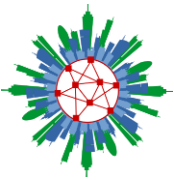


# Privacy and Smart Traffic Management

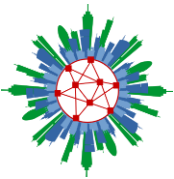
**Boris Reibach, LL.M.**

**[Boris.Reibach@uni-oldenburg.de](mailto:Boris.Reibach@uni-oldenburg.de)**



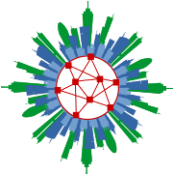
# Functions of Law in the Digital World

- Avoiding conflicts
- Common welfare
- Balance of inequality
- Trust
- Strengthening democracy



Legal framework shall provide for at least

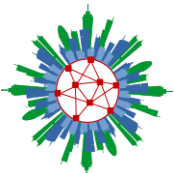
- Safety
- Security
- Freedoms and Basic Rights
- Privacy
- Liability
- Access



# Privacy as a Basic Right

## Article 8 of the European Convention on Human Rights

1. Everyone has the right to **respect for his private and family life, his home and his correspondence.**
2. There shall be **no interference** by a public authority with the exercise of this right except such **as is in accordance with the law** and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.



# EU Privacy Concept I

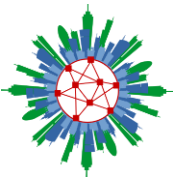
**Privacy**

**Data Security**



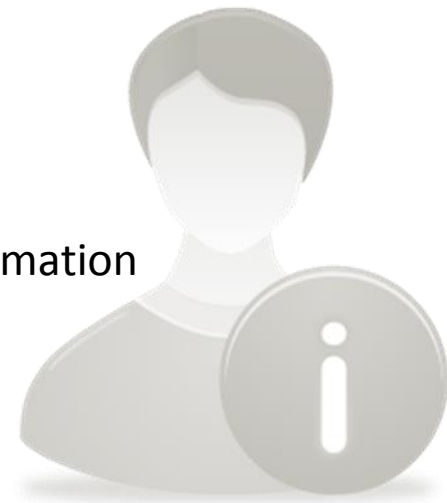
**Protects Humans**

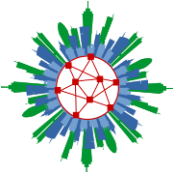
**Protects Data**



## Personal data

- means **any information relating to an identified or identifiable natural person** ('data subject')
- an identifiable natural person is one who can be identified, **directly or indirectly**, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
- applies **regardless of the sensitivity or relevance** of the data
- not limited to "private" data: includes publicly available/shared information





