Centro Nazionale
IOTePRIVACY

Whitepaper:

Physical Audience Measuring Technologies and Privacy Concerns

Analysis of the technological landscape and suggested best practices for the industry

v.01/2020

▸ Coordinating bodies

The **National Centre for IoT & Privacy** is a monitoring center for the in-depth study, discussion, research and updating of matters relating to the Internet of Things and the application of regulations on the protection and valorization of data and privacy. It focuses on the work of corporate Data Protection Officers, Data Protection Designers, and innovation 4.0-oriented organizations. The Centre also maintains relations with institutions and associations, in both Italy and Europe, to develop an ongoing dialogue on the issues it deals with.

▸ Contributors

The whitepaper and the related web tool are the result of a working table between some of the operators in the Audience Measuring Technologies sector. The study and analysis work, which lasted more than eight months, was held from September 15, 2019 to May 15, 2020.

Work Coordination

- Giulio Messori, CRCLEX
- Alex Buzzetti, Blimp.ai

Contributors

- Andrea Acquaroni, fabbricadigitale
- Luca Milanesi, fabbricadigitale
- Erika Salvatore, Clearchannel
- Marco Emanuele Carpenelli, Istituto Italiano Privacy
- Carlo Rossi Chauvenet, Centro Nazionale IoT e Privacy, CRCLEX.
- Luca Bolognini, ICT Legal Consulting and Istituto Italiano Privacy
- Francesco Carparelli, Luxottica
- Sabrina Costanzo, Luxottica
- Marco Orlandi, Grandi Stazioni Retail
- Flavia Quitadamo
- Alessandra Capomagi
- Michele Casali

▸ Promoters

CRCLEX is an Italian law firm dedicated to assistance in Digital, Enterprise and Family legal matters. Founded in 1982, today it has offices in Milan and Padua and an international network of professionals. In 2020 it was nominated a finalist among the Italian law firms in the Technology & Intellectual Property category for 'Il Sole 24 Ore' and a finalist in the Technology category for TopLegal.

The **Italian Institute for Privacy and Data Valorizations (IIP)** is a center for studies and advocacy funded by private subjects (individuals, associations, law firms and even multinational companies), as well as by the European Commission (under the Horizon 2020 Program for the Privacy Flag, Anita, NGIoT and Prevent projects). The institute dedicates itself to the issues of protection and valorization of personal data, information, and identity in the global ICT society. IT brings together many of Italy's leading privacy law specialists, as well as significant figures from both the public and private sectors who deal with sensitive personal data daily. Operating as a think tank, IIP is a point of reference for Italian experts in "new law" and numerous other players on the high-technology markets.

Index

Introduction

Purpose of the white paper

Today, technologies capable of detecting, measuring, or counting natural persons have become a reality, and the characterizing element of the growth and definitive affirmation of a new, global Audience Measurement market.

With this in mind, if on one hand the growth prospects for businesses operating in this sector are evident, on the other there are still some questions regarding the impact of these technologies on the rights and freedoms of EU citizens and the protection and distribution of personal data.

This white paper aims to make an initial step toward researching and analyzing the impact these technologies could effectively have on the protection of personal data.
In concrete terms, the paper aims to: i) offer an initial description of Audience Measurement technologies; ii) a study and systematic definition of the "state of the art" of the rulings and sentences (in jurisprudence) issued by European judicial bodies and data protection authorities and; iii) an analysis of other relevant technical studies, and in conclusion iv) share the guidelines developed from the above analyses, and; v) share the various case studies.

While initially developed by a group of Italian professionals, our study aims to extend to the rest of Europe, given that this is certainly the scope of the technology and, above all, the jurisdiction in which shared regulations such as EU 679/2016 operate (the General Data Protection Regulation).

Before proceeding, we wish to draw your attention to another significant white paper analyzing the marketing and business characteristics of one particular Audience Measurement technology, published by the Interactive Advertising Bureau (IAB) Italy, which highlights certain fundamental points in the definition of this new industry in its "Guidelines for the sale of advertising space and audience measurement" dated November 2018. Given its scope and relevance, we refer you to this study for a more in-depth analysis of characteristics mentioned above.

This white paper instead aims to offer a more strictly juridical analysis, specifically referred to Europe as a whole.

Laws and regulations to consider before reading

The following legal texts were consulted in the preparation of this white paper, to which we refer you for any further information:

🇪🇺 **Europe**

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), for brevity the "**GDPR**";

🇮🇹 **Italy**

- Legislative Decree no. 196/2003, Personal Data Protection Code, or "Privacy Code", as amended by legislative decree no. 101 dated 10 August 2018.[1]

Relevant definitions to consider before reading

The following standard definitions are used throughout the document.

Supervisory Authority or Privacy Authority: the independent public authority responsible for monitoring the application of personal data protection regulations, provided by each Member State in pursuance of article 51, GDPR.

Consent of the Data Subject or Consent: the legal basis for lawful processing of personal data, foreseen under art. 6(a) GDPR. Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her;

Anonymous Data: data rendered anonymous in such a way that a natural person is not or no longer identifiable (e.g. numbers, alphanumeric characters). As opposed to anonymized data, this category has not been subject to any anonymization process (e.g. from personal to anonymous data)

Anonymized Data: data rendered anonymous in such a way that a natural person is not or no longer identifiable (e.g. numbers, alphanumeric characters), but which has undergone a process of anonymization (e.g. from personal to anonymous data) to render it so.

[1] Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU Serie Generale n.205 del 04-09-2018).

Biometric data: means personal data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or fingerprint data.

Personal Data: means "any information relating to an identified or identifiable natural person ('data subject') as established by art. 4(1) GDPR. 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 on-line identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Sensitive Data: means Personal Data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and the processing of genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation, for the purpose of uniquely identifying a natural person;

Data concerning Health: means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

DPO or Data Protection Officer: means the natural person designated by the Controller or Processor, on a mandatory basis in the cases foreseen by art. 37 (1) GDPR, on the basis of their expert knowledge of data protection law and practices, to inform and advise them of their obligations pursuant to the GDPR;

Authorized Persons: means Collaborators authorized to Process Personal Data under the direct authority of the Controller and/or Processor in pursuance of arts. 4(10) and 29 GDPR.

Automated Decision Process: a decision based solely on automated Processing, including Profiling, which produces legal effects concerning the data subject or similarly significantly affects their person.

Profiling: means any form of automated Processing of Personal Data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

Pseudonymization: means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

Data Processor or Processor: means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller; the Processor must provide sufficient technical and organizational measures to ensure the Processing meets the requirements of the Regulation and protects the rights of data subjects;

Processing Controller or Controller: means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law

Processing: means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Personal Data Breach (Data Breach): means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

1. Physical Audience Measuring and data processing activities

In this chapter we describe several categories of technology used to measure and count audience. For each technology, in addition to an initial - brief - technical explanation, we define the categories of data that may be processed, and the relevant decisions and technical studies

The technology categories we analyze here are:

1) Image acquisition-analysis systems.
2) Radio frequency systems.
3) Cell network data acquisition systems.
4) SDK, Beacon and Bidstream systems.
5) Occupancy detection systems

1.1 Image or video stream analysis-acquisition systems

1.1.1 The technology

This category includes all technologies based on the use of video or photo cameras. More generally, it includes all systems cable of acquiring and processing a sequence of photographs or a video clip.
The frame sampling rate depends on the available processing capacity. If the rate is high, video sampling is possible. However, we point out that this category of systems differs in all respects from video surveillance systems, a technology requiring separate analysis and, in any case, strictly regulated.

⚙ **Functioning:** in most cases, image or video stream analysis-acquisition systems acquire a snapshot or video sequence of the area where the audience is to be measured. The snapshot or video is then processed by the measuring system computer, which extracts the required information.

The acquisition has limited duration and takes place in the area and at the same moment the photograph or video is acquired. The data is stored in the computer's volatile memory (RAM) for the time necessary for processing. After processing the data is erased. If properly implemented in technical terms, this measure prevents any image or video from being viewed, stored in the memory, transmitted to third parties, or otherwise processed further. This measure also prevents any kind of reverse engineering with the purpose of identifying any specific subject in any given area.

The data extracted from the photographs or videos are sent to a server for aggregation and display via a dedicated dashboard. Data transfer to the server is generally through an internet connection of the type most used, such as Ethernet, Wi-Fi, or data connection device.

1.1.2 Data categories

Depending on the setup and the technology used, the systems can process different types of personal data, as defined by art. 4(1) of the GDPR, these being:

1) **Photographs**: under EU Regulation 679/2016, photographs are classed either as Personal Data (as per art. 4(1) GDPR) or Biometric Data (as per art. 4(14) GDPR). The distinction between the two categories is made clear by Recital 51 GDPR, which points out that:

   "*The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the **unique identification or authentication of a natural person**.*".

