PANELFIT

PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

Guidelines on Data Protection Ethical and Legal Issues in ICT Research and Innovation.

LOCATION AND TRACING DATA

Brief summary

Iñigo de Miguel Beriain (UPV/EHU)

This document is an abbreviated version of the part of the Panelfit Guidelines related to Locatoin and Proximity data. For better information, it is advisable to consult the full version of our Guidelines, written by . Iñigo de Miguel Beriain (UPV/EHU) and Lorena Pérez Campillo (UPV/EHU), at: https://guidelines.panelfit.eu/geolocation/

This document follows the structure of the Locus Charter.[1] This is an important intent to create some common international principles to help users of geospatial data make better informed decisions, and provide the basis for communication with people affected by those decisions. PANELFIT is happy to cooperate in such a collaborative effort that was originally supported by the Benchmark and EthicalGEO initiatives. Following the Charter, we consider that there are ten basic principles that must be addressed when using position/proximity data: realize opportunities, understand impacts, do not harm, protect the vulnerable, address bias, minimize intrusion, minimize data, protect privacy, prevent identification of individuals and provide accountability. This part of the Guidelines is aimed at concretizing these ethical principles into tangible legal advice.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. *This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.*

[1] https://ethicalgeo.org/locus-charter/

DISCLAIMER

This document is an abbreviated version of the part of the Panelfit Guidelines related to Location and Proximity data. Anyone using it should think of it as a basic introduction, which is in no way intended to provide sufficient knowledge of the material. Its main purpose is to prevent the reader from making serious mistakes. For better information, it is advisable to consult the full version of our Guidelines, written by Iñigo de Miguel Beriain and Lorena Pérez Campillo (UPV/EHU).

Furthermore, one must always keep in mind that the information provided in our Guidelines does not constitute legal advice; instead, all information, content, and materials provided are for general informational purposes only. The Guidelines provide general advice around EU data protection law under the GDPR. Accordingly, the reader should be aware that the situation relevant in their specific processing context, as well as in their specific jurisdiction, may deviate from the guidance provided. Indeed, information in our Guidelines may not constitute the most up-to-date legal or other information. The legal situation in relation to data processing in the EU changes regularly. New laws and new interpretations of existing laws relevant to the topics covered by the Guidelines appear frequently and changes may not be reflected in the Guidelines.

In this regard, we would highlight, without any intention of being comprehensive, at the time of writing, the significance of the following draft EU laws to the topics covered in these Guidelines: the ePrivacy Regulation, the AI Act, the Data Governance Act, the Digital Services Act, the Digital Markets Act and the Data Act.

Where relevant at the time of writing, authors may have attempted to highlight provisions of draft laws in relation to the topics covered in these Guidelines. The reader should be aware that drafts may change and that such references may not remain valid over time. Equally, authors' choices to consider certain provisions from certain draft laws should not be taken as indicative of effort to be comprehensive in addressing all relevant provisions from all draft laws.

Readers of the Guidelines should contact their DPOs and DPAs to obtain advice with respect to any particular legal matter. No reader, user, or browser of the Guidelines should act or refrain from acting on the basis of information provided without first seeking legal advice from counsel in the relevant jurisdiction. Only DPOs and DPAs can provide assurances that the information contained herein – and your interpretation of it – is applicable or appropriate to your particular situation. Use of, and access to, the Guidelines do not create any relationship between the reader, user, or browser and the authors, reviewers, validators, or commentors, of the Guidelines.

The views expressed in, or through, our Guidelines are those of the individual authors writing in their individual capacities only – not those of EU Commission, of course. All reference to reviews, validations, or provision of comments or suggestions, refer to the personal opinions of individuals acting in their personal capacities – and do not refer to the opinions of the organisations these individuals represent or to acts of these individuals in their official capacities.

The Guidelines contain links to other third-party websites. Such links are only for the convenience of the reader, user or browser; the authors and the reviewers/validators do not recommend or endorse the contents of the third-party sites.

All liability with respect to actions taken or not taken based on the contents of the PANELFIT Guidelines are hereby expressly disclaimed.

1 Realize opportunities-business understanding and data protection plan

1.1 Define the goal of your project and the data protection issues involved

The initial business understanding phase is key in terms of data protection issues, since it focuses on understanding the project objectives from a business perspective, converting this knowledge into a data mining problem definition, and then developing a preliminary plan designed to achieve the objectives. It is a crucial moment since the data protection by design requires that data protection risks are taken into account when drafting the business case and are followed up during the progress of the project. Data protection by design should be a given mindset which is established within an organization and project team.

Some essential tips that you should follow are:

- Establish the main goals to be reached by the device and consider the data protection issues relevant to its development and implementation from this very beginning.
- Consider whether the amount of data or the type of processing needed by the service to work properly is compatible with the data protection legal framework.
- Implemented and document Privacy-by-design policies and decisions. Make sure that you will be able to demonstrate how they are aligning with the GDPR and the regulatory framework on location/proximity data.
- Consider the pros and cons of a centralised/decentralised system and made an informed decision that is available to the scrutiny of public opinion.
- Consult stakeholders about possible ethical and legal issues at stake.