# Examples

Vehicle  
Identification  
Number

Username

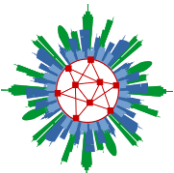
Personal  
Certificate

Licence  
Plate  
Number

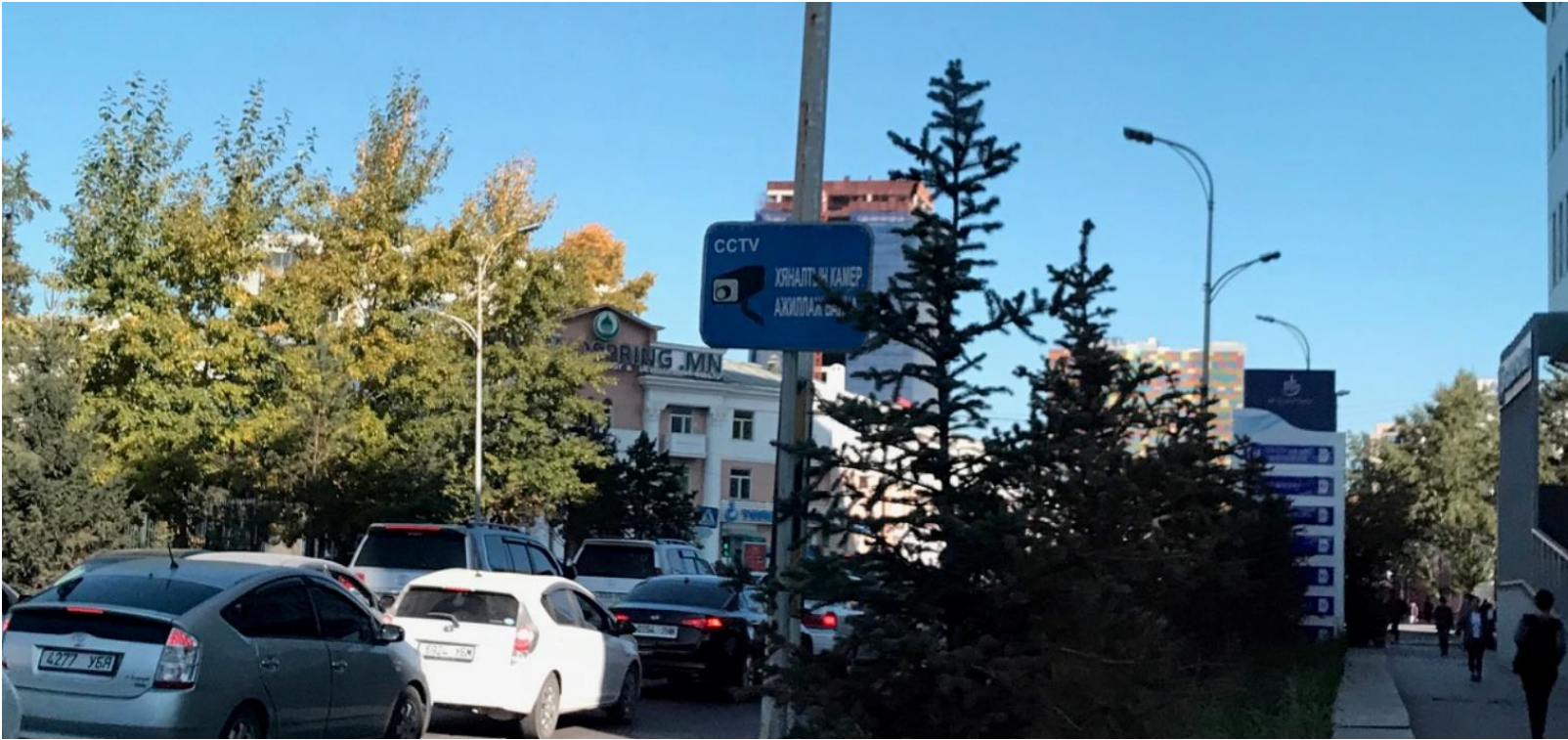
Video  
(Surveillance)  
Data

IP address

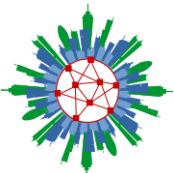
Audio Data



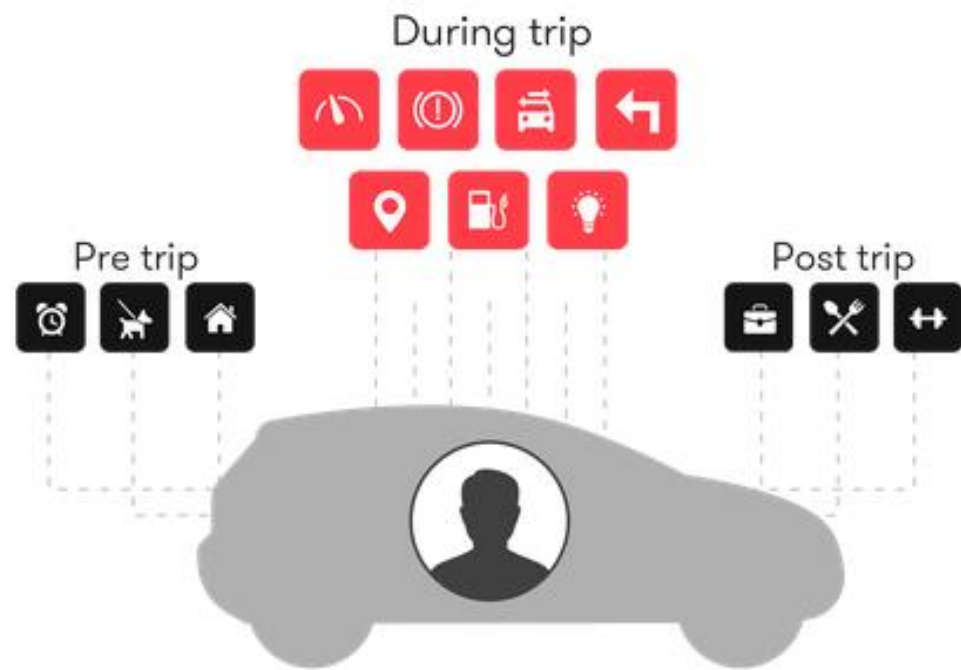
# CCTV is the Beginning

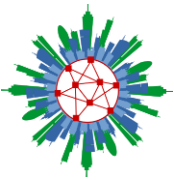




