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.

GEOLOCATION

Location and tracing data

Iñigo de Miguel Beriain and Lorena Pérez Campillo (UPV/EHU)

The last section of this document partially reproduces the part of AI originally written by Gianclaudio Malgieri and Andrés Chomczyk Penedo (VUB)

Mario Muñoz Organero and Julian Estévez provided valuable support regarding technical issues.

This part of the Guidelies was revised by Elena Gil González, IT and data protection lawyer and finally validated by Iñaki Pariente, former director of the Basque Data Protection Agency.

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.

Introduction

"In the context of online geolocation services provided by information society services three different functionalities can be discerned, with different responsibilities for the processing of personal data. These are: controller of a geolocation infrastructure; provider of a specific geolocation application or service and the development of the operating system of a smart mobile device. In practice, companies often fulfil many roles at the same time, for example when they combine an operating system with a database with mapped WiFi access points and an advertising platform".[1] In this section of the Guidelines, we focus on the two last types of controllers: those who are willing to provide a specific geolocation application or service or to design the operating system of a smart mobile device.

Similarly, we do not tackle data protection issues related to the processing performed by online third parties that enable the (further) processing of location data such as browsers, social networking sites or communication media that enable for example 'geotagging'. We do not consider here the development of a device or system based on location or proximity data. These activities are included in those parts devoted to social networks and online services.

It is also necessary to point out that the developers of the operating system of the smart mobile device might be the controller for the processing of proximity or location data when they interact directly with the user and collects personal data (such as by requesting initial user registration and/or collecting location information for the purposes of improving services). "A developer is also the controller for the data they process if the device has a 'phone home' functionality for its whereabouts. Since the developers in that case decide on the means and purposes for such a data stream, they are the controllers for the processing of these data. A common example of such a 'phone home' functionality is the automatic provisioning of time zone updates based on location."[2]

This chapter of the Guidelines follows the structure of the Locus Charter.[3] 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

1 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. 12, at: https://www.apda.ad/sites/default/files/2018-10/wp185_en.pdf

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. 12, at: https://www.apda.ad/sites/default/files/2018-10/wp185_en.pdf

3 https://ethicalgeo.org/locus-charter/

of individuals and provide accountability. This part of the Guidelines is aimed at concretizing these ethical principles into tangible legal advice.

DISCLAIMER

This part of the Guidelines was written at a time when the ePrivacy Regulation had not been passed. It may happen that at the time of using this tool, the Regulation is in force. If so, it will be necessary to take into account the possible changes that this may have produced in the regulatory framework. In any case, this document has attempted to introduce some of the main provisions included in the draft ePrivacy Regulation. This is because, at the very least, we should understand that they are ethical requirements that a proper implementation of the GDPR demands. In this sense, we have introduced in this part of the Guidelines the main instructions developed by the EDPB in this regard.[4]

Until the ePrivacy Regulation enters into force, a fragmented situation will exist. Indeed, supervisory authorities face now a situation where the interplay between the ePrivacy Directive and the GDPR coexist and pose questions as regards the competences, tasks and powers of data protection authorities in those matters that trigger the application of both the GDPR and the national laws implementing the ePrivacy Directive. [5]

1 Realize opportunities-business understanding and data protection plan

1.1 Description

Geospatial data offers many social and economic benefits, and these opportunities should be realized responsibly. Geospatial data is a wide category that includes, at least, these types of data:

- "**Geospatial data**" for a broad meaning. This is the term used in the EthicalGEO website. It includes both location and proximity data.
- "**Location data**": specific or very granular geospatial data, that allows for a very precise information of where a subject or device is geopositioned.
- "**Proximity data**": less precise geospatial data, that allows one to know in a general way where a subject or device is geopositioned. For instance, by dividing a map in bigger quadrants, by using postal code information rather than specific addresses, etc. In general, proximity data informs the user about whether a data subject has been near to another data subject or a concrete location.

4 EDPB, Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities Adopted on 12 March 2019, at: https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf

5 EDPB, Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities Adopted on 12 March 2019, at: https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf.

1.2 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 (see "Data protection by design and by default" subsection in the "Main Concepts" section within Part II of these Guidelines) 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.[6]

In practice, this means that whoever is willing to develop an ICT tool using geospatial data should start by asking themselves what the goal of the tool is. This is key in terms of designing their data protection policy. The developers of the device must know from the outset what they expect it to do. If the goal of the device cannot be reached without processing a disproportionate amount of personal data, if those data should be kept for months or years, if it involves important privacy risks for the users, if safeguards needed cannot be put in place, etc., the development process might be better left out. Furthermore, there might be some goals that collide with the key principles of the GDPR or the EU Charter of fundamental rights. This might happen, for instance, when location/proximity data are used to inadvertently gather sensitive data, such as religious beliefs of the data subject. For instance, in 2017, an interactive "Global Heat Map" showing the movements of users of the Strava fitness app inadvertently revealed the locations of deployed military personnel in classified locations[7]. This incident highlights some of the broader legal and ethical issues associated with open data sharing and public data sharing by default. Automatic activation of geolocation without human intervention must be carefully avoided, since it would provoke unlawful data processing.

Box 1: Examples of different devices using location or proximity data, and their consequences in terms of data processing and data protection issues

It is not the same to design a device aimed at protecting a person with a certain level of dementia as one that is only intended to let a healthy person know what trips he or she has made in the last few months. The former will probably require the use of tools that can determine their position very precisely, while the latter will be satisfied with a less precise location. The former will use more detailed personal data than the latter.

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

7 See: The Strava Heat Map and the End of Secrets, Wired, 2018, at: https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/

In the same way, there will be products that need technologies that do not need to specify the time that the user is spending in all concrete locations, while some others do (as in the case of the person with severe Alzheimer's disease). Furthermore, the design of the tool should always include options that allow a proportional use of data. Even in the case of someone suffering from Alzheimer disease, it should be possible to graduate the use of geospatial data according to their real needs. Finally, a developer has to know from the first moment whether it is necessary to keep the data gathered for longer or shorter periods of time. A device that only wants to know if its user has been in a place where a virus growth was detected will probably only need to keep location data for a few days, while another that wants to report on the travels made in the last few months will need to keep the data much longer. Each of these variants will have major implications in terms of personal data protection. What is undeniable is that the developers can hardly define their data protection policies if they have not defined adequately the goal of the device to be developed.

Developers should be particularly aware of the fact that sometimes any marginal increase in terms of accuracy of the location or contact tracing calls for a significant increase in the amount of personal data needed.[8] For instance, postal code-based location is much less precise and therefore less privacy invasive than exact location-based systems. The first one may be enough for advertising local restaurants to passing people, while the second one will be required for a service calculating the shortest route by bike between two points. Therefore, if data controllers are considering a fundamental modification in the level of accuracy of the location or tracing required, they should carefully consider if this works well with the data minimization principle (see "Data minimization principle" within Part II section "Principles" of these Guidelines. See further detail about this in the "Minimize data" section below in this Part IV.

