WI-FI TRACKING TECHNOLOGIES: GUIDANCE FOR DATA CONTROLLERS

English translation - Only the Spanish version is deemed authentic

V. may 2024

EXECUTIVE SUMMARY

Wi-Fi tracking is a technology that allows mobile devices to be identified and tracked through the Wi-Fi signals they emit, to detect the presence of the device in a specific area and to identify movement patterns, which is why it is used, for example, in the estimation of capacity, the analysis of flows of people or the measurement of dwell times.

Practical applications can be found in shopping malls, museums, places of special interest, workplaces, public areas, public transport or large public events. However, this practice poses serious risks to privacy, as it can allow the tracking of people's movements without any action or knowledge on their part and without an appropriate legal basis.

It is crucial to be aware that many of these uses of Wi-Fi tracking involve the collection and other processing of personal data and therefore must be subject to the set of principles, rights of natural persons and obligations for controllers set out in the GDPR.

The guidelines analyse both technically and legally the implications of the use of this technology, identify the main risks associated with it and offer a series of concrete recommendations for accountable use that is compatible with data protection regulations.

These guidelines have been prepared jointly by the Spanish Data Protection Agency, the Catalan Data Protection Authority, the Basque Data Protection Authority and the Transparency and Data Protection Council of Andalusia and are the result of the collaboration of the four control authorities in the face of the impact that an inappropriate use of "Wi-Fi tracking" technology can have on privacy and data protection of natural persons.

Keywords: Wi-Fi, tracking, risk, dpia, mobile

INDEX

I. INTRODUCTION

Today, smartphone is a ubiquitous personal device equipped with various wireless technologies such as Wi-Fi and Bluetooth, as well as supporting present and past generations of mobile network technologies (i.e., 2G–5G).

To carry out communications, all these technologies rely on the exchange of messages between these devices and other network equipment such as base stations and access points.

In particular, Wi-Fi technology is a wireless technology based on standardized communication protocols (IEEE802.11 protocol family), characterized by a set of terminals (mobile or not) that connect to an "Access Point" (AP). A set of APs managed under a single entity makes up a Wi-Fi network.

Wi-Fi communication is done through messages called "frames", a set of bytes that always contains a header that includes the identifier of the source device called the MAC (Media Access Control) address. Some of these frames are not encrypted and are emitted from the device periodically, even when the device has not connected to any Wi-Fi network.

The data contained in these frames, using various technologies currently available, can be captured, analysed and processed to determine an identifier that allows the source terminal of these frames to be identified. As in the world of the Internet, this set of technologies is known as "device fingerprinting", or just "fingerprinting". Throughout the text, these terms will be used interchangeably.

The information used to determine this digital fingerprint is sent by the device without any action or knowledge on the part of the person wearing it, which makes these technologies particularly sensitive from the perspective of privacy and data protection.

By constructing, storing and analysing this fingerprint, it is possible to detect the presence of the device in a certain area and to identify movement patterns of the device and, therefore, of the person wearing it.

This type of technology that collects data from Wi-Fi messages exchanged between terminals and APs, for further processing and analysis is called "Wi-Fi tracking".

The two main types of analytics offered by these technologies are presence and location. Presence analysis focuses on the study of the existence of terminals in a given area and their duration in it, while location analysis aims to trace the route followed by the terminal within a study area.

Its main uses include estimating capacity, analysing the flow of people, calculating attendance statistics and average times spent in specific locations or waiting in a queue, determining the most common routes or calculating the rate of repeated visits.

Practical applications can be found in shopping malls, museums, places of special interest, workplaces, public areas, public transport, large public events, emergency scenarios, etc.

Depending on the characteristics of the digital fingerprint generated by these technologies, the storage time and its processing, the use of Wi-Fi tracking may involve the processing of personal data, sometimes not only unknown to the user of the terminal, but also to the data controller himself, to the extent that he understands that it is not personal data. which may be wrong, as explained in section 3.

When considering deploying this type of technology, people's privacy should come first. All people should have the right to move freely without "feeling spied on", without a third party, whether public administration or private company, being able to observe or keep a record of what they are doing.

No one should be able to track which shops, health facilities, or cult places a person visits. This data must remain in her private sphere, so that she can be herself, without feeling inhibited by a possible registration or use of such information[1].

These guidelines analyse both technically and legally the implications of the use of this technology, identify the main risks associated with it and offer a series of specific recommendations for responsible use that is compatible with data protection regulations.

[1] https://edpb.europa.eu/news/national-news/2021/dutch-dpa-fines-municipality-wi-fi-tracking_en

II. DESCRIPTION OF THE TECHNOLOGICAL FRAMEWORK

A. THE USE OF FIXED AND RANDOM MAC ADDRESSES

The MAC address is a generally fixed and unique identifier of any device, used in communications between the different elements of a network.

When a device connects to an AP on a Wi-Fi network, all of its messages are initiated by identifying the MAC address of the device itself. In this way, the AP can read the contents of the frames, and through the MAC address, uniquely identify the terminal.

The coverage of Wi-Fi networks is provided by the APs that make it up. These APs can be located in open public spaces or inside buildings or facilities.

However, most mobile terminals that enter the coverage area of Wi-Fi networks do not connect to them. Even so, Wi-Fi-capable devices periodically search for networks that might be available in their coverage radius. This search is done by periodically sending frames called "Probe Requests" that the device transmits even if it is not connected to a Wi-Fi network and sometimes not even Wi-Fi functionality is activated. The main purpose of this type of frame is to send a "probe request" to the different Wi-Fi networks that may exist in the area. The APs are prepared to respond to these messages, sending information to the terminal that will allow it to connect to it if the user chooses.

A few years ago, in the Probe Request frames, in addition to certain technical information, the fixed and unique MAC address of the terminal was sent. Therefore, by collecting these frames over time together with location technologies, it was possible to uniquely identify the terminal by means of this identifier and record its journey within the coverage area of the Wi-Fi network even if it was not connected to it.

Due to the privacy concerns that this situation posed, mobile terminal manufacturers made the use of the random MAC address widely incorporated. This process started in Apple iOS8 and was followed and extended by Android.

The random MAC address is a "virtual" address used in Probe Request frames. In this way, different messages sent from a terminal do not share the same unique identifier (fixed MAC address) and therefore it is no longer possible to know the real MAC address of the device by capturing it through the analysis of the Probe Request frames. On the other hand, since the random MAC address is frequently changed and the frames themselves are sent randomly, it is also not easy to identify the device using the random MAC addresses directly.

This measure strengthened people's privacy; however, the following factors must be taken into account:

- The procedure for generating random MACs is not standardized, leading to disparate behaviours between terminals.
- Once the terminal has been connected to a given AP, the MAC address used remains constant throughout the connection, even if it has been randomly generated, and therefore allows the actions performed by the device throughout the connection to be linked, for example, its absolute and relative location with the location of other terminals.
- It is estimated that currently between 5% and 10% of devices do not use random MAC addresses.
- There are many techniques that are able to uniquely identify, in a high percentage of cases, mobile devices even if they use a changing random MAC address. These are the current techniques used in Wi-Fi tracking, based on the various information contained (or deduced from) the Probe Request frames combined with the

detection of statistical patterns of random MAC addresses. The most advanced techniques for linking information from different frames to the same device use machine learning algorithms and data analytics based on Big Data.

B. DATA USED IN WI-FI TRACKING

The various Wi-Fi tracking techniques aim to uniquely and accurately identify and track endpoints in Wi-Fi environments.

This method is based on the use of a wide variety of parameters and physical characteristics of both the devices and the transmission conditions themselves to generate an individualized fingerprint for each device.

The use of pattern recognition techniques and data analytics in general, together with a continuous evolution of the techniques used by device manufacturers in defence of privacy, leads to a situation of permanent change. As a result, some techniques that were fully effective a few years ago have lost their usefulness today. The main methods currently used are described below.

The "Probe Request" frame is a type of management frame covered by the Wi-Fi standard and is used when the device (for example, a smartphone) is not connected to a Wi-Fi AP. The device, on each of the available Wi-Fi channels, makes a poll "asking" for available APs in its coverage radius to which it can connect.

When a given AP receives the Probe Request frame, it responds with a frame called "Probe Response". With this frame, the device knows about the existence of that AP and its characteristics, in case it wants to connect.

This type of frame is emitted by all devices in Wi-Fi communications automatically without user control and without encryption, so that it can be received and decoded not only by any AP, but also by any low-cost device listening to the Wi-Fi channel. The specific characteristics of the broadcast of this type of frame depend on many circumstances, such as the manufacturer, the model and the operating system of the device itself. In some cases, the data sent in them (e.g., the SSID) may directly provide information related to the individual[2].

Wi-Fi tracking technologies take advantage of these features of Probe Request frames (sending across all devices, sending unencrypted, and with a large amount of data) to generate a unique fingerprint that allows the device to be identified.

In addition to the information directly sent in the Probe Request frames, it is possible to obtain information by indirect measurements from combinations of these or by heuristic techniques.

In practice, any measure or data that assists in the identification of the device can be used. Physical measurements or additional data that can be used by this type of technology include the Received Signal Strength Indicator (RSSI), which can also be used to determine the approximate location of the device, the time interval between the sending of the Probe Request frames, the statistical distribution of both the sequence number of the frames and the random MACs or the inherent deviations of the device clocks. In short, all of them can end up allowing the generation of a digital fingerprint.

The purpose of data collection and analysis such as those described above (and others depending on the specific solution of the manufacturer) is the generation of a unique digital fingerprint that allows each device to be identified.

[2] https://svs.informatik.uni-hamburg.de/publications/2022/2022-06-08_Probing_for_Passwords.pdf

The process of generating the fingerprint of mobile terminals on a Wi-Fi network involves, in general terms, the following phases:

- **Probe Request Frame Capture:** The Probe Request frames received in the different APs of the Wi-Fi network under observation are collected in bulk. In addition to frame information, data related to the physical conditions of the transmission, such as RSSI and others, can be collected. To accomplish this capture, you can use specialized equipment or even conventional Wi-Fi network equipment that provides these additional capabilities.
- **Extracting and sending information:** Extracting relevant information from the captured frames and the physical characteristics of the transmission. This information is sent to a centralized server for processing and analysis. The specific data sent will depend on the Wi-Fi tracking model implemented in the network.
- **Pattern analysis and fingerprinting**: After the information is extracted, a pattern analysis is carried out on the collected data. The goal is to combine specific characteristics of the collected data that make it possible to distinguish one device from another. This analysis will vary according to the system used and is essential to achieve a unique identification of the mobile terminals in the monitored area, and the use of advanced techniques, such as machine learning and probabilistic modeling, is already common.

