European Commission

JRC TECHNICAL REPORTS

Guidelines for public administrations on location privacy

European Union Location Framework

Leda Bargiotti
Inge Gielis
Bram Verdegem
Pieter Breyne
Francesco Pignatelli
Paul Smits
Ray Boguslawski

Version 1
2016






EUR 28202 EN

This publication is a Technical report by the Joint Research Centre, the European Commission's in-house science service. It aims to provide evidence-based scientific support to the European policy-making process. The scientific output expressed does not imply a policy position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use which might be made of this publication.

Contact information
Name: Francesco Pignatelli
Address: Via E. Fermi, 2749 21023 Ispra (VA), Italy
E-mail: francesco.pignatelli@jrc.ec.europa.eu
Tel.:+39 0332785659

JRC Science Hub
https://ec.europa.eu/jrc

JRC103110

EUR 28202 EN

ISBN 978-92-79-63495-6 (PDF)

ISSN 1831-9424 (online)

doi:10.2791/420310 (online)

How to cite: Leda Bargiotti, Inge Gielis, Bram Verdegem, Pieter Breyne, Francesco Pignatelli, Paul Smits Ray Boguslawski; Guidelines for public administrations on location privacy; EUR 28202 EN; doi:10.2791/420310

Table of contents

Abstract

Public administrations increasingly use location data to deliver public services such as location-enabled tools, apps for tourists, toll collection services or cadastral web applications. Location data such as addresses, GPS coordinates or camera images is key to many public services and can also be linked to all sorts of other data, generating new information that was not available before. Despite the increase consumption of location data, its potential to reveal personal information is often underestimated, especially in comparison to other sensitive data, for instance in the financial and health domains.

Location data not only says where an individual is, it also says who he/she is and what his/her interests and preferences are. Therefore, location data privacy is of paramount importance for public administrations dealing with location data. While location data privacy has many aspects in common with general data protection principles, it also has unique characteristics that require specific guidance.

The goal of this guideline is therefore twofold: to outline the key obligations that public administrations should comply with when handling personal location data and raising awareness about the importance of location data privacy, highlighting key implications and risks associated with the processing of location data. It does so by guiding the reader through concrete scenarios that public administrations might face when processing personal location data and provides a set of effective and practical recommendations that can help ensuring the adequate protection of personal location data.

Keywords: location data privacy, data protection, guidelines

1. Introduction

This document addresses public administrations that use or are planning to use location data in their products and services. It provides actionable recommendations to ensure that privacy-related aspects are taken into account when using personal location data.

1.1. Context

This guidance document has been prepared in the context of the European Union Location Framework (EULF). The EULF is funded under Action 2.13 of the European Commission's Interoperability Solutions for the European Public Administrations (ISA) Programme. The ISA Programme supports interoperability and sharing and reuse of solutions among European Public Administrations through the creation of, *inter alia*, frameworks, architectures and re-usable components to enable more cost effective e-Government services and support cross-border applications.

Public administrations increasingly use location data, consciously or unconsciously, to carry out their activities, both for the delivery of public services as well as for internal purposes. These services include location-based services such as toll systems for vehicles, tourist services or cadastres. Almost every service that is provided contains an element of location, e.g. addresses, GPS coordinates, camera images. Moreover, all sorts of data could be linked to a location, including even financial data or health data. In general, location data is closely linked to individuals, which increases the importance of location data privacy.

While location data privacy has many aspects in common with general data protection principles, it also has unique characteristics that require specific guidance.

1. *Identity inference*: location data might not explicitly reveal an individual's identity, but by aggregating disparate data, it is often possible to infer the identity of an individual.
2. *Embedded*: location data is not always the core element of a service but is frequently used implicitly, whether to upgrade the functionality of the service (e.g. location-based service) or for the supplementary use (e.g. direct marketing).
3. *Necessary*: location data is becoming an essential attribute in delivering added value services or products. Individuals expect to benefit from location based services and enjoy a certain level of comfort and automation.
4. *Abundancy*: location data is increasingly used in services and products resulting in large amounts of location data. As this amount of data rises, it becomes more difficult to manage and control.
5. *Undervalued*: individuals recognise the importance of protecting health or financial data. However, they are not yet aware of the value of the data they make available by constantly using their GPS, Wi-Fi and Bluetooth on their mobile devices. Location data not only says where you are, it says who you are.

Public administrations need to be prepared and anticipate the risks associated with the use of (personal) location data, keeping these characteristics in mind.

1.2. Target audience

These guidelines target public administrations that use (personal) location data to fulfil their mission. They are conceived particularly to help individuals that have a limited experience with data protection or the specific aspects of location data that may impinge on personal data privacy.

1.3. Scope

This guideline addresses the privacy implications of handling location data by public administrations and identifies potential risks related to the processing of personal location data. It aims to provide a practical interpretation of legal matters as part of the EU legal

framework. A main piece of this EU legal framework is the General Data Protection Regulation [1] (GDPR) which was adopted on 27 April 2016 and will enter into application 25 May 2018. The GDPR replaces the current data protection directive (officially Directive 95/46/EC[1]) and lays down the way of data protection in the new digital age.

This guideline does not however provide any legal advice nor give an extensive or complete overview of the applicable legal framework. As this guideline wants to reach the widest possible audience within public administrations, member state legislation or sector specific data protection regulation are not taken into account.

A piece of EU sector-specific legislation worth mentioning is the ePrivacy Directive (a.k.a. the "cookie-law"). Drafted in 2002 and updated in 2009, it intends to regulate the telecommunications industry by inter alia protecting the confidentiality of communications, establishing data breach notification and governing the use of cookies, location data and metadata. However, with the publication of the GDPR, both pieces of legislation are now misaligned (e.g. different time period for data breach notification or enforcement by data protection authorities rather than telecom regulators). The ePrivacy Directive is currently under revision and a new proposal is expected in 2017, which needs not to undermine the GDPR while at the same time trying to fix some loose ends the GDPR has created. As this guideline does not take into account sector-specific legislation and as the ePrivacy Directive is not in concert with the GDPR, this guideline doesn't refer to this specific piece of legislation.

For purposes of law enforcement and national security, personal (location) data is an indispensable and valuable asset. Although this guideline does not specifically address the processing of personal location data for law enforcement and national security purposes, it is worthwhile considering the variety of uses in this context. Below, some of many applications of personal location data processing in this context are described briefly.

- One of the main aids for surveillance activities are surveillance cameras. Fixed cameras at entrance points or drones patrolling a specific area, both register activity and support in deterring or responding to offences. Through these images, individuals can be identified and linked to a certain location.
- For traffic control purposes, (mobile) cameras register the movements of vehicles and their drivers. This data is used by competent authorities to identify traffic violations (e.g. speed or red-light cameras), taxation (e.g. road tolling), or optimising traffic. Through this data it is also possible to locate a car, and potentially its driver.
- Police are increasingly using body cameras during their missions. These cameras register all activities and are used to support police officers and their cases. This also implies the identification and localisation of individuals appearing in these images.
- Passenger Name Record (PNR) data are used for the prevention and investigation of terrorist offences and other crimes, but they also give an indication of the whereabouts of individuals.

Because of the dedicated legal frameworks for the above mentioned applications, the processing of (personal) location data in the context of criminal law enforcement and national security is considered out of scope.

1.4. Structure of the document

For public administrations it is important to know what the legal obligations and principles are, how these apply to realistic scenarios and what good practices are on the use and management of location data. This document provides more guidance on these topics and is structured as follows:

[1] http://eur-lex.europa.eu/legal-content/EN/LSU/?uri=celex:31995L0046

- Chapter 2 provides a definition of location data privacy;
- Chapter 3 outlines key legal obligations arising when handling personal location data;
- Chapter 4 describes specific challenges that public administrations face with regard to the processing of personal location data;
- Chapter 5 provides recommendations on personal location data;
- Chapter 6 concludes this guideline and summarises the most important elements; and
- In annex, three real-life case studies related to the protection of personal location data are described.

