside the vehicle, which enables transmission via a public mobile wireless communications network and which is "dormant" when the vehicle is being used, initiates an emergency call, which is triggered automatically by vehicle sensors only in the event of an accident. The call may be also triggered manually by the vehicle occupants and transmits the eCall to the appropriate PSAP. The Public Safety Answering Point may either be a public authority or a private service provider operating under the responsibility of a public authority.

In addition to activation of the audio channel, the second event triggered automatically as a result of an accident consists in generating the Minimum Set of Data and sending it to the PSAP, which is of key importance when there is no voice contact with the occupants of the vehicle. The eCall (data and voice), carried through the mobile network, is recognised by the mobile network operator as a 112 emergency call.

1.2. Initiatives of the European Parliament and the European Commission

One of the initiatives of the European Commission, to date, in the context of eCall, was the establishment of the eSafety Forum, a joint industry/public initiative for improving road safety by using advanced Information and Communications Technologies. eCall was identified as one of the highest priorities\(^1\), and a Driving Group on eCall involving all stakeholders was established. The eCall Driving Group has prepared various recommendations\(^2\), as well as a Memorandum of Understanding on implementing eCall\(^3\).

The Memorandum of Understanding binds the stakeholders in implementing the eCall initiative jointly on the basis of a common approved framework and certain interface specifications, including the Minimum Set of Data (MSD).

In Recommendation no. 2011/750/EU of 8 September 2011 on support for an EU-wide eCall service in electronic communication networks for the transmission of in-vehicle emergency calls based on 112 ("eCalls"),\(^4\) the Commission stressed the necessity of introducing a harmonised pan-European in-vehicle emergency call system. As the Commission has pointed out: "A harmonised solution across Europe would ensure interoperability for transmitting the voice/audio call and the minimum set of data generated by the in-vehicle eCall system to the public safety answering point, including the accurate location and time of the incident. A harmonised solution would also ensure the continuity of the eCall service across European countries. With the high volume of cross-border traffic in Europe, there is a growing need for a common data transfer protocol for passing such information to public safety answering points and emergency services in order to avoid the risk of confusion or wrong interpretation of the data passed" (point 5 of the Recommendation).

---


\(^2\) Some of the recommendations from the Driving Group eCall, can be found on the following website: http://www.imobilitysupport.eu/imobility-support/its-deployment/ecall/library/reports-13.

\(^3\) Memorandum of Understanding for Realisation of Interoperable In-Vehicle eCall (28.05.2004).

\(^4\) OJ L 303/46.
The European Parliament has expressed its support for the introduction of eCall on numerous occasions, including support for its mandatory deployment, as "an initiative that will create a feeling of greater safety for citizens when travelling". In its resolution of 3 July 2012, the European Parliament has, inter alia, called on the Commission, to take into consideration - while assessing the impact of the deployment of the eCall in the EU - not only the investment and operational costs but also the social benefits resulting from the deployment of the eCall. The European Parliament has also stressed that "it must remain a dormant system until an emergency call is triggered" as well as that "appropriate rules that respect transparency should be included for the processing of personal data relating to eCalls, not only by MNOs but also by all other actors involved, including vehicle manufacturers, PSAPs and emergency services".


In the framework of the Commission’s Proposal for a Regulation of the European Parliament and of the Council concerning type-approval requirements for the deployment of the eCall in-vehicle system and amending Directive 2007/46/EC COM(2013) 316 final; hereinafter referred to also as the “Proposal” or “Commission’s Proposal”), in addition to general and specific obligations imposed on manufacturers and the Member States concerning the type-approval requirements, the Proposal contains rules on privacy and data protection (Article 6 and Recital 13). In particular, the Proposal seeks to ensure that any processing of personal data through the eCall in-vehicle system complies with the personal data protection rules contained in Directives 95/46/EC and 2002/58/EC.

Recital 8 of the Proposal clarifies that the mandatory equipping of vehicles with the 112-based eCall in-vehicle system is "without prejudice to the right of all stakeholders such as car manufacturers and independent operators to offer additional emergency and/or added value services, in parallel with or building on the 112-based eCall in-vehicle system", and adds that such additional services should not distract the driver from the road.

---

5 Resolution of 3 July 2012 on eCall: a new 112 service for citizens (2012/2056(INI)).
6 Cf., point 34.
7 Cf., point 35.
## 2. MANDATORY 112-BASED ECALL IN-VEHICLE SYSTEM

### KEY FINDINGS

- The replacement of the current (voluntary) framework with a mandatory solution in the context of the in-vehicle eCall system would call for the imposition of a clear obligation on both the manufacturers (vendors) of new vehicles, and their users (i.e., the obligation to maintain the device in working condition).