Machine learning algorithms are able to learn patterns and establish correlations between different frame parameters to determine the probability that a frame belongs to a previously identified device or is from a new one. By combining these features into a probabilistic model, a unique fingerprint is generated for each device. These models can integrate different sources of information, such as historical data from previously identified devices, contextual information, and behavior patterns, to generate more robust and accurate fingerprints.

In short, a fingerprint is created that represents the device through a combination of multiple attributes allowing it to be singled out.

- **Comparison and recognition:** Once the fingerprints of different devices have been constructed, a comparison and recognition is performed to identify devices and determine if they have been previously detected by the system.

C. DEVICE IDENTIFICATION

After generating the fingerprint of the device, it is identified. If you track it through its fingerprint, it will be possible to obtain the following type of information:

- **Presence in the AP's coverage area:** The fingerprint allows you to determine whether or not the device is present in the area where the AP is located. This is especially useful for counting the number of devices present in a place or for obtaining data on the influx of visitors on different days.
- **Approximate dwell time:** In addition to indicating the presence of the device, the fingerprint allows you to estimate the approximate time that the mobile terminal spends in the coverage area. This data can be useful for understanding user habits and gaining insight into the duration and frequency of visits.
- **Trajectory tracking:** The device's fingerprint makes it possible to track its trajectory over time. This involves recording the device's movements in the Wi-Fi network's coverage area and getting information about the places it has visited.

To improve the accuracy of tracking the trajectory of a mobile terminal, triangulation techniques can be employed based on the strength of the signal received from three or more APs in the network. By combining the information from these APs, it is possible to achieve high accuracy in the location of the device, even reaching levels of up to 0.5 meters,

according to studies. This increased accuracy makes it easier to track and analyze the device's trajectory, providing greater detail of users' movement patterns.

It is important to note that the retention of the fingerprint of the same terminal for several days would allow for more intense and extensive monitoring. Thus, by storing and recognizing the fingerprint of a device over time, it would be possible to identify patterns of behavior, discover preferences or routines, daily activities, frequented places, among other intimate aspects of people's lives.

III. PERSONAL DATA AND PROCESSING INVOLVED

Wi-Fi tracking technology has evolved significantly, making it possible to collect and analyze multiple device characteristics. This capability is not limited to identification via MAC address, but also encompasses the creation of unique fingerprints. These fingerprints, created by combining multiple features, make it possible to identify devices continuously, overcoming anonymization measures such as MAC address randomization.

At the same time, the mobile phone, which has become an everyday and inseparable element, acts as a direct link with its user, generating both direct and indirect identifiability[3]. These devices are part of the private sphere of users, so they must be protected in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms[4] and the regulations governing the protection of personal data.

Therefore, in this technological context, it is crucial to analyse the possible existence of personal data processing, as well as, where appropriate, the content thereof.

A. SCOPE OF THE TERM "PERSONAL DATA"

The concept of "personal data" as set out in the GDPR has a very broad scope. Article 4.1 of the GDPR defines "personal data" as "any information relating to an identified or identifiable natural person".

The reference to "any information" in this definition underlines the intention of the legislature to give this concept a very broad meaning, which is not limited to confidential or privacy-related data, but may cover all types of information, both objective and subjective, provided that it is "about" the person concerned. To do so, it will be sufficient for the information to be related to a specific person due to its content, purpose or effects[5].

With regard to the concept of "identifiable", Article 4.1 provides that an identifiable natural person is "one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;".

Therefore, in order to classify information as personal data, it is not necessary for that information to be able, on its own, to identify the data subject[6].

Moreover, a natural person is identifiable as long as the data controller is able to distinguish and process him or her differently, even if that data alone is not sufficient to do so.

In this regard, it is useful to differentiate between unique identifiers that allow the individual to be identified unambiguously and "quasi-identifiers". The latter, at first glance, do not make it possible to identify a specific person. However, when combined with each other or with others, they allow the person to be identified due to the "unique combinations". This phenomenon, known as the "mosaic effect," illustrates how the accumulation of "quasi-identifier" data can lead to the identification of a person[7], a process that is facilitated by big

[3] Section 4.2.2. Opinion 13/2011 on geolocation services on smart mobile devices (WP29, WP185)

[4] Recital 24 Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

[5] Paragraphs 34 and 35. CJEU of 20 December 2017, case C 434/16

[6] Paragraph 41. CJEU of 19 October 2016, case C-582/14º

[7] Opinion 5/2014 on anonymisation techniques (WP29, WP216)

data analytics technologies. It is perfectly possible to speak of the existence of personal data even in cases in which there is no direct or express identification of the data subject.

> Example: Information is available from a mobile phone that have visited (knowing date, time, and time of dwell) on two occasions shop A, on 3 occasions establishment B, has stayed overnight in the hotel C for 16 days and is qualified as a tourist with a stay of more than 15 days and less than 1 month. This information itself is already so detailed that with very little additional information could be used to identify the person carrying that mobile terminal.

With regard to the ability to be "identifiable" as a person, recital 26 of the GDPR underlines that "account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly". In other words, it is not necessary that all the information that makes it possible to identify the data subject must be in the possession of a single person or within a single processing. What needs to be analysed is whether there is a reasonable possibility that the person can be identified by other additional means. On the other hand, it is a dynamic analysis, so the degree of technological progress at the time of processing and its possible development in the period during which the data will be processed must be taken into account. In short, this identifiability is also related to the fact that it does not require disproportionate efforts and, as has just been indicated, the constant technological evolution facilitates it.

B. WI-FI TRACKING AND FINGERPRINTING AS PERSONAL DATA

This broad definition of the concept of personal data established by the GDPR acquires particular relevance in the context of Wi-Fi tracking. This technology affects all devices with Wi-Fi functionality, without necessarily being connected to any specific network, and sometimes not even having this functionality activated. These devices include mobile phones, tablets, laptops, fixed computers, routers, printers, household appliances, toys, wearable (pacemakers, portable oxygen systems, diabetic devices, neural implants, etc.) and even cars[8].

The GDPR, in its Recital 30, warns of the ability to identify individuals through device fingerprinting:

" Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them."

In accordance with the above, the data transmitted by Wi-Fi signals used in this type of process can be considered as personal data insofar as it is related to identifiable persons and is likely to be used for their direct or indirect identification. In particular, fingerprinting in the context of Wi-Fi tracking may involve the processing of personal data in accordance with the provisions of the GDPR.

The concept of "fingerprinting" is defined as "a set of elements of information that identifies a device or application instance", thus encompassing any information that can be used to

[8] Some control authorities, such as Unabhängige Landeszentrum für Datenschutz (Schlewig Holstein, Germany) have expressed concern about the application of these technologies on cars that incorporate Wi-Fi access points, allowing people to be tracked. Location Services can Systematically Track Vehicles with WiFi Access Points at Large Scale

identify, link or infer a user or device over time[9]. This may include, but is not limited to, data derived from:

- setting up a user/device agent; or
- data exposed by the use of network communication protocols.

Fingerprinting therefore provides the ability to distinguish one device from another and could be used to track a user's location or behavior over time, even if there is no direct or express identification of the person.

C. WI-FI TRACKING AND LOCATION AND TRAJECTORY DATA

The position of a device can be known either approximately by "presence" (proximity to the sensor), or more precisely by triangulation. By maintaining the identification or individualization of the device and determining its position over time, it is possible to establish a trajectory during the time that the device is within the coverage area of the sensors.

This location data represents a type of personal data with a high risk to the privacy of individuals, as detailed in the section on risks to the rights and freedoms of natural persons.

Where the spatial and temporal scope of the data collected through Wi-Fi tracking is maintained, these may be sufficient on their own or in combination with others to allow the identification of individuals and the controller should consider this type of data as personal data.

D. PROCESSING OF PERSONAL DATA

In itself, Wi-Fi tracking technology is not a processing of personal data, but it could be part of one. In fact, when deciding how to carry out a processing or achieve a purpose, the controller may opt for solutions other than Wi-Fi Tracking or for options that do not involve the processing of personal data.

Wi-Fi tracking technology can appear in personal data processing operations derived from two main types of analytics: presence and location. Presence analysis focuses on the study of the existence of terminals in a given area and their permanence in it, while location analysis aims to trace the route followed by the terminal within a certain study area, even for an indefinite period of time.

On many occasions its purpose is to detect and analyse collective behaviour, however, it cannot be forgotten that it is based on the detection of individual data.

By way of illustration, some processing activities in which Wi-Fi tracking technologies have been used are indicated[10]:

- Geolocation service of the device, with or without the user's own agreement.
- Monitoring of people at the workplace.
- Emergency services, through search or location as part of the provision of life-saving assistance to people. This is a mechanism by which emergency call centers can automatically receive information about the caller's location, enriched by Wi-Fi location data.
- Surveillance of people, using Wi-Fi tracking to detect if there are people in certain premises or places, and individual control of access to these areas.

[9] Apdo. 3 Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting

[10] The list offered does not imply a position either for or against it by the data protection control authorities.

- Linking between people, to determine if two or more people have shared the same space, have approached, stopped at the same point, etc.
- Analysis of the flow of people in private facilities (e.g. workplaces or shopping centres) to optimise the design of physical space or staffing.
- Crowd management in places of public access: in crowded areas such as airports, public transport, stadiums, public roads, etc., to control maximum capacity, manage traffic of people or vehicles efficiently, optimize routes or provide information in real time, improving safety and comfort. It is common to find these uses within "smart city" projects.
- Targeted marketing and advertising, to deliver promotions or advertisements to users' devices when they access or approach a specific location or based on behaviour or movement patterns.
- Creation of user profiles based on movement patterns and behaviour.

In summary, it is important to note that many of these uses involve the collection and processing of personal data and must therefore be subject to the set of principles, rights of natural persons and obligations for controllers set out in the GDPR and the LOPDGDD.

IV. LEGAL BASES FOR PROCESSING PERSONAL DATA

Any processing of personal data must comply with the principles set out in Article 5 GDPR and comply with one of the lawfulness conditions listed in Article 6 GDPR, which applies to Wi-Fi tracking in cases where the data controller opts for a technological option that makes such processing possible.

The processing must be fair and transparent, and it must be completely clear to individuals what data and how it is being processed by Wi-Fi tracking and provide this information in an easily accessible and easy-to-understand way, regardless of the technical or practical difficulties that Wi-Fi tracking may entail for the data controller in complying with these principles.

The purposes of the processing via Wi-Fi tracking must be explicit, i.e. clearly stated, legitimate and communicated to the data subjects at the latest at the time of collection. In addition, data collected for a specific purpose via Wi-Fi tracking may not be used for a subsequent purpose that is incompatible. To this end, it is essential to ensure that the subsequent processing does not deviate from the purposes already established for the processing, and of which the persons concerned must be informed. For example, if data on the movements of persons within a commercial premises were processed in order to optimise the physical location of certain products based on a legitimate interest of the controller, it would possibly be difficult to justify the compatibility of processing that would involve those persons receiving notifications relating to commercial offers of those products.