Finally, developers should make a decision on whether the product will implement a centralized or a decentralized approach. Both should be considered viable options, provided that adequate security measures are in place, each being accompanied by a set of advantages and disadvantages. However, it is usually considered that decentralized systems respect users' privacy better. Indeed, the starting point for data processing should be decentralized systems that look to shift processing on to individuals' devices where possible. Safeguards and security measures need to accompany this, together with information and any needed additional safeguards when there are international transfers of data.[9]

8 Norwegian Data Protection Authority (2018) Artificial intelligence and privacy. Norwegian Data Protection Authority, Oslo, p.20. Available at: https://iapp.org/media/pdf/resource_center/ai-and-privacy.pdf (accessed 28 May 2020).

9 Denham, Elizabeth, UK Information Commissioner, Combatting COVID-19 through data: some considerations for privacy, at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/04/combatting-covid-19-through-data-some-considerations-for-privacy/

Thus, the conceptual phase of a device or system development should always include thorough consideration of these alternatives concepts carefully weighing up the respective effects on data protection/privacy and the possible impacts on individuals' rights.[10] If developers opt for the centralized system, the data processed by the centralized server should be in general limited to the bare minimum.

Whenever possible and relevant, stakeholders should be consulted about what ethical and legal issues they believe are at stake and how these issues should be dealt with. Stakeholders consulted should include representatives of the major groups that will be affected by the system – directly or indirectly. In this way, an appropriately diverse range of ideas and preferences will inform design choices.

Checklist:[11]

ü Developers have fixed the main goals to be reached by the device and considered the data protection issues that their development and implementation might bring together.

ü Developers have carefully considered whether the amount of data or the type of processing needed by the service to work properly is compatible with data protection considerations.

ü Developers can ensure an adequate implementation of Privacy-by-design policies. They can demonstrate how they are aligning with the GDPR and the regulatory framework on location/proximity data. Actions implemented to ensure such alignment have been carefully documented.

ü Developers have considered the pros and cons of a centralized/decentralized system and made an informed decision that is available to the scrutiny of public opinion. To this purpose, consultations with key stakeholders have been performed and documented.

ü Developers have consulted stakeholders about possible ethical and legal issues at stake.

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

This action is one of the most important pieces of advice to be considered from the very first moment of a business development using location or proximity data. Its designers

10 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

11 This checklist has been built on the basis of these documents: http://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics-8f394636/

(developers, programers, coders, data scientists, engineers) 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.

It is paramount that these key workers have the fullest possible awareness of the ethical and social implications of their work, and of the fact that these can even extend to societal choices.[12] This will help the developer avoid a lot of unnecessary ethical and legal issues. Thus, implementing basic training programs that include at least the fundamentals of the Charter of Fundamental Rights, the principles exposed in Article 5 of the GDPR, the need for a legal basis for processing (including contracts between the parties), privacy by design and by default principles, etc., is an excellent measure in terms of compliance.

However, training people who have never been in touch with data protection issues might be difficult. An alternative/complementary policy is the involvement of an expert on data protection, ethical and legal issues in the development team, so as to create an interdisciplinary team. This might be done by hiring an expert for this purpose (an internal worker or an external consultant) to design the strategy and the subsequent decisions on personal data required by the development of the tools, with the close involvement of the Data Protection Officer.

Adopting adequate measures in terms of ensuring confidentiality, integrity and availability of data is also strongly recommendable (see the "Measures in support of confidentiality" subsection in the "Integrity and confidentiality" section of the "Principles" within Part II of these Guidelines).

Checklist:

ü Developers have checked that tool designers and all those who will have to deal with data have acquired an adequate knowledge of the data protection framework, or they have ensured an adequate involvement of professionals trained in data protection issues in the developing team.

ü Developers have introduced a training program on confidentiality, integrity and availability of data issues.

ü Developers have involved an expert in ethical/legal uses since the preliminary stages of the research project.

12 CNIL (2017) How can humans keep the upper hand? The ethical matters raised by algorithms and artificial intelligence. Commission Nationale de l'Informatique et des Libertés, Paris, p.55. Available at: www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_ai_gb_web.pdf (accessed 15 May 2020).

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 legitimize 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[13] 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:

- A) it is necessary for the sole purpose of providing an electronic communication service;
- C) it is strictly necessary for providing a service specifically requested by the end-user;
- D) it is necessary for the sole purpose of audience measuring, provided that such measurement is carried out by the provider of the service requested by the end-user, or by a third party, or by third parties jointly on behalf of or jointly with provider of the service requested provided that, where applicable, the conditions laid down in Articles 26 or 28 of Regulation (EU) 2016/679 are met;
- DA) it is necessary to maintain or restore the security of information society services or terminal equipment of the end-user, prevent fraud or prevent or detect technical faults for the duration necessary for that purpose; or
- E) it is necessary for a software update provided that certain circumstances apply.

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 (that is, (a) it is done exclusively for, and only for the time necessary, the purpose of establishing or maintaining a connection; or (b) the end-user has given consent; or (c) it is necessary for the purpose of statistical purposes that is limited in time and space to the extent necessary for this purpose and the data is made anonymous or erased as soon as it is no longer needed for this purpose, (d) it is necessary for providing a service requested by the end-user.) and the corresponding safeguards have been successfully implemented (See article 8.2(d) of the ePrivacy Regulation draft[14].

13 https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf
14 https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf

Box 2: re-use of personal data

One of the most controversial issues in terms of data protection is the re-use of personal data and the possibility to proceed with a lawful processing on this basis. This issue has been the subject of in-depth analysis in documents such as the EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act). In a nutshell, The EDPB and the EDPS reiterate that all processing of personal data as referred to in the Proposal shall occur in full compliance with the GDPR, and thus accompanied by appropriate data protection safeguards. This means 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). The draft of the ePrivacy Regulation by the Council includes a clause devoted to this

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.** Thus, in principle the developer might use data already available to develop the device, without collecting new data. However, the controller must ensure and carefully document that this purpose is indeed compatible with the original one (see "Data Protection and Scientific research" within Part II section "Main concepts" of these Guidelines).[15]

Other than that, personal **data may be also be re-used after being subject to a process of anonymization.** That is, previously existing personal data can be turned into non-personal data. This leaves the processing out of the scope of the GDPR. It may still fall under the ePrivacy Regulation when it comes into effect. In this case, further use of anonymous data will be permissible. In this regard, the controller must bear in mind that the technical process consisting of subjecting personal data to an anonymization technique constitutes in itself a processing of personal data. This processing can be regarded as compatible with the original purpose of the processing on the condition that the process produces truly anonymized information, in the sense defined by the former

15 EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act), 77.

Article 29 Working Party.[16] (see the "Anonymization" and "Pseduonymization" sections in the Main Concepts part of these Guidelines)

The legal basis that provides the lawful ground for the use of location/proximity data should, in any case, incorporate meaningful **safeguards**. A clear specification of purpose and explicit limitations concerning the further use of personal data should be included, as well as a clear identification of the controller(s) involved. The categories of data as well as the entities (and purposes for which the personal data may be disclosed) should also be identified. 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.