1.2 Introduce a training programme on data protection issues for the personnel involved in the design of the device or system

The designers (developers, programmers, coders, data scientists, engineers) of and ICT device or tool are likely to be unaware of the ethical and legal implications involved in the use of those data. This could bring consequences in terms of adequate compliance with data protection standards. Thus:

- Check that tool designers and all those who will have to deal with data have acquired an adequate knowledge of the data protection framework by introducing a training programme on these issues, or
- Ensure an adequate involvement of professionals trained in data protection

issues in the developing team. Indeed, you should better involve an expert in ethical/legal issues since the preliminary stages of the research project.

1.3 Consider what legal basis will allow for the processing of personal data by the device or system

The last drafts of the ePrivacy Regulation include several legal bases that might serve to legitimise data processing. In general, consent will probably continue to play a key role in the processing of data through electronic communications. However, article 8 of the version of the ePrivacy Regulaton by the Council includes alternative bases for the use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, concerning even its software and hardware. You should always be sure that a legal basis allows for any data processing.

If you are thinking about a re-use of personal data and the possibility to proceed with a lawful processing on this basis, you shall keep in mind that that the re-use of personal data should always respect the principles of lawfulness, fairness and transparency as well as purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality in line with Article 5 of the GDPR (73). Thus:

- Make sure that you have a legal basis that allows for a lawful data processing
- If you are willing to use personal data for compatible purposes, you must perform the compatibility test and ensure that such uses are indeed compatible.
- If you are willing to use the data for a purpose other than that initially sought, you should make sure that a legal basis allows for it.
- In general, you should try that all ICT tool are designed in a way that serves well to inform the user (data subject) about any re-use of personal data.

1.4 Consider what legal basis will allow for the processing of personal data by the device or system

The last drafts of the ePrivacy Regulation include several legal bases that might serve to legitimise data processing. In general, consent will probably continue to play a key role in the processing of data through electronic communications. However, article 8 of the version of the ePrivacy Regulation includes alternative bases for the use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, concerning even its software and hardware (see article 8).

If the processing only involves the collection of information emitted by terminal equipment of the end-user to enable it to connect to another device and, or to network equipment, it shall be permitted if conditions such as those included in article 8.2 of the ePrivacy Regulation draft apply.

Furthermore, it might also happen that data are finally processed under an alternative legal basis, such as public interest. This is not at all impossible if circumstances recommend it and the processing is based on Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject. However, developers should keep in mind that such alternative basis are applicable only if the controller is a public authority. Furthermore, the regulation of public interest might be different in each Member State. Controllers should be well aware of such circumstance.

On the other hand, personal data **may be reused for purposes compatible with that for which it was originally collected.** However, the controller must ensure and carefully document that this purpose is indeed compatible with the original one. The draft of the ePrivacy Regulation by the Council includes a clause devoted to this issue, article 8, (g) and (h).

The legal basis that provides the lawful ground for the use of location/proximity data should, in any case, incorporate meaningful **safeguards**. In case the data is being used for more than one purpose, the controller should link which categories of data are being used for which purposes. In addition to all the previous, it is important to establish and communicate the period of time during which the data will be preserved. Moreover, the information must not be used to determine the nature or characteristics of an end-user or to build a profile of an end-user. Depending on the level of interference, additional safeguards should be incorporated, taking into account the nature, scope and purposes of the processing. See, on this, Article 8 of the ePrivacy Regulation. Thus.

- Check that you have a legal basis that allows for a lawful data processing
- If personal data are used for compatible purposes, you have performed the compatibility test and ensured that uses are compatible.
- If the data are used for a purpose other than that initially sought, you should make sure that a legal basis allows for it. In general, the tool must be designed in a way that serves well to inform the user about this re-use.

1.5 Special consideration of consent as a basis for processing

If consent is used as the legal basis for data processing, developers should ensure that their device includes the need to obtain the users' consent for processing in an informed and granular way and the documentation of such consent. Furthermore, such consent must be properly accredited. Some essential tips are:

- It must be crystal clear that consent by the data subject cannot be obtained freely through mandatory acceptance of general terms and conditions, or through opt-out possibilities. It must be granular in approach. On the other hand, the default settings of an operating system should ensure that location services are 'OFF', and users may explicitly consent to the switching 'ON' of specific applications. Furthermore, "it is important to distinguish between consent to a one-off service and consent to a regular subscription. For example, in order to use a particular geolocation service, it may be necessary to switch on geolocation services in the device or the browser. If that geolocation capacity is switched 'ON', every website may read the location details of the user of that smart mobile device. In order to prevent the risks of secret monitoring, the former Article 29 Working Party considers it essential that the device continuously warns that geolocation is 'ON', for example through a permanently visible icon."[2]