- The functioning of the mandatory (even “dormant”) in-vehicle eCall system may entail the processing of personal data.

- The scope of the Minimum Set of Data would need to be expressly enshrined in law. In defining the scope of the Minimum Set of Data, the principles of proportionality and minimisation should be observed, pursuant to which only data which is necessary to achieve the intended purpose, i.e. the proper handling of emergency calls, should be processed.

- The Proposal must be further clarified to ensure that the prohibition of constant tracking does not affect proper operation of the eCall system, since tracking is used to determine the direction of driving. In particular, the possibility of storing several (e.g. three) last locations of the vehicle should be sufficient.

- The general obligation to equip the in-vehicle eCall system with privacy enhancing technologies should be accepted.

- The wording of Article 6 (3) of the Proposal should be modified to ensure that the duty to provide certain information covers not only information “about the processing of data”, but broader information on the rules governing the operation of the eCall system, in particular with respect to privacy and personal data protection.

- The proposal to define in the proposed regulation the periods of retention of the data processed in the eCall system should be accepted.

- Although PSAP should be qualified as controllers of personal data processed under the mandatory eCall in-vehicle system, the specificity of the eCall system means that determining the scope of the responsibilities of actors other than the data controller at a regulatory level is an issue of key importance (e.g., responsibility for conveying basic information to the users to remain with the manufacturer).

### 2.1. From voluntary to mandatory system

The Commission’s Proposal envisages the introduction into the EU – with effect from 1 October 2015 – of a mandatory in-vehicle eCall system for new types of vehicles (Article 5 and Article 7 of the Proposal). As has been emphasised in Recital 5, “the mandatory introduction of the eCall system would make the service available to all citizens and thus contribute to reduce human suffering and healthcare and other costs”. This represents a material change in the current approach because, to date, the introduction of an in-vehicle eCall system relied on voluntary initiatives based on self-regulatory instruments. This change of approach would also be of paramount importance in the context of privacy and personal data protection. This is particularly because, in the case of a mandatory system, the legal ground for changes in the processing of data, and also the expectations of hard-law regulation, should be much more far-reaching.

Before more detailed analysis is embarked on in connection with the adoption and introduction into the EU of a mandatory in-vehicle eCall system, the issue of the mandatory
Policy Department A: Economic and Scientific Policy

character of the system should be raised, since this development not only affects manufacturers, as follows from the Proposal, but also vehicle users. This issue is also important in the context of issues related to the protection of privacy and personal data, especially with respect to the legality of a data subject (vehicle user) “raising an objection” against the processing of his/her data for the purposes related to handling of emergency calls (e.g. by deactivating the in-vehicle eCall system functionalities, even if the manufacturer does not make this easy for a vehicle user to do so without the intervention of a specialist technician). The Proposal does not address this issue, which may be interpreted as the absence of a prohibition on such potential action by users of eCall equipped vehicles. It seems, however, that the replacement of the current framework with a mandatory solution would call for the imposition of a clear obligation on all actors in the system, including both the manufacturers (vendors) of new vehicles, and their users (the obligation to maintain the device).

2.2. Risks for privacy and personal data processing

Reservations with respect to protection of the privacy of vehicle users are mainly connected with the risk that the data processed in the mandatory eCall system may be used for purposes which are inconsistent with the original purpose for which the system is created, which may lead to misuse. This risk relates in particular to all data based on the vehicle’s location, which, given contemporary technological developments, may be used to precisely define the place where persons (motor vehicle users) are travelling to and are located. As noted by the European Data Protection Supervisor (EDPS) in the Opinion of 27 July 2009, “the use of location technologies is particularly intrusive from a privacy viewpoint as it allows for the tracking of drivers and for the collection of a wide variety of data relating to their driving habits. (...) the processing of location data is a particularly sensitive matter involving the key issue of the freedom to move anonymously, and which requires the implementation of specific safeguards in order to prevent surveillance of individuals and misuse of the data” (point 45). This is also a significant risk in the context of a mandatory eCall system, which seems to be “dormant”, however, whose functionality allows the vehicle’s location to be established continuously, i.e., not only after the occurrence of an accident or another event (cf. further remarks).