Checklist: legal basis

üDevelopers have checked that they have a legal basis that allows for a lawful data processing.

üControllers have checked the EU or national regulatory framework regarding the use of personal data.

ü If personal data are used for compatible purposes, the controller has performed the compatibility test and ensured that uses are compatible.

ü If the data are used for a purpose other than that initially sought, the tool is designed to inform the user about this use.

ü The tool is designed to allow the re-use of personal data only when it is grounded in Union or Member State law which lays down a list of clear compatible purposes for which the further processing may be lawfully authorized or constitutes a necessary and proportionate measure in a democratic society.

1.5 Special consideration of consent as a basis for processing

Consent is not always the legal basis that legitimates data processing, as previously expressed. However, these are not the most common situations. Instead, the draft of the ePrivacy Regulation[17] considers consent as the main basis for lawful data processing in the context of electronic communications. Consent, however, will only apply if some

16 Article 29 Working Party, Opinion 5/2014 on Anonymization Techniques. Adopted on 10 April 2014, p-7-8., at https://iapp.org/media/pdf/resource_center/wp216_Anonymisation-Techniques_04-2014.pdf.
17 https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf

conditions are met. 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.

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.[18] **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."[19]

Finally, yet importantly, the former Article 29 Working Party recommended that providers of location applications or services should seek to renew individual consent (even where there is no change in the nature of processing) after an appropriate period of time. For instance, it would not be valid to continue to process location data where an individual had not actively used the service within the previous 12 months. Even where a person has used the service they should be reminded at least once a year (or more often where the nature of the processing warrants it) of the nature of the processing of their personal data. 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.

Box 3: Broad consent and additional safeguards

The German DPA recently listed some additional safeguards to be implemented in the case of broad consent.[20] These are:

18 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

19 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

20 DSK, Beschluss der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und

1. Safeguards to ensure transparency:

- Utilization of usage regulations or research plans that illustrate the planned working methods and questions that are to be the subject of the research project.
- Assessment and documentation of the question why in this particular research project a more detailed specification of the research purposes is not possible.
- Set up web presences to inform study participants about ongoing and future studies.

2. Safeguards to build trust:

- Positive vote of an ethics committee before use of data for further research purposes.
- Assessment of whether it is possible to work with a dynamic consent or whether a data subject can object before the data might be used for new research questions.

3. Security safeguards:

- No data transfers to third countries with a lower level of data protection.
- Additional measures regarding data minimization, encryption, anonymization, or pseudonymization.
- Implementation of specific policies to limit access to personal data.

Box 4: Example of best practice for providers of geolocation applications according to the former Article 29 Working Party-[21]:

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'. Users can continuously withdraw their consent, without having to exit the application. Users are also able to easily and permanently delete any location data stored on the device.

Checklist: consent

☐ The controllers are able to demonstrate that, after balancing the circumstances of the processing, they have concluded that consent is the most appropriate legal basis for processing.

---

der Länder zu Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung" im Erwägungsgrund 33 der DS-GVO 3. April 2019, at: www.datenschutzkonferenz-online.de/media/dskb/20190405_auslegung_bestimmte_bereiche_wiss_forschung.pdf (accessed 20 May 2020). The English translation comes from a nice summary of the measures that can be consulted here: www.technologylawdispatch.com/2019/04/privacy-data-protection/german-dpas-publish-resolution-on-concept-of-broad-consent-and-the-interpretation-of-certain-areas-of-scientific-research/

21 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. 15, at: https://www.apda.ad/sites/default/files/2018-10/wp185_en.pdf

- The controllers request the consent of the data subjects in a free, specific, informed and unequivocal manner, according to article 7 GDPR.
- The controllers have informed the data subjects about their right to withdraw consent at any time.
- Broad consent used for processing of special categories of data is compatible with national regulations.
- Where broad consent is used, the controller is particularly aware that 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.
- Controllers have a direct relationship with the subject who provides the data.
- The power imbalance between controllers and data subjects does not impede free consent. This is particularly important in certain contexts such as the labor framework.
- The controllers ask people to actively opt in.
- The controllers do not use pre-ticked boxes or any other type of default consent.
- The controllers use clear, plain language that is easy to understand.
- The controllers specify why they want the data, what they are going to do with it and for how long data will be processed.
- The controllers give separate distinct ('granular') options to consent separately to different purposes and types of processing.
- The controllers link which pieces of data of categories thereof will be processed for each purpose.
- The controllers have informed the data subjects about their right to withdraw consent at any time and how to do so.
- The controllers ensure that individuals can refuse to consent without detriment to their access to the service.
- The controllers avoid making consent a precondition of a service.

1.6 Be aware of the range of protection of the data involved in the processing

Developers should always keep in mind that the devices produced should minimize the intrusion in people's lives. Indeed, they should always remember that data are protected as follows:

• As "personal data", i.e. any information relating to an identified or an identifiable natural person (Article 4(1) of the GDPR), it is protected under the GDPR. Health data benefit from additional protection (Article 9 of the GDPR).

• As “location data”, i.e. data processed in an electronic communications network or by an electronic communication service, indicating the geographic position of the terminal equipment of the user, it will probably be protected under the ePrivacy Regulation[22]

• Additionally, the future ePrivacy Regulation will protect information emitted by users’ terminal equipment.

This might change in the next years, but at the present moment this provides a good summary of the situation that currently exists.[23]

2 Understand Impacts

2.1 Description

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. That understanding should be used to make informed and proportionate decisions, and to minimize negative impacts.

2.2 General ethical measures to be implemented

To meet this ethical requirement, two perspectives must be kept in mind. On the one hand, the need to consider the impact of data processing in terms of data protection as such. On the other hand, the impact that such processing may have on the environment, society, or human relations. With regard to the latter, it is essential to consider the recommendations made by the High-Level Expert Group on AI. Although they were developed in the context of AI, they are perfectly applicable to the use of geospatial data.[24] The recommendations of the Group were the following:

- Devices and systems using geospatial data promise to help tackle some of our most pressing societal concerns, but this must be achieved in the most environmentally friendly way possible. The system’s development, deployment and use processes, as well as its entire supply chain, should be assessed in this regard. This includes measures such as a critical examination of its resource use and energy consumption, opting for less environmentally harmful choices where available. Measures securing the environmental friendliness of devices and systems’ entire supply chain have been implemented.
- Ubiquitous exposure to location and tracing devices and systems in all areas of our lives - be it education, work, care or entertainment - may alter our conception of

22 https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf

23 COMMUNICATION FROM THE COMMISSION, Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection, Brussels, 16.4.2020 C(2020) 2523 final, p.6, at: https://ec.europa.eu/info/sites/default/files/5_en_act_part1_v3.pdf

24 High-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

social agency, or impact our social relationships and attachment. While these devices and systems can be used to enhance social skills, they can equally contribute to their deterioration. This could also affect people's physical and mental wellbeing. The effects of these systems must therefore be carefully monitored and considered.