- Poviders of location applications or services should seek to renew individual consent after an appropriate period of time. Thus, the developer could consider the possibility of incorporating in the device or system an e-tool capable of sending a request to the user in order to (re)gain (or not) their consent to continue with the processing. However, this is more a recommendation than a legal requisite.
- Broad consent might be acceptable, but only if some concrete circumstances apply, such as: it is difficult or improbable to foresee how this data will be processed in the future; broad consent used for processing of special categories of data is compatible with national regulations; where broad consent is used, the data subjects are given the opportunity to withdraw their consent and to choose whether or not to participate in certain research and parts of it. Furthermore, some safeguards must be implemented.
- An application that wants to use geolocation data clearly informs the user about the purposes for which it wants to use the data, and asks for unambiguous consent for each of the possibly different purposes. The user actively chooses the level of granularity of geolocation (for example, on country level, city level, zip code level or as accurately as possible). Once the location service is activated, an icon is permanently visible on every screen that location services are 'ON'. The user can continuously withdraw his consent, without having to exit the application. The user is also able to easily and permanently delete any location data stored on the device."

Some general tips about consent include:

- Check that consent is the most appropriate legal basis for processing.
- Request the consent of the interested parties in a free, specific, informed and unequivocal manner.
- Make sure that you strictly follow the best practices guidelines related to consent when children or people unable to provide consent are involved
- Make sure that broad consent is used for (and only for) scientific research, and only when it is difficult or improbable to foresee how this data will be processed in the future.

[2] Article 29 Working Party (2011) Opinion 13/2011 on Geolocation services on smart mobile devices Adopted on 16 May 2011. 881/11/EN WP 185, P. 13, at: https://www.apda.ad/sites/default/files/2018-10/wp185_en.pdf

- Assess that broad consent used for processing of special categories of data is compatible with national regulations.
- Where broad consent is used, the data subjects are given the opportunity to withdraw their consent and to choose whether or not to participate in certain research and parts of it.
- Build a direct relationship with the subject who provides the data to be used for training, validation and deployment of the IA model.
- Make sure that there is no power imbalance between controllers and data subjects.
- Ask people to positively opt in.
- Do not use pre-ticked boxes or any other type of default consent.
- Use clear, plain language that is easy to understand.
- Specify what kind of data you collect, why you want the data, what you are going to do with it and for how long.
- Give separate distinct (‘granular’) options to consent separately to different purposes and types of processing.
- Tell individuals they can withdraw their consent and how to do so.
- Ensure that individuals can refuse to consent without detriment.
- Avoid making consent a precondition of a service.

2 Understand Impacts

Users of location data have responsibility to understand the potential effects of their uses of data, including knowing who (individuals and groups) and what could be affected, and how. Controllers shall consider the recommendations made by the High-Level Expert Group on AI.[3] Some essential tips include:

- Check the impact of the device in different groups and documented the results obtained.
- Make sure that the device does not allow for a use of the data in a way that is not compatible with the preservation of privacy.
- Ensure that the device is mindful of principles of environmental sustainability, both regarding the system itself and the supply chain to which it connects (when relevant)
- Consider that the default configuration of the device shall not allow uses of data for surveillance purposes
- Do not design the device for purposes that are not compatible with the EU's main ethical principles.

In the case of location and proximity data, the EDPB considered “that a data protection impact assessment (DPIA) **must be carried out before implementing such tool as the**

3High-Level Expert Group on AI, Ethics Guidelines for Trustworthy Artificial Intelligence (84 and ff.), at: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

processing is considered likely high risk (health data, anticipated large-scale adoption, systematic monitoring, use of new technological solution). The EDPB strongly recommends the publication of DPIAs."[4]. In order to see if a DPIA is necessary:

- Determine the jurisdictions where data-processing activities will take place.
- Check if those jurisdictions have enacted lists indicating the processing that requires a mandatory DPIA and checked if the intended data processing is covered by those provisions.
- If you are unsure of the necessity of carrying out a DPIA, you must consult with the DPO or, in lieu of, the legal department of the controller.
- If necessary, file a prior consultation with the appropriate supervisory authority.

There is no standard way to perform a DPIA. However, Article 35.7 GDPR calls for specific elements that shall always be present. These are:

- a systematic description of the envisage processing operations;
- the purposes of the processing operations;
- an assessment of the necessity of the processing operations in relation to the purposes;
- an assessment of the proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of data subjects;
- the technical and organizational measures envisaged to address the risks.

3 Do not harm

One of the main issues that massive data processing might involve is the exposition of personal data to unauthorized third parties. A data breach could cause dramatic harm to thousands or millions of users, whose privacy could be compromised. These risks must be mitigated through the implementation of technical and/or organisational security controls.

Some essential tips include[5]

In general:

- Assess potential threats to which the tool could be vulnerable, introduced mitigation measures and documented them. Performing threat modelling is highly recommendable
- Consider different types and natures of vulnerabilities, such as data pollution, physical infrastructure and cyber-attacks.