Tracking the location of persons is a material interference with privacy, because it can reveal vast information concerning their lives and activities. It has been pointed out that “a person who knows all of another’s travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups — and not just one such fact about a person, but all such facts”. In the context of the discussed Proposal, this could lead to the processing of personal data, including sensitive data (Article 8 of Directive 95/46/EC). As noted by the Article 29 Working Party, “a behavioural pattern may also include special categories of data, if it for example reveals visits to hospitals and religious places, presence at political demonstrations or presence at other specific locations revealing

---


Data about for example sex life. These profiles can be used to take decisions that significantly affect the owner.”

2.3. Personal data – are they really involved?

Functioning of the in-vehicle eCall system may entail the processing of personal data, given the very broad definition of this concept in European legislation and practice (including the interpretation given to it by the Article 29 Working Party, the EDPS, and others). Such processing will in particular affect private cars (and their owners) in the situation when “the vehicle identification is directly related to the identity of the owner of the car who is in several cases identical with the driver”11. In such a case, it will be quite easy to identify a specific natural person using the Vehicle Identification Number (VIN).

Even if the Vehicle Identification Number (VIN) was not processed for the purposes of a mandatory in-vehicle eCall system (scope of the Minimum Set of Data is to be defined; cf. further remarks), there would be potential situations in which a specific person could be identified or “singled out” from among a particular group of persons. This has been pointed out by the Article 29 Working Party in the context of mobile technologies, such as mobile phones or smartphones, however, the same problem must be seen to exist in the case of geolocation of motor vehicles. In Opinion 13/2011, the Working Party states that: “It is a fact that the location of a particular device can be calculated in a very precise way, especially when the different geolocation infrastructures are combined. (…) Especially with repeated observations, it is possible to identify the owner of the device. (…) Moreover, following Opinion 4/2007 on the concept of personal data, it also should be noted that a unique identifier, in the context described above, allows the tracking of a user of a specific device and, thus, enables the user to be “singled out” even if his/her real name is not known”12.

Moreover, even if no personal data were involved (which is not the case here), the legal assessment of the mandatory eCall system should take into account the even broader concept of privacy (see, as an example, the regulation of “cookies” under Article 5(3) of the e-Privacy directive, where the qualification of cookie as personal data is irrelevant to the protection of the private sphere of individuals’ lives and activities).

2.4. Practical implications for the legislature

The proposal to include a separate provision in the proposed regulation dedicated to privacy and personal data protection issues (Article 6 of the Proposal) should be commended, considering the risks that the eCall system may pose in this respect. The following discussion considers issues which should be addressed in further work on the Proposal, as well as those whose detailed regulation does not seem to be necessary.

2.4.1. Scope of the data (Minimum Set of Data)

As provided for in the Commission’s Proposal, the Minimum Set of Data “sent by the eCall in-vehicle system shall include only the minimum information required for the appropriate handling of emergency calls” (Article 7 (2) of the Proposal). However, the Proposal does not

state is precisely what meant by “the minimum information required for the appropriate handling of emergency calls.” As a result, this provision has little normative value. Taking into consideration the mandatory model introducing the in-vehicle eCall system and its impact on privacy and data protection, it seems that it is necessary to expressly provide for the scope of the Minimum Set of Data in primary (i.e. the proposed regulation) rather than in secondary legislation\textsuperscript{13}. Such a solution will help avoid doubts when applying the regime as to those categories of data which are indispensable and those which are dispensable in the above sense. This should also materially strengthen the protection of the privacy of vehicle users, because the risk of processing a wider scope of data for purposes other than the proper handling of emergency calls will be avoided.

The need for such an express definition seems all the more justified if attention is given to the significant differences in the Minimum Set of Data which are present in the documents concerning this issue and which have been adopted to date. For example, the Minimum set of Data that has been standardised by the European Committee for Standardisation (CEN)\textsuperscript{14} as encompassing the following information (obligatory as well as optional):

- message identifier (MSD format version),
- activation (whether the eCall has been manually or automatically generated),
- call type (whether the eCall is a real emergency or a test call),
- vehicle type (passenger vehicle, buses and coaches, light commercial vehicles, heavy duty vehicles, motorcycles),
- vehicle identification number (VIN),
- vehicle propulsion storage type, which is important particularly for fire and electrical power source risk issues (e.g. gasoline tank, diesel tank, compressed natural gas (CNG), etc.),
- time stamp (timestamp of incident event),
- vehicle location, determined by the on-board system at the time of message generation (i.e. the last known vehicle position),
- confidence in position (this is to be set to “Low confidence in position” if the position is not within the limits of +/-150m with 95% confidence),
- direction (helpful in determining which side of the road the vehicle was using at the time of the incident),
- optional: recent vehicle location n (vehicle’s position in (n-1) and (n-2)),
- optional: number of passengers (number of fastened seatbelts),
- optional additional data.