- Beyond assessing the impact of a device or system's development, deployment and use on individuals, this impact should also be assessed from a societal perspective, taking into account its effect on institutions, democracy and society at large. Their implementation should always be given careful consideration, particularly in situations relating to restrictions of individual rights and freedoms.

Checklist:

ü The device does not include tools that allow for a use of the data in a way that is hardly compatible with the preservation of relevant privacy spaces.

ü The tool is mindful of principles of environmental sustainability, both regarding the system itself and the supply chain to which it connects (when relevant).

ü The default configuration of the device does not allow disproportionate uses of data for surveillance purposes.

ü Controllers have made sure that the tool takes the welfare of all stakeholders into account and general reduction of their well-being is not at all foreseeable.

ü The device is not designed for purposes that are hardly compatible with the EU's own ethical principles.

2.3 Legal issues: performing DPIAs

A DPIA is a process in which the data controller, before starting a data-processing procedure with **high risk** to the fundamental rights and freedoms of data subjects, assesses the impact of the envisaged processing operations on the protection of personal data (Article 35(1) of the GDPR). If controllers are dealing with a high risk, then a DPIA should be conducted following Article 35(7) of the GDPR. 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 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."[25].

It is important to highlight that a DPIA should be performed whenever the controller considers that a concrete processing involves a high risk. Most Data Protection Agencies are imposing DPIAs when processing involves systematic location of the data subjects.[26] Therefore, it might perfectly happen that a developer has to perform several DPIAs during the production process. Indeed, we consider that these assessments

25 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

26 See, for instance, the position adopted by the Spanish Data Protection Agency in: https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf

should be revisited and updated when possible and especially when the controller is to define the policies regarding data preservation and elimination.

In certain situations, if the result of the DPIA is that the intended processing activity has a high risk of causing harm to the fundamental rights and freedoms of data subjects, **the controller should request the opinion of the national supervisory authority**, as prescribed by Article 36 GDPR. Some Member States have issued lists that contain examples of data-processing activities that would trigger this mandatory DPIA; among those examples, we can identify situations that match with techniques processing location and proximity data. This is especially true if they incorporate AI techniques. Supervisory authorities can require the adoption of certain measures to mitigate the risk, if possible, or forbidding the use of the device or system if it is not possible.

Checklist: is a DPIA necessary?

ü The controller determined the jurisdictions where data-processing activities will take place.

ü The controller checked if those jurisdictions have enacted lists indicating the processing that requires a mandatory DPIA and has seen if the intended data processing is covered by those provisions.

ü If the controller is unsure of the necessity of carrying out a DPIA, they must consult with the DPO or, in lieu of, the legal department of the controller.

ü If necessary, the controller carried out a DPIA.

ü If necessary, the controller filed a prior consultation with the appropriate supervisory authority.

ü If changes were suggested, the controller followed the advice of the supervisory authority.

3 Do not harm

3.1 Description

Physical proximity amplifies the potential harms that can befall people, flora and fauna. Data users should ensure that the individual or collective location data pertaining to all species should not be used to discriminate, exploit or harm. Rights established in the physical world must be protected in digital contexts and interactions.

3.2 Ensure security

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. For instance, in Qatar a security flaw in their national contact tracing app exposed sensitive personal details of more than one million people in May 2020.[27]

These risks must be mitigated through the implementation of technical and/or organizational security controls. Technical measures include -but are not limited to- the use of state-of-the-art cryptographic techniques, able to secure the data stored in servers and applications, exchanges between applications and the remote server. Mutual authentication between the application and the server must also be performed. If the application reports users, this must be subject to proper authorization, for example through a single-use code tied to a pseudonymous identity of the user. If confirmation cannot be obtained in a secure manner, no data processing should take place that presumes the validity of the user's status.[28]

Organizational measures should ensure an adequate implementation of well-established security principles such as 'need-to-know' (i.e. allowing access to information or knowledge if required to perform an assigned task), the creation of roles with different permissions to access data, or 'layered security' (i.e. a defensive security strategy featuring multiple layers that are designed to slow down a security attack). It is important to know that the overall level of security of a solution is only as strong as the weakest link. Thus, "every component of a solution, whether central systems or remote devices, should be secured adequately".[29] Indeed, many times this weakest link may be caused by human error. Consider, for instance, the case of weak passwords being subject to phishing attacks or the loss of a device that stores data. For this reason, security measures shall include training and awareness programs for the personnel involved.

Before deploying the tool in the real world, it is advisable to perform security tests (random data testing, also called "fuzzing", vulnerability scanning, etc.). These will serve to check that the product continues to function acceptably when its normal use is abandoned and that it does not present any vulnerability that could allow third parties to compromise its security. Both types of tests are important for the proper functioning of the tool. For example, a continuous integration system should be set up to run tests automatically after every change in the source code.

Box 5: Verifying and checking identifiers and participants in the tool

When an application creates or uses a unique identifier, steps need to be taken to ensure that the identifier is linked to the legitimate user of the application and keeps this information up to date. Each party using identifiers is responsible for taking steps to:

27 https://www.amnesty.org/en/latest/news/2020/05/qatar-covid19-contact-tracing-app-security-flaw/

28 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

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

- implement measures devoted to guarantee that any unique identifier applies to only a single unique user. If this is too complex, introduce measures aimed at preventing or mitigating undesirable consequences and inform data subjects about it.

- ensure that unique identifiers are kept up to date and are retained only for as long as necessary to fulfill the purpose of the application and the reasons notified to users.

- prevent a unique identifier from being associated with another user, unless a justified PROJECT need requires it.

The use of a persistent identifier (such as an IMEI number or advertising ID) generally creates more risk than the use of a random or rotating identifier.

In addition, the management of end-user/participant profiles should be thought through prior to development. Authenticate users where possible using risk-appropriate authentication methods. Where assertion of a real-world identity is an important component of a service, stronger authentication, such as two-factor authentication using a cell phone and UICC, should be applied.

Checklist:[30]

 The controller assessed potential forms of attacks to which the tool could be vulnerable, introduced mitigation measures and documented them.

 The controller considered different types and natures of vulnerabilities, such as data pollution, physical infrastructure and cyber-attacks.

 The controller put measures or systems in place to ensure the integrity and resilience of the system against potential attacks.

 The controller verified how the system behaves in unexpected situations and environments.

 The controller considers to what degree the system could be dual-use. If so, the controller took suitable preventative measures against this.

 The controller ensured 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).

üThe data sent to the central server is transmitted over a secure channel. The use of notification services provided by OS platform providers is carefully assessed, and does not lead to disclosing any data to third parties.

üRequests are not vulnerable to tampering by a malicious user.

üState-of-the-art cryptographic techniques are implemented to secure exchanges

30 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.

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.

üThe central server does not keep network connection identifiers (e.g., IP addresses) of any users.

üIn order to avoid impersonation or the creation of fake users, the server authenticates the application.

ü The application authenticates the central server.

ü The server functionalities are protected from replay attacks.