   The determining criteria is therefore the technical possibility of identifying (or authenticating) a person.

2) **Video recordings**: video recordings can be classed as Personal Data (as per art. 4(1) GDPR) since technically composed of a series of frames (potentially) capable of identifying a natural person.

💡 **Focus Box: Face Detection vs. Face Recognition**

The term face detection refers to technologies capable of detecting the presence of a human face in an image or video. On the contrary, facial recognition technology not only detects the presence of a face but is able to associate the face with a specific person. Recognition is achieved by comparing the face identified by the algorithm with the facial images present in a reference database.

Through aggregation and anonymization processes it is possible to extrapolate new, strictly anonymized, and numerical audience data from Photographs and Video recordings, such as:

- the number of pedestrians or vehicles present in the area.
- the number of subjects of a given type.
- the number of subjects in each age group.
- the aggregate number of persons in each emotional state (e.g. 500 sad people, 200 happy, etc.).
- the number of faces.

1.1.3 Relevant rulings

The case studies on the technologies analyzed here come from the Italian Personal Data Protection Authority, and are:

a) **Ruling no. 13 dated 21 January 2016**
b) **Ruling no. 551 dated 21 December 2017.**

While both of the case studies date to before EU Regulation 679/2016 came into effect, here we feel it appropriate to briefly review the reasoning in fact and in law applied by the Authority, in that they certainly constitute key rulings for the players in the sector, in terms of continuity.

a) The Italian Data Protection Authority: “Prior check. Person detection system for marketing purposes” - **Ruling no. 13 dated 21 January 2016**”

In the case in question, Banca Monte dei Paschi di Siena S.p.A. made an application for prior check on a “pilot” project to install a person detection system for marketing purposes in one of its branches.

The **technology** installed would consist of a “system to detect the passage and dwell time of customers and non-customers, consisting of three distinct components: […] The first, called "Heatmap", is designed to “optimize the layout of the branch", including the arrangement of the various places the services are provided, and to generate automatic messages, for example, in case of long waiting times; the second, called "People counter", consists of a system of cameras for counting the people passing through the Branch; the third, known as "Dwell Time", would be capable of counting individuals "looking at the monitors in the windows" outside the branch and the "totems inside the branch", as well as counting the time each individual remains in front of the "advertising message" (see memo dated 18 February 2015), with the purpose of evaluating its level of attraction”.

The **purpose** of the installation was to “adequately measure accesses to the branch and attention to the promotional messages, in order to determine the rate of products sales with respect to the number of visitors to the individual Branch, thereby evaluating the advertising return of messages "transiting on the monitors", as well as to manage the staff more precisely and plan optimal business hours for customers”.

The **outcome** of the Prior Check was positive: The Supervisory Authority allowed “Banca Monte dei Paschi di Siena S.p.A. to use person detection systems for marketing purposes with a view to improving the services provided to customers” and, furthermore:

1. stressed the need to **verify respect of the principles of necessity, proportionality, purpose, fairness, and lawfulness, in concrete terms**;
2. prescribed a **simplified privacy notice**, **to supplement** with “more complete information available in the branch, available on website or through the QR code on the window banner”;
3. allowed, with **adequate precautions** to protect the fundamental rights and freedoms of the data subjects, as well as their privacy and dignity, the use of the “Heatmap”, “People Counter” and “Dwell Time” systems. In specific terms, this was **thanks** to the “attention paid to the **use of cameras as mere sensors**, the use of **processing software capable of extracting statistical data** from **images taken almost immediately, without biometric processing, image recordings or live access** [...]”;
4. underscored the need for the system to carry out the processing without recording the images and **limiting it to real time display exclusively to processors responsible for maintenance of the equipment**,
5. recognized [with respect to consent, *Ed*,] “**balance of interests** as an **alternative legal basis**, pursuant to art. 24, paragraph 1, point g) of the Code, when image detection is

carried out by Banca Monte dei Paschi di Siena S.p.A. on the conditions and within the limits specified in this ruling, with regard to the declared marketing purposes".

b) The Italian Data Protection Authority: Installation of "digital signage" type advertising devices (also known as Totems) at a railway station - **Ruling no. 551 dated 21 December 2017** [7496252];"

In the case in question, which was also prior to the introduction of EU Reg. 679/2016, the Authority opened an investigation after receiving reports of *digital signage* devices being installed at Milan Central station. In the display of the advertising messages, the devices were thought to use "facial recognition and tracking" systems on the individuals passing by the devices.
The investigation involved Grandi Stazioni Retail S.p.A., the company that held exclusive rights to commercially exploit the advertising spaces in all major Italian railway stations and was Controller of the data collected. This company, through its supplier Dialogica S.r.l., had already installed a considerable number of devices, and was planning to install more over time.

The **technology** used was built into devices "*connected to the Grandi Stazioni Retail network,* [...] *equipped with a screen for displaying advertising messages and information, a pc/media player (that sends the digital content for display to the screen) and sensors to collect audience data with which to evaluate the effectiveness of the displayed advertising messages".*
The audience data was collected and measured using software called VidiReports, created by the company Quividi s.a.s., able to "*analyze the images collected by the video sensor installed on the devices (usually a webcam) with the purpose of:*

- *determining the presence of a human face in the area covered by the sensor* [but not to identify it, hence using only *face detection* and not *facial recognition* algorithms];
- *measuring the time an individual remains in front of the device, namely the time a certain face remains in the sensor's field of vision;* ["forgetting" the passage of the individual as soon as they face leaves the sensor's field of vision, which differed from device to device].
- *obtaining some further information (albeit with a certain degree of approximation) deduced from the features of the face, such as: gender, age group, distance from the device;*
- *carrying out statistical analysis to determine the effectiveness of the various advertising messages*".

For the latter purpose VidiReports saved a dataset for each face identified in front of the screen, which included the following information:

- the dataset sequential number;
- the ID of the device that created the dataset;
- the date and time of arrival of the individual;
- the time the individual was present;
- the time for which the individual paid attention;
- the individual's gender [optional];
- the individual's age group [optional];
- the mean distance of the individual from the measurement point;
- an estimation of 5 levels of facial expression, from happy to sad [optional].

The images were stored in the RAM memory of the local device only for the time necessary for processing. The **Purpose** of installing the Digital Signage devices was to conduct a so-called anonymized analysis of the advertising audience.

In its **assessment,** the Supervisory Authority highlighted several important elements:

1. It is always necessary to give due consideration to the principles of necessity, lawfulness, and proportionality in processing personal data;
2. **While only for a few seconds, the system installed in any case involves personal data processing** (images of the face of the data subject);
3. Given that i) the images were erased by the system almost immediately; ii) no personal data was permanently stored by the system and; iii) the system only used face detection algorithms, the authority determined that the **data processing itself was compliant** with the principles of the Code.
4. However, the Authority determined that the nature of the **extrapolation of statistical** required **adequate precautions** to protect the fundamental rights and freedoms, as well as the dignity and privacy of the data subjects.
5. The Authority required the data processing Controller to provide **concise privacy notices** located in the vicinity of the advertising totems, **supplemented with complete information** readily available on the Controller's website, or through a **QR code** on the display itself.
6. it recognized [with respect to consent, Ed.] that **balance of interests** could be an alternative legal basis, pursuant to´art. 24, paragraph 1, point g) of the Code, provided that the image detection carried out by Grandi Stazioni Retail S.p.A took place on the conditions and within the limits specified by the ruling (the considerations as above).
7. it required the Controller to "take due precautions to protect the elements most critical in terms of personal data protection: the **image collection sensors** (the webcam installed on each device) and the **local memory** on which the images of the data subjects are temporarily stored". To this end, the Authority required that **the equipment undergo periodic monitoring, at intervals of at least six months**.

1.2 Radio frequency systems

1.2.1 The Technology

This category includes all technologies using a sensor based on Wi-Fi or Bluetooth wireless technology. More generally, the category includes all systems capable of acquiring and processing data packet sequences transmitted by wireless devices.

⚙ **Operation:** Using an antenna type sensor, systems in this category scan for wireless devices (smartphones, tablets, notebooks, etc.) in the area where the measurement is taken. The information generated by the scan is processed by a local computer that extracts audience information, such as the number of people and the time they remain in each area.

This data can then be sent to a centralized cloud/server for subsequent aggregation and display via a dedicated dashboard.

Data transfer to the server is generally through a secure internet/intranet connection of the type most used, such as Ethernet, Wi-Fi, or data connection device.

1.2.2 Data categories

The types of data that can be processed include:

User personal data

1. **Mac Address;** this is the unique identifier of each network device, which identifies the device in the network. In ruling no. 303 dated 13 July 2016 the Authority declared that the MAC Address was classified as personal data, given that it permits identification of the user, albeit indirectly, due to its unique characteristics.