Likewise, it is essential that the personal data processed is adequate and relevant, limited to what is strictly necessary for its purpose. It should be remembered that the purpose of the processing is not to carry out Wi-Fi tracking, so if it is possible to achieve the ultimate purpose with a less intrusive technique, the principle of data minimization would not be complied with. If no other technique other than Wi-Fi tracking is possible, in order to comply with the principle of minimisation, the data processed would have to be adjusted, in terms of categories, frequency, granularity, etc., to what is strictly necessary, as well as that their retention period is the minimum necessary, proceeding to their elimination or effective anonymisation, through automated processes whenever possible.

It will also be necessary to comply with the principle of accuracy, in particular if probabilistic techniques are being used to link actions to an individual, rectifying or deleting data that is inaccurate where appropriate, and ensuring the security and confidentiality of personal data, as discussed in detail below.

The data controller, in addition to complying with the principles set out above and being able to demonstrate it, must ensure that the processing complies with one of the lawfulness conditions established in article 6.1 GDPR.

However, before determining or considering the application of any lawfulness condition, it is important to remember that personal data should only be processed if the purpose of the processing could not reasonably be achieved by other means.

The legal basis applicable to each processing requires a detailed analysis of the specific case by the data controller, in accordance with the principle of accoutability (Article 5.2 GDPR), which will take into account the nature, scope, context and purposes of the processing. However, it is possible to provide general guidance to controllers to guide them in identifying whether any of the conditions that would legitimize a particular processing using Wi-Fi tracking technologies are met.

A. CONSENT (ARTICLE 6(1)(A) GDPR)

According to what was previously analyzed, most Wi-Fi tracking techniques operate without the need for the device to be connected to the Wi-Fi network and without the knowledge of the person who owns it. In other words, there is no means of communication between the data subject and the data controller. Therefore, it would be materially impossible to request consent from the data subject and should therefore in principle be discarded as a legitimate basis.

However, it would be possible to consider a specific scenario, where the user makes the connection to the Wi-Fi network voluntarily, and after this connection they are informed and consent is requested to process their data through Wi-Fi tracking. We cannot forget that in these cases such consent would have to be free, specific, informed and unequivocal. A practical example could be in scenarios where users are invited to allow their location to be tracked in exchange for commercial offers[11]. In these cases, systems should be put in place to ensure compliance with the principle of transparency, allowing the information to be concise, easily accessible and easy to understand, and to use clear and simple language and, where appropriate, to be visualised, as analysed in section 9.

In certain cases, such as in the workplace, education or also the public sector, it will be necessary to analyse whether there could be a clear imbalance of power in the relationship between the controller and the data subject, so the assessment of the freedom of consent will have to be carried out carefully.

B. PERFORMANCE OF A CONTRACT (ARTICLE 6(1)(B) GDPR)

The execution of a contract or pre-contractual measures could legitimise the processing of data only if it is related to the provision of a specific service in the context of Wi-Fi tracking. In this case, it will be essential to be able to demonstrate that the processing is necessary to comply with contractual obligations, which will not be common, except in certain cases of geolocation services requested by the user.

C. COMPLIANCE WITH A LEGAL OBLIGATION (ARTICLE 6(1)(C) GDPR)

This basis would only be applicable when there is a legal obligation requiring the controller to comply with a purpose for which the use of Wi-Fi tracking techniques is necessary. In addition, in accordance with the LOPDGDD, this obligation would have to be provided for in a rule of European Union law or a rule with the force of law. Such a legal basis or legislative measure must be clear and precise and its application foreseeable to its addressees, in accordance with the case-law of the CJEU, including measures to ensure lawful and fair processing, fulfilling an objective of public interest and proportionate to the legitimate aim pursued.

D. PROTECTION OF VITAL INTERESTS (ART. 6(1)(D) GDPR)

This condition of lawfulness could only apply when the processing was necessary to protect the life or physical integrity of a person. In principle, the processing of personal data in the context of Wi-Fi tracking could hardly be justified on these grounds. However, its application cannot be completely ruled out in situations where vital interests are really at risk,

[11] Recital 17. Opinion 01/2017 on the proposal for a regulation on privacy and electronic communications (2002/58/EC) (WP29, WP247).

such as emergencies, aid or search and rescue of missing persons, which would require a rigorous analysis of the specific case to justify its application[12].

E. PUBLIC INTEREST OR EXERCISE OF OFFICIAL AUTHORITY (ARTICLE 6(1)(E) GDPR)

Basing data processing of this nature on this legitimate basis implies a careful analysis of the requirements established in the data protection regulations. Thus, the controller must identify the regulation with the force of law that attributes to it a specific competence in which it can demonstrate that such processing by means of Wi-Fi tracking is necessary and proportionate to carry out a mission in the public interest or to exercise public powers. Such a legal basis or legislative measure must be clear and precise and its application foreseeable to its addressees, in accordance with the case-law of the CJEU, including measures to ensure lawful and fair processing, fulfilling an objective of public interest and proportionate to the legitimate aim pursued.

Caution should be taken against the use of excessively generic legal precepts as a basis for legitimacy. Given that there is no express legislation in this regard, it would be advisable to develop legislative measures, which, in accordance with the above, contemplate and regulate this type of processing.

It should be borne in mind that the Administration's action will focus mainly on public spaces and that people have a legitimate expectation to enjoy freedom of movement without being monitored. In these scenarios, the intrusion on people's privacy can be very high if the data controller does not take extreme safeguards[13].

F. LEGITIMATE INTERESTS (ARTICLE 6(1)(F) GDPR)

In the private sector, legitimate interest may be considered a valid condition of lawfulness provided that it is necessary for the satisfaction of those interests and the interests or rights and freedoms of the data subjects do not prevail, taking into account the reasonable expectations of the data subjects.

In any case, a meticulous assessment of whether the processing can be carried out, a balancing test, including whether a data subject can reasonably foresee it at the time and in the context of the collection of personal data, is required[14].

It is the responsibility of the person in charge to accredit the "weighing" test. Opinion 6/2014, of 9 April, on the concept of legitimate interest of the data controller, of the working group created by Article 29 of Directive 95/46/EC -WP 217, incorporates various guidelines for analysing the existence of legitimate interest, as well as the necessary safeguards in order to respect and guarantee the rights of those affected by this type of processing.

In a first approximation, the interests and rights of the interested party must be weighed against the processing that the controller intends to carry out, assessing the impact on privacy. It should not be forgotten that recital 47 of the GDPR states that, for the purposes of legitimate interest, "*The interests and fundamental rights of the data subject could in*

[12] Report 39/2019 of the Legal Office of the AEPD.

[13] See decision of the Dutch Data Protection Authority on the processing of personal data of users of mobile devices on which Wi-Fi was switched on in the city centre of Enschede without an appropriate legal basis.

[14] Recital 47 GDPR: "In particular, the interests and fundamental rights of the data subject may prevail over the interests of the controller when personal data is processed in circumstances where the data subject does not reasonably expect further processing to take place."

particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing." and, in the case of Wi-Fi tracking, the collection of data, as referred to at the beginning, is often beyond the knowledge of the owner of the terminal. In short, in such cases, it should be possible to clearly demonstrate that the legitimate interest of the controller is overridden.

Only in cases where, as a result of the balancing carried out, the interests and fundamental rights of the data subjects do not prevail, may the processing of personal data justified by a legitimate interest be carried out, which would also require that safeguards, guarantees and technical and organisational measures, including those relating to information security, that are necessary to protect the personal data processed are incorporated into the processing.

In other words, the lawfulness of the processing covered by this basis is also subject to the existence and intensity of adequate guarantees. These guarantees will undoubtedly depend on the more or less invasive nature of the proposed processing and, to a large extent, on how and when the irreversible dissociation of personal data is carried out. Generally speaking, the processing will be considered less intrusive when the anonymization of the data is carried out closer to the time when the traffic data was generated or received via the Wi-Fi-enabled device.

Without prejudice to the need for a case-by-case analysis and always in full compliance with all the requirements of the GDPR, measures such as prompt anonymisation of the data collected, obtaining only aggregated information on the number of visitors and the most or least visited areas (heat maps) inside an establishment, ensuring that no data is taken outside, neither in common areas of passage, nor on public roads and ensuring that it is not possible to monitor people, could bring them closer to a favourable balance, without prejudice to the result that the impact assessment relating to data protection may yield.

Other scenarios that contemplate a greater collection of personal data in space (larger areas of coverage), in time (longer periods of time), or in the scope (data on mobility, repeat visits, etc.) remove the possibility of favorable weighting, taking into account the difficulty of effective and practical mechanisms that allow people to object to the processing (opt-out mechanisms) in Wi-Fi tracking.

V. RISKS TO THE RIGHTS AND FREEDOMS OF NATURAL PERSONS

Article 24.1 of the GDPR establishes the obligation to manage the risk to the rights and freedoms of individuals posed by the processing of personal data, considering the nature, scope, context and purposes of the processing. Therefore, any organization that makes the decision to initiate the processing of personal data will need to manage these risks.

This section presents the main risks that could be associated with the processing of personal data that is implemented using Wi-Fi tracking technology. It is not an exhaustive list of risks, but an overview of the main risks to be considered and, in any case, data controllers must determine, based on the particularities of the specific processing, which risks are applicable in your case and determine the existence of other possible risks not identified in this guide.

Risk management for the rights and freedoms of individuals is different from risk management of compliance with the principles set out in the GDPR and applicable data protection regulations. Compliance risk management, like other risk management with other objectives (legal, financial, business, fraud, project, etc.), may be necessary to achieve certain organizational objectives, but it does not respond to the risk management obligations for the rights and freedoms of natural persons imposed by the GDPR. If the processing that is intended to be initiated does not comply with the principles of the GDPR, for example because it lacks an adequate legal basis or does not comply with the principle of necessity and proportionality, the processing would be unlawful and prohibited. The use of Wi-Fi tracking will be part of the processing of personal data and the organization that implements it is obliged to comply with the requirements and obligations established in the GDPR, and among others to manage the risks for the people who will be affected by the processing as a whole.

> Example: In order to preserve the safety of people at the entrances to a mass event, it is possible to determine if some of the access roads are becoming congested. To measure this congestion, the use of Wi-Fi tracking technology could be considered to carry out an approximate count and will be a means to implement one of the processing operations, the measurement of congestion. Measuring congestion alone will not achieve the purpose of preserving people's safety, since the treatment must have other operations, such as the decision to reduce congestion at a given time, the ability to do so effectively and actions to ensure that this occurs in an efficient and orderly manner. If these operations that give meaning to the ultimate purpose of the processing are not correctly implemented, the processing is not fulfilling a purpose that has a legal basis. Likewise, if there are already means with which these objectives are being achieved (video surveillance, people counters, etc.) the processing would not be necessary either, at the same time it could be unsuitable since such a measure entails an additional risk since there are less harmful means to achieve the possible purpose of this system.