ü The information transmitted by the central server is signed in order to authenticate its origin and integrity.

ü Access to all data stored in the central server and not publicly available is restricted to authorized persons only.

ü 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.

3.3 Enable mechanisms aimed at notifying data breaches as soon as possible

Data breaches involve a serious danger to the rights and freedoms of the affected data subjects. Controllers are expected to notify them to supervisory authorities and data subjects as soon as possible. Furthermore, if the data breach were 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. Contacting all users might be impossible in practice. Therefore, a public communication – if effective – can be considered sufficient. All communication towards data subjects should be transparent and in clear and plain language.[31]

Checklist:

üControllers have implemented adequate policies to notify data breaches as soon as possible and all participants in the development process are well aware of them.

ü Templates about the information to be included in the notifications have been designed.

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

ü Communication policies and tools, aimed at facilitating communication with the data subjects if a data breach happens, have been created.

4 Protect the vulnerable

4.1 Description

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.

4.2 Ethical and legal issues

One of the fundamental issues in the development of an ICT technology is that it must avoid reaching exclusionary results for a part of the population. This is especially true when we are talking about vulnerable populations, such as people with disabilities, people with low purchasing power or people with difficulties interacting with electronic devices. In the case of devices designed for traceability or location purposes, this implies, among other things:

- 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[32].

Checklist:

ü The controllers have additional checks in place for their profiling/automated decision-making systems to protect any vulnerable groups (including children).

ü Information and privacy policies should be accessible through different means (from voice, images, video or in an easy-to-understand language). This is especially important if the location device is targeted at a specific users group.

ü Consent is adapted to vulnerable populations and children's needs.

ü Use options facilitating the use of the device by vulnerable populations have been considered.

ü If the controller is willing to use the data for a purpose other than that initially requested, the tool is designed to ask vulnerable users for permission in a way that is compatible with their personal conditions.

5 Address bias

5.1 Description

Bias in the collection, use, and combination of location datasets can either remove affected groups from mapping that conveys rights or services, or amplify negative impacts of inclusion in a dataset. Therefore, care should be taken to understand bias in the datasets and avoid discriminatory outcomes.

5.2 Legal issues

Biases are one of the main issues involved in the use of ICT devices and systems, an issue that contravenes the fairness principle (see "Lawfulness, fairness and transparency principle" within Part II section "Principles" of these Guidelines). 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 (see Part III of these Guidelines devoted to AI systems). If this is the case, developers should pay special attention to ensure that they do not introduce biases in the functioning of the

32 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/.

location device or system. For this purpose, they must adopt a number of measures, as described in Part III of these Guidelines devoted to AI systems

- 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 should be kept in mind that, depending on the origin of the aggregated data, 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.[33] This may create problems of inequity, as some social classes (especially those who do not use the devices or suffer from a lack of the specific capabilities that make it possible to obtain the data) are underrepresented in the analysis and subsequent decision-making.[34] This could leave out entire populations, and misrepresent others, and lead to a deployment of resources that is not only biased and unjust — tilted toward the richest neighborhoods, for example — but ineffective from a public policy standpoint.[35] Of course, misrepresentation can also introduce biases in public order and police interventions, producing prejudicial results to low-income communities, for instance. 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.

Checklist: [36]
ü The controller has put in place ways to measure whether the tool is making an unacceptable number of biased predictions.
ü The controller has put in place a series of steps to increase the tool's accuracy.
ü The controller has put in place measures to assess whether there is a need for additional data, for example to eliminate biases.
ü The controller has verified what harm would be caused if the tool makes biased predictions.

6 Minimize intrusion

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

34 Frith J, Saker M. It Is All About Location: Smartphones and Tracking the Spread of COVID-19. Social Media + Society. July 2020. doi:10.1177/2056305120948257

35 Jay Stanley and Jennifer Stisa Granick The Limits of Location Tracking in an Epidemic, ACLU Whitepaper, April 8, 2020, at: https://www.aclu.org/report/aclu-white-paper-limits-location-tracking-epidemic?redirect=aclu-white-paper-limits-location-tracking-epidemic

36 This checklist has been adapted from the one elaborated by the 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 (accessed 20 May 2020).

6.1 Description

Given the intimate and personal nature of location data, users should avoid unnecessary and intrusive examination of people's lives, and the places they live in, that could undermine human dignity.

6.2 Legal issues: using anonymized data instead of personal data

Developers must keep in mind that data controllers in charge of their devices or systems will have to be able to demonstrate that the processing is **necessary for the objective being pursued** and is **less intrusive than other options** for achieving the same goal; not that it is a necessary part of their chosen methods.[37] If there are realistic, less intrusive alternatives, the processing of personal data is not deemed necessary.[38] Thus, developers should provide devices and systems with options that allow them minimize the use of data to what is strictly needed (see "Minimization principle" in "Main Concepts", Part II of these Guidelines). The concept of necessity is, however, complex, and has an independent meaning in European Union law.[39] In general, it requires that processing is a targeted and proportionate way of achieving a specific purpose. Although it does not have to be interpreted in such a strict way as to mean that only absolutely essential data are processed, it is not enough to argue that processing is necessary because controllers have chosen to operate their business in a particular way. For instance, the tool must not allow users to be directly identified when using the application.

The data minimization principle stipulates that personal data should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".[40] This ethical principle means that, when it comes to using location or proximity data, preference should always be given to the processing of anonymized data rather than personal data[41] (see the "Lawfulness and fairness" and "Anonymization" sections in Part II in these Guidelines). Indeed, if personal data can be substituted with non-personal data without affecting the purposes of the processing, the use of anonymized data should be clearly preferred, according to the GDPR.

---

37 EDPS (2017) Necessity toolkit: assessing the necessity of measures that limit the fundamental right to the protection of personal data, p.5. European Data Protection Supervisor, Brussels. Available at: https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en (accessed 15 May 2020); ICO (no date) Lawful basis for processing. 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/lawful-basis-for-processing/ (accessed 15 May 2020).

38 See CJEU, Joined Cases C-92/09 and C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen, 9. November 2010.

39 See CJEU, Case C-524/06, Heinz Huber v Bundesrepublik Deutschland, 18 December 2008, para. 52.

40 Article 5(1)(c) of the GDPR.

41 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

Checklist[42]**:**

ü The tool is based on an architecture relying as much as possible on users' devices.

ü Requests made by the applications to the central server do not reveal unnecessary information for the purposes of the service to the system.

ü 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.

ü 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.

6.3 If the use of anonymous data is not possible, use the minimal amount of personal data and pseudonymize them

If anonymization were not possible, controllers should at least try to work with pseudonymized data (see "Pseudonymization" subsection in "Main Concepts" in Part II of these Guidelines). Ultimately, each controller needs to define which personal data are actually needed (and which are not) for the purpose of the processing, including the relevant data retention periods. Indeed, controllers must keep in mind that the necessity of processing must be proven before using any legal basis from Article 6 or 9(2) of the GDPR. Although consent may seem to be the only legal ground which does not require necessity, it actually does involve necessity to a certain degree, as valid consent for the purposes of the GDPR is given for a specific purpose, and the processing must be necessary in relation to that purpose, according to Article 5(1)(c). In other words, data minimization, purpose limitation and lawfulness principles require controllers to ensure that the purposes sought by the device or system cannot be done without using less personal location or proximity data, or those categories of data with a lesser degree of detail.