User location data

1. **Distance from the device;** device refers to the sensor that picks up the wireless signal
2. **Dwell time;** means the time the user remains in the vicinity of the device

This data can be used to determine the number of wireless devices present and therefore the number of people in interest. The system is thus able to extract basic information, numerical rather than personal, such as the number of devices, type of operating system and dwell time in the area.

Other data

1. **Device manufacturer;** device refers to all wireless devices (smartphone, tablet, …)

1.2.3 Relevant rulings

The case studies on the technologies analyzed here come from the Italian Personal Data Protection Authority, and are:

a) **Ruling no. 360 dated 22 May 2018**
b) **Ruling no. 370 dated 29 November 2012**

While both of the case studies date to before EU Regulation 2016/679 came into effect, here we feel it appropriate to briefly review the reasoning in fact and in law applied by the Authority, in that they certainly constitute key rulings for the players in the sector, in terms of continuity.

a) The Italian Data Protection Authority: "Data collection, analysis and processing, through the installation of equipment, for the purposes of marketing and market research - **Ruling no. 360 dated 22 May 2018**"

In the case in question, the companies Ors S.r.l. and Taggalo S.r.l. requested prior checking of the possibility of offering its customers (purportedly) anonymous data collection, analysis and processing services, through the installation of devices located on the ceiling or near to the window of a shop.

Purpose: Regarding the passage of people and dwell time, the system would be able to record images and behavior, as well as the presence of mobile devices, for marketing and market research purposes.

Technology: The device in question consisted of a video camera for acquiring the images and temporarily storing them in a volatile memory; a numerical output would then be generated by an aggregation algorithm. The system also permitted the detection, again in a purportedly anonymous manner, of certain behavior such as *"the passage of persons and/or objects by means of virtual lines traced in the device's field of vision"*, to provide a measurement of the number of passages or time spent in a given area of the place monitored by the device. The system had an additional function able to detect the mobile devices of people in the vicinity of the device with Wi-Fi service active, as well as the corresponding MAC address, which would be subsequently "encrypted in an irreversible manner". The device would indeed be able to track the movements of the mobile devices, measure their dwell time in each place and the frequency with which their users returned to the monitored area.

Data Processed: Personal data (Mac address), Biometric data (Facial images), Location data (Tracking movements of data subjects by means of virtual lines in the vicinity of the device).

In this respect:

- the MAC address of mobile device held by the subject detected is classed as personal data (the MAC address is considered so due to its "unique" nature, which persists even after encryption);
- the data processed by the detection system is likewise considered as personal data (and biometric data), given that it includes images (the faces) of passers and their behavior;
- despite the asserted counting function, tracing the passage of persons and objects over virtual lines in the device's field of vision appears more like an effective form of mobility tracking, given the possibility of following the trajectory of the images in the monitored area or the movements of the mobile devices held by the subjects;

The **outcome** of the Prior Check was negative: The Authority rejected the "collection, analysis and processing of data through the installation of equipment for marketing and market research purposes" and, moreover:

1. determined that such processing could not be carried out without the prior informed consent of the data subjects and;
2. location tracking of mobile terminals to trace the physical movements of people (for example "Wi-Fi" or "Bluetooth" tracking) was likewise forbidden without the consent of the data subjects or anonymization of the data collected (given that the "MAC addresses are personal data and remain so even after adopting security measures such as hashing");
3. even if the processing were limited to simple counting operations without any mobility tracking, and it were possible in this case to legitimize use of a different legal basis for processing, a legitimate interest of the controller or a third party recipient of the data is lacking with respect to the declared marketing and market research purposes.

b) The Italian Data Protection Authority: “Personal data processing by an RFID remote monitoring system for patients with implantable cardioverter defibrillators. Prior Check requested by Hospital and SAS” – **Ruling no. 370 dated 29 November 2012**

In the case in question, the Hospital and the SAS requested prior check of the possibility of remotely monitoring the clinical data of patients with implantable cardioverter defibrillators, by means of an RFID system.

Purpose: To allow physicians to remotely monitor the clinical data recorded by the implanted cardiac devices of patients, to monitor abnormalities and carry out defibrillation.

Technology: The system in question is known as a “Remote Monitoring System” (or RMS). The data recorded by the implanted device is sent by wireless RFID technology to a monitor installed in the patient’s home. The data received is then transferred by GPRS or land line to a central server where it is stored and processed to generate reports (in PDF format). The reports can be examined and analyzed by the patient’s doctors via a web interface application, without the need for the patient to attend an appointment.

The system is made up of the following elements:

- a monitor (consisting of an electrical box)) at the patient’s home, which connects by radio frequency to the implanted device and automatically transfers the raw data to the central server using the public telephone network; no data is stored, given that the device functions simply as a transmitter.
- a back office, consisting of a central server that allows physicians to consult and examine reports containing the data saved by the cardiac implant through a web application;
- a back-office analyzer, consisting of various software applications that process the raw data from the cardiac implant and produce the aforementioned reports for examination via the web interface.

Data Processed: Personal data (patient's details, device serial number, Monitor serial number), Sensitive data (patient’s clinical data), Technical data (system operation).

- the personal data is saved on the system through the web application by the physicians responsible for the patient with the implanted device, and can only be edited by those physicians;
- the sensitive data is transmitted to the monitor by RFID technology, and from there to the system server by land line. It is then processed into reports by the applications installed on system and made available to the physicians in read-only format through the web interface. the patient’s clinical data is erased within five years of collection, unless indispensable for the exercise of rights in legal proceedings or to comply with a specific legal obligation.
- the technical data is generated automatically by the RFID Tag and the monitor and is accessible to the supplier of the device and other outsourced operators entrusted with system safety and maintenance.

Outcome: The Prior Check did not end in a result as such. In effect, the personal data processing the request referred to did not fall under the types requiring approval, given that the sensitive data was processed by the hospital itself.

However, specific, and strict attention needed to be paid to safeguarding fundamental rights and freedoms. For this reason, for the purposes of compliance with current rulings, the Supervisory Authority felt it appropriate and necessary to introduce the measures outlined below:

1. Given that the system is designed to monitor any cardiac arrhythmia in patients and carry out defibrillation if necessary, the personal data collected can be said to be processed for the purposes of prevention, diagnosis and treatment of the data subject. Therefore, in compliance with the Code, such personal data **may be processed exclusively by subjects operating in the health sector** and with the prior, informed **consent** of the data subject, even without authorization by the Supervisory Authority. With respect to the principle of purpose, the processing of such information is therefore permitted exclusively **within the limits of the therapeutic relationship between the hospital and the patient**. This relationship of trust excludes all third parties, even other health sector operators to whom the patient has not given explicit consent to communication of their data.
2. The RFID system must be configured such as to **avoid the use of the data subject's personal data or identity,** where not strictly necessary for the declared purpose. In specific terms, access to the patient clinical data must be limited exclusively to the clinical staff of the Hospital treating the patient, and the patient him/herself. The SAS, on the other hand, would be limited to processing only the technical data necessary for the safety and maintenance of the system. Lastly, the outsourced operators responsible for technical assistance to the physicians and/or patients could have access to patient identifying data for the sole purpose of satisfying requests for technical service made by users.
3. However, the Authority felt that there were insufficient technical/organizational measures in place to ensure that patient clinical data was inaccessible to the service provider and the outsourced operators it employed.
4. It therefore recommended the adoption of the following technical/organizational measures:

   in case of specific interventions, the Hospital must be promptly informed of the intervention itself;

   a. the operations carried out by the service provider or outsourced operators must be registered, indicating the users involved, any use of encryption keys and the reasons for using them;
   b. the above registrations (or access logs) must be complete, unalterable, verifiable in terms of their integrity and adequate for achieving the purposes for which they are required. They must be kept for an appropriate period, which should be no less than six months.
   c. IT procedures should be adopted to prevent data download from the central server, which include an appropriate alert system in case of anomaly.
   d. access control mechanisms should also be adopted, to prevent access to the personal data of multiple patients by the same user.
   e. data subjects must be able to easily obtain deactivation of the system, and control the personal data subject to remote monitoring
   f. the file systems or database systems must be implemented with advanced encryption functions based on robust algorithms.

g. backup systems must be implemented;

h. secure communications protocols must be implemented, based on the use of transmission encryption standards;

i. suitable procedures must be implemented in the attribution of the authorization profiles for the processors, according to their roles and processing/access requirements;

j. suitable encryption-based measures must be established to ensure that the clinical data transmitted to the central server is complete and inalterable.

k. to prevent accidental loss the data must be periodically backed-up on an emergency site with the same anti-intrusion measures such as firewalls and anti-intrusion systems (IDS) protecting the central server. Periodic checks should also be carried out on the quality and coherence of the authentication and authorization profiles assigned to the processors;

l. audit log systems should be implemented to control access to the system and detect any anomalies;

m. perimeter security systems must be implemented, such as infrastructures with suitably robust and reliable characteristics.