Risk management should be done considering the processing of personal data as a whole. A mere isolated analysis of the possible risks of Wi-Fi tracking technology would be meaningless and insufficient under the GDPR, since this technology is a means that can be used in processings of varying complexity that involve the combined use of other technologies (cloud, blockchain, AI, IOT, etc.).

> Example: processing whose sole purpose is to control capacity to ensure the safety of an individual physical store of an SME that is decided to implement using Wi-Fi tracking, does not involve the same risks as a processing with the same purpose but in all the physical stores of a chain nationwide or a processing whose purpose is to offer online advertising aimed at people based on the establishments or sections visited inside an establishment.

Using the same technology at the provincial or regional level to determine regular flows of tourists, obtaining repetition rates of tourist visits whose responsibility is an authority or public body, will involve more risk than using it in a single physical store to estimate capacity. Using essentially the same technology, the treatments are different and the risks are different.

A. IMPACT ON PEOPLE'S PRIVACY

The use of Wi-Fi tracking technology means that in certain circumstances it is possible to single out[15] people, locate them in a precise location, and infer[16] data about people based on the context of the location.

Example: The implementation of this technique in the workplace, for example, in a building can provide information about part of the activity that is currently protected by labour regulations, such as the control of how much time is spent in common areas, with whom you talk and for how long, attendance at toilets, location outside strictly working hours (library, recreation areas), etc.

B. INTRUSION INTO THE HOME OR PUBLIC AREAS

Wi-Fi tracking technology makes it difficult to set clear and defined physical boundaries about where the device's signal is picked up and where it can't be picked up. On a camcorder, certain masks can be set and the lenses oriented, but these types of limits are more expensive to implement in a radio frequency-based system.

Example: The installation of a Wi-Fi tracking system in a building may be collecting the signal from devices located in homes or private homes that are behind a wall, from workers from other entities, or from the entity itself that should not be data subjects for the processing or even from people who travel on public roads. Such an intrusion would not be a risk, but a breach of the principle of legitimacy of the processing.

C. SCALE OF PROCESSING AND RESTRICTION OF FREEDOM OF MOVEMENT

Analyzing the impact of certain technological systems only in terms of the scope of an entity provides a limited view of the potential intrusion into people's privacy. Technologies are currently implemented on a large scale and it is necessary to analyze their impact when they are implemented on a massive scale, as they can jointly produce a limiting effect on the rights and freedoms of citizens.

Example: A security company offers, in addition to the usual services, a Wi-Fi tracking service for small businesses, so that 30% of the commercial premises in a city implement this service, which allows the identification of passers-by near the commercial premises to be recorded. In this way, it would be possible to have recorded and controlled the wandering around the city of any citizen at any given time.

[15] Singularization refers to the possibility of individualizing a person in a dataset by highlighting certain records. Singling out can occur even without the need for the person to be identified.

[16] Inference occurs when it is possible to deduce the value of a personal characteristic with a high degree of probability from the values of a number of other attributes, such as location in certain locations, the context of such locations, or others.

D. TRACKING BY DEFAULT: INTERFERENCE WITH RELIGIOUS FREEDOM OR THE PROCESSING OF SPECIAL CATEGORIES OF DATA

The record of which sites are visited by a person allows us to infer lifestyle habits and tastes or interests with themes related to the points where they can be located. However, it should be noted that those areas that a person does not visit and that can allow profiling based on special categories of data also provide a lot of information, or even more. In addition, it is independent of whether or not the information disclosed by the processing in question is accurate and whether the controller acts in order to obtain information that falls within one of the special categories[17].

> Example: Within the framework of a treatment that incorporates Wi-Fi tracking technology at the level of a shopping center, which allows a person to be singled out, he or she could be tracked by visiting sports shops, traditional food restaurants in a specific country, with breaks in the usual worship hours of a certain religion, not accessing establishments linked to other religions and never stopping at alcohol displays to profile his or her age, sex, religion, and estimated origin, with or without sufficient foundation. In the same way, a shopping centre that has a certain religious centre in its vicinity could obtain information from people who habitually attend religious worship according to their beliefs, including minors or people at risk of social exclusion or other situations of risk.

In essence, when these processes are carried out in places related to special categories of data, such as a hospital, a clinic of a medical specialty, or the headquarters of a political party, the controller could be engaging in the processing of special categories of data, which increases the risk to the rights and freedoms of individuals.

> Example: The possibility of attributing to an individual person visits to an oncology clinic in a hospital where Wi-Fi tracking technology is used may lead to the inference of the person's disease, and that in the future they may find it difficult to take out health insurance.

E. PERSONAL FREEDOM AND SELF-CENSORSHIP

A person's knowledge that he or she is going to be tracked in his or her wanderings through public areas, a building or a shopping centre may cause him or her to exercise self-censorship in order to preserve his or her interest in certain political or religious associations, cultural centres or leisure activities and may condition his or her personal freedom, freedom of movement and produce situations of self-censorship.

This may occur even in those cases where the data subject is adequately informed about the processing of their personal data, due to their own expectations about the processing that will be applied to the data captured from their mobile terminal.

> Example: A person who is curious about some type of product, service or leisure offered in a shopping center but that contravenes some precept of their social environment, may have a media impact or may be bad interpreted in any other circumstance, may change his behavior if he knows that mere wandering near it can be recorded.

[17] CJEU (CJEU Judgment C-252/21 Meta vs. German Competition Office) considers the collection of visits to pages or Apps related to one or more special categories of data to be processing of data in special categories, even if sensitive data is not collected per se. Extrapolating this decision to the case of processing that incorporates Wi-Fi Tracking, it would imply that in cases where these treatments occur in premises or establishments related to special categories of data, the controller could be processing data from special categories.

F. THE IMPACT OF RE-IDENTIFICATION

Even when the aim is to obtain collective data or aggregate statistics and it is not intended to single out individuals, the origin of the data will be based on processing operations on unique identifiers, such as MAC addresses of the devices, a digital fingerprint or fingerprint of the devices or others to which in the best of cases some pseudonymisation or anonymisation processing of personal data will be applied[18].

Pseudonymization is a processing of personal data that generates, from a set of personal data, a new set of pseudonymous information and information that allows individuals to be re-identified. The GDPR still applies to a pseudonymized dataset since individuals are identifiable.

> For example, replacing the MAC addresses in a dataset with a hash of the MAC address could be a pseudonymization processing operation.

Anonymization is a processing of personal data that generates, from a set of personal data, a new set of anonymous information. Therefore, in any case, from the time the data is collected until it is anonymised, there is always a phase in which there is a processing of personal data.

On the other hand, in any data anonymisation process, there is a certain likelihood that there will be a re-identification of the data subjects[19]. That is, a supposedly anonymous dataset ceases to be anonymous[20] because the data subjects have been identified or can be identified. When this happens, the risk to people's rights and freedoms materializes because, among other consequences, it makes it possible to single, link or infer.

Even applying anonymization strategies, it is necessary to assess the likelihood of re-identification and personal data breaches, as well as the impact it may have on the rights and freedoms of data subjects. To this end, it is necessary to consider the worst-case scenarios, such as attempts at re-identification by people internal or external to the organization, with access to auxiliary data, including those available by illegal means, by court orders or by information agencies, in addition to considering that adequate resources are available and taking into account both the technology available at the time of processing and technological advances.

> Example: In some applications, it is intended to guarantee the impossibility of reuse of Wi-Fi tracking information by the use of a specific hashing method, to the use of "salts" or keys for each owner. Although it is a method to increase security, it must be borne in mind that a technique of "security through darkness" is being followed, which any security principle establishes that it should not be the pillar of guarantees due to its intrinsic weakness. In any case, it may be one of the many measures to be adopted, with no guarantee of absolute effectiveness.

Such a probability exists due to the type of data collected, a possible absence of a robust anonymization mechanism, the time or phase of the processing in which anonymization is applied, the fact that the anonymization process may not actually be anonymous or the existence of the technology that would allow such reidentification to be carried out.

---

[18] Pseudonymisation and anonymisation are separate processing operations and should not be confused. See Anonymization and pseudonymization.

[19] Anonymization (III); the risk of re-identification.

[20] A. Di Luzio, A. Mei and J. Stefa, "Mind your probes: De-anonymization of large crowds through smartphone WiFi probe requests," IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications, San Francisco, CA, USA, 2016, pp. 1-9, doi: 10.1109/INFOCOM.2016.7524459.

Example: In a supposedly anonymized database with data of more than 8 millions of probe requests, through one of the fields (WPS) contained in this type of frames, it was possible to re-identify more than 90% of the identifying data of those terminals that transmitting such field[21].

G. RISKS ASSOCIATED WITH LOCATION DATA

It is necessary to stress the particular difficulty of anonymizing data sets when they include different location data of the same person or trajectory data[22] due to the ease of reidentification they present.

Example: The races of 173 million cabs in New York were published, anonymizing (supposedly) the license number of each taxi with a hash. The data included hashes of license number, start, end, duration, time, cost, and tip. In a very short time, the license number of the taxis was re-identified and with Google searches images of people with public relevance taking the re-identified taxis were obtained[23].

The European Data Protection Board (EDPB) and previously the Article 29 Working Party have warned on several occasions about the particularly sensitive nature of location data[24]. A person's travel can provide revealing information, such as their place of work, place of residence, and places of interest, including places of worship or activities related to their sexual orientation, which could allow a detailed profile of their sexual orientation behaviors to be created.

The identifiability of location data is well known and often only a few spatial points are needed to single out a person within a population with high accuracy, considering usual patterns of mobility. This means that even when unique identifiers such as the MAC address are suppressed, because the device is singled out, location data can lead to the identification of a person. Logically, the greater the temporal and spatial scope of the location, the more feasible identification will be.

A data pattern containing a person's location over time cannot be completely anonymized, even if the accuracy of the recorded geographic coordinates is reduced or specific itinerary details are removed. In addition, this also applies to incompletely aggregated location data. That is, simply anonymizing data does not guarantee privacy protection, since if mobility patterns are unique enough, external information can be used to link data back to a specific individual. Thus, there may be specific circumstances such as the existence of uncrowded areas at certain times where it would be easy to identify the person and their behaviors or even combine the capture of an indicator with the images of a video surveillance system, giving rise to the automatic identification of the person.