1.5. Glossary

This section provides a number of common definitions used throughout this report.

Table 1: *Glossary*

Term / Acronym	Description
Anonymisation	The processing of personal data in such a way that the data does no longer relate to an identified or identifiable natural person. [1]
Data controller	The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law. [1]
Data processor	The natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. [1]
Data subject	A data subject is an identified or identifiable natural person. 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. [1]
Location data	Described in section 2.
Personal data	Described in section 2.
Personal location data	Described in section 2.
Privacy	The rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure and disposal of personal data. [2]
Processing	Any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission,

Term / Acronym	Description
	dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. [1]
Pseudonymisation	The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional data, as long as such additional data is kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person. [1]

2. What is location data privacy?

Location data privacy has no clear-cut legal definition. For this study, we derive a definition from the definition of personal data and location data both defined in the European Union legal framework.

Personal data

Definitions of personal data are available in various sources. Throughout this document, we will use the definition provided by the General Data Protection Regulation (GDPR) [1] adopted in May 2016. Article 4 of the GDPR defines personal data as follows:

''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;

Location data

In the context of this guideline, location data covers any data with an implicit or explicit geographic or geospatial reference, ranging from address data to radio signal-based triangulation or IP address location, including data published under the INSPIRE Directive [3].

Personal location data

For the purpose of this study, personal location data is any location data directly or indirectly linked to an individual or that can be directly or indirectly used to identify an individual. This becomes possible by making any combination of (different/several) location and personal data. Figure 1 depicts the relationship between personal data and location data.

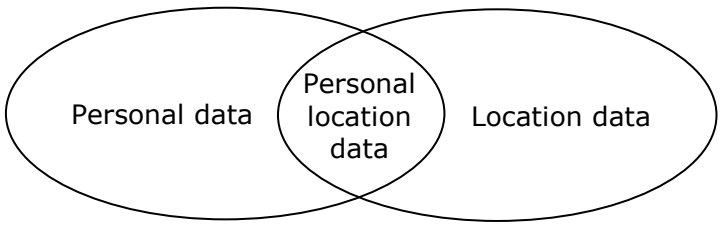

Figure 1: *Relationship between personal data and location data*

The definition for personal location data is illustrated describing some examples (see Table 2) where combining personal data and location data leads to the identification of the location of an individual.

Table 2: *Examples of personal location data*

Example of location data	Example of personal data	Personal location data
GPS coordinates of the location of a smart phone	Telephone subscription account information linked to the smart phone	By combining the two data sources, the location of the individual can be identified.
Public IP address	Internet subscription account information	
Cadastral information about a realty	Realty owner information	
Traffic camera footage on a specific location	License plate owner information	

Location data privacy
Location data privacy is the individual's right not to be subjected to unauthorised collection, aggregation, processing and distribution (including selling) of his location data. It is the right to be protected by the ability to conceal information of whereabouts, which can be derived from personal location data.

3. Legal obligations when processing personal (location) data

The protection of personal data is a fundamental right. New technologies introduce new privacy risks and a more privacy-aware and assertive society requires fully fledged control measures to protect private life. Policy makers and standardisation organisations are responding to this by updating data protection legislation and guidelines.

The right to the protection of personal data however is not an absolute right. It should always be considered in relation to other fundamental rights such as freedom of expression and information, or freedom to conduct a business. Specific to public administrations is the right to access public sector information such as official documents, which may contain personal data.

This chapter consolidates the main privacy obligations that public administrations should comply with when processing personal location data. Each obligation is structured in three parts: (1) **explanation**, (2) **example** of how the obligation applies to location data and (3) **references** to specific data protection regulations and guidelines. The following example is used throughout to illustrate the concrete application of each principle with regard to location data privacy:

A public Tourist Information Office provides visitors with a paying smartphone app for guided tours through the city. The app uses GPS coordinates to define the visitor's location and indicates on a map the route to take. The app has other functionalities as well, such as suggesting where to have a drink or take a meal, to rate restaurants and pubs and to evaluate tourist attractions. All the information provided by the users of the app is hosted on a central system, owned by the responsible public administration for tourism.

3.1. Appoint a responsible individual for data protection

Appoint a responsible individual for data protection within your organisation, to supervise the management of personal location data and provide the necessary level of transparency within the organisation and towards data subjects. The responsibilities should encompass a number of tasks from strategy to execution, including but not limited to: counselling, defining policies, monitoring compliance, raising awareness and training staff, executing privacy risk assessments or communicating with supervisory authorities and data subjects.

According to the General Data Protection Regulation [1] each public administration shall appoint a Data Protection Officer (DPO).

Example

The Tourist Information Office could appoint its own DPO. An alternative option could be to appoint one DPO for all Tourist Information Offices in the region or the whole country, depending on the total number of Tourist Information Offices. Additional national legislation might also give more guidance on this. The role of the DPO does not have to be a full time function, however the time and effort the DPO spends on data privacy should be in line with the extent of the app usage or other personal data processing activities performed by the Tourist Information Office. The workload of the DPO could be impacted by e.g. the number of app users, the amount of processed personal data, the number of complaints or the pace at which new functionalities are introduced (and need to be assessed). The tasks of the DPO can be combined with other tasks in the organisation, as long as there is no conflict of interest.

Related regulation or guidelines

- GDPR [1], article 37: Designation of the data protection officer
- GDPR [1], article 38: Position of the data protection officer
- GDPR [1], article 39: Tasks of the data protection officer
- Regulation 45/2001 [6], article 24: Appointment and tasks of the Data Protection Officer

- Regulation 45/2001 [6], article 25: Notification to the Data Protection Officer
- OECD Privacy Framework [4], Part II, Accountability Principle

3.2. Ensure lawful processing of personal location data

The processing of personal location data has to be lawful and fair (a.o. individuals may not be deceived or misled) and has to be transparent in relation to the data subject.

In particular, public authorities and bodies can lawfully process personal (location) data if they have a legal basis, i.e. a data subject has given consent for the specific purpose, if the processing is necessary for the performance of a contract of which the data subject is party, if the processing is necessary to comply with their legal obligation, if it is necessary to protect the vital interests of a natural person or if it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

This means that public administrations do not have to ask for the consent of the data subject if there is a legal basis or legislative measure that regulates the processing of personal location data for performing a specific task. However, this legal base does not imply that the other applicable privacy principles (see the other obligations in this section) become irrelevant. Lawful processing is only one of many mandatory requirements.

Example

In order for the Tourist Information Office to process location data lawfully, there must be a legal basis or legislative measure justifying the processing activities. It might be legal for the Tourist Information Office to store a limited set of personal location data, but most likely there is no legal context or public interest to process numerous detailed personal location data that is collected through the app. In the absence of a legal basis or legislative measure, the Tourist Information Office can however process the data lawfully only if (1) it asks users for explicit consent or (2) it completely anonymises all collected data so it cannot be tracked back to an identifiable individual.

Related regulation or guidelines

- GDPR [1], article 5: Principles for personal data processing
- GDPR [1], article 6: Lawfulness of processing
- Regulation 45/2001 [6], article 4: Data quality
- Regulation 45/2001 [5], article 5: Lawfulness of processing
- Data Protection Directive [6], article 7
- OECD Privacy Framework [4], Part II, Collection Limitation Principle
- OECD Privacy Framework [4], Part II, Use Limitation Principle

3.3. Apply data protection by design and default

Data controllers and data processors shall ensure that each new service or business process that makes use of personal location data takes the protection of such data from the start of any project. In fact, adding privacy features when the development of a new solution or service is already completed is costly and more difficult to implement.