[4] EDPB, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak Adopted on 21 April 2020

[5] This checklist has been built on the basis of these documents: EDPB, Guidelines 04/2020 on the use of cation data and contact tracing tools in the context of the COVID-19 outbreak Adopted on 21 April 2020; High-Level Expert Group on Artificial Intelligence (2019) Ethics guidelines for trustworthy AI. European Commission, Brussels. Available at: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

- Put measures or systems in place to ensure the integrity and resilience of the system against potential attacks.
- Verify how the system behaves in unexpected situations and environments.
- Consider to what degree the system could be dual-use. If so, the controller took suitable preventative measures against this (e.g. not publishing the research or deploying the system).

Fallback plan and general safety. Ensure that:

- The system has a sufficient fallback plan if it encounters adversarial attacks or other unexpected situations (e.g. technical switching procedures or asking for a human operator before proceeding).
- The data sent to the central server is transmitted over a secure channel and the use of notification services provided by OS platform providers is carefully assessed, and does not lead to disclosing any data to third parties.
- Requests are not vulnerable to tampering by a malicious user.
- State-of-the-art cryptographic techniques are implemented to secure exchanges between the application and the server and between applications and, as a general rule, to protect the information stored in the applications and on the server.
- The central server does not keep network connection identifiers (e.g., IP addresses) of any users.
- In order to avoid impersonation or the creation of fake users, the server authenticates the application.
- The application authenticates the central server.
- The server functionalities are protected from replay attacks.
- The information transmitted by the central server is signed in order to authenticate its origin and integrity.
- Access to all data stored in the central server and not publicly available is restricted to authorised persons only.
- The device’s permission manager at the operating system level only requests the permissions necessary to access and use the communication modules, to store the data in the terminal, and to exchange information with the central server.
- The personnel and other physical person in the project has been informed and given awareness of security measures.

Data breaches notification:

- You have developed and implemented adequate policies to notify data breaches as soon as possible and all participants in the development process are well aware of them
- Templates about the information to be included in the notifications have been designed.
- Communication policies and tools, aimed at facilitating communication with the data subjects if a data breach happens,

4 Protect the vulnerable

Vulnerable people and places can be disproportionately harmed by the misuses of location data, and may lack the capacity to protect themselves. In these contexts, data users should take additional care, act proportionately, and positively avoid causing harm. Some essential tips include:

- Developing products that can be used through different types of devices, smartphones, tokens, etc., so that those who do not have one of the devices can acquire another.
- Introducing adapted operating options for people with disabilities, so that these do not prevent them from using the designed tools.
- Simplify as much as possible the functioning of their basic operations, so that any person can use them without making an excessive effort in relation to their capabilities.
- Privacy policies must be redacted in a user-friendly style, so that everyone can understand them.
- If the device is specifically targeted at vulnerable people (for instance, a location device to prevent sight impaired people from getting lost) or under aged users, privacy policies must be adapted to that specific target group. This can mean being accessible through voice rather than only in text, images rather than long texts, or that the language is adapted, for instance, to an average teenager's understanding.

The case of children is particularly important. According to Recital 38 of the GDPR, "children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing". The ICO has developed some extremely useful recommendations for this purpose[6].

5 Address bias

Biases are one of the main issues involved in the use of ICT devices and systems, an issue that contravenes the fairness principle. In the case of devices based on location and/or proximity data, biases might be derived from at least two different situations:

- Biases created by an AI system interacting with the location devices or systems. Sometimes location devices or systems incorporate or interact with AI tools. If this is the case, developers should pay special attention to ensure that they do not introduce biases in the functioning of the location device or system. For this purpose, they must adopt a number of measures, as described in the part of these Guidelines devoted to AI systems

[6] https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/10-geolocation/.

- Biases created by the data gathered. This type of bias is particularly probable if the ICT tool is aimed at providing information based on data gathered from an entire population. It is very likely that its degree of social representation is inaccurate. Indeed, as locative media research has shown, context and marginalization matter with location data.[7] This may create problems of inequity. Developers of location devices or systems should make an effort to avoid this type of bias, either by **providing devices to those who would otherwise be marginalized or by integrating complementary information that corrects the error.** If it is impossible to avoid it, they should make a record of the existence of the bias, so that those who would have to make decisions thanks to the developed mechanism would be aware of it. Some essential tips are:
    - Establish a clear and available acceptability threshold of bias and ensure that compliance is monitored.
    - Put in place a series of steps to increase the tool's fairness
    - Put in place measures to assess whether there is a need for additional data, for example to eliminate biases.
    - Document what harm would be caused if the tool makes biased predictions.

6 Minimize intrusion and data

6.1 Data minimization

Developers should provide devices and systems with options that allow them minimise the use of data to what is strictly needed. Thus, anonymized data should be used whenever possible. If this were not possible, controllers should at least try to work with pseudonymized data. In practice, the EDPB considered that this principle means that "the application should not collect unrelated or not needed information, which may include civil status, communication identifiers, equipment directory items, messages, call logs, location data, device identifiers, etc.
Data broadcasted by applications must only include some unique and pseudonymous identifiers, generated by and specific to the application. Those identifiers must be renewed regularly, at a frequency compatible with the purpose of containing the spread of the virus, and sufficient to limit the risk of identification and of physical tracking of individuals."[8]. Furthermore, the collection and processing of Service Set Identifiers (SSIDs) is not necessary. Therefore, the collection and processing of SSIDs is excessive for the purpose of offering geolocation services based on mapping of the location of WiFi access points[9]

[7] Graham, M., Zook, M. (2013). Augmented realities and uneven geographies: Exploring the geolinguistic contours of the web. Environment and Planning A, 45, 77–99.