To increase the security level of the measures implemented to reduce unauthorized access or processing not permitted or in compliance with the declared purpose, the user authorized as local administrator at the hospital must have access to controls able to statistically monitor user accesses and activate alerts in case of anomalies, whether with regard to system operation or access to the data by authorized users.
these must include the possibility of displaying the information viewed during the last session opened with the same credentials.

Lastly, hospital personnel authorized to access the system and other staff involved in system maintenance and security must be adequately trained in the correct use of the available applications.

1.3 Cell network data acquisition systems

1.3.1 The Technology

This category includes all data derived from SIM cards used by mobile phone companies and the data derived from cell network technology, for the sole purpose of audience measurement.

⚙ **Functioning:** each SIM card dialogues via cell phone or similar device with the cell towers of the network providing voice and data services. There can be many cell towers, and therefore cells in a city, and this effectively permits the approximate location of the devices connected to them. Each SIM has its own unique code and is associated with a contract containing information on the user (the natural person) who signed it.

The location of the device is tracked every time it connects for data exchange or voice services. Modern smartphones need virtually uninterrupted connectivity, and consequently, mobile phone companies can determine the location of their smartphones virtually all the time.

The cell towers described above can be installed in certain areas of a city even for the sole purpose of audience counting and measurement.

1.3.2 Data categories

The personal data processed by mobile phone companies includes:

1. The **geographical location** of SIM card users;
2. The personal data provided on purchasing the SIM card.

As previously mentioned, mobile phone companies need to have this information to provide the service.

The companies can sell this information in aggregate form, but never any information pertaining to an individual user. They do not provide individual or small groups of GPS traces, but are required to provide information on:

- presence in each area
- Italian/Foreign residents
- age group (based on the information given in contract)
- gender (based on the information given in contract)
- unique user movements
- return rate

This data is updated at intervals that can be as short as 15 minutes.

1.3.3 Relevant rulings

There are no specific rulings of the European Data Protection Authority concerning the sale of aggregated personal data.

Having said this, there are a number of rulings of the Italian Authority - both general and specific - regarding the profiling carried out by telecommunications service providers (i.e. mobile phone companies), using aggregated data, for example, to classify data subjects into certain categories.

The most significant of these rulings are:

a) Requirements for providers of public telecommunications services concerning profiling activities – **25 June 2009;**

b) Customer data processing for profiling purposes. Prior check requested by Tiscali Italia SpA – **24 October 2013**.

As we said, these rulings do not directly concern use of the technology for the purposes described above, but although prior to the entry into effect of EU Reg. 679/2016 they certainly constitute key measures for operators in the Audience Measurement sector, from which to draw the principles of the technology in question.

a) The Italian Data Protection Authority: “Requirements for providers of public telecommunications services concerning profiling activities – **Ruling dated 25 June 2009**”

The ruling in question is one that the Authority issued after conducting a series of investigations, including audits, to: i) monitor the activities of public telecommunications service providers and: ii) acquire information on the methods each provider uses to profile their customers and classify them into given homogeneous categories (so-called "*clusters*").

The investigations revealed that service providers conduct profiling activities using personal data that has been aggregated based on parameters identified according to their requirements. This data may include various types of personal information, such as contractual data and information on consumption, from which it is possible to gather further information on each data subject (for example, consumer type, level of spending sustained at regular intervals, services enabled on each user).

The circumstance that a provider can obtain and process such data, even in aggregated form, requires the availability of a wealth of information that goes well beyond the individual data relative to each individual natural person. Indeed, by comparing customer information, providers can gather information that allows them to monitor economic trends in society and use this information to develop targeted marketing campaigns based on their analyses.

The ruling focuses on two circumstances: the first in which profiling regards “individual” personal information and requires consent for processing, and the second in which profiling is based on “aggregated” personal data.

For the purposes of this analysis, we consider the rulings the Authority applied in the second of the above cases.

First and foremost, the ruling in question required the data controller to submit a request for prior checking, in accordance with art. 17, Leg. Dec. 196/2003. Considering that today this kind of prior check is no longer applicable (after introduction of the GDPR and its implementation in the various member States), mobile phone companies now have to independently check compliance of the type of processing they intend to perform, based on the principle of responsibility pursuant to art. 24 of the GDPR. This check can take the form of an impact assessment as per art. 35 of the GDPR, namely by requesting Prior consultation in accordance with subsequent art. 36.

Outcome: In addition to the above, through the ruling in question the Authority listed a series of minimum conditions that must be met by profiling activities on aggregated personal data.

1. that the personal data subject to profiling, although derived from detailed original data that the controller still holds for operative and legal purposes, consists exclusively of aggregated personal data from which **it is not immediately possible to gather detailed information on the individual data subjects**;
2. that the aggregated personal data subject to profiling be stored in one or more systems specifically dedicated to profiling operations, functionally separate from the original system source of the aggregated data and any other systems used by the data controller for other purposes (for example, marketing);
3. if referring to large number of data subjects, the aggregated personal data to profile must undergo a process to make immediate identification of the individual data subjects impossible.
4. the data processors performing the profiling operations must have a limited authentication profile, different to those who perform any other activities, even after the profiling itself;
5. the profiled personal data must be stored for a limited period, after which it must be erased;
6. the Data Controller must provide the data subjects with a personal data processing privacy notice.

b) The Italian Data Protection Authority: "Customer data processing for profiling purposes. Prior checking requested by Tiscali Italia SpA - **Ruling no. 468 of 24 October 2013**"

In the case in question, which was also prior to the introduction of EU, Tiscali Italia S.p.A. ("**Tiscali**") requested *prior checking* to obtain authorization to process the aggregated data of its customers for profiling purposes, even without specific consent of the data subjects. The Authority allowed the company to conduct the processing, but with the proviso of implementing specific technical and organizational measures within 90 days of receiving the notification. Subsequently, after informing the Authority of the implementation of most of the required measures on profiling its service users, Tiscali requested a further check by the Authority with regard to certain of those users, on the basis of a different approach to the assumptions justifying the measures.

Through the ruling in question, the Authority ruled on this further request by Tiscali, requiring that before initiating the processing of aggregated customer information, the company should implement the necessary measures to safeguard such users and their rights.

Outcome: For the purposes of this white paper and in the light of the measures indicated in the Ruling of 25 June 2009 as above, here we offer a list of the actions the Authority required in relation to the level of aggregation of the data used for profiling activities, and the period of time such data must be conserved:

1. use of a **range** of values in the creation of the *clusters* (e.g. using age groups such as 20-30 or 30-40, or geographical areas larger than the single municipality the users belong to), or implementation of equivalent measures with the purpose of reducing the risk of reaching a level of detail sufficient to permit the identification of users, even indirectly;

2. *ex post* checks on each *cluster* extracted, to prevent the creation of *clusters* of users containing less than 100 units and thereby significantly reduce the capacity of the data to identify users after processing;
3. conservation of the data used for profiling for a maximum of 12 months (which may be extended for a further 3 months), after which the data must be erased or irreversibly and permanently transformed into anonymous form;
4. issue of a privacy notice concerning the processing of the personal data the company intends to use for profiling purposes, specifying that the processing is conducted using aggregated personal information and therefore does not require specific consent of the data subjects, in accordance with the Authority Ruling of 25 June 2009.

1.4. SDK, Beacon & bidstream systems

1.4.1 The technology

This category includes all technologies based on user location detection systems, most of which included in Apps for smartphones.

⚙ **Operation:** these technologies operate differently depending on whether they use:

- *BidStream*: the GPS position given by the banner in Programmatic advertising, namely marketing activities using display campaigns that make use of spaces bought at auction (as is the case of Google keywords))
- *Beacon/SDK*: GPS position given by the App and shared through SDK technology, namely the part of mobile App code that permits collection and sharing of the data between a series of advertisers.

BidStream: in the scope of programmatic advertising, when an advertising banner is provided, the information on the individual’s position is recovered: for example, on opening a web page containing a banner, the phone provides the location, by GPS or via the connectivity provider.

The data collected and delivered to publishers via the BidStream includes the user’s latitude and longitude, along with the advertising ID, unique for each mobile device and resettable by the user. In terms of privacy, the data collected and shared with advertisers for programmatic advertising (substantially used for purchases of ad hoc advertising spaces by Real Time Bidding, or “RTB”) using BidStream poses compliance problems in particular as regards the indiscriminate audience of subjects (advertisers) able to access the data, and the indeterminacy of the data transferred (location updating frequency, advertising ID that may or may not be reset, etc.).

To proceed with Real Time Bidding, the advertisers (usually a fairly large network, with hundreds of subjects involved) receive user position data and advertising ID. This data transfer is not regulated and, in most cases, takes place without users being informed. The need to transfer the data to a large number of advertisers, even though the advertising space itself is allocated only to the highest bidder, is determined by the need to ensure information symmetry for all participants in the bidding process.