The Memorandum of Understanding, on the other hand, in Annex B (“The in-vehicle eCall minimum data set”) defines the mandatory Minimum Set of Data as follows:

- time stamp (time of incident),
- precise location,
- vehicle identification,
- service Provider Identifier,
- eCall qualifier (as a minimum, an indication stating whether the eCall has been made manually or automatically).

\textsuperscript{13} The same position was expressed by EDPS in its Opinion of 29 October 2013 (point 49-50).
\textsuperscript{14} EN CEN 15772.
A similar scope of data is provided for in the **recommendations of the Driving Group on eCall**, where it has been indicated that precise location also includes the direction of driving. In defining the scope of the Minimum Set of Data, the principles of proportionality and minimisation (Article 6 (1) (c)) of Directive 95/46/EC should be observed, pursuant to which only data which is necessary to achieve the intended purpose, i.e. the proper handling of emergency calls, should be processed. In this context, doubts emerge as to whether processing such data as the **Vehicle Identification Number (VIN)** is necessary to achieve this purpose. It seems that for the needs of handling an emergency call per se, precise knowledge of whose vehicle the signal has been sent from will not be required. It seems that for the emergency services (in particular the fire brigade) the knowledge of such data as the vehicle type and the vehicle propulsion storage type will be sufficient; this information relates to a group of vehicles and does not allow for the identification of a specific vehicle and, consequently, a specific person. However, data such as the Vehicle Identification Number (VIN) may be indispensable for other purposes, in particular those related to counteracting misuse of the eCall system (e.g. calling emergency services without a legitimate reason). It seems that for such purposes the possibility of identifying a specific vehicle, and – consequently – a specific person perpetrating such acts, may be indispensable. The Proposal, and in particular Article 6 (2), fails to address this issue. This must therefore be addressed in further work.

### 2.4.2. Constant tracking

Considering the risks related to tracing the location of motor vehicles (especially constant tracking), as well as the postulates of the Article 29 Working Party and the European Data Protection Supervisor, the Commission has included in the Proposal an explicit ban on constant tracking in the **“normal operational status related to the eCall”** (Article 6 (1)). It seems from the Proposal that the eCall system, including its functionality which enables determination of the vehicle’s precise location, is to be activated only after the occurrence of an accident or another event. However, the legality of constant tracking must first be established per se before discussing if it should be only excluded from the **“normal operational status related to the eCall”**. In order to designate the direction of driving, which is one of the key parameters in the Minimum Set of Data, it ought to be noted that the geographical coordinates of a vehicle must be determined at specific time intervals. This means that the functionality allowing the vehicle’s location to be accurately established is **active continuously**, and not only after the occurrence of an accident or another event. Thus, from this perspective the notion of “dormant” system may be quite misleading, since the system (i.e. the in-vehicle device) is in fact active even before an accident or another event. Nonetheless, in the normal course of events, only the last three location measurements are sufficient in determining the direction of driving.

---


16 The direction of driving is particularly important in the case of motorways where the lanes leading in opposite directions are separated by permanent barriers, which is of paramount importance for the planning of an optimum route of access of the emergency vehicles to the accident site.


Consequently, Article 6 (1) of the Proposal must be further clarified to ensure that the prohibition of constant tracking does not affect the proper functioning of the eCall system, i.e. determination of the direction of driving. In particular, the possibility to store several (e.g. three) last locations of the vehicle should be allowed\(^{19}\). However, this possibility should be limited exclusively to storing data in the internal memory of the in-vehicle device, while there should be a guarantee (also in the technical sense) that data:

- is continuously, automatically removed from the system so as to ensure that at any time the system does not store more than several (e.g. three) last locations of the vehicle;
- is not available from outside of the in-vehicle system to any entities before system activation (thus, upon activation of the system, the following would be communicated to the PSAP: location of the vehicle at the time of the accident and its several immediately preceding locations to enable the determination of the direction of driving).