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

42 This checklist has 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

of containing the spread of the virus, and sufficient to limit the risk of identification and of physical tracking of individuals."[43]

In general, for the purpose of offering geolocation services, 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.[44]

Box 6: Contact tracing app in pandemics

This type of application provides us with some good examples of data policies that respect the data protection regulations. Some useful tips developed by the ICO are:

- the exchange of information between devices does not include personal data such as account information or usernames;
- matching processes take place on-device and are not undertaken by the app host or with the involvement of any other third party; and
- the information required for the core functionality of contact tracing apps built using CTF does not use location data, either in the exchange between devices, the upload to the app host or subsequent notifications to other users from the app host.

Checklist[45]:

ü According to the data minimization principle, the application does not collect data other than that which is strictly necessary for its purposes.

ü When possible for the purpose of the processing, controllers will set a preference for the use anonymous data. If personal data must be used, pseudonymous data will prevail over direct personal data.

ü 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.

ü Requests made by the applications to the central server do not reveal unnecessary information for the purposes of the service to the system.

ü 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.

43 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

44 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

45 This checklist has 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

ü The use of the application does not allow users to learn anything about other users, if it is not strictly necessary.

ü The central server does not maintain nor circulate a list of the pseudonymous identifiers of users

6.4 Legal issues: Use only the type of data that is strictly necessary

In general, devices should not collide with a data subject's position as the holder of the right to privacy. This means that, in general, users must be protected against being unnecessarily deprived of their privacy. Thus, a user should not have to take action to prevent tracking, as the device should provide this by default. If the tool can function without direct identification of individuals, appropriate measures should be put in place to prevent re-identification. Moreover, the collected information should reside on the terminal equipment of the user and only the relevant information should be collected when absolutely necessary.[46] In general, data should only be processed if it is strictly necessary.

Furthermore, 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. For instance, no identifiers should be included in the server logs. Similarly, information on the proximity between users of the application should be obtainable without locating them. This kind of application does not need, and thus should not involve, the use of location data (directly or by combination of data), but only proximity data. Instead, if you wish to know the concrete geolocation of an individual, you should not gain access to proximity data by combining different datasets. Thus, 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. For instance, if some features of the tool may enhance the user experience, but are not strictly necessary for the tool to function properly, e.g. geolocation to simplify a geographic search, the participant should be able to choose whether or not to use geolocation to simplify the geographic search. In these cases, more invasive tracking must be deactivated by default, leaving it to the user's decision to opt-in.

Box 7. The issue of the exactitudine

46 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, p. 7. At: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

In principle, personal data must be accurate. However, in the case of location or proximity data, excessive accuracy may threaten the privacy of the data subject or third parties. Therefore, the developer of the tool should attempt to reduce the precision or accuracy with respect to the location data to the minimum level necessary to ensure that it fulfils the purpose for which it was designed. Location data can be very precise (such as a device being located on a specific street corner) or more imprecise (postal codes, quadrants, a city or even a country). The more precise and accurate the data, the more revealing it tends to be, and the greater the risk of re-identification.

It is particularly important to avoid, as much as possible, known locations that are linked to a person's identity, such as that person's home or workplace. The reason is that these data often contribute to the identification of the subject.

In addition, some locations are especially sensitive because of what they may reveal about the owner of the device, such as hospitals, schools, nightclubs, abortion clinics, dispensaries, or political organizations and events. While these locations do not always increase the risks of re-identification, they do carry greater risks of abuse or unexpected uses. Therefore, it is ideal to avoid accuracy in the use of data referring to these locations as much as possible.

Checklist[47]**:**

ü The tool does not collect data in addition to those that are 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.

ü If the tool is aimed at tracing contact purposes, it does not allow users to identify other users' movements

ü In general, no data leaves the users' equipment if it is not strictly necessary.

ü The design of the devices or the tool takes into account privacy by design principles and aims at not collecting more data than necessary.

ü If the design of the device or the tools allow for several options regarding the collection and further processing of data, the most protective one will be set by default.

7 Minimize data

47 This checklist has 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

7.1 Description

Most business and mission applications do not require the most invasive scale of location tracking available in order to provide the intended level of service. Users should comply with practices that adhere to the data minimization principle of using only the necessary personal data that is adequate, relevant and limited to the objective, including abstracting location data to the least invasive scale feasible for the application.

7.2 Legal issues: Purpose limitation

In order to minimize intrusion in the data subject's life, it is essential that the device is designed in a way that serves well to preserve the purpose limitation principle. Whenever processing location or proximity data, recipients must only use the information for the task for which it was provided to them. They must keep in mind that data that was collected for specified "initial" purposes shall only be processed for these initial purposes, or for compatible purposes. Further processing of data is allowed under certain circumstances under the GDPR. First, when the controller seeks another lawful basis, and subject to compliance with all other legal requirements, such as transparent information and granting users' rights. Second, for some pre-authorized purposes, such as scientific research or archiving. Third, when the further processing has compatible purposes. For the general case, the GDPR gives criteria for how to determine the compatibility of purposes, which includes the link between the original and further processing, the nature of the data, the expectations of the data subject or the existence of appropriate safeguards (see Art. 6(4) and see "Purpose limitation" subsection in the "Principles" section, within Part II of these Guidelines).

If you 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 behavioral 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.** For example, if a company originally stated it would not share personal data with any third party, but now wishes to share it, this processing will most likely not pass a compatibility test. Therefore, considering that the best lawful basis in this case is users' consent, the controller must seek the active prior consent of each customer for

this further processing activity. A lack of response (or other kind of opt-out scenario) does not suffice. 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.**[48] **This can hardly be considered a compulsory requirement for the controller, but it is certainly a good practice that must be recommended.**

Checklist[49]**:**

 The controllers have clearly identified their purpose or purposes for processing, which must be "specific".

 The controllers have documented those purposes.

 The controllers 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.

ü The tool cannot be inadvertently diverted from its primary use.

ü The tool does not use walls to collect unnecessary data

ü If the controller initiates a further processing of personal data, a compatibility test has been carried out and documented in order to comply with the accountability principle. This test must take into account, at least, the factors listed in Art. 6(4) of the GDPR.

ü If the controller wishes 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, the controller must find the most adequate lawful basis.

ü 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.

48 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

49 This checklist 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).

ü 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.

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

Devices should be programed 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 (see "Storage limitation" in "Principles", Part II of these Guidelines). Of course, this will probably depend on the goal required by the application. Storage is only acceptable if it is necessary to reach the aim of the tool. For example, if an app is intended to keep track of someone suffering from Alzheimer's disease, in case they wander due to the effects of the disease, data will probably have to be deleted very often. If we are thinking about a device aimed at helping users know if they have been close to someone suffering from an infectious disease, data will have to be kept for days or weeks.