Beacon / SDK: These technologies operate on specific instructions present in the Apps installed on the mobile device (smartphone). After obtaining user consent on installing the App, these technologies provide companies using the data collection service (more often than not the company that developed the App) with the GPS position of the smartphone, updated approx. 25 time per day. Beacon is a signal from an antenna physically installed by the company interested in collecting data from “nearby” subjects, which help the App locate the user more precisely (especially indoors where GPS is very inaccurate).

SDKs are usually developed by a third party who provides its codes to the developers of certain types of mobile apps (which by nature require consent to the use of GPS, e.g. Map applications) who need to collect user location data for advertising purposes (which by nature differ from the original purpose of the app the SDK is installed on). For this type of data collection, both the developer of the app and the developer of the SDK require the explicit consent of the end user. So, using SDKs developers of this type of technology can obtain the location data of people using a given app. The means by which the data is gathered also determines its identifying capacity.

1.4.2 Data categories

The personal data obtainable includes:

a. GPS coordinates;
b. inertial data from the accelerometer;
c. Advertising ID of the device.

This data is updated about 25 time per day. Using technology like SDK, BidStream and Beacon it is possible to extract personal generic data on user location, as well as data on the device used (MAC Address) and consumer preferences (advertising ID). While it is not possible to unequivocally identify a person taking the above data individually, considering it as a whole could render the data subjects identifiable. For this reason, it is considered as personal data.

However, as a partial exception to this affirmation, data associated with location may in any case be considered personal in itself, for example, in the case of data collected constantly with background, the habitual movements of a given subject could lead to their identification.

By combining the above data, companies operating in this sector provide aggregated data on the presence of persons in a given area, and the volume of unique users. The precision of BidStream data is uncertain, while SDK/Beacon are much more precise.

1.4.3 Relevant rulings

Whether for reasons to do with a lack of understanding of the technology, or the impossibility of determining the subjects belonging to the chain of management of the data with any certainty, the authorities have been somewhat reluctant to permit an indiscriminate use of this technology.

On this subject in particular, in Europe, the French CNIL authority expressed its opinion through a series of rulings that effectively called default on a number of small SDK service development companies.

1. **Décision MED-2018-022 du 25 juin 2018 - TEEMO**
2. **Décision MED-2018-023 du 25 juin 2018 - FIDZUP**
3. **Décision MED-2018-042 du 30 octobre 2018 - VECTUARY**

These were decisions of particular importance by the CNIL against developers of SDK technology whose codes were inserted in a number of apps.

In specific terms, the CNIL called default of Fidzup and Teemo for their failure to take the appropriate steps to make the function of the technology transparent for users, as well as for their unlawful collection and consequent use of the data.

As regards Fidzup, in using SDK the company didn't limit its data collection to location data, but also collected the advertising ID of the device (unique, associated with the device but that can be reset by the user) and the MAC address (unique, associated with the device and persistent).

The use of SDK by Fidzup was accompanied by the use of other technologies, such as Beacon ("Fidbox") which, installed in the vicinity of the sales outsets of Fidzup's partner, collected further information on the MAC Address and Wi-Fi of the user's device.

Given the existence and enormous potential of the technology, the CNIL declared its use unlawful due to (i) lack of information provided to users, (ii) lack of consent and (iii) retention times. Through ruling 3) the CNIL highlighted the unlawful nature of the data collection conducted by the company in question using SDK, focusing in particular on the question of consent and the information notices provided to users.

In ruling 3) the CNIL highlighted the unlawful nature of the data collection conducted by Vectuary using SDK, focusing once again on the question of consent and the information provided to users.

With regard to consent, the CNIL affirmed the need for the company to obtain consent in order to use location data with the advertising ID of all users for promotional purposes (in the case at hand, the use of the above data to display advertising messages according to the proximity of the user to a given retailer).

With regard to the need to provide detailed information on the means and purpose of the processing, the CNIL condemned the fact that at no point in the interaction with the app users were provided with information about the way the data is collected (through SDKs installed in the app, for the precision) and the purposes for which it is used and shared with third parties.

From this series of rulings and guidelines, we can glean a number of fundamental requirements for the lawful and transparent use of this type of technology.

Any time apps containing SDK or other codes able to access BidStream for data transfer to advertiser networks, the user must:

1. be specifically informed of this additional processing (with respect to the “standard” processing by the SDK “carrier” app);
2. be specifically informed about the series of subjects who will process the data collected by SDK (companies developing the technology and networks of subjects acquiring the data);
3. give their explicit consent to the use of their location data for additional purposes, to both the SDK developer and the network of subjects to whom the data will be sent.
4. be informed of the retention times of the data collected (since the term of 13 months indicated by Fidzup was considered excessive, the term of 3 months was considered sufficient.

1.5. Occupancy Detection Systems

1.5.1 The Technology

This category includes all technologies based on sensors using light pulse type remote detection techniques. It includes Lidar (Laser Imaging Detection and Ranging) sensors and passive infra-red (PIR) occupancy sensors.

⚙ **Functioning:** This category of sensors operate uses micro-pulses of electromagnetic radiation or light. By measuring the time between the emission of the pulse and its return, it is possible to calculate the distance of objects in the sensor’s field of vision. In effect, these sensors work like a veritable radar, scanning the surrounding area. Audience information can be obtained by differentiating between moving objects and fixed objects.

Occupancy Detection systems can be implemented using a vast range of technologies, including:

- Passive infra-red (PIR): PIR sensors are designed principally to detect movement or variations in heat sources within the sensor’s field of vision (FOV). Although PIR are excellent at detecting dynamic movement, the technology is not capable of detecting real occupancy. This type of sensor does not collect personal data;
- Laser Imaging Detection and Ranging (Lidar): this is a remote acquisition technique, namely a method that acquires qualitative and quantitative information on the environment and objects by means electromagnetic radiation that interacts with the physical surfaces of interest. In short, Lidar can determine the distance of an object or surface using a laser pulse. The data obtained cannot be associated with a physical person;
- Microwaves and ultrasound: Microwave sensors emit pulses and measure their reflection from moving objects. Similar to PIR, microwave sensors can be used to detect movement and are generally used in larger areas. However, higher production costs generally prevent the large-scale implementation of the technology. This type of sensor likewise does not process personal information;
- Video cameras: Video cameras produce a vest range of data on their environment, providing a focused and detailed view of a specific area. Aided by standardized algorithms, video cameras are systematically distributed in public areas to detect and analyze the movements of people. Although undeniably versatile, the use of video cameras implies serious risks to privacy and security;

- Lensless Smart Sensors (LSS): Lensless smart sensors (LSS) are a novel way of sensing. The technology combines a standard sensor, such as those found in focused and defocused cameras, but replaces the lens with an extremely small anti-phase binary diffraction grating. LSS do not capture focused images, nor do they capture deliberately de-focused images. Rather, they create what is called a ‘blob’ domain, which is a series of point spread functions (PSF) of light. LSS are able to detect and isolate movement within a specific area and identify the number of occupants and their positions. This is achieved without ever forming a recognizable image of a physical person at any point in the processing chain. In this case as well, the process does not involve personal information.

1.5.2 Data categories

The data obtainable from this technology consists of the presence of persons, namely, the number of people crossing the pulse emitted by the sensors. The acquisition frequency of the data depends on the type of sensor used and can reach up to real time.

The functions of the technology imply limited privacy problems since it does not permit recognition of unique personal features and does not involve personal information processing. Consequently, it does not present significant risks.

1.5.3 Relevant rulings

The Supervisory Authority has not issued any specific provisions regarding the use of Lidar systems and occupancy sensors.

2. Comparing technologies: other privacy aspects to consider

This chapter analyses a series of other aspects inherent to personal data protection, considered applicable in a "lateral" sense in reference to all the technologies analyzed in this paper.
Whatever the technology developed or marketed, it is indeed important to conduct an analysis of the necessary legal basis that legitimizes the processing of personal information (**section 2.1**) and whether (and how) further processing can be conducted (**section 2.2**); the proper exercise of data subject rights must also be ensured (**section 2.3**) and, very often, a Data Protection Impact Assessment (**section 2.5**) is required, to identify the risks inherent to the processing and the use of a given technology, but above all to determine the correct measures for mitigating the residual risks; last but not least, the security measures implemented must also be assessed (**section 2.6**).

The analysis of these aspects aims to extend the scope of the framework of notions necessary for the marketing and production of *Physical Audience Measurement* technologies.

2.1. Legal bases for data processing. General overview

Pursuant to the GDPR, the processing of personal data must among other things respect the principle of lawfulness, as per art. 5(1), point a), by which "*personal data shall be […] processed lawfully […]*". The Regulation itself thus defines a series of "Principles of lawfulness" (or legal bases) with which the data collection must comply before processing.
To this end, we can distinguish between *(i)* common personal data and *(ii)* data belonging to the "*special categories*" defined by art. 9(1) of the Regulation (*infra*, "special category data").