H. LACK OF MEDIA ACCOUNTABILITY

Typically, data controllers who incorporate technologies of this type into their processing do so through data processors or providers that offer Wi-Fi tracking services, even in combination with other technologies.

---

[21] *Mathy Vanhoef, Célestin Matte, Mathieu Cunche, Leonardo Cardoso, Frank Piessens. Why MAC Address Randomization is not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms. ACM AsiaCCS, May 2016, Xi'an, China. ff10.1145/2897845.2897883ff. ffhal-01282900*

[22] de Montjoye, YA., Hidalgo, C., Verleysen, M. et al. Unique in the Crowd: The privacy bounds of human mobility. Sci Rep 3, 1376 (2013).

[23] On Taxis and Rainbow Tables: Lessons for researchers and governments from NYC's improperly anonymized taxi logs.

[24] See WG29 Opinion 13/2011 and 01/2017, and EDPB Guidelines 04/2020.

In this type of project, there is often insufficient control by the controller of the means that are being used to implement the processing. Many controllers, instead of independent professional advice, will make decisions based on purely commercial information with ignorance of the implications for rights and freedoms, possible collateral processing and loss of control of the processing.

Data is usually found in the technological environment of data processors with very complex relationships, with multiple data transfers, in which cloud infrastructures are usually involved, subject to advanced data analytics and including in many scenarios machine learning techniques and processing on behalf of the data processors.

Faced with the eventual generalization of this type of service, and given the competitiveness of economies of scale, the situation will probably be that the same or a few processors will provide their services to almost all or many of the controllers. Therefore, these processors will process data from multiple different sources, from several controllers, with the multiplier impact that personal data breaches are already having on processors that provide services to multiple entities and could use them for their own purposes[25] such as improving their service, offering personalized online advertising or obtaining profitability from the data by making it available to third parties. This poses a risk to the rights and freedoms of individuals that must be managed by the data controller.

> Example: A Wi-Fi tracking service provider provides free of charge to all establishments on a street, gallery or shopping centre the possibility of offering a Wi-Fi connectivity service to its customers that includes Wi-Fi tracking technology that can be used independently by all managers. Each controller will only obtain statistical and supposedly anonymised data from customers who enter their establishment. However, the data processor will receive the data of all establishments. The processor may keep the data unanonymized or even have linked the data with other databases of its own or third parties to keep individuals singled out or identified and base its business model on the sale of that personal data, in which case, it could be using data outside its role as processor and become a data controller for which it would not be legitimate.

In fact, even if the controller does not intend to identify the data subjects and does not intend to carry out processing for other purposes, a data processor or third party could have the intention of carrying out other processing, using the data for their own purposes, linking[26] the data with other databases that allow the identification of people and ensuring that the anonymisation of the data is not really effective. Although these treatments will be manifestly illegal, the environment of this type of treatment prevents in many cases having guarantees or control over whether they are taking place.

I. PERSONAL DATA BREACH SCENARIOS

The fact that neither the controller nor the processors intend to single, identify the data subjects, or profile the data subjects does not mean that this cannot happen[27]. In particular, this risk materializes when personal data breaches occur both by internal and external

[25] In this case, the processor becomes responsible for these own treatments and cannot carry them out without informing the initial controller, obtaining their approval and ensuring that the new purposes are compatible with the initial ones.

[26] Linkability is when it is possible to link at least two records on the same data subject or group of data subjects (in the same database or in two different databases).

[27] See decision of the Dutch Data Protection Authority on the processing of personal data of users of mobile devices on which Wi-Fi was switched on in the city centre of Enschede without an appropriate legal basis. "The fact that they don't use these resources in practice to identify people in the city center doesn't detract from the fact that they could reasonably do so."

elements to the organization itself. Any processing of personal data is liable to suffer a personal data breach regardless of the technical and organisational measures implemented in the processing.

When a personal data breach occurs not only in one controller, but in some processors or sub-processors that provide services to multiple controllers, the impact could be much greater both in terms of the volume of data and the different areas of the personal lives of the affected data subjects.

In general, in the processing of personal data using Wi-Fi tracking, it is especially important to consider the probability of a confidentiality breach occurring, either because a data exfiltration occurs, or because the anonymization applied to the dataset can be reversed.

> Example: A security company offers, in addition to the usual services, a Wi-Fi tracking service for small businesses, so that 30% of the commercial premises in a city implement this service, which allows the identification of passers-by near the commercial premises to be recorded. The data is anonymized by the security company, so that small businesses only have access to anonymized data. The security company suffers a cyber incident and data is exfiltrated that includes logs from the Wi-Fi tracking system for the last 5 years of a phase of processing in which the data is not yet anonymized. This data makes it possible to single people out, in some cases identify them, obtain their location and follow their journeys through the city over the last 5 years.

The reality of personal data breaches makes it clear that the materialization of threats to datasets is a matter of time, and that the only unknown is the size of the breach. In these cases, the problem is not only in the set of data that has been leaked from a responsible party, but when that data set is linked to data from previous breaches, not only in the framework of treatments using Wi-Fi tracking, but also from other Internet services.

> Example: A Wi-Fi tracking database can leak to the dark web. It should be considered that on the dark web you can find other databases that allow you to link actions of the same individual in two completely different environments, or even a database has been previously leaked that allows Wi-Fi data to be linked to other personal data.

Therefore, before implementing a processing with Wi-Fi tracking technology, in particular when selecting technology providers and processors, it is essential to consider what can go wrong and what consequences a personal data breach may have for the rights and freedoms of natural persons so that, before implementing the processing, Design privacy safeguards to minimize the impact of a breach materializing, and establish the mechanisms for reacting to it in order to minimize the risks to the rights and freedoms of those affected[28].

J. INTERNATIONAL TRANSFERS AND THE INTERNATIONAL REGULATORY CONTEXT

Hand in hand with the use of technological infrastructures of data processors and the combined use of multiple technologies, often with sub-processors and technological infrastructures in the cloud, there is the possibility that the processing involves international transfers of data to countries outside the European Economic Area (EEA).

[28] Recital 83 GDPR: ... When assessing the risk in relation to data security, account should be taken of the risks arising from the processing of personal data, such as destruction, loss or unauthorised disclosure of or access to such data, in particular which may cause physical, material or non-material damage.

In situations where international data transfers occur, the controller must assess scenarios such as breaches of the rule of law, national or international emergencies or crises in international relations and agreements.

> Example: Processing that incorporates Wi-Fi tracking, that makes it possible to link a person with the headquarters of a political party or trade union linked to a certain ideology, that uses data processors with cloud technologies, could involve international data transfers to third countries. Being able to identify it could have consequences, including legal consequences, for individuals (e.g. refusal of a visa or criminal charges).

K. CONCLUSION ON RISK MANAGEMENT

The controller must take into account and manage all risks to the fundamental rights and freedoms of the data subjects applicable in the processing, reviewing each of the threats, how they may affect fundamental rights, taking into account the specific case in its context, scope, nature and purposes, and analysing the entire processing, not just some of the processing operations.

Risks are often linked to each other, and the materialization of some threats or risk factors implies that others can also materialize. The technical and organisational measures to minimise these risks will be dealt with in a specific section below.

VI. OBLIGATION TO CARRY OUT A DATA PROTECTION IMPACT ASSESSMENT

The GDPR sets out the obligations related to data protection impact assessment (DPIA) in Articles 35 and 36. It does not oblige any processing of personal data to be carried out in a DPIA, but it does require processing of personal data where it is likely to involve a high risk. The existence of a reasonable degree of presumption that the treatment may involve a high risk makes it essential to carry out a DPIA.

DPIA is a process of evaluation of a treatment that extends over time, throughout its entire life cycle, and should be reviewed on an ongoing basis, at least when there is a change in the risk posed by the treatment operations. In no case should it be considered a mere documentary formalism.

Broadly speaking, a DPIA:

- It is enforceable when there may be a high risk to rights and freedoms.
- It is a specific obligation of the responsible party.
- It requires passing an assessment of the appropriateness, necessity and proportionality of the processing in relation to its purposes.
- It requires the assessment to determine that the residual risk has been reduced through the implementation of measures and safeguards to a tolerable level.
- It requires it to be carried out before the start of the processing activities.
- It requires the advice of the DPO when it should be appointed or has been appointed at the will of the responsible party.
- It will take into account compliance with approved codes of conduct and certifications that may be applicable.
- Its outcome must be taken into account in order to assess the feasibility or non-feasibility of the processing from the point of view of data protection. The outcome of the DPIA is binding on the controller, and depending on the level of residual risk, requires prior consultation with the competent data protection supervisory authority or even a decision not to carry out the processing.

For processing incorporating Wi-Fi tracking technology, as for any other processing, the risk assessment and assessment of the need for a DPIA should be considered in the light of the processing as a whole, i.e. taking into account its purpose, nature, scope and context.

In accordance with Article 35.3 of the GDPR, in those processes that incorporate Wi-Fi tracking and that involve a large-scale systematic observation[29] of a publicly accessible area, DPIA will be mandatory. Even if the controller does not intend to carry out such systematic observation on a large scale, the DPIA will also be mandatory, since in view of the inherent risk of the processing we would be talking about high-risk processing and, consequently, the requirements of the GDPR apply to such processing. Likewise, it should be considered as an aggravating circumstance, due to the very nature of many of the operations that are part of Wi-Fi tracking, that it will be more difficult for the interested parties to exercise their rights[30].

If the processing complies with two or more criteria from the list of types of data processing that require an impact assessment related to data protection (article 35.4) published by the AEPD, it will also be necessary to carry out a DPIA.

[29] WP243 explains the term large-scale and not exclusively in absolute terms of the number of stakeholders.

[30] Recital 91 of the General Data Protection Regulation.

Some of the relevant criteria on this list for treatments that incorporate Wi-Fi tracking are:

- Processing that involves the systematic and exhaustive observation, monitoring, supervision, geolocation or control of the data subject, including the collection of data and metadata through networks, applications or in publicly accessible areas, as well as the processing of unique identifiers that allow the identification of users of information society services such as web services, Interactive TV, mobile apps, etc.
- Processing involving the use of special categories of data referred to in Article 9.1 of the GDPR, data relating to criminal convictions or offences referred to in Article 10 of the GDPR or data that makes it possible to determine the financial situation or solvency of assets or to deduce information about individuals related to special categories of data.
- Processing that involves the use of data on a large scale. To determine whether a processing can be considered on a large scale, the criteria set out in the WP243 guide "Guidelines on Data Protection Officers (DPOs)" of the Article 29 Working Party will be considered.
- Processing that involves the association, combination or linking of database records of two or more processing for different purposes or by different controllers.
- Processing that involves the use of new technologies or an innovative use of consolidated technologies, including the use of technologies on a new scale, with a new objective or combined with others, in a way that involves new forms of data collection and use with risk to the rights and freedoms of individuals.

