



**1609/06/EN
WP 125**

Working document on data protection and privacy implications in eCall initiative

**Adopted on
26th September 2006**

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Civil Justice, Rights and Citizenship) of the European Commission, Directorate General Justice, Freedom and Security, B-1049 Brussels, Belgium, Office No LX-46 01/43.

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

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

Set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995¹,

Having regard to Articles 29 and 30(1)(c) and (3) of that Directive,

Having regard to its Rules of Procedure and in particular to Articles 12 and 14 thereof,

HAS ADOPTED THIS WORKING DOCUMENT:

1. INTRODUCTION

The aim of this working document is to outline data protection and privacy concerns arising in connection with the planned introduction of a harmonised pan-European in-vehicle emergency call ("eCall") service that builds on the single European emergency number 112².

One of the initiatives of the European Commission 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, and a Driving Group (DG) on eCall involving all the stakeholders was established³. The eCall Driving Group has prepared recommendations including a deployment roadmap that should facilitate making eCall a reality in all Member States and as a standard option available in all new vehicles from 1 September 2010 onwards⁴.

The DG eCall produced a Memorandum of Understanding (MoU) on implementing eCall. The aim of the MoU is to ensure that eCall will work in any EU Member State. The MoU binds the stakeholders in implementing the eCall initiative jointly on the basis of a common approved architecture and interface specifications, including the Minimum Set of Data (MSD). The MoU was signed by the European Commission, ACEA on behalf of the automotive industry and the multi-sector partnership ERTICO in August 2004. It has now over 60 signatures, including seven EU Member States⁵, Switzerland and Norway.

Recently, the European Parliament approved by a vast majority a resolution supporting the eCall Deployment⁶ urging the Member States to sign the MoU.

¹ OJ L 281, 23.11.1995, p. 31, available at: http://ec.europa.eu/justice_home/fsj/privacy/

² Communication from the Commission: The 2nd eSafety Communication: Bringing eCall to Citizens (COM(2005) 431, available at: http://europa.eu/information_society/activities/esafety/index_en.html

³ Communication from the Commission: Information and Communications Technologies for Safe and Intelligent Vehicles, COM(2003) 542 Final, 15.9.2003

⁴ The Recommendation from the Driving Group (DG) eCall, including all the annexes, can be found in the following website: http://www.esafetysupport.org/en/ecall_toolbox/driving_group_ecall.

⁵ Finland, Sweden, Greece, Italy, Lithuania, Slovenia and Cyprus

⁶ Report on Road Safety: Bringing eCall to citizens. Rapporteur: Gary Titley (A6-0072/2006)

Whereas the Article 29 Working Party recognises the socio-economic benefit that the wide introduction of the eCall service might bring to citizens, the deployment of the eCall service has privacy and data protection implications that have to be emphasized and properly addressed.

The Article 29 Working Party therefore considers it necessary, in view of the tasks entrusted to it by Article 30(1)(a) of the Data protection directive and in order to respond to the questions related to privacy and data protection arising in connection with the contemplated deployment of the eCall to analyze the current situation and dedicate this working paper to these issues.

2. PRINCIPLE OF ECALL

The proposed eCall architecture is based on a quasi-simultaneous voice-data link from an eCall generator to a first level Public Safety Answering Point ("PSAP"). The PSAP will either be a public authority or a private service provider operating under the responsibility of a public authority.

The eCall generator initiates an eCall triggered automatically by vehicle sensors in case of an accident or manually by the vehicle occupants, and transmits the eCall to the appropriate PSAP.

The eCall consists of two elements: a pure voice (audio) telephone call based on 112 and a Minimum Set of Data (MSD). The eCall (data+voice) carried through the mobile network, is recognized by the mobile network operator (MNO) as a 112 emergency call. Based on the 112 handling procedure, the MNO enriches the call with the CLI (caller line identification), and, according to the Universal Service Directive⁷ and the E112 Recommendation⁸, adds the best location available.

After this handling, the telecom operator delivers the 112-voice together with the CLI, best mobile location and the eCall MSD to the appropriate PSAP. Then the PSAP transmits an acknowledgement to the eCall generator specifying that the MSD has been properly received.

It is important to highlight that with the eCall service proposed, the in-vehicle system will not continuously be tracked by a third party, as it will not be permanently connected to the mobile communications networks, but only when it is activated in case of an accident or manually by the vehicle occupants.