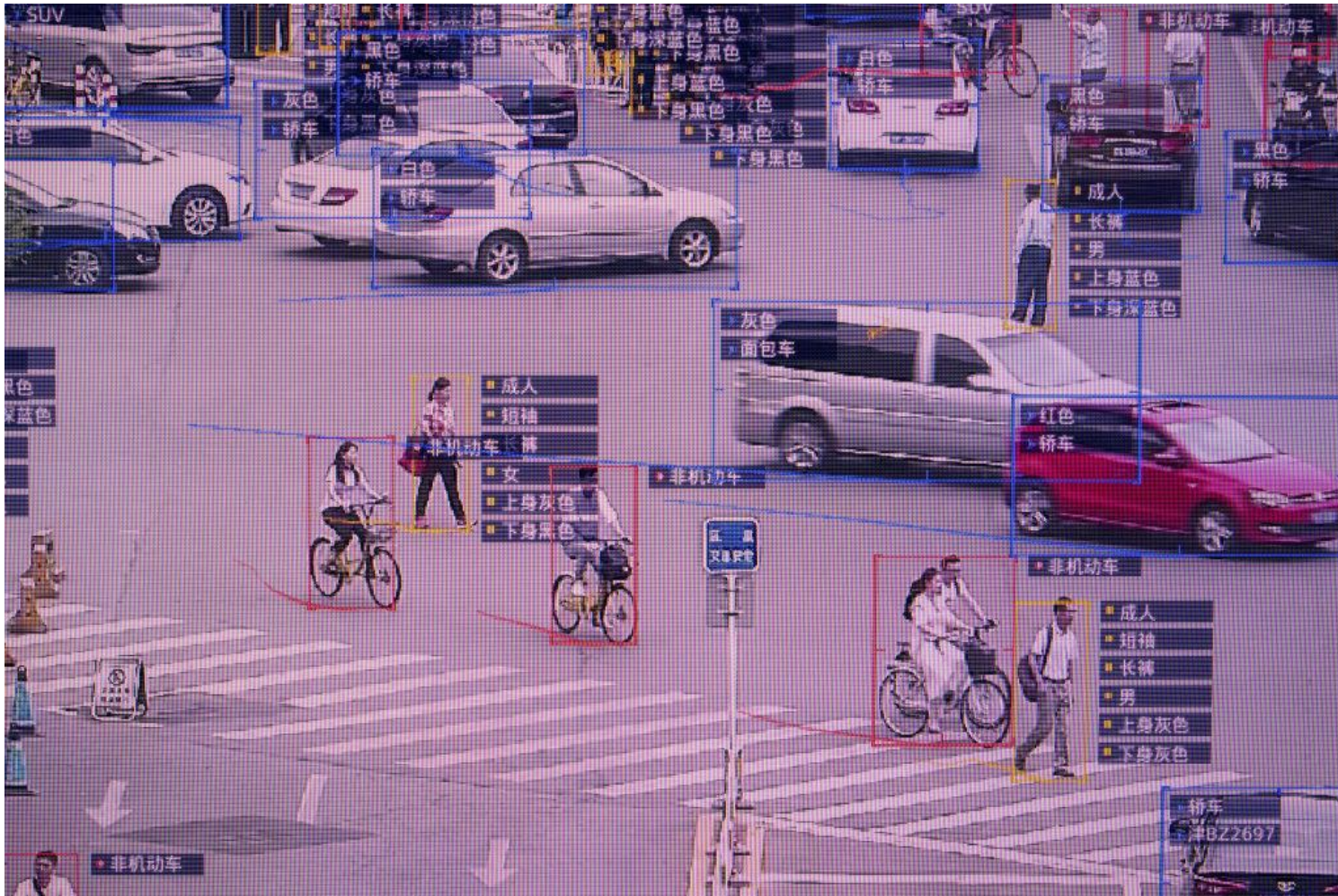


# Profiling as the Major Threat for Privacy

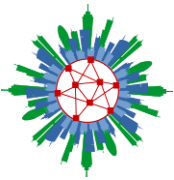




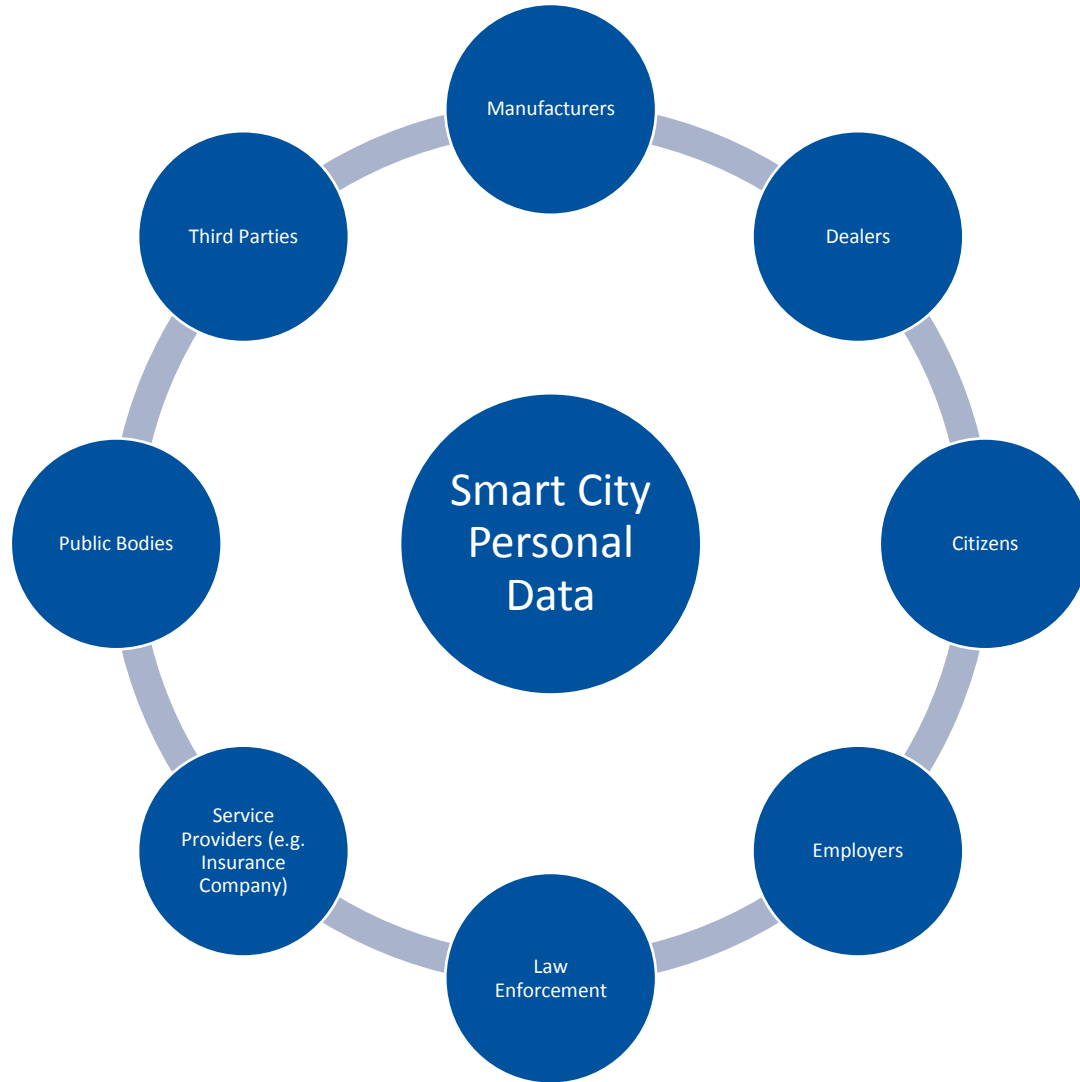
# Data Collection leads to a „Surveillance Society“

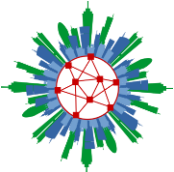


bloomberg.com



# Personal Data Desires



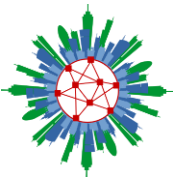


- In the context of smart cities lots of personal data are being processed
- Privacy remains an essential and crucial issue
- Consequence: Smart Cities = balancing act between the use of personal data to improve processes and services on the one hand and the guarantee of the citizen's right to privacy on the other
- Is it possible to establish Smart Cities with the given legal framework?