[8] EDPB, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak Adopted on 21 April 2020

[9] Article 29 Working Party (2011) Opinion 13/2011 on Geolocation services on smart mobile devices Adopted on 16 May 2011. 881/11/EN WP 185, P. 16, at: https://www.apda.ad/sites/default/files/2018-10/wp185_en.pdf

Finally, a developer should only use the type of data that is strictly necessary for the purpose of the processing, and in order to avoid the use of any third party software developer kit (SDK) collecting data for other purposes. By default, developers must ensure that the device does not send data to third parties without notification to the data subject. Similarly, information on the proximity between users of the application should be obtainable without locating them. The device should be designed to avoid such a scenario by default. In general, the tool should not collect additional data that are not strictly necessary for its purposes, except on an optional basis and for the sole purpose of assisting in the decision making process of informing the user.

Some essential tips involve ensuring that[10]:

- The tool is based on an architecture relying as much as possible on users' devices.
- Requests made by the applications to the central server do not reveal unnecessary information for the purposes of the service to the system.
- Requests made by the tool to the central server do not reveal any unnecessary information about the user, except, possibly, and only when necessary, for their pseudonymous identifiers and their contact list.
- In order to avoid re-identification by the central server, proxy servers are implemented. The purpose of these non-colluding servers is to mix the identifiers of several users before sharing them with the central server, so as to prevent the central server from knowing the identifiers (such as IP addresses) of users.
- The application and the server are carefully developed and configured in order not to collect any unnecessary data (e.g., no identifiers should be included in the server logs, etc.) and in order to avoid the use of any third party collecting data for other purposes.
- The tool only collects data transmitted by instances of the application or interoperable equivalent applications. No data relating to other applications and/or proximity communication devices are collected.
- The use of the application does not allow users to learn anything about other users, if it is not strictly necessary.
- If data processing is necessary, it is documented.
- The central server does not maintain nor circulate a list of the pseudonymous identifiers of users
- If the design of the device or the tools allows for several options regarding the collection and further processing of data, the most protective one will be set by default. This decision must be documented.
- If the tool is aimed at tracing contact purposes, it does not allow users to identify other users' movements

[10] These tips have been built on the basis of the one included in the EDPB, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak Adopted on 21 April 2020, at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

6.2 Purpose limitation

Whenever processing location or proximity data, recipients must only use the information for the task for which it was provided to them. Thus:

- If controllers are planning to offer an advertising platform and/or a webshop-like environment for applications that will be able to process personal data resulting from the (installation and use of) geospatial data applications, independently from the application providers, this should be carefully explained to the users. They should provide explicit consent to these purposes. Rejecting unnecessary processing should not provoke the impossibility to use the device or system. In general tracking walls, that is, the type of system that links the service to the consent for the use of data, and that are not needed for the functioning of the tool, should be carefully avoided.
- If the tool has been designed to work on proximity data, it should not allow the developer or a third party to use such data to draw conclusions about the location of the users based on their interaction and/or any other means. If the tool has been designed to work on location data, it should not allow the developer or a third party to draw conclusions on the interaction of the users with other people.
- The controller must pay specific attention to purposes that a data subject does not expect, such as for example profiling and/or behavioural targeting. If the purposes of the processing change in a material way so as to be incompatible with the original processing, the controller **must seek** a new valid lawful base, such as a **new specific consent.** Additionally, the controller must provide a genuine option to withdraw consent at any time, as well as the possibility of exercising users' rights, such as erasure of data or restriction of processing.
- It is also important to distinguish between consent to a one-off service and consent to a regular subscription. For example, in order to use a particular geolocation service, it may be necessary to switch on geolocation services in the device or the browser. If that geolocation capacity is switched 'ON', every website may read the location details of the user of that smart mobile device.
- In order to prevent the risks of secret monitoring, the Article 29 Working Party considered it essential that the device continuously warns that geolocation is 'ON', for example through a permanently visible icon.[11] This can hardly be considered a compulsory requirement for the controller, but it is certainly a good practice that must be recommended.