To ensure that data protection by design and by default is an overarching principle, it is important to include privacy risks when drafting the business case and to follow up on them during the progress of the project. When designing a new solution or service, technical (e.g. use of pseudonymisation or anonymisation software) and/or organisational (e.g. process for complaints handling) privacy controls should be added. Privacy by design should be a default mindset which is to be established within an organization and project team.

Example

The Tourist Information Office should take data protection into account from the moment the idea of creating an app for guided tours is conceived. This can be done by asking some

basic questions: *What is the goal of the app? What personal data do we actually need? To what privacy risks will users be exposed by using our app? What safeguards do we need to put in place to protect app users' personal data?* By asking these questions upfront, the Tourist Information Office avoids major changes to its app during the development phase, or even worse, when already in use.

Related regulation or guidelines

- GDPR [1], article 23: Data protection by design and by default
- Information and Privacy Commissioner of Ontario – Privacy by Design (PbD) [7]
- ENISA - Privacy and data protection by design [8], chapter 3: Privacy Design Strategies

3.4. Apply data minimisation

Only adequate and relevant location data can be collected and processed. The collection must be limited to what is strictly necessary for the purpose for which data was collected in the first place. The challenge consists in establishing the right level of specificity and granularity of location data needed for the service or product. Redundant data should be deleted or anonymised as from the moment it is no longer of use.

Next to limiting the amount of personal location data collected, public administrations should also limit the length of time for which data will be kept and be clear about the reason why the location data is retained. It is a fundamental requirement because personal location data collected for one purpose cannot be retained once that initial purpose has ceased. Unfortunately, there is no mathematical formula to calculate the retention period. When defining the retention period, a balance should be made between the protection of individual's privacy and the public administration's needs for which the personal data was collected.

Example

The Tourist Information Office wants to improve its app's functionality by suggesting tourist routes based on the typical interest of a tourist age category. Therefore, they want to ask users for their birthday to see what touristic attractions are more popular with a certain age category. However, for this purpose it would be sufficient if users indicate in what age category (e.g. ages 18–21; 22-28; 29-36; …) they are situated instead of asking for their day of birth.

As the Tourist Information Office is collecting personal (location) data, it must also communicate to its app users for how long all the data will be retained. There can be different retention periods for different types of data or some basic data could be retained for a longer time, even if the app user deleted his profile. If the Tourist Information Office would anonymise the data it retains when the initial purpose has ceased, there are no limitations as it is no longer classified as personal data.

Related regulation or guidelines

- GDPR [1], article 5: Principles for personal data processing
- GDPR [1], article 17: Right to erasure / Right to be forgotten
- Data Protection Directive [6], article 6 (c)
- OECD Privacy Framework [4], Part II, Collection Limitation Principle
- OECD Privacy Framework [4], Part II, Purpose Specification Principle

3.5. Perform periodic privacy risk assessments

To guarantee an accurate level of data protection towards data subjects, public administrations should assess the risks they expose data subjects to when processing their location data. This is not a one-off activity. As risks evolve, the likelihood and impact of these risks should be re-assessed regularly.

Next to the risks data subjects are exposed to, public administrations expose themselves to risks as well when processing personal location data. The risk of e.g. non-compliance, data leakage, insufficient or ineffective security controls should be assessed as well.

This risk assessment usually takes the form of a Data Protection Impact Assessment (DPIA) or Privacy Impact Assessment (PIA).

Example

Throughout the life cycle of the app, the Tourist Information Office should identify and assess privacy risks, at least yearly or whenever the app undergoes a significant change. New functionalities might introduce new privacy risks, threats and vulnerabilities may evolve or new ones arise and not to mention, people's privacy risk appetite changes over time.

An example of a new functionality for the app could be the integration with social media platforms (e.g. Facebook or Instagram) to share information with your friends (or the public) such as for example the tourist route you have been travelling or the next stop on your tourist route you are heading to. The implementation of this functionality should be subject to a privacy risk assessment. As probably not every individual will make use of this new functionality, the app user should have the option to opt-in or opt-out.

Related regulation or guidelines

- GDPR [1], article 35: Data protection impact assessment
- Location Data Privacy Guidelines [9], part 4: Location Data Privacy Risk & Transparency Assessment

3.6. Secure data processing activities

Irrespective of the lawfulness of the processing of personal location data, processing activities should be secured adequately. As described above, the mandatory privacy risk assessment identifies privacy risks. These risks must be mitigated through the use of technical and/or organisational security controls. Commonly mentioned security controls are encryption or pseudonymisation, but all well-established security principles such as 'need-to-know' (*i.e. allowing access to information or knowledge is only if required to perform an assigned task*) or 'layered security' (*i.e. a defensive security strategy featuring multiple layers that are designed to slow down a security attack*) contribute to the overall level of security. Important to know is that the overall level of security of a solution is only as strong as the weakest link. This implies every component of a solution, whether central systems or remote devices, should be secured adequately.

There are many security control frameworks that a DPO can refer to. Some of these focus on protecting personal data, such as ISO 27018[2]. Other more general frameworks, such as the ISO 27000 family of standards[3], ISF Standard of Good Practices[4], NIST[5] or SANS[6] publications, are applicable as well.

Example

The Tourist Information Office should safeguard data at three levels to secure its service: data residing on the smartphone, data in transit when transferring it to the central system, and data residing on the central system. It seems appropriate to apply typical safeguards such as developing the app according to secure coding principles, encrypting the data transferred to the central system or limiting access to the central system on need-to-know

[2] ISO/IEC 27018:2014: Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
[3] http://www.iso.org/iso/iso27001
[4] Information Security Forum (ISF) - https://www.securityforum.org/tool/the-isf-standardrmation-security/
[5] National Institute of Standards and Technology (NIST) http://csrc.nist.gov/publications/PubsSPs.html
[6] https://www.sans.org

basis. These are only a subset of adequate security controls, but there are many more as referred to in the paragraph above.

Related regulation or guidelines

- GDPR [1], article 32: Security of processing
- Regulation 45/2001 [6], article 22: Security of processing
- Data Protection Directive [6], article 16: Confidentiality of processing
- Data Protection Directive [6], article 17: Security of processing
- OECD Privacy Framework [4], Part II, Security Safeguards Principle
- ENISA - Privacy and Data Protection by Design [8], chapter 4: Privacy Techniques

3.7. Comply with data subjects' rights

Data subjects remain owners of their personal location data (elaborated on in 5.3). This means they can invoke numerous rights related to that ownership. This section briefly describes the rights of data subjects that data controllers (i.e. public administrations processing personal location data) should respect. These rights are described in full details in the respective articles of the GDPR [1], referred to in the remainder of this section. In general, data subjects have the right to:

- *Receive certain information*: be provided with information regarding to the processing of their data at the time when the personal data are gathered (or at some time thereafter when the data is not gathered directly from the data subject) spontaneously by the data controller). This includes, amongst others, the identity and contact details of the controller and data protection officer, the purposes of the processing, and the legal basis for the processing. (GDPR [1], article 13 & 14, *information to be provided*)
- *Access their data*: obtain information regarding to the processing of their data upon its request. This includes, amongst others, the data being processed itself, where data is processed and why it is processed, the recipients to whom the data have been or will be disclosed, or for how long the data will be stored. (GDPR [1], article 15, *right of access*)
- *Correct their data*: have inaccurate or incomplete data relating to them rectified. (GDPR [1], article 16, *right to rectification*)
- *Erase their data*: have the data erased when the collected data are no longer necessary, the data subject withdraws consent, the data subject objects to the processing, or the data have been processed unlawfully or for compliance reasons. (GDPR [1], article 17, *right to erasure / right to be forgotten*)
- *Withdraw their consent*: withdraw consent for processing data at any time. The withdrawal of consent should be as easy as giving the consent. (GDPR [1], article 7, *right to withdraw consent*)
- *Restrict the processing of their data*: restrict the data processing in certain circumstances such as unlawful processing or withdrawal of consent. When the processing has been restricted, the personal location data can only be stored but not being processed until the restriction is lifted. (GDPR [1], article 18, *right to restriction of processing*)
- *Right to data portability:* if the processing is carried out by automated means and if it is based on consent or a contract, the data subject has the right to receive the data and transmit this data to another data controller. (GDPR [1], article 20, *right to data portability*)
- *Right to object*: in certain situations (e.g. direct marketing, statistical purposes) data subjects have the right to object to the processing of their personal location data. (GDPR [1], article 21, *right to object*)
- *Right not to be subject to a decision based solely on automated processing*: the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. (GDPR [1], article 22, *right not to be subject to a decision based solely on automated processing*)