### 2.4.3. Privacy by Design / Privacy Enhancing Technologies

The general obligation of equipping the in-vehicle eCall system with privacy enhancing technologies, provided for in Article 6 (1) (2) of the Proposal, should be accepted. It is all the more important if the fact that current EU laws do not directly impose such an obligation is taken into consideration. To cater for privacy, it is necessary to design the internal memory of the in-vehicle eCall system device in such a manner that it ensures the storage of several (e.g. three) last locations of the vehicle, while the previous system records are permanently removed on an ongoing basis. Specific security measures will also be of paramount importance in this context, including those related to establishing the location of data processing at a specific time (e.g. the requirement to store data on most recent locations of the vehicle in the internal memory of the in-vehicle device while the eCall system is dormant)\(^{20}\). Detailed requirements in this respect should be defined in delegated legislation, in accordance with the proposed wording of Article 6 (4) of the Proposal.

### 2.4.4. Informational obligations

It is advisable that informational obligations, including the scope of information required and its formulation (Article 6 (3) of the Proposal) be defined in the text of the proposed regulation\(^{21}\). However, it seems expedient that the wording of this provision should be modified to ensure that the duty to provide certain information covers not only information “about the processing of data”, but broader information – about the rules governing the operation of the eCall system, in particular with respect to privacy and personal data protection. This is all the more justified since the catalogue of detailed information (though given by way of example only) which has been provided does include issues related to the operation of the eCall system as such (e.g. the fact that the eCall in-vehicle system is activated by default), whose importance extends beyond issues of privacy and personal data protection.

It is also recommended that the rules pursuant to which the informational obligations are to be discharged in practice (e.g. as part of technical documentation of the vehicles) be further

\(^{19}\) The same position has been expressed by the Article 29 Working Party, *Working document on data protection...*, p. 5.


\(^{21}\) The same position was taken by EDPS in the Opinion of 29 October 2013 (point 26).
clarified\textsuperscript{22}. Any potential examples of discharge of the obligation included in the proposed regulation should not impose any restrictions on manufacturers as to providing the information in other ways, including highly user-friendly ones (e.g. a dedicated document / a special insert to be attached to the vehicle technical documentation).

2.4.5. Other principles of personal data processing

The proposal to define the \textbf{periods of retention} of the data processed in the eCall system in the proposed regulation should be accepted\textsuperscript{23}. The general data protection rules are not sufficient to specify the retention period. According to general data protection rules the data may be processed for no longer than is necessary for the purposes for which the data was collected. This highly general and not very precise rule may pose problems in practice. If possible and reasonable, it would be better to exactly define specific retention periods for the eCall system. The defined retention period would need to be grounded on the basis of how long the data is needed for the purposes of the eCall system. For the immediate task of sending an ambulance this would usually be only a few minutes, and in any case not much longer than the greatest margin of time an ambulance might possibly need to get to the place of accident - which would hardly ever be more than a single day. For other purposes, however, a much longer period might be necessary. This would, in particular, be the case to ensure that the victim of an accident could prove the PSAP’s liability in case no ambulance was actually sent. In order to provide the necessary evidence for a claim in damages for the tardy arrival of, or no response from, the emergency services, a retention period of at least two years, and perhaps even longer, would be necessary. Simply as a starting point for the discussion, not as a fully reflected proposal, one could envisage that a specific regulation relating to the eCall system would require the data to be blocked in favour of the data subject within a rather short time after the eCall was made. However, the blocked data should then continue to be stored for a rather long time to allow the data subject to prove that no ambulance came or came late.

It may even be that the determination of a uniform time frame, which would additionally apply throughout the EU, could not be achieved. Therefore, it seems that a certain minimum solution in this respect could be represented by one similar to that adopted in Commission Delegated Regulation (EU) No 305/2013 of 26 November 2012 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the harmonised provision for an interoperable EU-wide eCall\textsuperscript{24}. According to Article 7 (2) of this Regulation, “both the raw MSD [Minimum Set of Data] received with the eCall and the MSD contents presented to the eCall operator shall be retained for a determined period of time, in accordance with national regulations. Such data shall be stored in accordance with Articles 6, 13 and 17 of Directive 95/46/EC”.