**YES**

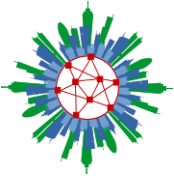


aclu.org



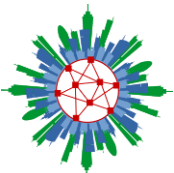
# Starting Point: 9 Privacy Principles

- Lawfulness
- Fairness
- Transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage Limitation
- Data security
- Accountability



# Satisfy the 9 Privacy Principles

- Lawfulness: Encode Parliament Law that explicitly allows for data processing
- Fairness: Give data subjects rights to control their data
- Transparency: Publish privacy policies and give data subjects access
- Purpose limitation: Prohibit usage of data for different purposes without consent
- Data minimization: Promote pseudonymization and anonymization techniques
- Accuracy: Enable an easy rectification of personal data
- Storage Limitation: Define retention periods and implement retention policies
- Data security: Provide for minimum controls or standards for data security
- Accountability: Encode sanctions and set up a supervisory authority




# Example: Amsterdam

### The 6 principles of our manifesto:

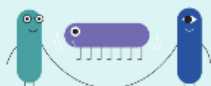
#### 01 Inclusive

Our digital city is inclusive. We take into account the differences between individuals and groups, without losing sight of equality.



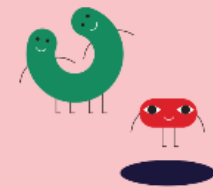
#### 02 Control

Data and technology should contribute to the freedom of people. Data are meant to serve the people. To be used as seen fit by people to benefit their lives, to gather information, develop knowledge, find room to organize themselves. People stay in control over their data.




#### 03 Tailored to the people

Data and algorithms do not have the final say. Humanity always comes first. We leave room for unpredictability. People have the right to be digitally forgotten, so that there is always an opportunity for a fresh start.




#### 04 Legitimate and monitored

Citizens and users have control over the design of our digital city. The government, civil society organizations and companies facilitate this. They monitor the development process and the resulting social consequences.



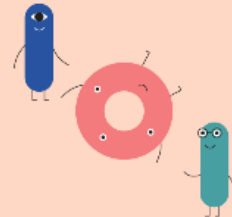
#### 05 Open and transparent

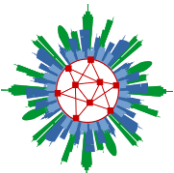
What types of data are collected? For what purpose? And what are the outcomes and results? We are always transparent about those aspects.



#### 06 From everyone - for everyone

Data that government authorities, companies and other organizations generate from the city and collect about the city are held in common. Everyone can use them. Everyone can benefit from them. We make mutual agreements about this.





# Example: Seattle



## City of Seattle Privacy Principles

The City of Seattle collects personal information from the public so that we can provide many important services including community and critical infrastructure protection, 911 call response, waste management, electricity delivery and other services.

*We work to find a fair balance between gathering information to provide needed services and protecting the public's privacy.*

While privacy laws protect some personal information, the information we collect becomes a government record that others can ask to see through public records requests. Therefore, it is important for you to know when and how your personal information is collected, how we use it, how we disclose it and how long we keep it.

The following Privacy Principles guide the actions we take when collecting and using your personal information:

**1** **We value your privacy...**  
Keeping your personal information private is very important. We consider potential risks to your privacy and the public's well-being before collecting, using and disclosing your personal information.

**2** **We collect and keep only what we need...**  
We only collect information that we need to deliver City services and keep it as long as we are legally required and to deliver those services. Whenever possible, we tell you when we are collecting this information.

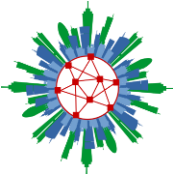
**3** **How we use your information...**  
When possible, we make available information about the ways we use your personal information at the time we collect it. We commit to giving you a choice whenever possible about how we use your information.

**4** **We are accountable...**  
We are responsible for managing your personal information in a manner that is consistent with our commitments and as required by law. We protect your personal information by restricting unauthorized access and by securing our computing resources from threats.

**5** **How we share your information...**  
We follow federal and state laws about information disclosure whenever we work with outside governmental agencies and in answering Public Disclosure Requests (PDRs). Business partners and contracted vendors who receive or collect personal information from us or for us to deliver City services must agree to our privacy requirements.

**6** **Accuracy is important...**  
We work to maintain and use accurate personal information for City business. When practical, we will work to correct inaccurate personal information. We also direct our partners and contracted vendors to follow the same guidelines.