- *Right to lodge a complaint*: the right to lodge a complaint with a supervisor authority if the data subject considers that the processing of personal information infringes the GDPR. (GDPR [1], article 77, *right not to lodge a complaint with a supervisory authority)*
- *Right to an effective judicial remedy against a supervisory authority*: the right to an effective judicial remedy against a legally binding decision of a supervisory authority. (GDPR [1], article 78, *right to a judicial complaint with a supervisory authority*)
- *Right to an effective judicial remedy against a controller or processor*: the right to an effective judicial remedy if data subjects consider that their rights have been infringed. (GDPR [1], article 79, *right to a judicial complaint with a controller or processor*)
- *Right to compensation and liability*: a data subject who has suffered material or immaterial damage shall have the right to receive compensation from the data controller or data processor for the damage suffered. (GDPR [1], article 82, *right to compensation and liability*)
- To respect these rights, public administrations should identify the data subject's rights applicable for the specific case and implement the necessary internal processes and procedures.

Notice however, the right of privacy is not an absolute right. Data subjects cannot invoke the right to object to legal tasks public administrations should perform. Therefore, it is important to identify those data subject rights that are applicable and those that are not.

Example

The users of the tourist app have several rights when it comes to their data. In order to respect these rights, the Tourist Information Office should provide app users with the option to e.g.:

- limit the processing of personal location data by limiting the required data,
- delete their restaurant rating or comments to a tourist attraction when they withdraw their consent,
- allow them to update/rectify their personal data stored by the app, or
- access all their personal location data collected through the app.

Related regulation or guidelines

- Regulation 45/2001 [6], article 13: Right of access
- Regulation 45/2001 [6], article 14: Rectification
- Regulation 45/2001 [6], article 15: Blocking
- Regulation 45/2001 [6], article 16: Erasure
- Regulation 45/2001 [6], article 18: The data subject's right to object
- Data Protection Directive [6], article 12: Right of access
- Data Protection Directive [6], article 14: The data subject's right to object
- OECD Privacy Framework [4], Part II, Data Quality Principle
- OECD Privacy Framework [4], Part II, Individual Participation Principle

Note: references to the GDPR [1] are made in the text itself.

3.8. Notify data breaches to data subjects and relevant bodies

Supervisory authorities and data subjects expect to get notified about data breaches. Unless a data breach is unlikely to result in a risk to the rights and freedoms of the affected data subjects (e.g. if the leaked data would be unintelligible by the use of e.g. encryption), the competent supervisory authority should be informed. Furthermore, if the data breach would likely result in a *high* risk, the affected data subjects should be informed personally and without undue delay.

The notification should describe the details of the data breach, the control measures already taken, and recommendations for the effected data subjects to control damage. All communication towards data subjects should be transparent and in clear and plain language.

Public administrations might process personal data of numerous data subjects, which makes a personal notification to each data subject practically infeasible. Therefore, a public communication – if effective – is considered to be sufficient.

Example

If the Tourist Information Office was to be hacked and all data of their users were compromised, the Tourist Information Office should first inform the supervisory authority of the data breach. Afterwards and in consultation with the supervisory authority, it should inform its users without undue delay. It could use the application to push a message to all users, or use other communication channels to inform its users that their data is compromised.

Communication in case of data leakage should not be a one-off. It is advisable to provide the effected users and the supervisory authority with regular updates on the progress of controlling the data breach and the measures taken to avoid future data breaches.

Related regulation or guidelines

- GDPR [1], article 33: Notification of a personal data breach to the supervisory authority
- GDPR [1], article 34: Communication of a personal data breach to the data subject
- Data Protection Directive [6], article 10 and 11

4. Using location data: scenarios, challenges and risks

This chapter provides a brief overview of the use of personal location data in the public sector with a focus on the use of this data. The general use is described below, followed by four concrete examples of personal location data processing:

- Location-aware browsing: use of geolocation data
- Electronic eID: use of address data
- Use location data for business intelligence or statistical purposes
- Working with private third parties: exchanging personal location data

For every example, related challenges and risks are identified and reference is made to the privacy principles from chapter 3 that are linked directly to the example.

In general, we identify three main scenarios where a public administration is involved in the processing of personal location data.

- **Scenario A: intra-administration**: a public administration processes personal location data when providing services in the context of its public task(s) and keeps the data within its organisation. These services can be emergency services, regular public services [10] or law enforcement services.
- **Scenario B: administration-to-administration:** public administration X processes personal location data and exchanges this data with public administration Y.
- **Scenario C: administration-to-business**: public administration X processes personal location data and exchanges this data with private organisation Z.

Independently from the scenarios and examples provided, it is important to highlight the potential added value location based services might bring. Some individuals are happy to share their location to benefit from the associated advantages, others are more sensitive to their privacy and might only use a service if their privacy is fully guaranteed. As a service provider, it is important to be able to support both.

4.1. Location-aware browsing: use of geolocation data

4.1.1. Context

A public administration offers a service to its citizens through an online portal. To provide a more personalised service, the public administration collects geolocation data of its citizens' mobile device or computer (e.g. IP addresses or GPS coordinates).

4.1.2. Challenges and risks: protection of location data

Citizens are exposed to risks by sharing their location and should always be wary of inappropriate use. A public administration is facing the challenge of protecting the location data that a citizen shares with the public administration. In the case of location-aware browsing geolocation data can, in most cases, only be collected if citizens give their explicit consent. Moreover, public administrations are recommended to provide the option to citizens to choose the level of detail they want to share.

Next to that, a citizen should have the option to withdraw consent. Withdrawing consent implies that a public administration must delete all gathered personal location data of a particular citizen, unless legal grounds for the processing remain.

A specific scenario where geolocation data is used is to block access to (for example copyrighted) content made available through online portals. Based on a visitor's IP address the country from where the access request originates, can be retrieved and blocked if required. Although this action identifies the location (country), a visitor is not traced back to an identified individual. Therefore, no privacy issues arise if content blocking is setup correctly.

4.1.3. Privacy principles

For this specific example the immediately applicable privacy principles are:

1. Achieve lawful processing of personal location data: ask for the citizen's explicit consent (see 3.2)
2. Apply data minimisation: reflect on the level of detail of location data your provided service requires. Besides that, provide the citizen with the option to choose the level of detailed location data he wants to share (see3.4)
3. Comply with the data subject's rights to withdraw their consent or to be forgotten (see 3.7).

4.2. Electronic eID: use of address data

4.2.1. Context

A public administration collects and processes citizens' address data provided via the national electronic eID to fulfil a public task in the context of a legal obligation. This data can be collected in different ways, for example either through an online tool or an application form.

Over time the public administration creates a new service and wants to promote it to its citizens to point out the opportunities this new service introduces. To do so, the public administration sends out personalised information brochures to its citizens whose address data is already available through the collection in the context of its public task.

As address data is probably the most frequently requested and stored personal (location) data by public administrations, this scenario is closely linked to the once-only principle. This principle implies that citizens should not be asked for the same data more than once, with the objective to reduce the administrative burden for the citizens. However, this does not imply that address information can be shared freely between public administrations and reused for whatever purpose. As described in 3.2, there should always be a lawful base for processing personal (location) data. If a public administration wants to reuse address data, originally collected by another public administration for a specific purpose, the second public administration needs to ascertain whether it can use this piece of data.