Indicating the necessity to apply EU laws concerning processing of personal data (i.e. Directive 95/46 and Directive 2002/58) in the proper body of the regulation and not only in the recitals (Recital 13) to the Proposal, does not seem to be necessary\textsuperscript{25}. The obligation to apply the national laws adopted on the basis of the abovementioned EU laws is provided for precisely in those national laws, as a result of which it does not need to be emphasised and repeated in each subsequent EU legal act whose subject matter may to any

\begin{itemize}
\item \textsuperscript{22} See also EDPS in its Opinion of 29 October 2013 (point 27).
\item \textsuperscript{23} The same position was taken by EDPS in point 18 of the Opinion of 29 October 2013.
\item \textsuperscript{24} OJ EU L 91/1.
\item \textsuperscript{25} Cf. remark by EDPS in point 8 of its Opinion of 29 October 2013.
\end{itemize}
degree involve the processing of personal data. In this respect a reference to those data protection regulations made in the recitals seems to be sufficient, however:

- the suggestion that the application of these provisions stems from a recommendation by the Article 29 Working Party should be removed;
- the wording should make it absolutely clear (as does Recital 13 of the Proposal) that the provisions are applicable in the case of processing of personal data, so as to avoid the suggestion that they will be applicable in any event, also if the scope of the processed data – in the circumstances of a specific case – does not allow for such data to be classified as personal data within the meaning of Directive 95/46.

Furthermore, it does not seem to be necessary to provide a detailed definition in the Proposal (whether among the substantive provisions, or in the recitals) of the **basic principles** governing the processing of personal data, such as the principle of proportionality or the purpose limitation principle. Under the national laws adopted on the basis of the EU directives, these principles will also apply to the personal data processed using the in-vehicle eCall system. Moreover, the introduction of a ban on the processing of personal data used for the purpose of handling emergency calls for **other purposes** would in fact rule out the possibility of providing additional emergency services and the added value services referred to in point 8 of the recitals (cf. further remarks).

### 2.5. Actors involved – who should be responsible and for what?

Since numerous actors are participating in influencing various aspects of the eCall system (both with regard to its design, including the construction of particular IT devices and systems, and to its functioning), it is difficult to determine the status of particular actors within the context of personal data processing, and consequently the scope of their responsibilities. It is rather clear that the **PSAPs** are **controllers of personal data** processed under the mandatory eCall in-vehicle system aimed at purposes connected with the handling of emergency calls (increasing road safety). In addition, it was already decided in the provisions of the Commission Delegated Regulation (EU) No 305/2013 of 26 November 2012 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the harmonised provision of an interoperable EU-wide eCall to qualify the PSAP as data controllers. The PSAP would be burdened with the fundamental scope of responsibilities resulting from regulations concerning personal data, including those connected with handling the rights of entities (e.g. handling access requests). One may wonder whether this needs to be specifically regulated in the Proposal under discussion here since this should already follow from the existing legal framework.

However, the specificity of the eCall system requires the scope of responsibilities of actors other than the data controller to be determined at a regulatory level. This is because of the eCall’s technological features and the fact that actors other than the formal data controller have an impact on them. These actors include manufacturers of the eCall device who determine technical rules governing, for instance, the scope of data processed in an in-vehicle device to which they might not later have real access. In other words: The proposal...
should determine the scope of responsibilities of the other actors involved, besides the PSAP and in particular that of the manufacturers.

2.5.1.  Practical implications for the manufactures

Excluding the requirements imposed on data controllers (i.e. the PSAPs), the fundamental weight of responsibility shall apply to the manufacturers, due to their influence on the system’s construction (especially including particular devices), as well as due to the actual circumstances, including those connected with the stage at which a particular piece of information should reach the interested persons (vehicle users). In this respect, the Proposal correctly assumes that the responsibility for conveying the basic information to the users shall be borne by the manufacturer (Article 6 (3)).

2.5.2.  Practical implications for other actors

The role of other actors with respect to data processing does not seem important enough to be included in the provisions of the Proposal. This applies in particular to the national type-approval authorities. Nevertheless, mobile network operators, who shall act as data and voice signal conveyors to the Public Safety Answering Points, should ensure compliance with the provisions of the ePrivacy Directive. As the Commission states, “mobile telecommunications operators need to handle eCalls in the same was as they handle 112 calls”\(^{30}\). Obviously, the classification of the above actors may change significantly with regard to providing added value services if they provide such services on their own account and process – as data controllers – personal data for their own purposes.