For common personal data processing to be lawful, it must be based on one of the principles defined by art. 6(1) of the Regulation.
All of the legal bases (six in all, each fully defined in the article itself) merit particular attention for the purposes of this paper:

- the consent required under art. 6(1), point a) of the Regulation, by which "*the data subject has given consent to the processing of his or her personal data for one or more specific purposes*; and
- the legitimate interest of the data controller or third parties (see art. 6(1), point f) of the Regulation, by which "*processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*").

On the other hand, for special categories of data (for example, biometric data capable of unequivocally identifying a person), art. 9(1) establishes a general prohibition, not applicable only in the few exceptional cases indicated in paragraph 2.
Of these cases (ten, in total, each likewise fully defined in the article), this paper focuses on the case of art. 9(2), point a) in which "*the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject*".

The paragraphs that follow offer an analysis of the lawful bases mentioned above.

2.1.1 Consent in accordance with art. 6(1), point a) of the Regulation

Where processing is based on the data' subject's consent in accordance with art. 6(1), point a) of the Regulation, the data controller is required to comply with the requirements of art. 7 of the Regulation (see *Recitals* 42 and 43 of the Regulation)

In specific terms, the controller must:

- be able to prove that the data subject has given consent, that is to say, it must keep a record of it for the purposes of full *accountability*. In this respect, it is always advisable that the data subject's consent is effectively explicit;
- ensure that in the scope of a written declaration even regarding other questions, the data subject is fully aware that they are giving valid consent and the manner it is given. For this reason the data controller should establish adequate guarantees and measures, such as *(i)* preparing forms on which the request for consent is clearly distinct from other matters, *(ii)* use understandable and easily accessible formulas, *(iii)* use clear and simple language and *(iv)* avoid the use of abusive clauses;
- ensure that the data subject offers their consent freely, that is to say that when giving their consent they are in a condition to make an authentically free choice and can refuse to consent without suffering any consequence;
- establish easy methods for revoking their consent.

2.1.2 Legitimate interest of the data controller or third parties, as per art. 6(1), point f) of the Regulation

The legitimate interest of a data controller or third party, as per art. 6(1) of the Regulation, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller.

What does "not overriding" mean? If a data controller intends to base personal data processing on a legitimate interest of its own or third parties, it must carefully assess the opposing interests, namely the legitimate interest of the controller and third parties on one hand and the rights and fundamental freedoms of the data subject on the other. This assessment is called a *legitimate interest assessment*, also referred to by the acronym "LIA" (as with the previous type of consent, the controller would be advised to adequately document this assessment with a view to maintaining full *accountability).*

In terms of method, in conducting a LIA the data controller should be guided by the principles established by art. 5 par. 1 of the Regulation, especially the following:

- the principle of minimization, proportionality, and necessity pursuant to art. 5(1), point c) GDPR: the data processed must be adequate, relevant, and limited to what is necessary for the purposes for which it is processed; and
- the principle of purpose limitation as per art. 5.1, point B) GDPR: the data must be processed for specified, explicit and legitimate purposes.

Controllers must also take account of a great many other elements when conducting a LIA, including:

- the purposes of the processing;
- the nature and merit of the interests pursued;
- the nature of the interests, rights, and fundamental freedoms of the data subjects;
- the reasonable expectations of the data subjects;
- the pros and cons of the processing for the controller/third parties and the data subjects;
- the possible consequences if the processing does not take place;
- the nature of the data processed;
- the nature and category of the data subjects involved, especially if they are vulnerable.
- the absence of other suitable legal bases;
- the absence of conflict with sector regulations;
- the potential negative impact on the data subjects, their rights and fundamental freedoms and the corresponding technical and organizational measure to mitigate this risk;
- The necessity/opportunity of conducting a data impact assessment based on the legitimate interest in protecting the data ("DPIA").

2.1.3 Consent as per art. 9(2), point a) of the Regulation

With regard to consent as per art. 9(2) point a) of the Regulation, for the data subject to consent to the processing of special categories of data, the procedure is the same as described in paragraph 2.1.2 of this white paper in reference to common data. However, note that is this case since the information is overly sensitive, the consent must always, and necessarily, be "explicit".

2.1.4 On the applicability of consent and legitimate interest to the technologies described in chapter 2

With the exception of the circumstances described below, the possibility of calling on one legal basis rather than another to justify personal data processing generally depends on the specific purpose of the processing in concrete terms.

Using the technologies described in this white paper, one such purpose could be *marketing.* Note that by "*marketing*" we are not referring exclusively to *direct marketing* (the delivery of communications with advertising and promotional purposes) but more generally to a form of evaluation for commercial purposes without personalization, namely a generalized diagnostic survey of *audience*, aimed at defining the most appropriate marketing actions for achieving and realizing reciprocal benefit for both customer and company. In this case it is reasonable to assume that the legitimate interest of the company-data controller and that of the consumer-data subject may, in principle, provide the ideal legal basis for justifying processing of the data collected using the technologies described in this *white paper*.

Before proceeding with processing, the controller is required to conduct a LIA:

- If the LIA finds that the interests, rights and fundamental freedoms of the data subject do not override the controller's legitimate interests, even taking account of the reasonable expectation of the latter based on their relationship with the controller itself, the controller may proceed to process the data on this legal basis;
- If this is not the case, the data controller cannot invoke legitimate interest and must obtain the consent of the data subject.

So, in principle, the weaker the LIA finds the legitimate interest, the more opportune it would be for the controller to request specific consent by the data subject.

An exception to this rule, by which the legal basis substantially depends on the purpose of the processing, is the case in which the data processed falls into the category of "location data", defined by art. 2, point c) of Directive 2002/58/EC (the so-called "e-Privacy Directive") as "any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service". Indeed, in this case the e-Privacy Directive gives relevance to the nature of the data in question and in art. 9 specifies that the only suitable legal basis for processing is the effective consent of the data subjects.

2.2. Further Processing activities

The question of *further processing* arises any time a subject (data processing controller), after having legitimately collected and processed data for a specific purpose (the "**original purpose**"), intends to process the same data further and for different purposes (the *"***new purpose**") applying the **same legal basis** underlying the collection and processing for the original purpose.

In such cases, there is the problem of verifying compliance with the principle of purpose limitation, as defined by art. 5(1), point b) of the GDPR, according to which personal data must be "*collected for specified, explicit and legitimate purposes and not further processed in a manner that is not compatible with those purposes*".

2.2.1 Analysis of "non-incompatibility" between new purpose and original purpose

Before proceeding with *further processing*, the data controller is required to check that the new purpose is not incompatible with the original purpose; note that in this provision the GDPR does not require full compatibility between the purposes, but merely their "non-incompatibility".
In the assessment, the data controller must take account of and valorize the following elements (see art. 6 para. 4 of the GDPR and Recital 50):

1. the connection between the original and new purposes;
2. the context in which the personal data was collected and, especially, whether the *further processing* can be included in the reasonable expectations of the data subject based on their relationship with the data controller;
3. the nature of the personal data, especially if it falls under special categories of personal data as per art. 9, para. 1 of the GDPR, or data relating to criminal convictions or offences as per art. 10 of the GDPR;
4. the possible consequences of *further processing* for the data subjects;
5. the existence of appropriate safeguards, which may include encryption or pseudonymization.

Thus, non-incompatibility analysis serves to verify the lawfulness of *further processing* and quantify the related level of risk to the rights and freedoms of the data subjects, in order to develop the most suitable technical/organizational counter-measures to eliminate or mitigate such risks. The findings in terms of privacy would also offer the data controller an opportunity to reflect on the ethical issues that could derive from *further processing*.

2.2.2 Possible scenarios

The above analysis could result in either of two distinct scenarios.
1) The controller (fully accountable as required by the Regulation), finds the new purpose incompatible with the original: in this case, no *further processing* is allowed, since it would not be legitimized by the same legal basis underlying the original processing.

2) In the light of their *accountability* the controller finds that the new purpose is not incompatible with the original: in this case, *further processing* is allowed (based on the same legal basis underlying the original processing).
It is important to stress that before proceeding with further processing, the data controller is required to provide the data subject with a new information notice, in pursuance of art. 13, para. 3 of the GDPR, specifically illustrating the new purposes of the processing and all other pertinent information.