[11] Article 29 Working Party (2011) Opinion 13/2011 on Geolocation services on smart mobile devices Adopted on 16 May 2011. 881/11/EN WP 185, P. 13, at: https://www.apda.ad/sites/default/files/2018-10/wp185_en.pdf

Some essential tips are[12]:

- Identify the purpose or purposes for processing, which must be "specific" and limit them in time and scope.
- Documented those purposes.
- Include details of their purposes in the privacy information for individuals, ensuring that the data subject is adequately informed, according to art. 12-14 GDPR.
- Ensure that the tool cannot be inadvertently diverted from its primary use and it does not use walls to collect unnecessary data
- If you plan to use personal data for a new purpose other than a legal obligation or function set out in the law, check that this is compatible with their original purpose or they get specific consent for the new purpose.
- If you wish to further process the data for a purpose other than that initially obtained which is incompatible with the original purpose, and in the case that consent is the most suitable lawful basis, the tool is designed to ask users for permission. In any other case, you shall find the most adequate lawful basis.
- Make sure that if the tool has been designed to work on proximity data, it cannot be used to draw conclusions on the precise location of the users based on their interaction and/or any other means.
- Check that if the tool has been designed to work on location data, it cannot be used to draw conclusions on the interaction of the users with other people or to make inferences about further categories of data based on the places visited by the person or any other means.

6.3 Do not keep the data longer than strictly needed (storage limitation)

Devices should be programmed in a way that minimizes the time they store the data: they should only keep data during the time that is strictly needed to reach their aim. For instance, do not forget that a randomly attributed Unique Device Identifier (UDID), such as a unique number, should only be stored for operational purposes, for the time that is needed for the purposes of the processing. "After that period, this UDID should be further anonymised while taking into account that true anonymisation is increasingly hard to realise and that the combined location data might still lead to identification. Such a UDID should neither be linkable to previous or future UDIDs attributed to the device, nor should it be linkable to any fixed identifier of the user or the telephone (such as a MAC address, IMEI or IMSI number or any other account numbers)."[13]

Some essential tips include: Ensure that

[12] This list of tips has been built on the basis of these documents: EDPB, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak Adopted on 21 April 2020; ICO (no date) Principle (b): purpose limitation. Information Commissioner's Office, Wilmslow. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/ (accessed 17 May 2020).

[13] WP29 Opinion 13/2011 on Geolocation services on smart mobile devices, at: https://www.apda.ad/sites/default/files/2018-10/wp185_en.pdf

- Contact history or location data stored on the central server is deleted once they are no longer needed for the purposes of the processing.
- A time limit is always be considered. Necessity cannot be forever
- The procedure for data erasure is adequately designed and implemented and the controller and the users are well aware of it.
- Any identifier included in the local history is deleted after X days from its collection (the X value being defined by the purpose of the processing).
- Data in server logs are minimised and comply with data protection requirements
- If there is a central server and it needs to store data identifiers, these are deleted once they are distributed to the other applications unless a legal/technical reason recommends otherwiseProtect Privacy

6.4 Introduce an adequate privacy policy

The developer should always make sure that the device or system incorporates an adequate privacy notice. This must describe how the tool collects, uses, retains and discloses personal data. Furthermore, the device should include information about the data subjects' rights in an accessible way[14].

In addition to the compulsory information requirements, controllers are encouraged to follow the following best practices regarding the provision of transparent information in projects that involve the processing of location or proximity data. These are not compulsory, but they are highly recommended:[15]

- What are the concrete uses that will be given to the data collected
- State the frequency and detail in which the geospatial data are collected;
- State the nature and the type of data collected;
- When applicable, remind data subjects that they may forget they are being tracked, and that the device may record their visits to private locations or their proximity to some concrete people (this is not compulsory, but might be considered good practice);
- When applicable, remind participants that evidence suggesting illegal activities may be uncovered by geospatial data. If so, disclosure may not be protected by the research institution's confidentiality policy and could be potentially discoverable by law enforcement (see art. 10 of the GDPR);
- Provide for an easy means of reminding data subjects that they are being tracked. For instance, by activating an icon when location or proximity data are being collected and deactivating this icon when data is not being collected.

[14] JRC Technical Reports, Guidelines for public administrations on location privacy, at: https://publications.jrc.ec.europa.eu/repository/handle/JRC103110

[15] Goldenholz DM, Goldenholz SR, Krishnamurthy KB, et al. Using mobile location data in biomedical research while preserving privacy. *Journal of the American Medical Informatics Association*, ocy071, https://doi.org/10.1093/jamia/ocy071.

- Provide a statement explaining that individuals will not be identified in any research publication or presentation without explicit participant consent (unless an alternative legal basis for processing is applicable);
- Provide a statement explaining that identifiable data will not be shared with third parties without the subject's consent, but that de-identified data may be shared;
- When applicable, remind and show data subjects how they can disable or temporarily pause location tracking or proximity data gathering whenever they wish;
- Build a list of recipients who will have access to the data;
- Assess risk that participants will be re-identified from the data provided;
- Assess risk for possibility of harm if data were inadvertently re-identified including, when relevant, financial loss, psychological harm, and/or physical harm.
- Inform data subjects about their rights and the way to enforce them
- Provide data subjects with contact information of the corresponding DPO

It is recommended to opt for legal design options that can make the privacy policies more visual and easier to understand. It is also necessary to provide participants with a "privacy self-management" model where participants have easy access (via a link or menu item) to brief contact details of the entity. The app landing page is an excellent place to post relevant privacy information, contact information and provide a hyperlink to a "second layer" of more detailed privacy information, according to article 12.7 of the GDPR.