The Minimum Set of Data (MSD)⁹ consists of the following (i) time of incident, (ii) precise location including direction of driving, (iii) vehicle identification, (iv) eCall qualifier giving the severity of the incident (as a minimum, an indication if eCall has

⁷ Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services. OJ L 108, 24.4.2002, p. 51

⁸ Commission Recommendation 2003/558/EC of 25 July 2003 on the processing of caller location information in electronic communication networks for the purpose of location-enhanced emergency call services. OJ L 189, p. 49.

⁹ See MSD description, eCall DG Final recommendations, section 4.2.2.4

been manually or automatically triggered), (v) information about a possible service provider.

The optional data related to the crash status foreseen in the MSD are still under discussion. The data included in this optional field (i.e., type of fuel that the vehicle uses) should comply with data protection regulations. In particular, they should comply with the principle of proportionality: only those data necessary for an appropriate handling of an emergency should be included.

The proposed eCall architecture contemplates the possibility that the effect of eCall could be further enhanced if additional vehicle and personal data are provided from a service provider based on additional data –Full Set of Data (FSD).

3. eCALL FROM PRIVACY AND DATA PROTECTION POINT OF VIEW AND LEGAL REASONING

3.1. *Mandatory or voluntary basis*

The European Commission has for the time being chosen a self-regulatory approach together with the Member States and industry, but in case the eCall roll-out fails to progress according to the agreed roadmap, it may consider further measures, including regulatory actions.

While the Article 29 Working Party recognises the socio-economic benefits and public safety value that the wide deployment of the eCall service might bring, there are nevertheless several data protection and privacy concerns that need to be addressed in this context.

Before looking closer at the data protection implications, the Article 29 Working Party took into consideration two options for implementation of eCall that should be looked into at the very beginning and then be further analysed:

- Option (1) eCall should be chosen on a voluntary basis or;
- Option (2) eCall should be a mandatory service.

Ad Option (1)

In case the eCall is deployed on a voluntary basis as a kind of advanced service supporting road safety, an easy way of activation/de-activation must be introduced.

In this case, the system is *de facto* embedded in the vehicle and its activation should be voluntary¹⁰. The user, who is not necessarily the owner of the vehicle, shall at anytime have the possibility to switch on or off the system without any technical or financial constraint. This possibility of choice could be offered, for instance, by the implementation of a dedicated and easy to use button/switch similar to that of the passenger airbag.

¹⁰ This does not mean that the service cannot be activated automatically when the engine is armed, but that the user should be free to deactivate/activate it at any moment.

This position is based on the fact that one of the central criteria for making data processing legitimate is Article 7 (a) of the Data protection directive which allows processing to take place if the data subject has unambiguously given his consent to the processing. Such consent shall be "freely given" and should also allow the data subject the opportunity to withdraw consent. It has to be stressed that the consent would not be freely given if the data subject has to accept a clause in this regard in the framework of a contract of non-negotiable clauses (as is generally the case with car sale contracts).

Furthermore, the Article 29 Working Party considers as illegal situations e.g. pressure from car insurance companies or car rental companies to keep the eCall tool activated. A similar obligation might be put on employees using company cars, where a consent to use eCall could be directly or indirectly forced.

The Article 29 Working Party would like to emphasize that if the eCall system cannot be activated or especially de-activated on the spot anytime without making additional efforts and free of charge, users will be afraid of possible privacy implications and may choose not to make use of it. As this may also be a stepping stone for the envisaged wide-spread adoption of eCall, an easy and costs-free de-activation must be introduced also in this respect.

Although in many cases the data processing may be in the vital interest of the data subject, and then the eCall deployment might be supported by Articles 7 (c), (d) and (e) of the Data protection directive, it will not be so in every case. For instance, there may be cases where an accident occurs, and the eCall is triggered automatically but there is no need for the emergency services.

The Working Party understands, on the basis of the information that is currently available on configuration of the eCall system, that it will be possible to geolocalize the relevant vehicle, which however will not be permanently tracked – that is, the system will be booked into the communication network only when an accident occurs or when it is manually triggered. The Working Party welcomes this feature and would like to stress that it would not be acceptable, from a data protection viewpoint, to have such devices permanently connected and vehicles thus permanently be trackable in view of the possible activation of eCall devices. This means that, for instance, it might be acceptable to retain, in the eCall device memory, the three vehicle locations last detected by GPS/Galileo systems (where available on board and interfaced with the eCall device), without communicating any data in the absence of a triggering factor (i.e. accident or manual activation). In such a case, it would be necessary to clearly limit the scope of the collected data and prevent any further use of the information – i.e. for purposes other than ensuring road safety.