2.3.3 Examples of further processing for audience measuring technologies

As in the cases ruled by the Supervisory Authority examined above (see Ruling n. 551 dated 21 December 2017 and Ruling n. 13 dated 21 January 2016), we can assume the purpose of processing of data collected using *audience* measurement technology to be *marketing*, with the legal basis for such processing as defined in art. 6, para. 1, point f) of the GDPR, by which "*processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*"). As specified in chapter 2.1, "*marketing*" in this context is intended as an analysis for commercial purposes without any form of personalization, that is to say, an analysis of demand with the aim of defining the best commercial actions for meeting it, with reciprocal benefit to both customer and company.
Here we offer a number of *further processing* examples for assessment in terms of non-incompatibility with the original purpose of *marketing*. Naturally, for a more in-depth and coherent analysis, the peculiarities and specific circumstances of the processing should be evaluated case by case.

a) **Anonymization**
Anonymization is the most important example of *further processing*. Through anonymization, "personal data" - understood as any information relating to an identified or identifiable natural person as per art. 4(1) of the GDPR - irreversibly ceases to be "personal" and concern the data subject; in other words, anonymization is a method that prevents/prohibits identification of the data subject (*Recital* 26 of the GDPR). There are no personal data protection regulations applicable to anonymous information - namely, information that certainly and effectively does not or no longer refers to an identified or identifiable natural person.

To all effects, data anonymization constitutes further processing of personal information and, as such, requires a non-incompatibility analysis between the purpose of anonymizing the data and the original purpose of the previous processing before it can be done. However, as highlighted by the European Data Protection Board under Working Party 29, anonymization tends to be considered compatible with the original purpose (Opinion 5/2014) if the risk of re-identification of the data subject is zero.

Ultimately, if the data controller has sufficiently advanced instruments capable of certifying the anonymization of the personal data, and thus the absence of any risk of re-identification, anonymization will always be compatible.

b) **Market research for statistical monitoring and evaluation**
Above and beyond *marketing* purposes, controllers may have interests in documenting business performance through statistical monitoring and demand assessments.
Considering the fact that this purpose effectively coincides with the new purpose of improving customer satisfaction levels, given that it increases the data controller's knowledge of the market, and that the *further processing* also comes under the reasonable expectations of the average customer-data subject based on their relationship with the controller-company, in a general and abstract sense there doesn't seem to any impediment to this kind of *further processing*.
Naturally, it is always preferable to anonymize the data wherever possible.

c) **Communication to other companies in the same business group for internal administrative purposes**
As indicated in *Recital* 48 of the GDPR, data controller-companies belonging to the same business group may certainly well have a legitimate interest in communicating customer personal data for internal administrative purposes (art. 6(1), point f) of the GDPR). From this we can easily conclude that the above marketing purposes are effectively 'not incompatible'.
Naturally, even in this case it is always preferable to anonymize the data wherever possible.

d) **Communication to other companies <u>not</u> belonging to the same business group, for example, in the scope of a transfer against payment**
Data communication between independent controller-companies not belonging to the same business group can be categorized as a transfer of intellectual property against payment; this case, as opposed to case c) above, cannot be considered as having the same legal basis as the original processing for *marketing* purposes. Indeed, there is no connection at all between the original purpose and the new one; moreover, the new purpose does not easily fit with the reasonable expectations of the customer-data subject.
Obviously, this kind of *further processing* would be possible only if the data were previously anonymized.

e) **Data crossing with other data (e.g. Video surveillance images, consumer purchases data, etc.) to determine customer satisfaction and loyalty *brand***
Crossing is a special processing operation that permits joint analysis of two or more personal data sets to obtain further information, which if regarding the same data subject, takes on a distinct, autonomous conceptual identity and can therefore be considered as new personal data. This is the case when comparing data collected using the technologies discussed in this *white paper*, with

data collected by video surveillance cameras or data contained in company databases regarding purchases made by customers. In theory, data crossing could be carried out to determine the satisfaction level of a specific customer and their loyalty to a *brand* The question of the non-incompatibility of this purpose with the original marketing purpose causes some confusion because data crossing can be seen as an invasive forms of customer "profiling", even if not necessarily automated, which certainly lies outside the reasonable expectations of the data subjects and is subject to serious risks in terms of ethics.

f) ***Direct marketing*** **(including *push* notifications)**
In the specific case of SDK technology, controller-companies could use location and advertising ID data to send pop-up advertising messages based on the proximity of users to a given *retailer*. In this case the processing purpose cannot be considered simply as *marketing* as previously defined ('an analysis of demand with the aim of defining the best commercial actions for satisfying it, with reciprocal benefit to both customer and company') Sending advertising messages to the data subject's own *personal* device is indeed a form of *direct marketing* and requires further, and far more invasive personal data processing. As highlighted by the French Authority (in the VECTUARY case analyzed above: https://www.cnil.fr/fr/applications-mobiles-mise-en-demeure-absence-de-consentement-geolocalisation-ciblage-publicitaire-2), in this case it is always necessary to obtain the consent of the data subject. We can therefore confidently conclude that the purpose of simple *marketing* and that of *direct marketing* cannot be considered "non-incompatible" (but rather, totally incompatible).

2.3. Rights of Data subjects

In this section we tackle the subject of the rights that can be exercised by data subjects, already contemplated both by the EU Directive of 1995 and the Privacy Code of 2003, and now introduced again in the GDPR, but with extended scope and a few additions.

2.3.1 Modalities for the exercise of rights

The modalities for the exercise of the rights of the data subject are established by articles 11 and 12 of the GDPR. In specific terms:

- *Term for reply*: one month for each right, which can be extended to 3 months in particularly complex cases. The data controller must provide the data subject with information on action taken within 1 month of the request, even in case of denial;
- *Reply*: usually in written form by electronic means to facilitate accessibility, but can be verbal only if specifically requested by the data subject;
- *The information provided to the data subject*: must be concise, transparent, and easily accessible, using clear and plain language;
- *Measures to facilitate the exercise of rights*: the controller must take all appropriate steps, both technical and organizational, to this end. While only the controller is required to provide information in response to the exercise of rights, the processor is required to collaborate with the controller to facilitate the exercise of the rights of the data subject (art. 28, paragraph 3, point e);

- *Free exercise of rights*. In principle, the exercise of rights is free for the data subject, but there may be exceptions depending on the complexity of the request and the effort necessary to satisfy it;
- *Information*: the controller has the right to request the information necessary for identifying the data subject, and the data subject is required to provide it, in a suitable format;
- *Exceptions*: there are some exceptions to the rights acknowledged by the Regulation, but these are based mostly on national legislation in accordance with article 23 and other articles dealing with specific contexts.

2.3.2 Description and applicability

In this section we offer a brief description of the rights of data subjects included in the GDPR and, for each, the possible applicability to the technologies examined in chapter 2.:

1. **Right of access** (art.15): The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information.

1. Image acquisition systems or video streams	2. Radio frequency systems	3. Cell network data acquisition systems	4. SDK, Beacon and Bidstream systems	5. Occupancy Detection systems
✗	✓	✓	✓	✗

2. **Right to rectification** (art. 16): the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Considering the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement;

1. Image acquisition systems or video streams	2. Radio frequency systems	3. Cell network data acquisition systems	4. SDK, Beacon and Bidstream systems	5. Occupancy Detection systems
✗	✗	✗	✗	✗

3. **Right to Erasure** (art. 17): the right to obtain the erasure of personal data and any trace thereof, on the conditions described in the article;

1. Image acquisition systems or video streams	2. Radio frequency systems	3. Cell network data acquisition systems	4. SDK, Beacon and Bidstream systems	5. Occupancy Detection systems
✗	✓	✓	✓	✗

4. **Right to restriction of processing** (art. 18): Considering the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement;

1. Image acquisition systems or video streams	2. Radio frequency systems	3. Cell network data acquisition systems	4. SDK, Beacon and Bidstream systems	5. Occupancy Detection systems
✗	✓	✓	✓	✗

5. **Right to portability** (art. 20): the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided

1. Image acquisition systems or video streams	2. Radio frequency systems	3. Cell network data acquisition systems	4. SDK, Beacon and Bidstream systems	5. Occupancy Detection systems
✗	✓	✓	✓	✗

6. **Right to object** (art. 21): The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her

1. Image acquisition systems or video streams	2. Radio frequency systems	3. Cell network data acquisition systems	4. SDK, Beacon and Bidstream systems	5. Occupancy Detection systems
✗	✓	✓	✓	✗

From this analysis it emerges that the rights of the data subjects cannot be exercised for some of the technologies. In the contexts and for the purposes analyzed in chapter 1, "Occupancy Detection" and "Image or video stream acquisition" systems do not envisage personal data processing and consequently there is no need or obligation to ensure the exercise of rights.

2.3.3 How to facilitate the exercise of rights

Requests can be received from the data subjects via different channels and modalities, not necessarily just through the contact data given in the privacy notice; a request can be inserted in a complaint, or any communication addressed to the data controller, via e-mail, certified mail, fax or regular mail. The data controller is thus free to channel the requests received through a section of an application, a Service Desk Portal, or any other means.