# Example: EU eCall Regulation

## Article 6

### Rules on privacy and data protection

1. This Regulation is without prejudice to Directives 95/46/EC and 2002/58/EC. Any processing of personal data through the 112-based eCall in-vehicle system shall comply with the personal data protection rules provided for in those Directives.
2. The personal data processed pursuant to this Regulation shall only be used for the purpose of handling the emergency situations referred to in the first subparagraph of Article 5(2).
3. The personal data processed pursuant to this Regulation shall not be retained longer than necessary for the purpose of handling the emergency situations referred to in the first subparagraph of Article 5(2). Those data shall be fully deleted as soon as they are no longer necessary for that purpose.
4. Manufacturers shall ensure that the 112-based eCall in-vehicle system is not traceable and is not subject to any constant tracking.
5. Manufacturers shall ensure that, in the internal memory of the 112-based eCall in-vehicle system, data are automatically and continuously removed. Only the retention of the last three locations of the vehicle shall be permitted in so far as it is strictly necessary to specify the current location and the direction of travel at the time of the event.
6. Those data shall not be available outside the 112-based eCall in-vehicle system to any entities before the eCall is triggered.
7. Privacy enhancing technologies shall be embedded in the 112-based eCall in-vehicle system in order to provide eCall users with the appropriate level of privacy protection, as well as the necessary safeguards to prevent surveillance and misuse.
8. The MSD sent by the 112-based eCall in-vehicle system shall include only the minimum information as referred to in the standard EN 15722:2011 'Intelligent transport systems — eSafety — eCall minimum set of data (MSD)'. No additional data shall be transmitted by the 112-based eCall in-vehicle system. That MSD shall be stored in such a way as to make its full and permanent deletion possible.
9. Manufacturers shall provide clear and comprehensive information in the owner's manual about the processing of data carried out through the 112-based eCall in-vehicle system. That information shall consist of:
  - (a) the reference to the legal basis for the processing;
  - (b) the fact that the 112-based eCall in-vehicle system is activated by default;
  - (c) the arrangements for data processing that the 112-based eCall in-vehicle system performs;
  - (d) the specific purpose of the eCall processing, which shall be limited to the emergency situations referred to in the first subparagraph of Article 5(2);
  - (e) the types of data collected and processed and the recipients of that data;
  - (f) the time limit for the retention of data in the 112-based eCall in-vehicle system;
  - (g) the fact that there is no constant tracking of the vehicle;
  - (h) the arrangements for exercising data subjects' rights as well as the contact service responsible for handling access requests;
  - (i) any necessary additional information regarding traceability, tracking and processing of personal data in relation to the provision of a TPS eCall and/or other added value services, which shall be subject to explicit consent by the owner and in compliance with Directive 95/46/EC. Particular account shall be taken of the fact that differences may exist between the data processing carried out through the 112-based eCall in-vehicle system and the TPS eCall in-vehicle systems or other added value services.

10. In order to avoid confusion as to the purposes pursued and the added value of the processing, the information referred to in paragraph 9 shall be provided in the owner's manual separately for the 112-based eCall in-vehicle system and the TPS eCall systems prior to the use of the system.

11. Manufacturers shall ensure that the 112-based eCall in-vehicle system and any additional system providing TPS eCall or an added-value service are designed in such a way that no exchange of personal data between them is possible. The non-use of a system providing TPS eCall or an added-value service or the refusal of the data subject to give consent to the processing of his or her personal data for a TPS eCall service or an added value service shall not create any adverse effects on the use of the 112-based eCall in-vehicle system.

12. The Commission shall be empowered to adopt delegated acts in accordance with Article 8 in order to establish:

- (a) the detailed technical requirements and test procedures for the application of the rules on personal data processing referred to in paragraphs 2 and 3;
- (b) the detailed technical requirements and test procedures for ensuring that there is no exchange of personal data between the 112-based eCall in-vehicle system and third party systems as referred to in paragraph 11.

The first such delegated acts shall be adopted by 9 June 2016.

13. The Commission shall, by means of implementing acts, lay down:

- (a) the practical arrangements for assessing the absence of traceability and tracking referred to in paragraphs 4, 5 and 6;
- (b) the template for the user information referred to in paragraph 9.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 10(2).

The first such implementing acts shall be adopted by 9 June 2016.



**Boris Reibach, LL.M.**

University of Oldenburg  
Interdisciplinary Centre for Law  
in the Information Society (ZRI)



+49 441 798-4132

[Boris.Reibach@uni-oldenburg.de](mailto:Boris.Reibach@uni-oldenburg.de)