Ad Option (2)

In case the eCall service is to be obligatory, the system would *de facto* be embedded in the vehicle and its activation would be mandatory. However, this option would need to be enforced by a dedicated EU-wide regulation. Such regulation would have to be properly justified in terms of data protection.

If eCall would be a mandatory tool then all privacy limitations while applying principles set out by the Data protection directive, such as among others, the principle of proportionality, must be spelled out clearly in the law. Privacy enhancing technologies

should be embedded in the eCall system in order to provide eCall users with the desired level of privacy protection. Also safeguards that will prevent surveillance and misuse have to be developed and integrated. This shall *vis a vis* apply to the scenario under Option 1. National data protection authorities should be consulted in order to provide advice regarding the best possible practices.

To sum up: If the eCall is optional, a user-friendly solution taking care of self-determination of car users by introducing the technical possibility to switch off/on eCall on a case-to-case basis must be introduced, for instance by means of electronic switches, smart cards or other devices allowing the voluntary activation of the eCall device and also, if desired, enabling the communication of data beyond the MSD. If the eCall is mandatory, rules have to be embodied in a dedicated law, taking into account data protection principles.

In both above mentioned cases, the Article 29 Working Party will support awareness raising with focus on the privacy and data protection implications. National data protection authorities under the umbrella of the Article 29 Working Party shall help to disseminate eCall awareness with emphasis on data protection issues such as transparent and legitimate processing of data collected via eCall.

The Article 29 Working Party privileges the voluntary approach for the introduction of the eCall service. In case the mandatory option is implemented, a system of proper data protection safeguards has to be introduced.

3.2. Two levels of services

Regardless of whether the eCall would be mandatory or optional, the eCall initiative anticipates the possibility of having an extended system with service providers providing value added services. In that case the two following service levels will exist:

(1) The first contemplated service triggers the communication of the information included in the Minimum Set of Data (MSD) to the appropriate PSAP, as the position of the vehicle, the time when the accident occurred, the identification of the vehicle and an eCall status (as a minimum, an indication if eCall has been triggered manually or automatically), which will provide identification as to the seriousness of the accident.

This "basic" service is the one promoted by the European Commission.

(2) The second level of the service lies in adding to the exchanged "basic" information included in the MSD, additional information held by a third party providing added value services, e.g. insurance companies, automobile call centres, medical companies, lawyers, motor clubs, etc. In case a "full set of data - FSD" is transmitted, a contract between the owner of the vehicle and the service provider is required.

In this scenario the user would allow the service provider to receive the additional data related to the incident or the vehicle occupants, for providing i.e. insurance company assistance, motor club support or linguistic support, etc. This extended service is expected to be developed by the market forces.

There is no reason to oppose such a scheme as a matter of principle. However, the issues here are more complex and require a more thorough assessment. Especially the rules on the security of data must be strictly complied with, in particular as some of that data to be processed is of a sensitive nature. For the extension of the eCall basic functionalities, that is a Full Set of Data sent to a private service provider in addition to the MSD, a detailed definition is required. These services should fully comply with the relevant regulations on data protection and privacy.

The Article 29 Working Party wants to recall the basic principles to be taken into account by third party providers:

- (i) The Working Party would like to stress that the FSD will not be an “*a priori*” set of information, as it will rather result from the stipulations made in the contracts between the vehicle owner /user - depending on the implementation of the FSD extension and the individual service providers (insurance companies, automobile clubs, medical companies, etc.). Hence, the purposes for which the FSD, and the individual items in the FSD, may be used are to be clearly spelled out in the individual contracts. The contracts should also clearly set out that the third party service provider is the controller of the relevant data and is bound by all the data protection and privacy obligations that pertain to data controllers under both the Data protection directive and national laws.
- (ii) Only such data which are “necessary” and “relevant” for the specific purposes may be transmitted, i.e. it must be ensured that each third party provider only receives those data that are required for the purposes of the respective contract. As it is obvious from a data protection viewpoint, no “en-bloc” transfer of the FSD may be permitted. This will likely require suitable technical arrangements in order for the eCall system to select only those data that are relevant to the individual service providers. In this connection, it will also be necessary to consider whether the relevant information is to be transmitted in all cases – as mentioned above, there may be cases in which an incident occurs and the system is triggered, but there is no need for emergency (medical) services.
- (iii) The categories of information included in the FSD should be defined clearly by the car industry and the stakeholders concerned, and suitable information must be provided to vehicle owners on the functioning and operation of the system. Such information should also include the consequences in case the owner decides to withdraw consent to transfer of the FSD, or part of the FSD; once again, withdrawing this consent should not be detrimental to the vehicle owner’s interests.
- (iv) Should the FSD also include medical or other sensitive data, it will be necessary to take extra care in dealing with the information set. As well as the vehicle owner’s explicit consent, processing these data requires specific security measures to be taken which in some cases are detailed in national legislation.
- (v) The provisions on onward transfers of the data will have to be complied with, in particular if any third party service provider were to outsource (part of) its processing operations to entities established in third countries; see, as useful guidance, the considerations contained in document WP74¹¹.