4.2.2. Challenges and risks: use of location data for purposes other than the one for which they were collected in the first place

The address data was originally collected lawfully in the context of a public task assigned to the public administration (i.e. for the national electronic identity cards). However, the use of the address data for promoting the new service does not fall under the public task assigned to the public administration. If the public administration wants to use the address data of its citizens in another context, the public administration should explicitly ask for consent.

4.2.3. Privacy principles

For this specific example the key privacy principles are:

1. Achieve lawful processing of personal location data: ask for a citizen's explicit consent before using his address data (see 3.1).
2. Comply with the data subject's rights to withdraw their consent (see 3.7).

4.3. Use of personal location data for business intelligence or statistical purposes

4.3.1. Context

A public administration has been collecting personal location data for several years in the context of its public task. To improve its service towards the citizens, the public administration decides to subject all collected personal location data to business intelligence processing. The IT department of the public administration has the experience and the tools to provide the necessary support. Moreover, external key-experts and the software supplier will be involved in this process to achieve high-quality results.

4.3.2. Challenges and risks: Re-identification of anonymised or pseudo-anonymised personal location data

A potential risk that may arise in this scenario is unlawful disclosure of personal location data to IT-staff, external consultants or suppliers. Therefore, it is important that the public administration takes the necessary measures to protect the citizens' personal (location) data. It should verify to what extent other parties need the full data set or if a limited data set would be sufficient and it is appropriate to apply data anonymisation or pseudonymisation on the personal location data. Besides these technical controls, contractual agreements for external staff on non-disclosure and acceptable use should also be put in place.

Next to the risk of unlawful disclosure as described above, public administrations might also run the risk of re-identifying individuals even if the data were anonymised. Typically, this could happen when a dataset is minimal or granular. For instance, the inclusion of geographic details in a dataset makes it much easier to re-identify users that live in small geographic areas. If a public administration publishes research results on farm subsidies by area and there is only one farm in a particular area, the farm owner can be easily re-identified.

There are different actions that public administrations can take to limit such risk, including: delete records of small areas, remove from the disclosed dataset some of the non-geographic variables, reduce the precision of geographical areas or aggregate the small geographic areas into larger ones.

Each option has certain disadvantages with regard to the richness of the dataset, therefore when making a decision, public administrations should make a careful assessment.

4.3.3. Privacy principles

For this specific example the key privacy principles are:

1. Apply data minimisation: reflect whether a full dataset is necessary to achieve the desired outcome or some personal data can be omitted (see 3.4).
2. Secure data processing activities: apply security techniques to protect personal location to unlawful disclosure (see 3.6).

4.4. Working with private third parties: exchanging personal location data

4.4.1. Context

A public administration processes personal location data in the context of its legal obligations. For the execution of this task, it appoints an external private partner to support the processing and storage of personal location data.

4.4.2. Challenges and risks: disclosure of personal location data to third parties

Public administrations do not always have the same technological or organisational capabilities to process data and might therefore decide to rely on specialised third parties. If third parties take part in data processing activities, the following attention points should be kept in mind:

- Make sure privacy risks are identified and mitigated using technical and organisational controls. To support this process, a public administration should perform a data protection impact assessment.
- Contractual agreements in which clear responsibilities are defined should be established between the parties involved. These responsibilities describe, amongst others, non-disclosure, notification processes, right to audit, required level of security and liabilities.
- The necessary legal permissions for the public administration or private third party should be identified and obtained.
- Appoint someone responsible for data protection within every party involved. This person should have sufficient competences and experience and acts as a single point of contact amongst the parties involved and the citizens.

4.4.3. Privacy principles

For this specific example the key privacy principles are:

1. Perform periodic risk assessments: risks should be identified from two points of view: (1) the privacy risks citizens are exposed to and (2) the risks the public administration is facing. Note that non-compliance to a legal requirement should be treated as a risk. (see 3.5)
2. Appoint a responsible for data protection (see 3.1)
3. Notify data breaches to data subjects and relevant bodies: assigned third parties must notify a public administration in case of a data breach; a public administration should notify the supervisory authority and, in some cases, its citizens. (see 3.8)

5. Recommendations

Chapter 3 describes the legal obligations related to the collection and processing of personal (location) data. Chapter 4 elaborates on some specific location data scenarios and examining the related challenges and risks. Insights gained from both chapters are used to define a set of effective and practical recommendations that allow public administration going to next level in their quest for adequate personal location data protection. In order to obtain the best possible set of recommendations, these gained insights are supplemented with the expertise of cyber security and data protection professionals. Moreover, all recommendations take into account the specific characteristics identified at the start of this document.

The all-encompassing recommendation would be to set-up a personal location data protection programme, which goes beyond complying with applicable laws and regulations. This personal location data protection programme can be part of a bigger personal data protection programme. Depending on the amount of (personal) location data an organisation processes, it can pay more attention to location data privacy.

It enables public administrations to become a privacy-aware organisation with respect to personal data protection throughout all its processes. The recommendations described in this chapter all contribute to this idea.

5.1. Set up governance structure for location data protection

Governance is about setting responsibilities and practices with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that resources are used responsibly. A governance structure provides an answer to the issue of *identity inference* and the fact that location data is *undervalued* (see 1.1).

A location data protection governance structure consists of several building blocks. To achieve an adequate governance structure, the activities below should be completed. Note that these activities are rather generic and can easily be applied to any type of personal data.

- Develop a data protection strategy in line with the organisation's strategy.
- Put together a data protection team and assign responsibilities. One of the most important roles within this privacy team will be the Data Protection Officer (DPO) (see 3.1)
- Implement a policy framework including data protection policies, standards and guidelines. This framework sets out the direction how to process personal data during its entire data life cycle.
- Define activities w.r.t. education and awareness, data management (see 5.1), risk assessments (3.5), incident management and audit & compliance.
- Define metrics to measure to what extent the established data protection programme is effective and adhered to.

Depending whether location data plays a major role in a public organisation's activities, governance activities specific to personal location data could be defined. Some examples of specific governance activities are:

- Guidelines on how to perform self-checks if location data can potentially identify an individual;
- Minimum set of security and privacy controls specific to location data that shall be applied when processing location data (e.g. how to apply anonymisation or pseudonymisation techniques);

- Risk assessment process and supporting risk assessment tools focussing on threats specific to location data.

By putting in place an adequate governance structure, public administrations mitigate the risk of not having full control of the management and protection of personal location data, which is derived from the increased availability and ways of using of location data.

5.2. Set up a location data management programme

Data management is the development, execution, and supervision of plans, policies, programs and practices that control, protect, deliver and enhance the value of data and information assets [11].

Good location data management is crucial as processes and activities become more inter-functional, activities become more data-driven, technology becomes more complex and location data becomes more prevalent. However, not only the use of data plays a major role, but the exchange becomes more crucial as well. To manage the *abundancy* of location data (see 1.1) and to guarantee adequate data quality, it is important to apply good data management.

To set up a location data management programme, it requires four essential building blocks: (1) data principles & guidelines, (2) roles & responsibilities, (3) processes and (4) supportive tools. If applicable, these buildings blocks should be aligned with a broader (public sector) location data strategy or location data management.

Based on the above building blocks, location datasets and their use can be identified. Using these insights data architectures can be modelled. A next step is the introduction of the concepts of reference data and master data management in order to improve the use and management of (location) data. And a final aspect of good data management is the monitoring and maintenance of data quality.

In parallel to the building blocks, change management is an important element to successful data management programme. Create awareness amongst all involved employees on the necessity and potential of data management through training and communication.