2.6.  Other possible uses of eCall data

Issues connected with using data processed for the purposes of the mandatory (“dormant”) eCall system for other purposes (change of personal data processing purpose) also need to be decided, in particular:

- issues connected with establishing causes of a possible road accident (e.g. based on the average speed of the vehicle calculated on the basis of defined parameters, including vehicle location) and using this data for the purposes of prospective proceedings (civil, criminal, etc.)\(^{31}\);
- issues connected with the use of the eCall in-vehicle system as the “vehicle’s black box” which could enable recreating the behaviour of vehicles participating in an accident (in addition to speed, the considered parameters may include the force on the brake pedal, the condition of some APS sensors, ABS sensors, etc.)\(^{32}\);
- construction of databases to be processed for purposes related to the prevention of mandatory eCall system misuse, such as prevention of cases of unauthorised calls for emergency services\(^{33}\).

---


\(^{31}\) Ch. Geuens, J. Dumortier, Mandatory implementation for in-vehicle eCall..., p. 387.

\(^{32}\) H. Gut, Możliwości budowy systemu eCall... (Possibilities of Constructing an eCall system...), p. 11-12.

3. ADDITIONAL EMERGENCY AND/OR ADDED VALUE SERVICES (“PRIVATE” SERVICES)

KEY FINDINGS

- Due to the potentially significant impact on the privacy of the vehicle users, having regard to the obligation to prevent surveillance and misuse and taking Privacy by Design / Privacy Enhancing Technologies into account, the provision of additional emergency services, as well as added value services, should be subject to the same rules which apply to the mandatory (public) emergency services.
- It is reasonable to specify in detail in the proposed regulation the informational obligations with respect to such “private” services.
- The additional emergency services and added value services do not require more detailed regulation for rules similar to the regulation regarding the “public” eCall services. The rules of data processing in the context of additional services are governed by general provisions, therefore, it does not seem particularly necessary to define, in the provisions of the analysed Project, the following issues:
  - scope of the data (Full Set of Data),
  - legal basis, on which data processing for purposes connected with providing additional emergency/added value services should be based,
  - rights of vehicles users to deactivation of additional emergency/added value services,
  - retention periods.
- On the one hand, the prohibition of permanent tracking applicable also to added value services may be contrary to the expectations of the market, as well as of the vehicle users themselves. On the other hand, accepting the possibility of permanent tracking for purposes connected with providing added value services raises the question of the effectiveness of the prohibition of permanent tracking with regard to the eCall system’s normal functioning mode.

3.1. Examples of additional emergency/added value services

Private emergency services (referred to as “additional” services in the Proposal) have been provided for some time now by some automobile manufacturers such as Volvo, GM, Fiat, and BMW. The scope of these products is being constantly extended with services of other kinds (“added value services”) connected with such features as breakdown assistance, onboard mobile telephony or dynamic navigation. Opportunities to develop additional services are also discernable in other business models, including tourism, insurance, medical care or logistics (transport of dangerous goods by road, etc.) and many others. In practice, e.g., when the eCall generator installed inside the vehicle initiates an emergency call and transmits the eCall data to the appropriate PSAP, it may – at the same time, or later – transmit data to the emergency breakdown service in order to call them for additional help.

The Proposal also provides for the possibility of offering various services on the basis of the mandatory 112-based eCall system. In accordance with Recital 8 of the Proposal “The mandatory equipping of vehicles with the eCall in-vehicle system should be without prejudice to the right of all stakeholders such as car manufacturers and independent

---

operators to offer additional emergency and/or added value services, in parallel with or building on the 112-based eCall in-vehicle system. However, these additional services should be designed not to increase driver distraction. Chapter 3 of this note deals with such “private” services, in the context of privacy and data protection.

3.2. General or specific regulation – which approach should apply?

Due to the potentially significant impact on the privacy of vehicle users, having regard to the obligation to prevent surveillance and misuse and taking Privacy by Design / Privacy Enhancing Technologies into account, the provision of additional emergency services, as well as added value services, should be subject to the same rules which apply to mandatory (public) emergency services. In particular, such private services should – with the broadest scope possible and from the earliest possible stage (starting from technological design, as well as business modelling) – be defined in a manner considered “friendly” from the point of view of data protection and user privacy. It is also reasonable to specify in detail in the regulation the informational obligations with respect to such “private” services. Such specification should cover the scope of required information (in a more detailed manner than in Article 6 (3) (i) of the Proposal and in Article 10 of the Directive 95/46/EC), as well as the form and manner of its transfer to interested actors (e.g. under an agreement for providing such services, a dedicated document, etc.).