If processing involves third parties, a contractual clause with recipients of data, whether they are controllers or processors, must be signed. This clause can state that the recipient refrains from trying to re-identify data subjects and that, in case re-identification occurs, such data must be deleted and the fact must be notified.

Some essential tips include[16]:

- ºReview your processing and, where necessary, update your documentation and privacy information for individuals.
- Ensures that users are informed of all personal data that will be collected. These data are collected only if a legal basis for processing applies
- Explain how people can access details of the information that is used for the services offered by the tool.

6.5 Protect the rights of the users

Data subjects can invoke numerous rights related to their data, which are described in full detail in the corresponding section In general, devices using location and proximity

[16] This list of tips has been built on the basis of these documents: EDPB, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak Adopted on 21 April 2020; ICO (no date) Principle (b): purpose limitation. Information Commissioner's Office, Wilmslow. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/ (accessed 17 May 2020).

data should enable their users to obtain access to their data in a human readable format and allow for rectification and erasure without collecting excessive personal data.

Rights	Tip
Right of access	Provide a functionality to display all data related to a data subject. If there is a lot of data, it can be split into several screens. If the data is too large, offer the person the possibility to download a file containing all their data. As regards location or proximity data, controllers may allow data subjects to access the information in usable formats such as in maps visualizations, in case they already use such formats
Right to rectification	Allow direct modification of data in the user's account (if applicable and/or possible). Provide advice on why it might not be advisable under some circumstances.
Right to erasure	Provide a functionality to erase all data relating to an individual to which the right to erasure applies (and only to those data). In addition, provide for automatic notification to data processors to also erase such data. Provide for the deletion of such data in backup copies, or provide an alternative solution that does not restore deleted data relating to that person. Introduce a functionality that always alerts the user to the consequences of deletion.
Right to restriction of processing	Provide a functionality that allows the data subject to object to the processing of specific personal data. When the data subject exercises his or her right to object in this way, the tool must delete the data already collected and must not subsequently collect any more such data.
Right to data portability	Provide a function that allows the data subject to download their data in a standard machine-readable format (CSV, XML, JSON, etc.).

It is necessary to mention that the ePrivacy Regulation includes additional rights such as confidentiality of communications, calling line identification, or rights specifically targeted at location data other than traffic data (See chapter III of the Proposal). Controllers should ensure that the tool does not enable a violation of such rights by introducing measures devoted to limit the use of geospatial data if this is not essential for the service.

Some essential tips are[17]:

- Users are able to exercise their data and access rights via the application.

[17] This list of tips has been built on the basis of the EDPB, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak Adopted on 21 April 2020

- If the tool has been designed to work on proximity data, it is not used to draw conclusions on the location of the users based on their interaction and/or any other means.
- If the tool has been designed to work on location data, it cannot be used to draw conclusions on the interaction of the users with other people.
- If data are used for compatible purposes, you must perform the compatibility test.
- If you (as controller) wish to use the data for a purpose other than that initially sought, the tool asks users for permission.

7 Provide accountability

7.1 Description

Accountability consists of two requirements for controllers:

- **Compliance** with the principles of the GDPR;
- **Demonstration of compliance.**

Compliance is achieved by implementing ***technical and organizational measures*** that are adequate compared to the risks to the rights and freedoms of data subjects, correspond to the state of the art of technology, and are cost-effective. Every description of the principles has provided examples of such technical and organizational measures. For a systematic application of these measures, controllers can create ***data protection policies***. ***Approved codes of conduct***, where available, are similar but are pre-approved and usually address an entire sector. Compliance is not a state that is reached once, but **a continuous process** that spans the whole life cycle of a processing activity.

Demonstration of compliance is predominantly achieved by **documentation**. Documentation should be continuous like the process of compliance. Every implemented measure, including data-protection-relevant considerations and decisions, should be documented. The GDPR requires two formal documents as part of demonstrating compliance towards supervisory authorities: the **register of processing** and, where the risks are likely to be high, a **data protection impact assessment.** Certification can support the demonstration of compliance.

7.1.1 Documenting of processing[18]

The main decisions made by the data controller "have to be documented in order to comply with the requirement of data protection by design" (of Article 25 of the GDPR). Indeed, an organization who is processing personal data (including both, controllers and processors) needs to documents its activities primarily for consumption by the

[18] This part of these Short Guidelines was originally written by Bud Brugger, see: https://guidelines.panelfit.eu/the-gdpr/main-tools-and-actions/documentation-of-processing-personal-data/

competent Data Protection Supervisory Authorities (DPA). This includes the ***records of*** **processing** that is maintained centrally by the organization across all its processing activities and **additional documentation** that pertains to an individual data processing activity.

Records of processing can be kept in written or electronic form[1]. So expect to either fill in an organization-specific form or enter your information into some (data protection) management system.