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 anonymized while taking into account that true anonymization is increasingly hard to realize 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)."[50]

Checklist:

ü Contact history or location data stored on the central server is deleted once they are no longer needed for the purposes of the processing.

ü The procedure for data erasure is adequately designed and the controller and the users are well aware of it.

ü 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).

ü Data in server logs are minimized and comply with data protection requirements

ü If there is a central server and it needs to store data identifiers, these must be deleted once they are distributed to the other applications unless a legal/technical reason recommends otherwise.

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

8 Protect Privacy

8.1 Description

Tracking the movement of individuals through space and time gives insights into the most intimate aspects of their lives. In the rare cases when aggregated and anonymized location data will not meet the specific business or mission need, location data that identifies individuals should be protected and only used on the basis of a legal reason that allows the data processing.

8.2 Introduce an adequate privacy policy

The developer should always make sure that the device or system incorporates an adequate privacy notice, according to articles 12 and 13 of the GDPR and the requirements introduced by the ePrivacy Regulation and the national legal framework. 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[51].

The information included must be explained in a comprehensible language, which can be understood by people who know almost nothing about ICT systems. This notice must include, at least, all the topics listed in arts. 13-14 of the GDPR, namely: information related to the (1) purpose of processing, (2) what personal data is collected, (3) how the collected data is used, (4) with whom the personal location data is shared, (5) how data subjects can withdraw consent, and access or rectify their personal location data, (6) information about rights linked to automated decision-making, (7) the contact information of the corresponding DPO, in case they need to be contacted, (8) information about the retention periods, etc.[52] Moreover, it is important to keep data subjects informed of any changes to the processing of their personal data, which should be reflected in the privacy notice. Furthermore, the system should be designed in a way that makes the data subject aware of the changes (through messages, icons, alerts, etc.).

In addition to the compulsory information requirements mentioned, 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, of course, but they are highly recommended:[53]

- What are the concrete uses that will be given to the data collected

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

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

53 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.

- 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.
- 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. For example, you can opt for iconography to comply with the duty of information of the data controller, videos, storytelling, or even simple formatting like the use of charts. It is 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.

Checklist:[54]

54 This checklist has been built on the basis of these documents: EDPB, Guidelines 04/2020 on the use of

 The controllers regularly review their processing and, where necessary, update their documentation and privacy information for individuals.

ü Users are informed of all personal data that will be collected. These data are collected only if a legal basis for processing applies

ü The controllers explain how people can access details of the information that is used for the services offered by the tool.

8.3 Protect the users' rights

Data subjects can invoke numerous rights related to their data, which are described in full detail in the corresponding section (see "Data Subject Rights" in Part II of these Guidelines). In general, developers should do their best to design the device or tool in a way that will respect users' rights and also help users to exercise them. This can be done, for instance, by implementing a simple way to access data or by developing technical measures to aid portability rights. However, restrictions on the rights and obligations provided for in the Proposal for an ePrivacy Regulation and/or in the GDPR are possible, when they constitute a necessary, appropriate and proportionate measure within a democratic society for certain objectives.[55] In general, devices using location and proximity 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.

Some concrete tips to facilitate the implementation of rights		
Rights	**Issue**	**Tip**
Right of access	Data is often stored in a highly diversified form, making it difficult to access, especially for an unskilled data subject.	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	On some occasions, the data	Allow direct modification of data in

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).

55 See Article 15 of the ePrivacy Directive and Article 23 GDPR.

rectification	collected by the device will not be accurate. Data subjects must be able to rectify such data.	the user's account (if applicable and/or possible). Provide advice on why it might not be advisable under some circumstances.
Right to erasure	Data subjects have the right to have their personal data deleted. However, this right may be limited under certain specific circumstances. Furthermore, users should be aware of the technical implications of a general deletion of the data. Thus, controllers must allow data subjects to erase only those data to which the right applies and introduce some information prior to allowing them proceed.	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	It is often in the interest of data subjects that data of a particular type is not processed. The tool should be adapted to their preferences if the conditions of article 18 of the GDPR apply.	Provide a functionality that allows the data subject to object to the processing of specific personal data. When data subjects exercise their 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	Users should be able to receive the personal data they have provided to the controller from the device without advanced technical skills. They also have the right to have their data transferred to another controller (that is, provider of another service). Note: this does not include data gathered through other means like external sources or through analytical or inference processes.	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. For example, "regardless of whether the end-user has prevented access to the terminal equipment's Global Navigation Satellite Systems (GNSS) capabilities or other types of terminal equipment based location data through the terminal equipment settings, when a call is made to emergency services, such settings may not prevent access to GNSS such location data to determine and provide the caller calling end-user's location to emergency services an organization dealing with emergency communications, including public safety answering points, for the purpose of responding to such call" (ePrivacy Regulation, article 13.3).[56]

Checklist[57]**:**

ü Users are able to exercise their rights via the application.

ü If the tool has been designed to work on proximity data, it cannot be used to draw conclusions on the location of the users based on their interaction and/or any other means.

ü 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.

ü If data are used for compatible purposes, the controller has performed the compatibility test.

ü If the controller wishes to use the data for a purpose other than that initially sought, the tool is designed to ask users for permission.

9 Prevent identification of individuals

9.1 Description

As an individual's mobile location data is situated within more and more geospatial context data, its anonymity erodes. Therefore, measures should be put in place to prevent subsequent use of the data resulting in identification of individuals or their location.

56 https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf

57 This checklist 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

9.2 Legal issues: using anonymized data instead of personal data

See section "Legal issues: using anonymized data instead of personal data" in this Part IV.

9.3 Legal issues: If the use of anonymous data is not possible, use the minimal amount of personal data and pseudonymize them

See section 7 "If the use of anonymous data is not possible, use the minimal amount of personal data and pseudonymize them" in this Part IV.

10 Provide accountability

10.1 Description

People who are represented in location data collected, combined and, used by organizations should be able to interrogate how it is collected and used in relation to them and their interests, and appeal those uses proportionate to levels of detail and potential for harms.

10.2 Legal issues

According to Article 5(2) of the GDPR, the controller shall be responsible for, and must be able to demonstrate, compliance with all principles of the GDPR mentioned at Article 5(1). This includes the principle of accountability (see "Accountability principle" within Part II section "Principles" of these Guidelines).

The accountability principle in the GDPR is risk-based: the higher the risk of data processing to the fundamental rights and freedoms of data subjects, the greater the measures needed to mitigate those risks.[58] The accountability principle is based on several compliance duties for data controllers, including: transparency duties (Articles 12-14); guaranteeing the exercise of data protection rights (Articles 15-22); keeping records of the data-processing operations (Article 30); notifying eventual data breaches to a national supervisory authority (Articles 33) and to the data subjects (Article 34); and, in cases of higher risk, hiring a DPO and carrying out a DPIA (Article 35).