¹¹ http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp74_en.pdf

4. OTHER ISSUES AROUND eCALL

In general, there are also concerns related to the creation of databases by telecommunication operators, storage periods of collected data as well as issues related to the security of the data stored.

4.1. Databases

Another data protection concern arises in connection with the databases created in order to avoid misuse/abuse of the system which would link the car owner's identity and the SIM card of the eCall system whose main purpose would be to look for persons who abuse the system, for instance car drivers who get lost, etc.

In case of misuse/abuse of the system that could create prejudice to the PSAPs (i.e. a system makes multiple eCalls without valid reason) the PSAPs should establish a procedure to track the misusing system. In such a case, the following two procedures may be envisaged: (i) requiring the Mobile Network Operators to identify the owner of the device (via the information stored in the SIM database), as is the case for the 112 calls (ii) requiring the identification of the authority controlling the Vehicle Identification Numbers (VIN).

One of the main concerns of the Article 29 Working Party is the potential risk that any other third party might have access to these databases for different purposes. Therefore, the Article 29 Working Party wishes to emphasise that any secondary use of data, e.g. for enforcement procedures related to traffic, should not be allowed as it would be contrary to the principles of the Data protection directive.

4.2. Security issues

Another group of concerns is created by security issues as to whether the eCall system is secure enough against unauthorized entries. In order to implement a trustworthy system and avoid unauthorised access by various third parties to the personal data included in the eCall, a sufficient level of security needs to be ensured in the in-vehicle system and in the transport protocol¹².

4.3. Proportionality

While using eCall, a Minimum Set of Data (MSD) to handle the emergency will be circulated. The Article 29 Working Party considers that MSD including the complete VIN number as currently indicated could be excessive in relation to the clearly defined purpose.

The Article 29 Working Party is concerned about the possibility that the introduction of the eCall service may not be necessary in all cases in view of the currently running

¹² It is expected that automotive OEMs would ensure a sufficient level of security of the data stored in the in-vehicle system. On the other hand it is expected that the transmission protocol being standardised by ETSI would provide a sufficient level of security.

system of emergency calls which operates well across the Member States. This argument seems important as it raises a question of proportionality, i.e. is it proportionate to introduce a system of emergency calls based on geolocalisation in countries where a system of emergency calls already now works well?

4.4. Nature of data controller

The data controller in the eCall case will be the Public Safety Answering Point (PSAP), which should establish protocols concerning personal data storage, processing and protection similar to the ones implemented for any other emergency calls. The Mobile Network Operators will transmit the Minimum Set of Data in a transparent way, and they should ensure that there is no storage of the eCall data other than the time necessary to ensure its adequate transmission to the appropriate PSAP. The MSD should be deleted afterwards.

Concerning calling line identification, and localisation information transmitted to the PSAPs, similar protocols to the ones used to process E112 (location enhanced emergency calls) according to the Universal Service Directive and the Commission Recommendation on the processing of caller location information in electronic communication networks for the purpose of location-enhanced emergency call services, would have to be established.

4.5. Storage period

The Article 29 Working Party wishes to emphasise that adequate storage periods of eCall data should be defined for the different parties in the eCall service chain. National authorities shall monitor that periods are defined and properly observed.

5. CONCLUSIONS

The Article 29 Working Party, while identifying privacy concerns related to the eCall, privileges and recommends the voluntary approach for the possible introduction of the eCall service.

From a data protection point of view, an emergency call released automatically by a device or triggered manually and transmitted via mobile networks resulting in geolocalization of the emergency event is in principle admissible, provided that there exists a respective specific legal basis and sufficient data protection safeguards are provided. However, the purposes of the emergency call system and the relevance of the data to be processed must always be taken into account, in particular if the processing involves the so-called Full Set of Data.

Done in Brussels, on 26th September 2006

For the Working Party
The Vice-Chairman
Jose Luis Piñar Mañas