To provide an initial idea, the minimal content of the records of processing for controllers includes the following items[2]:

- The **name** and **contact** details **of the controller**, the controller's **representative** and the **data protection officer**;
- the **purposes** of the processing;
- a description of the **categories of data subjects** and of the **categories of personal data**;
- the **categories of recipients** to whom the personal data have been or will be disclosed;
- where applicable, **transfers of personal data to a third country** together with the documentation of suitable safeguards;
- where possible, the envisaged **time limits for erasure of the different categories of data**
- where possible, a general description of the **technical and organizational *security* measures**

Documentation: checklist		
1	Personal data protection policy	Article 24.2
2	Privacy notice	Articles 12, 13, 14
3	Data Retention Policy	Articles 5, 13, 17, and 30
4	Data Retention Schedule	Article 30
5	Record of processing activities (if applicable)	Article 30
6	Consent form (if applicable)	Articles 6, 7, 9
7	Data processing agreement with suppliers	Articles 28, 32, 82
8	Data Protection Impact Assessment	Article 35
9	Appointment of an EU representative (if applicable)	Article 27
10	Data Breach Response and Notification Procedure	Articles 4, 33, 34
11	Data breach notification to Supervisory Authority (if applicable)	Article 33
12	Data breach notification to data subjects (if applicable)	Article 34

Some documentation is necessary only when specific *criteria* apply. Keep always in mind that:

- Your organization may use a different set of items since on one hand, it already is in possession of some of this information (such as the first bullet), and on the other hand, it may require additional information (such as the contact of the person responsible for the single processing activity at hand).
- It is possible that the legally required record keeping is combined with the management needs of the organization, such as an internal inventory of computing and computing resources.
- Your organization may also use multiple systems, e.g. depending on whether it is acting as a controller or as a processor; or distinguishing between permanent data processing activities (such as communication systems and accounting) and temporary ones (such as those linked to temporary projects or assignments). The creation and maintenance of records across multiple systems is not prohibited under the GDPR.

Some essential tips are:

- Data protection (like security) is a process, not a final state. Continuously document that process rather than only the final characteristics of the processing activity.
- When applying data protection by design[4], the processing activity can be seen as the results of a series of many considerations and decisions. It is these considerations and decisions that should be documented.
- Deciding on a structure and format to systematically collect this information at the point of time when you conceive your processing activity.
- Where the documentation itself contains personal information (see below), make sure to protect is sufficiently and limit its further use to the purpose of demonstrating compliance with the GDPR.

7.2 Ensure transparency

Transparency is key to accountability. The tool must be designed in such a way that transparency and user control can become a reality [19]. "In order to ensure their fairness, accountability and, more broadly, their compliance with the law, the ICT tools must be auditable and should be regularly reviewed by independent experts. Some tips include:

- The application's source code should be made publicly available for the widest possible scrutiny".20 Thus, the source code of the application and of its backend must be open, and the technical specifications have been made public, so that any concerned party can audit the code, and where relevant, contribute to improving the code, correcting possible bugs and ensuring transparency in the processing of personal data

[19] EDPS. Opinion 7/2015. Meeting the challenges of big data. A call for transparency, user control, data, protection by design and accountability. Recuperado de https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf

[20] EDPB, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak Adopted on 21 April 2020

- You must ensure that their devices incorporate functions that allow end-users to be fully aware of the processing that will be given to their data.
- It must be ensured that the tool adequately informs data subjects of what information the tool needs and why it needs it.
- The introduction of a "personal data area" where they can be informed of the personal data being processed, and even modify, correct or update this if necessary and if appropriate, is highly recommended.
- Finally, it is recommended to opt for legal design options that can make the privacy policy more visual and easier to understand.

7.3 Risk assessment and DPIAs (see section 2 of this document)

7.4 Processor due diligence

The accountability principle is also present when a controller chooses to require the services of a processor. Therefore, a researcher using location or proximity data that needs to hire a third party for certain processing activities would need to ask two questions: (1) what type of conduct is expected to demonstrate compliance with this obligation; and (2), if some form of positive action is expected, how should controllers proceed to carry such due diligence. In general, **any question that You would ask themselves when developing the AI should be asked to the processor.** These comprise:

- Require information regarding where the data-processing activities will take place, and: (1) carry out the case law review suggested below; and (2) assess if the jurisdictions, in case of non-EU countries, are deemed as adequate by the EU Commission.
- Review case law from the national supervisory authorities where the processor operates to check for potential sanctions.
- Require proof of adherence to a code of conduct or certification.
- Require proof of relevant ISO certification.
- Require a copy of records of processing activities.
- Enquire about the development process of the AI, in particular which kind of data were used for training the AI and the data that the AI needs to operate and deliver a useful result.

7.5 Data protection Officers (DPOs)

In the case of location and proximity devices and systems**, the appointment of a DPO will most likely be necessary.** Three essential tips are:

- Appoint a DPO if possible and whenever it constitutes a legal requirement
- If your are not required to appoint it and you do not proceed to name it on a voluntary basis, introduce the necessary organisational and security measures

- Make sure that the DPO is aware of every step taken to allow room for their intervention if deemed relevant and able to carry them out.