These criteria must be taken into account both for the controller itself and for the processor(s) used by the controller.

It is also worth recalling the obligation of processors and sub-processors to assist the controller in carrying out the DPIA and the due diligence of those responsible in the recruitment of processors who offer adequate guarantees.

Given the factors and risk elements inherent to the use of Wi-Fi tracking technology set out in this guide, in general, the conditions for the DPIA to be mandatory in the processing of personal data using Wi-Fi tracking technology will be met. Even in those cases in which the controller may not be clear about the obligation to carry out a DPIA, which does not exclude the analysis and updating of the associated risks, the recommendation of the data protection supervisory authorities, given the risk factors set out in this guide, is to carry it out.

Finally, it should be recalled that, where appropriate, the controller must seek the opinion of the interested parties or their representatives in relation to the intended processing. In particular, in the field of public administrations, it could be appropriate to carry out a participation procedure so that the citizens concerned could express their opinion on the matter, in the case of actions carried out under letters c) and e) of article 6.1 GDPR.

VII. ASSESSMENT OF THE NECESSITY AND PROPORTIONALITY OF THE PROCESSING

The first step in the DPIA process is the obligation to carry out an assessment of the necessity and proportionality of the processing in relation to the purpose pursued, and involves carrying out a balancing exercise according to three criteria: suitability judgment, necessity judgment and proportionality judgment in the strict sense[31].

This evaluation should end with a decision on whether or not to take the treatment, or if necessary, modify it until it passes the three-pronged analysis mentioned above.

The controller should opt for the least privacy-intrusive option that involves the least risk to people.

> Example: A manager intends to control the maximum capacity of a premises in order to guarantee the safety of people. In the implementation of the treatment, you could decide to use basic elements for counting people entering/leaving the premises, use human means, or any other set of sensors, volumetric, CO2, photoelectric cells, pressure cells, video surveillance with some degree of analysis or use Wi-Fi tracking technology. Even if they pursue the same purpose in all cases, some of the options do not in principle involve the processing of personal data, while others may involve processing of personal data with varying degrees of intrusion on the privacy of individuals, we could even speak of high-risk processing for the rights and freedoms of natural persons. and it will be necessary to determine the necessity and proportionality of the various options available.

A. OBJECTIVE ASSESSMENT OF THE APPROPRIATENESS OF TREATMENT

When defining the requirements of the processing that could be implemented with Wi-Fi tracking, it is necessary to determine whether the quality of the data that can be obtained through this technology is suitable for executing the necessary processing actions, taking into account that it will not be infallible.

> Example: Is a treatment to enforce a legal obligation that no more than 30 people are in a certain room. Using Wi-Fi tracking, there may be a situation that some people may not have a phone, be minors without a phone, have it deactivated so as not to be counted or without a battery, others may carry two or more mobile phones (personal, professional, etc.) and all this may depend on age, the type of service, the activity previously carried out and others. Therefore, such a system would not be ideal.
>
> Example: Be a treatment to make decisions about expanding surface area or staff in a customer service. To do this, we want to obtain a statistic of occupancy of a certain premises or waiting room. First of all, it is necessary to determine the level and degree of confidence of the data that allows a decision to be made, for example, 90% +- 2%. This will make it possible to determine which methods or technologies will be appropriate.

B. OBJECTIVE ASSESSMENT OF THE NEED FOR TREATMENT

Depending on the purpose of the processing, a certain degree of singling out may be intrinsically necessary to fulfil the purposes of the processing, but at other times the singling out will not be necessary for the purpose being pursued.

---

[31] Guide to Risk Management and Impact Assessment in the Processing of Personal Data – Section XIII. Assessment of the necessity and proportionality of treatment.

> Example: A treatment that incorporates Wi-Fi tracking in a physical store with several rooms and whose sole purpose is to determine the capacity of each room so as not to exceed the maximum capacity, in principle would not need to single out people in any way. It would be sufficient to determine the total number of devices present at any given time. It might even be unnecessary to process any identifier but only keep track of the Probe Request frames that are being generated.

However, a similar treatment in a museum in which the usual routes between rooms are intended will need to single out individuals at least for certain periods of time and before anonymizing the data to determine, for example, the order of visit of each individual's rooms or a heat map of the busiest spaces.

In any case, for treatments that are already being carried out and it is decided to carry out a technological update that implies a greater intrusion into the privacy of users, it will be necessary to consider what need is being covered that was not previously reached within reasonable margins of effectiveness:

> Example: You intend to update time and attendance using Wi-Fi tracking. Presence control is a treatment that has been carried out for many years with a reasonable degree of effectiveness. It is necessary to consider the need to change to a more intrusive technology that may also incorporate limitations in its effectiveness and possibilities for fraud that are not known.

Likewise, throughout the life cycle of the treatment, it will be necessary to verify that these needs continue to be met and continue to be necessary for the objective purposes of the processing, establishing expiry dates to limit the execution of a treatment that no longer responds to these needs.

VIII. APPROPRIATE TECHNICAL AND ORGANISATIONAL MEASURES

Once the risk factors have been identified and the level of risk of the processing has been determined, this level of risk must be reduced to an acceptable value through appropriate technical and organisational controls and measures, data protection, data protection and privacy by design policies and security measures. These measures should be aimed at reducing the impact or likelihood of the materialization of one or more specific risk factors. Accumulating measures and guarantees without a specific objective can lead to new vulnerabilities.

However, risk management for the rights and freedoms of data subjects should not be confused with strict compliance with the rest of the precepts and principles imposed by data protection regulations. The nature of the GDPR gives freedom to the controller and the processor in the way to implement the guarantees of compliance with the principles and other obligations of the GDPR, without this implying that the controller or the processor can choose which precepts to comply with and which not.

One of the data protection measures to be applied by design is anonymization, but it is not the only possible option, nor should the responsible party renounce the application of other additional measures such as differential privacy[32], "compute-to-data" and others.

In its Legal Report 2019/017, the AEPD highlights the obligations for data controllers who use Wi-Fi tracking technology. They should be understood as obligations established by data protection regulations and which may also include some technical and organisational measures. Some of them are listed below:

- Measures should be taken to ensure the early anonymisation[33] of data.
- The area in which the Wi-Fi tracking is carried out must be assessed. For example, in the private sphere, the existence of a commercial relationship will be taken into account, so that they are customers or potential customers, avoiding, in any case, their use on public roads.
- The areas in which it is carried out must be limited and delimited, avoiding control of movements in very large areas, as well as in those that may involve excessive interference with the privacy of the person, such as, for example, in the case of toilets.
- They may not be used, without the consent of the data subjects, in areas where they may reveal special categories of data, such as those containing health-related products.
- Under no circumstances may the geolocation data obtained in this way be cross-referenced with other data from other sources (such as credit card payments or images captured by video surveillance systems) that may allow the identification of the person.
- In accordance with the criterion of data minimisation, even if the data collection had to be continuous, the storage and subsequent processing operations of the position must be limited to indicating the areas indicated as being of interest, preventing a detailed and continuous collection of the movements of the interested parties.

[32] Anonymization and pseudonymization (II): differential privacy.

[33] Not to be confused with pseudonymization of data.

- The data collected from a data subject on the premises of different managers must not be cross-referenced. If the controller has several premises, different identifiers must also be collected.
- The same identifier should not be assigned to the same mobile device during the different visits made over time to the same location.
- Access to the Data Controller's Wi-Fi will not be conditional on the data subject's consent to data processing through Wi-Fi tracking.
- Where the legal basis for the processing is the legitimate interest of the controller or the fulfilment of a task in the public interest, data subjects must be allowed to exercise their right to object by opt-out of the collection of their data[34].
- It must be ensured that individuals are fully aware that their personal data is being processed at all times, as well as the exercise of their rights under the GDPR.
- In the same vein, the French Commission Nationale de l'Informatique et des Liberté (CNIL)[35] and the EDPB[36] express themselves, in particular, the latter also indicating the following measures:
- Anonymization must be carried out immediately after collection, so that re-identification is technically excluded.
- If immediate anonymisation is not possible in view of the purpose (e.g. because you are recording a trajectory), personal data may be processed for a period in which they are not anonymised only under the following conditions:
    - The purpose of data collection should be limited to mere statistical counting.
    - Tracking is limited in time and space to the extent strictly necessary for this purpose.
    - The data is deleted or anonymized immediately afterwards.
    - There is an effective possibility of opting out

Controllers must also take other mitigation measures to ensure that there is no impact on the fundamental rights of third parties, for example, protecting the privacy of individuals living next to a collection point.

In section VIII. Risk Mitigation Controls The Guide to Risk Management and Impact Assessment in Personal Data Processing presents a comprehensive overview of risk mitigation controls that may be appropriate for any processing of personal data. The responsible party who decides to implement a treatment with Wi-Fi tracking technology must implement all those that are applicable to the specific treatment they intend to carry out.

Below are some relevant technical and organisational measures that could help manage risks in processing that incorporates Wi-Fi tracking technology.

A. ANONYMIZATION

Anonymization is a processing of personal data that generates, from a set of personal data, a new set of anonymous information.

Like any processing, it must comply with the principles of the GDPR, including the principle of proactive responsibility. This implies that the controller must take the appropriate measures

[34] Using probe requests with random MACs can seriously hinder the ability to offer an opt-out option.

[35] CNIL: Audience and attendance measurement devices in spaces accessible to the public: the CNIL recalls the rules

[36] Opinion 01/2017 on the proposal for a regulation on privacy and electronic communications (2002/58/EC) (WP29,WP247)

to carry out the anonymisation processing with the necessary guarantees and, in particular, must consider what risk the anonymisation process poses to individuals that the anonymisation process can be reversed.

The AEPD makes available to those responsible various tools with extensive information on the anonymisation of data on the Innovation and Technology microsite , as well as the Opinion 05/2014 on anonymization techniques of the Article 29 Working Party.

The anonymization process is not a trivial process and involves a probability of re-identification that depends on several factors, including:

- The point at which the data is anonymized. In general, the earlier the anonymization of the data, the less personal data is processed and the lower the risk to data subjects[37]. However, in order to carry out certain purposes in a processing, it may be necessary to anonymise at a later stage. For example, when the aim is to track people's trajectories over a significant time interval, there is a possibility that the data will be stored unanonymized for extended periods of time. Late anonymization of data increases some risks.
- Anonymization technique used: There is a risk of using weak anonymization procedures that can be reversed.
- Regardless of the proposed anonymization, there may be specific circumstances such as the existence of uncrowded areas at certain times or the availability of several location points on the same device[38], where it would be easy to identify the person or even their behaviors.