5.3. Data subjects are always the data owners

Data ownership is a complex matter. In theory data is no more than a set of characters, which should be contextualised to have meaning or value. Contextual data constitutes information.

According to A. M. Al-Khouri's paper on data ownership [12] , personal data comprises, in its strict sense, just personal attributes, which are owned by a data subject. Data subjects sharing their personal data implicitly or explicitly with data controllers, implies delegation of a 'data processing mandate' towards these data controllers. So personal data might have multiple owners as sharing increases. Moreover, if data controllers rely on data processors for the processing of personal data, these data processors are considered data custodians or data stewards.

The 'true owner' however lies with the data subject. As data is shared and information is generated, these data should be subject to scrutiny and verification. The only source able to verify the data and confirm the veracity, the 'true owner', is the data subject.

To underpin the above statement, a data subject has been empowered with a series of rights (see 3.7) to be able to scrutinise and verify his data. Public administrations should acknowledge these rights. Moreover, as location data is often *embedded* in services or applications (see 1.1), public administration should always be conscious of the potential collection of location data through their services or applications, and protect it accordingly.

5.4. Create trust through transparency

Data subjects are more inclined to trust you as a data controller or processor if you use an open and transparent communication. Explaining the purpose of your collection, the means for safeguarding security or the privacy principles applied in plain and simple text, makes it easier to digest and accept the data processing activity. As location data is often *undervalued* (see 1.1), it is even more important to make individuals aware of the value of their location data and that this valuable data is protected adequately.

To promote transparency, it is appropriate to establish a privacy contact point, which data subjects can contact for every possible privacy-related question. This contact point can include different communication channels, like a public website, a hotline, an email or even a chat box.

Another means to support transparent and simple communication is the use of standardised icons for data processing activities or controls in place to protect data subjects' privacy. In order for these icons to be effective, they should be comprehensive and evoke similar responses to everyone. Standardised icons should give an overview of the intended processing in an easily visible, intelligible and clearly legible manner (GDPR [1], article 12(7)). Below some examples of privacy icons are depicted to illustrate their use and added value.

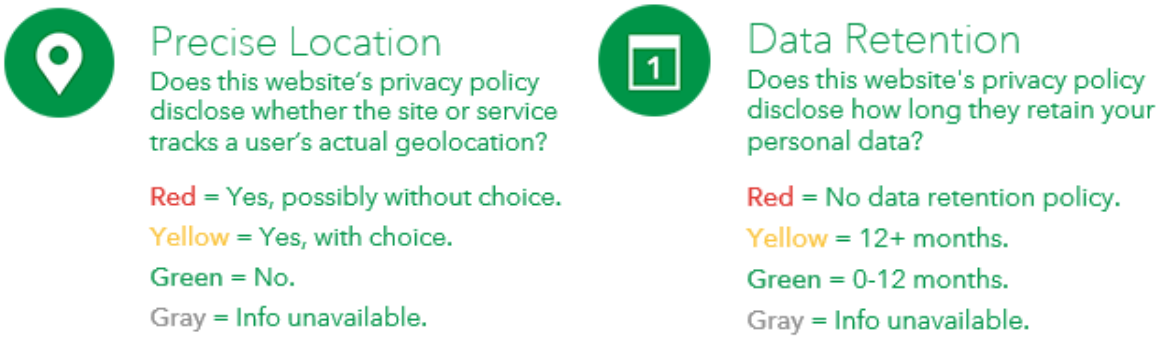

Figure 2: *Examples of privacy icons from https://disconnect.me/icons*

5.5. Publish a privacy notice

An important element of a location data protection programme is a privacy notice, sometimes referred to as a privacy policy or privacy statement. A privacy notice describes how an organisation collects, uses, retains and discloses personal data. Unless a (public) organisation's main activity is related to location data, the aspects of location privacy can also be added to a general/organisation privacy notice. Besides a general privacy notice, organisations can also publish application-specific privacy notices and elaborate on how privacy is dealt with within this specific application.

A privacy notice elaborates on the (1) purpose of processing, (2) what personal location data is collected, (3) how the collected data is used, (4) what organisational and technical security measures are in place to protect the personal location data, (5) with whom the personal location data is shared, (6) how a data subject can access or rectify his personal location data, and, not the least, (7) the contact information of the responsible DPO.

As location data is often an *embedded* or simply a *necessary* element in a lot of services or applications (see 1.1), public administrations should explicitly mention the collection and use of (personal) location data in their privacy notice. Moreover, it is important to keep data subjects informed of any changes to the processing of personal (location) data, which should be reflected in the privacy notice.

5.6. Do not confuse privacy and security

Many equate privacy to security, but privacy goes beyond that. Security is just one element for achieving privacy. The Organisation for Economic Co-operation and Development (OECD), has broken privacy down into eight principles[7], of which security is one component. This security component aims at minimising the risk of data loss, unauthorised access, destruction, inappropriate use and improper modification.

The above risks should be weighted and mitigated accordingly. In case of location data, if these risk are insufficiently managed, they might lead to *identity inference* (see 1.1). In order to identify the existing privacy risks, a privacy risk assessment should be carried out (see 3.5).

5.7. It's only as secure as the weakest link

Applying security safeguards is one of the main principles to achieve adequate data protection. When securing data processing activities, security best-practices must be considered. The security principle 'securing the weakest link' states that a solution is only as secure as the weakest link in the whole series of data processing activities. E.g. securing a central information system with top-notch security controls while local end-points are largely ignored, is a waste of money. Every link of the chain must be secured adequately to have an overall secure solution.

Location data might lead to the risk of *identity interference*. As location data is often *undervalued* or the use of it *embedded* in the service, the chance is real that this type of data is insufficiently protected. To know what safeguards to implement at which phase of the information lifecycle, it's important to identify all security and privacy risks throughout the data processing activities. A Data Protection Impact Assessment (DPIA), as described in section 3.5, can support in this process and should be performed for every new initiative or change to an existing one.

5.8. Reduce privacy risks to an acceptable level

Privacy risks should not be reduced to the absolute minimum at any cost. Internationally accepted risk management standards all dictate to mitigate risks to an acceptable level. This acceptable level is called *risk appetite* and defines the impact and likelihood someone can reconcile with. To know what cost is permissible and what cost is excessive, apply the rule of thumb which says that the cost of security controls should never transcend the cost of the impact of a risk. In case of location data, the risk of e.g. *identity inference* (see 1.1) exists and should be mitigated to an acceptable level. This does however not imply that the remaining after mitigation should have been reduced to null.

In order to obtain an acceptable level of risk, Privacy Enhanced Technologies or PETs can be applied. According to Article 29 Working Party, these PETs protect privacy by reducing or eliminating personal data or by preventing the undesired processing of personal data. [13] Moreover, PETS not only help achieving compliance with data protection legislation, but also support in protecting of e.g. corporate information.

PETs can be communication anonymisers, which conceal online identifiers such as IP addresses, or encryption which hides and protects information. There exist much PETs that enable the protection of privacy, but elaborating on these would go beyond the purpose of this study. More examples of PETs can be found on the website of the International Association of Privacy Professionals (IAPP)[8].

---

[7] The other OECD principles relate to collection limitation, data quality, purpose specification, use limitation, openness, individual participation and accountability. Reference is made to all of these principles in the legal obligations described in chapter 3.

[8] https://iapp.org/news/a/2008-05-introduction-to-privacy-enhancing-technologies

5.9. Prepare for the worst

Public administrations should prepare themselves to respond to major data leaks. Location data is often *undervalued* but just as health or financial data, it might cause serious damage to individuals' private life when leaked, whenever their identity is inferred. Adverse effects for both data subjects and public administrations need to be limited in order to protect data subjects' private life and to retain the trust of stakeholders, despite the data leak.

Crisis management is an organisation's *pre-planned* capability to *respond* to and *recover* from crises, such as major data leaks.