Nevertheless, a basic doubt remains on whether such “private” services require detailed regulation at the same level as the proposed European legislation with rules similar to those in the regulation regarding the “public” eCall services, in the context of other legal issues, other than those mentioned above. In accordance with the standpoint of the European Data Protection Supervisor, one of the Proposal’s basic weaknesses is the lack of reference between the rules specified in Article 6 and the additional emergency services and the added value services. It does not seem as though these services require – apart from the abovementioned general issues – such detailed regulation, since it is to be noted that the basis for data processing as regards such services (i.e. basically the consent of interested persons or an appropriate agreement, i.e. the basis indicated in Article 7 of Directive 95/46/EC) is fundamentally different. The rules of data processing in the context of additional services are governed by general provisions (current internal regulations of Member States compliant with Directive 95/46/EC, and in the future – provisions of the EU regulation). Therefore, it does not seem particularly necessary to define the following issues in the provisions of the analysed Proposal:

- **scope of the data (Full Set of Data)**: it does not appear possible to determine precisely the scope of data which could be processed for these purposes (no matter whether at the level of a proposed regulation or in delegated legislation); this could also pose a limitation for the development of such services, since it is not possible to predict in advance any services and data which might be required for their purposes;

- **the legal basis** on which data processing for purposes connected with providing additional emergency/added value services (the legal grounds are to be tracked in a general regulation, i.e. in the provisions of Directive 95/46/EC). However, it will be important to assess the opportunities and prospective access requirements by actors

---

35 According to Article 29 Working Party, “there is no reason to oppose such a scheme as a matter of principle”, Working document on data protection..., p. 7.

36 EDPS Opinion (29.10.2013), point 31 et seq.

37 EDPS Opinion (29.10.2013), point 20 et seq.
providing such services with regard to “historic” data processed for purposes connected with providing “public” eCall services;

- **rights of vehicles users** (data subjects) to deactivate additional emergency/added value services, since this right may be derived from the general rules (Directive 95/46/EC, Article 9 (2) of the Directive 2002/58/EC, as well as the freedom of contract);

- additionally, if – as stated above – the proposal to define, at least generally, the **retention periods** of data processed within the eCall system, is justified in terms of purposes connected with the functioning of the mandatory system, then the suggestion to determine retention periods as regards purposes connected with providing additional emergency/added value services seems far-fetched. The last issue mentioned should be governed by general rules which allow data processing for the time necessary to achieve the purposes for which they were collected (Article 6 (1) (e)) of the Directive 95/46/EC).

### 3.3. Other specific issues that may need to be regulated

The **prohibition of permanent tracking** adopted in the Proposal has been limited to the “*normal operational status related to the eCall*” (Article 6 (1)). The prohibition is – legitimately – referred to 112 eCall services, as well as to private eCall services, however, not to added value services. The European Data Protection Supervisor suggests also that, “by analogy with 112 and private eCall services, added value services shall not allow constant tracking”. The prohibition, however, may result in a real exclusion from the possibility to provide certain added value services, which require permanent contact with the in-vehicle device and downloading data on the vehicle location. The prospective prohibition may thus be contrary to the expectations of the market, as well as of the vehicle users themselves, for whom (at least for a part of them) the permanent monitoring while driving may not pose any problem. It should be noted that they would need to agree to such tracking, so permanent tracking would not be of a hidden nature.

On the other hand, accepting the possibility of permanent tracking for purposes connected with providing added value services raises the question as to the effectiveness of the prohibition of permanent tracking with regard to the eCall system’s normal functioning mode. For the implementation of both of the above mentioned objectives, the same in-vehicle system is used, which raises a doubt (mainly technical, not to be solved here) as to whether it is possible to allow permanent tracking for purposes connected with added value services on the one hand, whilst simultaneously on the other hand, effective implementation and observance of the prohibition of permanent tracking for purposes connected with the eCall system’s normal functioning mode.

---

38 EDPS Opinion (29.10.2013), point 53.
REFERENCES


- Commission, *Recommendation no. 2011/750/UE of 8 September 2011 on support for an EU-wide eCall service in electronic communication networks for the transmission of in-vehicle emergency calls based on 112 (‘eCalls’).*


- Memorandum of Understanding for Realisation of Interoperable In-Vehicle eCall (28.05.2004).
ROLE

Policy departments are research units that provide specialised advice to committees, inter-parliamentary delegations and other parliamentary bodies.

POLICY AREAS

- Economic and Monetary Affairs
- Employment and Social Affairs
- Environment, Public Health and Food Safety
- Industry, Research and Energy
- Internal Market and Consumer Protection

DOCUMENTS