For all these reasons, after anonymisation, the controller must determine by means of analysis and practical tests that it is not possible to re-identify the data set. The controller must carry out an analysis of the risks of re-identification and consider the conditions of the worst-case scenario, and it is advisable that they be carried out by a third party periodically. If, under these conditions, all or part of the dataset can be re-identified, there is no risk of re-identification, the dataset is simply not anonymous.

As for the timing of anonymization, early anonymization is the most effective measure to protect people's rights and freedoms.

To do this, it is necessary to bring the anonymization process as close to the moment of data acquisition as possible. A system that acquires personal data and anonymises it at the point of acquisition, before any other type of processing and even before it is stored, will generally entail fewer risks to the rights and freedoms of individuals than a system that anonymises the data after a few hours, days or months.

In essence, whenever possible, anonymization should be applied immediately and as close as possible to the point of data collection, preferably locally on the capture device.

In cases where the aim is to delay the time at which anonymisation operations are carried out, early pseudonymisation should be applied until such time as anonymisation is possible. However, pseudonymization cannot be a substitute for anonymization, nor does pseudonymization of data justify delaying or not applying data anonymization.

[37] Article 25.2 GDPR.

[38] de Montjoye, YA., Hidalgo, C., Verleysen, M. et al. Unique in the Crowd: The privacy bounds of human mobility. Sci Rep 3, 1376 (2013).

B. MASKING MAC ADDRESSES AND METADATA

Masking is a technical data protection measure widely used in the processing of personal data. The masking of unique identifiers, such as the MAC address, at the same time as data capture and through the same capture interface before it is stored even in logs, is a measure that in certain scenarios can be effective in making it difficult to single out and identify people.

> Example: A MAC address has 24 bits identifying the manufacturer and 24 bits for free assignment by the manufacturer. If you want to control different people in a room, it may not be necessary to use 48 bits, it is possible to mask from the moment of data capture and use only a fragment of the MAC address, for example the last 24 bits. If you want to distinguish 1000 people at once, with 14 bits there will only be a 6% chance that two will match. If you want to distinguish between 100 people, with 11 bits there will only be a 5% chance that two will coincide.

However, this technique will not be useful when the MAC address is not the identifier used or devices send the Probe Request frames with random MAC addresses. When what is used to identify user devices is a fingerprint, the masking of metadata at the time of capture will be the measure to be applied to make it difficult to single out and identify people.

C. SEPARATION

It consists of implementing measures that allow data captured in different geographical areas and in different periods of time to be decoupled.

> Example: The fingerprints of the device (or any other identifier) are replaced by a hash with salt, with the particularity that a different salt is used in each location and that changes randomly from time to time (every 12/24 hours).

D. AGGREGATION

It consists of grouping information relating to several subjects using generalization and suppression techniques[39]. It is used when no individual records are required and the aggregated data is sufficient for the purpose pursued, as may be the case in some treatments that use Wi-Fi tracking.

> Example: To obtain heat maps of the main trajectories followed by people in a museum, unique identifiers would not be necessary, a simple statistical count would suffice.

E. DATA MINIMIZATION

It consists of adopting measures aimed at ensuring compliance with the data minimisation principle established in the GDPR (personal data shall be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed") in the design of processing using Wi-Fi tracking. Practical examples of this would be:

- Limit the period of activity of the sensors to the minimum necessary.
- Limit the area subject to Wi-Fi tracking, avoiding including private areas.
- Limit as much as possible the area subject to monitoring of people's trajectories[40].
- Prevent the capture and storage of data from Wi-Fi frames that facilitate the identification of individuals (e.g., SSID).

---

[39] K-anonymity as a measure of privacy.

[40] Only when it is necessary to monitor trajectories for the purpose pursued by the treatment.

- Avoid capturing data from certain types of devices (fixed devices, IOT sensors, body/healthcare implants, etc.).

F. DATA RETENTION PERIOD

As in any processing of personal data, the effective limitation of the retention period of the data, both non-anonymised and anonymised due to the residual risk of re-identification, is particularly relevant.

G. THIRD-PARTY AUDITING AND SECURITY MEASURES

Security measures must be understood in a broad sense. In the case of processing implemented by Public Administrations, the information systems used will be subject to the National Security Scheme (ENS)[41] in the category corresponding to the level of risk to rights and freedoms according to the corresponding DPIA. This obligation also includes information systems of private sector entities, when they provide services or solutions to public sector entities for the exercise of their administrative powers and competences. The appropriate security measures are not limited to those listed in the ENS, but must be extended, if possible, to those necessary to ensure a level of security appropriate to the risk to the fundamental rights and freedoms of each specific processing in accordance with Article 32 of the GDPR.

In the case of processing that is not subject to the obligation to comply with the ENS, the necessary measures will have to be implemented to manage the level of risk to the fundamental rights and freedoms of each specific processing in accordance with Article 32 of the GDPR.

It should be recalled that Article 32 of the GDPR, in its section 1.d), requires a process of regular verification, evaluation and assessment of security measures.

Independent third-party audits help demonstrate compliance with security measures appropriate to the level of risk to fundamental rights.

H. ORGANISATIONAL AND PROCESSOR MEASURES

The GDPR requires controllers to perform due diligence to ensure that the processing complies with data protection regulations and to be in a position to demonstrate this.

The controller shall select processors with sufficient guarantees to implement appropriate technical and organisational measures so that the processing complies with the requirements of the GDPR. This provision also extends to processors when they subcontract processing operations to other sub-processors.

The processing by the processor shall be governed by a contract or any other equivalent legal relationship. Likewise, the processor may not process the data for its own purposes, but only following the documented instructions of the controller, and avoiding international data transfers without sufficient guarantees.

In accordance with the obligations of the GDPR for data processing contracts, they must explicitly contain clauses that prevent the use of another processor without the prior written authorisation of the controller and the processing of personal data by the processor for its own purposes, or, where appropriate, that limit and conditions what processing compatible

[41] First additional provision of the LOPDGDD: "Security measures in the public sector: 2. The controllers listed in article 77.1 of this organic law must apply to the processing of personal data the security measures that correspond to those provided for in the National Security Scheme, as well as promote a degree of implementation of equivalent measures in companies or foundations linked to them subject to private law."

with the purpose of the initial processing can be carried out by the processor on its own behalf. In addition, they must explicitly state the response to a personal data breach that may occur in the processor, both for the processing carried out on behalf of the controller and for possible processing by the processor itself.

The controller must ensure that international data transfers are prevented without adequate safeguards.

Equally, controllers must implement data protection measures by design and by default to minimise the risks to rights and freedoms that could be caused by a personal data breach. With regard to security measures, it should be recalled that, according to the experience and doctrine of the Supreme Court[42], they are an obligation of means, but not of ends.

In general, in the processing of personal data using Wi-Fi tracking, it is especially important to consider the probability of a breach of confidentiality, so the controller must adopt a priori measures to minimise the risks to the interested parties and, in the event that they occur, provide for the response of the controller and processors to minimise the impact on the rights and freedoms of individuals. It is important to identify in advance the degree of responsibility of each of the parties involved in the processing in the different scenarios in which a confidentiality breach may occur, and what obligations each of them will undertake to properly manage the breach, including the obligations of notification to the competent data protection supervisory authority and communication to those affected, when they are mandatory.

I. CONTINUOUS RISK MANAGEMENT

The controller must analyse the risks of the treatment in the light of all its particularities and circumstances, and if at any time there is a change in the treatment or in factors affecting the treatment, the risks must be reassessed and managed.

The GDPR (Article 24) and Organic Law 7/2021 (Article 27 transposing Article 19 of Directive 680/2016) require the controller to review and update the measures implemented in the processing to ensure that it complies with data protection regulations. The regulation itself establishes that such review and updating must be carried out when necessary[43].

[42] C.G.P.J - Judicial News (poderjudicial.es)

[43] When data protection measures need to be reviewed.

IX. TRANSPARENCY AND INFORMATION

It should be considered that the use of Wi-Fi tracking technology in which information is collected as a result of communication between a terminal (mobile phone or any other device) of a natural person and a Wi-Fi network, in order to generate a digital fingerprint of the device that differentiates it from other terminals, may involve the processing of personal data. and therefore the controller and processor must respect the principles and rights set out in the GDPR.

Among these principles, Article 5.1 a) of the GDPR recognises the principle of transparency together with the principles of lawfulness and fairness.

The particularity of the fact that this processing may go unnoticed by the owners of the terminals makes it even more necessary to comply with the principle of transparency through clear and accessible information.

Article 13 of the GDPR details the necessary information that must be provided to the data subject when personal data is obtained from the data subject.

Persons must be previously informed in relation to the following aspects:

- Identity and contact details of the data controller and, where applicable, their representative.
- Contact details of the data protection officer.
- Purposes and legal basis of processing.
- Legitimate interests of the controller or a third party.
- Recipients or categories of recipients of personal data.
- Planned international transfers.
- Retention period.
- Rights of access, rectification or deletion, limitation of processing, opposition and portability.
- Possibility of revocation of consent.
- Right to lodge a complaint with a supervisory authority.

A. LAYERED INFORMATION

- The information provided should be concise, transparent, accessible, easy to understand and presented in clear and simple language, especially that aimed specifically at children.
- Thus, article 11 of the LOPDGDD has provided that the controller may comply with the duty of information established in article 13 of the GDPR, providing the interested party with basic information, and indicating an electronic address or other means that allows simple and immediate access to the rest of the information (this is what has come to be known as "layered information").

The minimum content that basic information should have is:

- The identity of the data controller.
- The purpose of the processing.
- The possibility of exercising the rights set out in Articles 15 to 22 of the GDPR.
- Information on whether the personal data obtained is to be processed for profiling, and on your right to object to automated individual decision-making that produces legal effects on the data subject or similarly significantly affects him/her, where this right is exercised pursuant to Article 22 of the GDPR.

- The information will be provided in writing or by other means, including electronic, if applicable. Information may be provided orally, at the request of the data subject, provided that the identity of the applicant is established by other means.

The Article 29 Working Party Guidelines on transparency under the GDPR, adopted on 29 November 2017 (revised on 11 April 2018), identified as possible ways of transmitting information to data subjects, in an environment such as Wi-Fi tracking, the use of:

- Clearly visible dashboards with information.
- Public signage throughout the coverage area.
- public information campaigns.
- icons (standardised icons that provide an easily visible, intelligible and clearly legible overview of the intended processing, in accordance with Art. 12.7 GDPR).
- Voice alerts.
- Written details included in setup instructions.
- Videos embedded in digital setup instructions.
- written information about smart devices, SMS or email messages.