Pre-planned refers to the proactive resilience processes and activities that both prevent and mitigate the impact and the duration of a crisis. Such processes and activities include for example risk management, implementing security measures, audit & assurance and prepare respond and recover plans (e.g. crisis management plan, crisis communication plan).

Respond refers to the recognition and activation of the prepared plans by higher management and taking actions to contain the crisis and mitigate damage.

Recover involves dealing with the long-term effects of a crisis and how to return to business as usual.

6. Conclusion

Location data can range from ordinary address data over security and traffic control footage to IP addresses or GPS coordinates. At first glance, this data does not appear to be personal data nor it seems possible to directly identify an individual through this location data. However, although location data might not explicitly reveal an individual's identity, by aggregating disparate data it may be possible to infer an individual's identity.

Personal location data differs from general personal data in some other respects as well. Location data is regularly used by public administrations, but in most cases not as the core of a provided service. Sometimes it is used as a necessary functionality, sometimes it is embedded and used unknowingly. And most importantly, location data is wrongly undervalued when compared to financial or health data. Location data not only says where an individual is, it says who he is and what his interests or preferences are.

As with personal data, the existing general data protection regulations and principles are applicable to personal location data, but there are no specific European legal obligations on location data privacy. As the use of location data presents complications beyond those typically found with respect to other (more obvious) personal data, this document attempts to explain these complications through a series of scenarios and provide with specific guidance on the use and protection of personal location data.

By describing some specific scenarios in which location data is used, this guideline creates awareness amongst public administrations on their use of location data. The applied approach for the scenarios can easily be transferred to scenarios specific to a public administration.

The recommendations in this guideline target personal location data. The reasoning behind this narrow focus is, because of the characteristics peculiar to location data, specific guidance adds value to the secure and privacy-aware processing of personal location data.

To conclude, it is important to point out the scope limitations applied for this guideline. The existing legal framework and available best practices for the protection of personal data are elaborate. This guideline deliberately keeps the processing of personal location data in the context of law enforcement and national security out of scope. However, as mentioned in the introduction of this guideline, there are numerous applications where location data is used in these context. Therefore, further research is considered advantageous and would provide practical guidance to public administrations on how to protect location data in these cases.

References

[1] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC,* 2016.

[2] American Institute of Certified Public Accountants, Inc. and Canadian Institute of Chartered Accountants., "Generally Accepted Privacy Principles," August 2009. [Online]. Available: http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/DownloadableDocuments/GAPP_BUS_%200909.pdf. [Accessed January 2016].

[3] *Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE),* 2007.

[4] Organisation for Economic Co-operation and Development, "The OECD Privacy Framework," 11 July 2013. [Online]. Available: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. [Accessed 11 January 2016].

[5] *Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data,* 2001.

[6] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,* 1995.

[7] "Privacy by Design," [Online]. Available: http://www.privacybydesign.ca/. [Accessed 20 May 2016].

[8] European Union Agency for Network and Information Security (ENISA), "Privacy and Data Protection by Design - from policy to engineering," 12 2014. [Online]. Available: https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design. [Accessed 22 02 2016].

[9] The Location Forum, "Location Data Privacy - Guidelines, Assessment & Recommendations," 1 May 2013. [Online]. Available: https://iapp.org/media/pdf/resource_center/LocationDataPrivacyGuidelines_v2.pdf. [Accessed 11 January 2016].

[10] DG CONNECT, "eGovernment indicators for benchmarking eEurope," 22 02 2001. [Online]. Available: https://ec.europa.eu/digital-single-market/en/news/egovernment-indicators-benchmarking-eeurope. [Accessed 23 05 2016].

[11] Dama International, The Dama Guide to the Data Management Body of Knowledge (DAMA-DMBOK), Technics Pubns, 2009.

[12] A. M. Al-Khouri, "Data Ownership: Who Owns 'My Data'?," *International Journal of Management & Information Technology,* vol. 2, no. 1, November 2012.

[13] DG Justice and Consumers, "Glossary," 24 09 2015. [Online]. Available: http://ec.europa.eu/justice/glossary/index_en.htm#glossary-p. [Accessed 2016].

[14] Transport for London, "Oyster card," [Online]. Available: https://tfl.gov.uk/corporate/privacy-and-cookies/oyster-card. [Accessed 9 May 2016].

[15] *Directive (EU) 2015/413 of the European Parliament and of the Council of 11 March 2015 facilitating cross-border exchange of information on road-safety-related traffic offences,* 2015.

[16] *Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime,* 2008.

[17] Interoperability Solutions for European Public Administrations (ISA), "sTESTA," 6 4 2016. [Online]. Available: http://ec.europa.eu/isa/ready-to-use-solutions/stesta_en.htm. [Accessed 2016].

[18] European Public Sector Award (EPSA), "The spanish cadastre, an example of open public administration," 13 June 2012. [Online]. Available: http://www.epsa-projects.eu/index.php?title=The_spanish_cadastre,_an_example_of_open_public_administration#tab=Project_info. [Accessed 14 March 2016].

Annex I – Case studies

This section contains a list of case studies that have been conducted.

I.1. Case study 1: Oyster

I.1.1. Context

Oyster is an electronic ticketing system of *Transport for London* (TfL), the local government body responsible for the transport system in Greater London. The Oyster card is a contactless smartcard which can hold a credit that can be used to travel through London on bus, tram, Tube and several other public transportation services.

Next to the Oyster card, TfL also offers an Oyster photocard, which bears a photograph of the corresponding traveller and enables reduced rates for specific user groups (e.g. children, students, veterans). *Note*: for this case study, we focus on the regular Oyster card.

Travellers can, optionally in most cases, register their Oyster card through TfL's website and benefit from some extra features. A registered Oyster card allows travellers to pay for purchases in a more simplified way, view journey history of the past eight weeks, protect Oyster cards from loss of theft, or receive updates on planned disruptions on their regular routes.

However, registering an Oyster card is required for e.g. purchasing bus and tram passes valid longer than one month or to use the 'auto top-up' feature, which automatically tops up your Oyster card, based on the provided credit or debit card data, when its balance drops below a certain amount.

When registering an Oyster card, TfL collects a traveller's contact details (name, address, email address and telephone number) and Oyster card unique number. The latter enables TfL to provide a traveller with his journey history. When accessing the online account linked to the Oyster Card, TfL also collects the IP address used by the traveller's computer for the purpose of fraud prevention and detection. [14]

I.1.2. Issues w.r.t. location privacy

The data collected via the Oyster card enables tracking someone's movements throughout the London's grid. For privacy and safety concerns, it is very important to secure this data and protect it from unacceptable use. Moreover, if the data would be combined with surveillance images, it could be a very powerful tracking tool.

Next to the challenge of protecting this valuable location data, TfL faces another challenge. It shares the personal (location) data with a number of third party providers which provide the majority of the administration and 'back office' services for the Oyster card. Some of these third party providers process data outside the United Kingdom, e.g. in the USA. By relying on these third parties and transporting personal data overseas, TfL must be able to guarantee that all data is processed and managed in a secure way at all times, with respect for the applicable privacy legislations and regulations.

I.1.3. Solution

In order to comply with the requirements of the Data Protection Act 1998 and to control and safeguard the personal data associated with Oyster cards, TfL implemented a range of policies, processes and technical measures.

An example of one of these safeguards is the use of data retention policies for the different types of customer data collected by TfL. These retention periods try to find the right balance between customer privacy and business operations. Some examples of applied data retentions periods are listed below.

Data about individual journeys are kept for 8 weeks, after which the data is disassociated from the traveller's Oyster card.

Customer name and contact details are stored for 2 years after an Oyster card was last used.

Debit or credit card data is stored for 18 months.

IP addresses collected are stored for 13 months.