Checklist[59]:

58 See Articles 24, 25 and 32 of the GDPR, which require controllers to take into account the "risks of varying likelihood and severity for the rights and freedoms of natural persons" when adopting specific data protection measures.

59 This checklist 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

ü The controller has documented how undesirable effects of the system or tool are detected, stopped and prevented from reoccurring.

ü The controller has documented all the organization's measures, and the safeguards implemented, to ensure compliance with the data protection regulation.

ü If data are used for compatible purposes, the controller has adequately documented the performance of the compatibility test.

ü The controller has documented all DPIAs performed, the activities performed by the corresponding DPO and his or her interactions with the corresponding DPAs (if applicable)

10.3 Ensure transparency

Transparency is key to accountability. One can only guarantee accountability if information about the functioning of the system or device is available in a transparent and proper way. The tool must be designed in such a way that transparency and user control can become a reality [60].

Furthermore, as the EDPB stated, "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. The application's source code should be made publicly available for the widest possible scrutiny".[61] However, this might collide with intellectual property considerations. In any case, developers 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. It is also advisable to establish an appropriate information strategy. It is advisable in any case that the information is written in characters that are not excessively small so that the participant can visualize the information easily via the screen of a smartphone. We must try to prevent the participant from starting to use the tool without having read and understood what will be done with their data. Finally, it is recommended to opt for legal design options that can make the privacy policy more visual and easier to understand. (See section "Transparency" in "Lawfulness, fairness and transparency principle" within Part II section "Principles" of these Guidelines).

Checklist[62]:

60 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

61 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

62 This checklist has been built on the basis of the EDPB, Guidelines 04/2020 on the use of location data

ü The source code of the application and of its backend is 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.

10.4 Risk assessment and DPIAs

See "Integrity and confidentiality" subsection in the "Principles" section of Part II of these Guidelinesof this document.

10.5 Processor due diligence

The accountability principle (see "Accountability principle" within Part II section "Principles" of these Guidelines) is also present when a controller chooses to require the services of a processor. In this regard, Article 28(1) of the GDPR[63] requires controllers to perform certain due diligence actions, prior to providing processors with access to personal data for the performance of data-processing activities. As with other provisions of the GPDR, it is not stated which specific actions a controller should carry out when evaluating processors. The only criteria provided by the GDPR is that **controllers should judge processors on the basis of their ability to demonstrate that they can carry out processing activities in compliance with the GDPR.**

Controllers should always keep in mind that the development of localization tools often involves the use of different data sets. Registries should ensure traceability of processing, information on possible reuse of data and the use of data belonging to different datasets in the same, or different, lifecycle stages.

If the controllers are conducting a development that needs to count on a third party for certain processing activities, they 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 out such due diligence?

For the first question, the GPDR indicates that if controllers intend to remain compliant with the GDPR, they can only retain a processor that is able to demonstrate its compliance with the GDPR. Therefore, controllers need to request information to assess this. In other words, the GDPR expects controllers to actively ask their potential processor about this; it is not sufficient to rely on a representations and warranties clause in the data-processing agreement (see "Integrity and confidentiality" within "Principles" in Part II of these Guidelines). As a way to ensure this, controllers may send questionnaires to all processors or require processors to prove that they have passed an external auditing process. In addition to this, controllers may add an auditing

---

and contact tracing tools in the context of the COVID-19 outbreak Adopted on 21 April 2020

63 'Article 28 Processor 1. "Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject."

contractual clause by which the controller itself can carry out on an audit on a processor in case further evidence is needed.

As for how controllers should carry out this due diligence, again the GDPR does not provide concrete issues to analyze. Nevertheless, certain national supervisory authorities have proposed topics to consider, such as whether the processor follows industry standards, to request the provision of both legal and technical information about how the processor processes personal data, if they adhere to a code of conduct, or if they have gone through a certification scheme.[64]

Besides these general considerations, and depending on how the processing requested by this third party integrates within the framework of the developed tool, further questions should be asked. In this regard, **any question that the controllers would ask themselves when developing the tool should be asked of the processor.** We defer to the issues posed in the Checklist included in the box below for further guidance.

Checklist: processor due diligence

ü If there is processing involving international transfer of data, the controllers acquired information regarding where the data-processing activities will take place, and (1) carried out the case law review suggested in the point below; and (2) assessed if the jurisdictions, in the case of non-EU countries, are considered adequate by the EU Commission.

ü The controllers reviewed case law from the national supervisory authorities where the processor operates to check for potential sanctions.

ü The controllers required proof of adherence to a code of conduct or certification (this is not strictly necessary but may be considered as good practice).

ü The controllers required proof of relevant ISO certification (this is not strictly necessary but may be considered as good practice).

ü If there is a processor involved, controllers required a copy of records of processing activities.

ü The controllers enquired about the development process of the tool, in particular which kind of data were used for training the tool and the data that it needs to operate and deliver a useful result.

64 ICO (no date) Guide to the General Data Protection Regulation (GDPR), What responsibilities and liabilities do controllers have when using a processor? 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/contracts-and-liabilities-between-controllers-and-processors-multi/responsibilities-and-liabilities-for-controllers-using-a-processor/ (accessed 20 May 2020).

10.6 Data protection Officers (DPOs)

DPOs play a crucial role when designing and implementing data-processing activities in a GDPR-compliant manner. They are another safeguard that the GDPR mandates on certain occasions and, in general, it is recommended to appoint such a figure. The Article 29 Working Party considers that this "is a cornerstone of accountability and that appointing a DPO can facilitate compliance".[65]

Article 37(1) of the GDPR[66] outlines when controllers and processors should appoint a DPO. In the case of location and proximity devices and systems**, the appointment of a DPO will most likely be necessary, as most of them process personal data in such a way that may require a regular monitoring of data subjects at a large scale, or may be carried out by public authorities**.

It would be useful if each Member States' regulations on the need for DPOs expanded the list of activities that demand the appointment of a DPO or, at least, provided clear examples that could help to interpret which data-processing activities carried out by controllers and processors demand such an appointment.

If a DPO has to be appointed, for any of the reasons mentioned above, it is necessary to have their participation from the outset of the project, such as the drafting of a DPIA (required by Article 39(1)(c)) as well as any other issue related to data protection within the entity (as prescribed by Article 39(1)(a)). This may include reviewing a potential processor, as described in the previous item.

Checklist: DPOs

ü The controllers checked if the institution has already appointed a DPO.

ü If not, they checked with the legal department if the intended data-processing activities trigger the appointment of a DPO, either by looking at European authoritative interpretations, local regulations, local authoritative interpretations, and relevant national and European case law.

ü The controllers required the appointment of a DPO if necessary, and its involvement in the tool development process as necessary.

ü As a general rule, the DPO should be aware of every step taken to allow room for their intervention if deemed relevant.

---

65 Article 29 Working Party (2017) Guidelines on Data Protection Officers ('DPOs'), p.4. European Commission, Brussels.

66 Article 37. Designation of the data protection officer. 1. The controller and the processor shall designate a data protection officer in any case where: (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.