In the specific case of the use of these technologies by public administrations, the following set of transparency measures is additionally recommended, through the publication of[44]:

- A record of Wi-Fi tracking sensors deployed on public roads.
- The specific objectives to be pursued, indicating the start and end dates of the treatment.
- An adequate excerpt (without sensitive information) of the impact assessments that are carried out.
- The relevant information from the anonymization algorithms used.
- Information accessible in several languages if it were an area with a large influx of tourists.

In any case, in accordance with Article 31 of the LOPDGDD, data controllers and processors or, where appropriate, their representatives must keep the register of processing activities referred to in Article 30 of the GDPR, unless the exception provided for in section 5 applies. The subjects listed in article 77.1 of the LOPDGDD must make public an inventory of their processing activities accessible by electronic means and their legal basis.

[44] More information is available at:

https://www.autoriteitpersoonsgegevens.nl/uploads/imported/investigation_report_development_of_dutch_smart_cities.pdf

X. EXERCISING RIGHTS UNDER THE GDPR

In accordance with Article 11 of the GDPR, if the purposes for which a controller processes personal data do not or no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, obtain or process additional information with a view to identifying the data subject for the sole purpose of complying with the GDPR, and in such cases, if the controller is able to demonstrate that it is not in a position to identify you, it will inform you accordingly, if possible, and Articles 15 to 20 of the GDPR (rights of access, rectification, erasure, right to restriction of processing, and data portability) will not apply, except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.

This will be the case when the controller has carried out a process of anonymisation of the personal data processed and is able to demonstrate that it is not in a position to identify the data subject. Articles 15 to 20 of the GDPR will not apply to anonymised data, but they will apply to personal data that the controller is processing in processing phases prior to its anonymisation.

The controller shall be obliged to inform the data subject of the means available to him or her to exercise the rights recognised in Articles 15 to 22 of the GDPR. The means must be easily accessible to the person concerned. The controller should establish visible, accessible and simple mechanisms, including electronic means, for the exercise of rights. These mechanisms, in particular, in the case of exercise by electronic means, must incorporate procedures to verify the identity of the affected persons who use them, as well as the receipt of the exercise of the corresponding right, and its timely response.

A. RIGHT OF ACCESS (ARTICLE 15 GDPR)

The data subject has the right to obtain confirmation from the controller as to whether or not personal data concerning him or her is being processed and, if so, the right of access to the personal data and information detailed in Article 15.1 of the GDPR.

The exercise of the right of access on more than one occasion during the period of six months may be considered repetitive, unless there is a legitimate cause for it (art. 13.3 LOPDGDD), in which case the data controller may charge a reasonable fee based on the administrative costs or refuse to act on the request. In any case, the data subject has the right to know and to be informed, in particular, of the purposes for which the personal data are processed, the categories of personal data, the recipients, the storage period, information on their origin, the existence of automated decision-making, including profiling as referred to in Article 22 of the GDPR and, at least in such cases, information on the logic applied, as well as the significance and expected consequences of such processing for the data subject.

Even when the controller has carried out anonymisation processes by which it is unable to identify the data subject's data and provide a copy of the personal data subject to processing, it must provide all the necessary information about the processing in order to comply with the principle of transparency.

B. RIGHT TO ERASURE (ART. 17 GDPR)

The data subject has the right to obtain without undue delay from the controller the erasure of personal data concerning him/her in any of the following circumstances:

- The personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed.

- The data subject withdraws the consent on which the processing is based in accordance with Article 6(1)(a) or Article 9(2)(a) of the GDPR and the processing is not based on another legal basis.
- The data subject objects to the processing pursuant to Article 21(1) of the GDPR, and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2) of the GDPR.
- The personal data has been processed unlawfully.
- Personal data must be erased in order to comply with a legal obligation under Union or Member State law that applies to the controller.
- The personal data has been obtained in connection with the provision of information society services referred to in Article 8.1 GDPR.

Where the controller has made the personal data public and, in any of the circumstances referred to, is obliged to erase such data, taking into account the available technology and the cost of its implementation, it shall take reasonable measures, including technical measures, with a view to informing the controllers processing the personal data of the request, of the data subject, to delete any link to that personal data, or any copy or replica thereof.

Personal data will not be deleted in the cases referred to in Article 17.3 of the GDPR.

The data controller will be obliged to block the data when it is deleted (article 32 of the LOPDGDD). The blocked data will be at the exclusive disposal of the judges and courts, the Public Prosecutor's Office or the competent Public Administrations, in particular the data protection authorities, for the enforcement of possible liabilities arising from the processing and for the limitation period thereof. After this period, the data must be destroyed. Blocked data may not be processed for any purpose other than those indicated above.

The controller shall notify each of the recipients to whom the personal data has been communicated of the erasure, unless this is impossible or requires a disproportionate effort, and shall inform the data subject about these recipients if the latter so requests (Article 19 GDPR).

C. RIGHT OF RESTRICTION OF PROCESSING (ART. 18 GDPR)

It allows the data subject to request the controller to suspend data processing when:

- The accuracy of the data is contested, while the accuracy is verified by the controller.
- The data subject has exercised his/her right to object to the processing of data, while it is verified whether the legitimate grounds of the controller prevail over those of the data subject.
- Request the controller to retain your personal data when:
    - The data processing is unlawful and the data subject opposes the erasure of his or her data and instead requests the restriction of its use.
    - The controller no longer needs the data for the purposes of the processing, but the data subject does need them for the establishment, exercise or defence of legal claims.

Subject to limited processing of the personal data of the data subject, such data may be processed, with the exception of their retention, only with the consent of the data subject himself or for the establishment, exercise or defence of legal claims, or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

The fact that the processing of personal data is limited must be clearly stated in the information systems of the data controller (article 16.2 LOPDGDD).

Any data subject who has obtained the restriction of processing will be informed by the controller before the restriction is lifted.

The controller shall communicate the restriction to each of the recipients to whom the personal data has been disclosed, unless this is impossible or requires a disproportionate effort, and shall inform the data subject about such recipients if the latter so requests (Article 19 GDPR).

D. RIGHT TO DATA PORTABILITY (ARTICLE 20 GDPR)

The data subject has the right to receive the data provided to the controller in a structured, commonly used and machine-readable format, and to have the data transferred to a controller be transmitted directly to another controller, provided that the processing is based on the consent of the data subject or within the framework of the performance of a contract and that such processing is carried out by automated means.

However, this right does not apply where the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

E. RIGHT TO OBJECT (ART. 21 GDPR)

The data subject has the right to object at any time, on grounds relating to his or her personal situation, to the processing of personal data concerning him or her by the controller on the basis of Article 6(1)(e) and (f) of the GDPR, including profiling on the basis of those provisions.

Upon exercise of the right to object, the controller shall cease to process the personal data, unless it proves compelling legitimate grounds for the processing that override the interests, rights and freedoms of the data subject, or for the establishment, exercise or defence of legal claims.

The right to object must be explicitly communicated to the person concerned, presented clearly and regardless of any other information.

Data subjects should be made easy to object to the processing.

As an additional guarantee to reduce or mitigate the impact on the data subjects, whose personal data is collected through Wi-Fi tracking, the controller could choose to enable a general "opt-out", beyond the objection itself; ceasing to process data without the need for any justification.

F. AUTOMATED INDIVIDUAL DECISION-MAKING, INCLUDING PROFILING (ARTICLE 22 GDPR)

The very nature of Wi-Fi tracking technology makes it feasible to carry out Wi-Fi tracking-based processing that involves automated decision-making, including profiling.

The data subject has the right not to be subject to a decision made by the controller based solely on the automated processing of his or her personal information, including profiling, which produces legal effects on him or similarly significantly affects him/her.

However, it will be lawful to carry out the processing and make an automated decision:

- Where it is necessary for the conclusion or performance of a contract between the data subject and a controller or when it is based on the explicit consent of the data subject.
- Where it is authorised by Union or Member State law, applies to the controller and also provides for appropriate measures to safeguard the rights and freedoms and legitimate interests of the data subject.

In both cases, the controller shall take appropriate measures to safeguard the rights and freedoms and legitimate interests of the person concerned, at least the right to obtain human intervention from the controller, to express his or her point of view and to challenge the decision.

Special categories of personal data referred to in Article 9(1) of the GDPR shall not be used in such processing, unless the processing is carried out with the consent of the data subject or it is an essential public interest imposed by Union or Member State law. In such cases, it shall be ensured that appropriate measures have been taken to safeguard the rights and freedoms and legitimate interests of the person concerned.

XI. ARTIFICIAL INTELLIGENCE REGULATION

Given the current technological situation, it is possible that personal data processing will be carried out in combination with the use of Wi-Fi tracking technology and artificial intelligence (AI) systems. This type of processing of personal data is subject to the system of principles, obligations for controllers and rights for data subjects established by the GDPR. Additionally, the use of certain AI systems will be regulated by the Artificial Intelligence Regulation (RIA).

At the time of publication of this Guide, the Artificial Intelligence Regulation (RIA) has not yet been published, which will enter into force within 20 days of its publication and will be applicable in most of its provisions two years after its publication.

From the perspective of personal data protection, the RIA is not intended to affect the application of the fundamental right to data protection. The RIA is complementary to the GDPR and shall apply without prejudice to the GDPR for the purpose of enabling controllers and processors to be in a position to comply with their data protection obligations when incorporating AI systems into their processing (recital 78 GDPR) to implement data protection by design of the processing.

Therefore, the placing on the market, the commissioning and use of AI systems should facilitate effective implementation and allow the exercise of data subjects' rights and other remedies guaranteed by data protection law, as well as other fundamental rights.

This includes the obligations of providers and those responsible for the deployment, or of other actors and operators where applicable, of AI systems to the extent that the design, development or use of AI systems involve the processing of personal data, as well as the roles and powers of independent data protection supervisory authorities. Among others, the latter shall have the power to request any documentation created or maintained under the RIA relating to high-risk AI systems referred to in Annex III to that Regulation where access to such documentation is necessary for the effective performance of their powers.

It should also be clarified that data subjects continue to enjoy all the rights and guarantees conferred on them by data protection regulations, including rights related to fully automated individual decisions, such as profiling.

In this sense, as an example, when, based on the data obtained through Wi-Fi tracking technology as input information, decisions are implemented that produce legal effects for a person or significantly affect him or her through artificial intelligence systems (regardless of the type they are) based solely on the automated processing of personal data, the provisions of the GDPR will apply (articles 13, 14, 15 and 22 and recital 71 of the GDPR).

In addition, for this case, in the specific case where the artificial intelligence system on which the decision is based is high-risk according to the RIA, in addition to the rights provided for in the GDPR, when the individual considers that the decision has an adverse impact on their health, safety or fundamental rights, the provisions of the AI Regulation shall apply in relation to the fact that the data subject may have the right to receive clear and meaningful explanations about the role of the artificial intelligence system in the decision-making procedure and the main elements of the decision taken.