I.2. Case study 2: EUCARIS (EUropean CAR and driving licence Information System)

I.2.1. Context

EUCARIS is a peer-to-peer data exchange network facilitating the exchange of mobility related information between European countries. This mobility data includes vehicle registration data or driving licences data and the accompanying personal data. All countries registered to EUCARIS can consult the vehicle and driving licence registers of all participating countries through the *National Contact Points* (NCPs). These NCPs are often the Vehicle and Driving Licence Registration Authorities of the participating countries.

EUCARIS facilitates a number of services including a Cross Border Exchange (CBE) service. The CBE service is used to retrieve vehicle-holder-owner information for vehicles involved in traffic offences on the territory of other participating member states. Furthermore, the CBE can be used to verify if vehicles are registered in multiple country and thus preventing registration fraud. Another application of EUCARIS is checking compliance with the one-driving-licence-principle preventing registration fraud.

I.2.2. Challenges w.r.t. location privacy

EUCARIS is communication platform that is used to transfer personal (location) data but does not store any personal location data. Even though it does not store the personal (location) data, EUCARIS still has to take appropriate measures to safeguard the privacy of the data subjects involved and fulfil its legal obligations. As data is transferred between different member states, it should take into account not only the directives and regulations regarding data protection on a European level, but national data protection laws of the different member states as well.

Another challenge EUCARIS is facing is proper access management to the EUCARIS platform as it has to rely on the NCPs to grant and facilitate access. It is the NCP's responsibility to decide on what instances get access to the data and the means used to propagate this data to these instances. NCPs are not obliged to give third parties access through the secured EUCARIS web application and thus they can use their own system to propagate the data. This means EUCARIS has no insights on the level of security of that system.

I.2.3. Solutions

In order to protect the rights and freedoms of data subjects, EUCARIS implemented several safeguards. This case study highlights three main safeguards EUCARIS implemented to protect the data subjects' privacy.

Streamlining a host of legal directives and regulations

All of EUCARIS's processing activities happen on a lawful base: some of them are laid down in EU legislation (e.g. the cross-border enforcement directive [15] or the Prüm Decision [16]), others in the EUCARIS treaty or in bilateral or multilateral agreements. Even though EUCARIS is not bound by national regulation, it did consider the possible differences between countries when drawing up the EUCARIS treaty, leaving enough room for national authorities to decide for themselves how the data will be further processed once on national soil.

Applying data minimisation

To avoid any risk of unlawful processing or insufficient data erasure, EUCARIS does not process or store any personal (location) data. It only provides the platform to facilitate the exchange. The NCP of each member country has its own local EUCARIS server on national soil. Via the central EUCARIS server, bilateral connections are set up to the servers in the other member countries. This way, data does not have to be stored in the EUCARIS system and data is only processed when needed.

Securing data processing activities

The exchange of data between member countries is facilitated by the sTesta [17] network. This provides a highly secure exchange mechanism between NCPs. However, the overall security position also depends on the safeguards applied by the NCPs in their exchange with national entities.

Messages sent throughout the system are plain-text XML-messages. As these messages do not leave the protected environment, it is considered secure. Once the data arrives at the requesting NCP, it can be exchanged with subscribed national entities. This exchange must meet the terms laid down in national and European Law. One example of these terms is the requirement of an audit trail within the Prüm Decision [16].

I.3. Case Study 3: Location data in the Spanish Cadastre [18]

I.3.1. Context

The Spanish Cadastre is a public register containing Spanish real property and real estate. It constitutes a complete digital data model for the whole Spanish territory, except for the Basque Country and Navarra. Next to property identification data (like municipality, address or location of the real estate), the cadastre also holds juridical data (like name and address of the property owner), physical data (like land area) and economic data (like the value of the land).

The cadastral data is primarily collected for taxation purposes, but it also serves as an input for various other public administrations. The Spanish Cadastre also made some of the cadastral data openly available to all citizens in a response to the numerous requests they received, which initially were to be processed in a non-automated manner.

I.3.2. Challenges w.r.t. location privacy

The Spanish Cadastre is a very open system. Many public administrations can not only access cadastral data, but some are allowed to update the data as well. These are mostly people from municipalities and public administrations. The Spanish Cadastre has only limited control over the actions performed by these public administrations. They have to rely on the agreements made with the other administrations.

Another challenge relates to the introduction of the GDPR [1]. The Spanish Cadastre is waiting for information from the Central Administration of the State in Spain on how Spanish institutions (like the Spanish cadastre) can prepare themselves for the GDPR [1]. According to the Data Protection Authority of Spain, the Spanish cadastre is already partially compliant with the new GDPR, but certain changes will have to be made to be compliant with the new Regulation. The additional requirements will be communicated by the Data Protection Authority in due time.

As a last point, the Spanish Cadastre is finding a compromise between its duties as a public administration (making data open to the public) and protecting the privacy of the citizens. In this respect, the Spanish Cadastre is investigating whether it is possible to also open up data relating to the value of a property.

I.3.3. Solutions

In order to protect the rights and freedoms of data subjects, the Spanish Cadastre implemented several safeguards. This case study highlights three main solutions the Spanish Cadastre implemented to protect the data subjects' privacy.

Harmonizing open data and protection of privacy

To ensure protection of individuals' privacy, the cadastre provides a secure service guaranteeing data privacy whilst fully supporting transparency within public services. Only data, not subject to data protection law, is visible for all citizens (e.g. surface, location, use, shape, boundaries, cartographic representation, and type of constructions …). The cadastre's policy of open access is compliant with INSPIRE Directive, PSI Directive and Spanish law on citizens' electronic access to public services.

Implementing the rights of the data subject

The Spanish Cadastre has implemented procedures to handle requests relating to the rights of the data subject. For the right to rectification, data subjects can request the Spanish cadastre to update their personal contact details. Notaries, municipalities and registries can access and change the data directly, e.g. a notary can change the ownership of a property when the owner of the property has died. They have the right to process these changes, because the reason for these changes results from a demand from the data subject itself. Afterwards, a civil servant of the cadastre will validate the changes, finalising the procedure.

Balancing data protection and open data

All Spanish citizens can access the publicly available data via the website of the Spanish Cadastre, but they can also access the data offline by going to the office of the Spanish Cadastre or to one of the cadastral information points. A citizen can identify himself on the website using his Spanish e-ID card. This allows him to also access his personal data (name, address and national Identifier Number of tile holders and cadastral values), cadastral certifications of various types, and consult and download additional data like a sketch by plant, facade photo, etc.

Entities that collaborate with the Cadastre, like a company, can also access the public services described above. In addition, in case it is described by law, they can access also the data of all real estate within its sphere of competence (non-protected and protected data). For this purpose, it is necessary to be registered off line as a "registered user of cadastre". During this offline registration procedure, the Cadastre checks whether the collaborator has a legal ground and determines what data he will get access to: only data that is necessary to fulfil the purpose can be accessed.

Every access to a property is registered in the logs, allowing property owners to view who accessed their data and for what reasons.

List of abbreviations and definitions

EULF	European Union Location Framework
ISA	Interoperability Solutions for the European Public Administrations
PNR	Passenger Name Record
GDPR	General Data Protection Regulation
IP	Internet Protocol
GPS	Global Positioning System
DPO	Data Protection Officer
OECD	Organization for Economic Cooperation and Development
ENISA	European Union Agency for Network and Information Security
PbD	Privacy by Design
DPIA	Data Protection Impact Assessment
PIA	Privacy Impact Assessment
ISF	Information Security Forum
NIST	National Institute of Standards and Technology
PET	Privacy Enhanced Technology
IAPP	International Association of Privacy Professionals

List of figures

List of tables

LF-NA-28202-EN-N

JRC Mission

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new methods, tools and standards, and sharing its know-how with the Member States, the scientific community and international partners.

Serving society
Stimulating innovation
Supporting legislation

Publications Office

doi:10.2791/420310

ISBN 978-92-79-63495-6