1. **Image or video stream analysis-acquisition systems**

Non applicabile: il trattamento è “volatile”, non vi è acquisizione di dati personali (come indicato nel capitolo 1.1.1) di conseguenza non vi è la possibilità d’esercizio di alcun diritto.

Image and video stream acquisition systems.	Means of exercise				
	e-mail	*Certified e-mail*	*FAX*	*Postal mail*	*Service Desk*
Access	×	×	×	×	×
Rectification	×	×	×	×	×
Right to be forgotten	×	×	×	×	×
Limitation	×	×	×	×	×
Portability	×	×	×	×	×
Objection	×	×	×	×	×

2. Radio frequency systems

Applicabile for all rights

Radio frequency systems	Means of exercise				
	e-mail	*Certified e-mail*	*FAX*	*Postal mail*	*Service Desk*
Access	✓	✓	✓	✓	✓
Rectification	✓	✓	✓	✓	✓
Right to be forgotten	✓	✓	✓	✓	✓
Limitation	✓	✓	✓	✓	✓
Portability	✓	✓	✓	✓	✓
Objection	✓	✓	✓	✓	✓

3. Sistemi di acquisizione dati tramite cella telefonica

Not applicable to the right to rectification

Cell network data acquisition systems	Means of exercise				
	e-mail	*Certified e-mail*	*FAX*	*Postal mail*	*Service Desk*
Access	✓	✓	✓	✓	✓
Rectification	×	×	×	×	×
Right to be	✓	✓	✓	✓	✓

forgotten					
Limitation	✓	✓	✓	✓	✓
Portability	✓	✓	✓	✓	✓
Objection	✓	✓	✓	✓	✓

4. SDK, Beacon e bidstream

Applicable for all rights

SDK, Beacon and bidstream	Means of exercise				
	e-mail	*Certified e-mail*	*FAX*	*Postal mail*	*Service Desk*
Access	✓	✓	✓	✓	✓
Rectification	✓	✓	✓	✓	✓
Right to be forgotten	✓	✓	✓	✓	✓
Limitation	✓	✓	✓	✓	✓
Portability	✓	✓	✓	✓	✓
Objection	✓	✓	✓	✓	✓

5. Occupancy detection

Not applicable: there is no acquisition of personal data (as indicated in chapter 1.6.1), consequently no possibility of exercising any right.

Image and video stream acquisition systems	Means of exercise				
	e-mail	*Certified e-mail*	*FAX*	*Postal mail*	*Service Desk*
Access	×	×	×	×	×
Rectification	×	×	×	×	×
Right to be forgotten	×	×	×	×	×
Limitation	×	×	×	×	×
Portability	×	×	×	×	×
Objection	×	×	×	×	×

2.3.4 Consequences of the impossibility of exercise

The exercise of privacy rights, explicitly guaranteed by the European Regulation, may be impossible only in two circumstances:

1. **The privacy rights cannot be exercised due to technical impossibility**: the exercise of rights may be impossible for example, because the data no longer exists, has been erased or is unmodifiable or inaccessible even to the controller; not intentionally, but due to the configuration of the technology itself. In this circumstance it is impossible for the data subjects to exercise their rights

   It is important that the Data Controller provides correct information (as required by articles 13 et seq. of the Regulation) to the data subject regarding the possibility of such 'non exercise', for example through a correct privacy notice. It is equally important that the Controller respond to any request received, giving proof of the impossibility of exercise and that a *Data Protection Impact Assessment (DPIA)* has been conducted, as required by art. 35 of the GDPR. Impossibility of exercise is indeed one of the conditions the European Authorities have established as sufficient reason to conduct a DPIA.

2. **The rights cannot be exercised due to negligence of the Data Controller**: this is the circumstance in which the Controller does not reply to the request or gives an inadequate or late reply.

   In this case, the data subject may lodge a complaint with the Supervisory Authority or judicial authorities to uphold their rights.

   Any person who has suffered material or non-material damage as a result of an infringement of the Regulation shall have the right to receive compensation from the controller or processor for the damage suffered (article 82 of the GDPR). The subjects liable for the damage are both the controller and the processor of the data; any controller is liable for the damage caused by processing which infringes the Regulation, whereas the processor is liable for the damage caused by processing only where it has not complied with specific obligations or where has acted contrary to the instructions of the controller.

   There are various instruments the data subject can use to uphold their rights, including:

   → ***Claim against the controller*** (and if this is to no avail, appeal to the Supervisory Authority or the competent Court of law). A claim does not involve any particular formalities and can be served by e-mail or regular mail. Each Authority provides a complaint submission form to use for the exercise of rights, available from this link.

   The Controller must give a suitable answer without undue delay (1 month from receipt). The period may be extended for two further months where necessary, considering the complexity and number of requests. The controller shall inform the data subject of any such extension within one month of receipt of the request

→ ***Direct complaint to the Supervisory Authority*** (and, once a ruling is given, judicial remedy by the competent court of law). If the data subject deems the controller's reply to the claim to be inadequate, they can appeal to the judicial authorities or the Supervisory Authority for remedy, in the latter case by lodging complaint pursuant to art. 77 of the GDPR.

The complaint is an evidenced deed by which the data subject presents a breach of the personal data protection act (art. 77 GDPR and articles 140-bis to 143 of the Code) by the Data Controller. A complaint may be signed directly by the data subject (or on their behalf by an attorney, proxy or a non-profit organization or association). In the latter cases, power of attorney must be registered with the Supervisory Authority along with all documentation necessary for assessing the claim. The complaint and any power of attorney must be signed by authenticated signature (digital or autographed signature)

→ ***Direct appeal to the competent court of law***. As an alternative to lodging a complaint with the Supervisory Authority, the data subject may appeal directly to the district judge (at the court where the data controller is established) for an effective judicial remedy against a legally binding decision of a supervisory authority concerning them. The appeal must be lodged within 30 days of receiving notice of the decision.

2.4. Personal data aggregation through audience measuring technologies

2.4.1 An introduction to data aggregation

In a general sense, the term "**aggregation**" refers to the combination of homogeneous data sets (at least 3) and their statistical examination as a whole to obtain additional information in absolute numerical or percentage form, with which to express a statistical value. This information is considered as "**aggregated data**".
In this *white paper* we consider two possible aggregation scenarios:

1. In the first, information collected by *audience* measurement technology is combined with other information collected using the same technology;
2. In the second, information collected by *audience* measurement technology is combined with information from other sources (for example, *datasets* purchased from other companies).

In both cases, the information must be checked for homogeneity (a requirement that must be met for statistical reasons) before proceeding with the aggregation.

The information being aggregated may or may not concern identified or identifiable natural persons, and so may be of a personal nature. In this sense:

- The aggregation of information not of a personal nature is not within the scope of the data protection regulations.

- On the other hand, the aggregation of personal data is to all effects considered as personal data processing (art. 4, para. 2) of the Regulation) and, as such, must be conducted in full compliance with the data protection regulations.

To establish whether the aggregated data is effectively of a personal nature (art. 4, para. 1) of the Regulation), we must determine whether the controller is effectively capable of re-identifying the natural persons to whom the aggregated data refers. That is to say, considering solely the aggregated data, we must determine whether the controller **still has the effective possibility of identifying the natural persons involved, by relating all the various components of its intellectual property using all reasonable means available**. In this sense:

- if the controller is still able to re-identify the data subjects, the aggregated data will still be considered as personal data, and as such subject to application of the data protection regulations;
- if the controller is no longer able to re-identify the data subjects, the aggregated data will no longer be considered as personal data, and its use not subject to application of the data protection regulations.

2.4.2 Re-identification of data subjects to whom the aggregated data refers: methodology

To ascertain whether the possibility of re-identifying the data subjects really exists, we have to consider all the specific elements of the individual cases (see art. 4, para. 1), 5) and 6) and *Recital* 15 and 26 of the Regulation; see also Opinion 05/2014 on anonymization techniques by the Working Party under Article 29, adopted 10 April 2014). The concrete elements to consider should include:

- all components of the data controller's intellectual property (for example, *databases*, paper archives, any other structured personal data), regardless of whether these components are centralized, decentralized or distributed functionally or geographically;
- Any other information reasonably accessible to the data controller;
- the effective possibility of correlating all of the information available to the data controller,
- for example by interconnection, comparison, or other types of association between the data elements;
- all of the means available to the data controller that could be reasonably used to directly identify a natural person;
- all of the means available on the market the data controller could reasonably use to directly identify a natural person;
- the reasonable possibility that the data controller uses such means to identify natural persons directly or indirectly;
- other objective factors such as;
  - the costs, resources, and other expenses the data controller would sustain for this type of identification;
  - the time such identification would take;
  - the state of the art of the technology available when the data is processed;
  - the technological developments that could be reasonably forecast to arrive on the market over the relatively short term.

2.4.3 The principles safeguarded and technical/ organizational measures to mitigate the risk of re-identification of the data subjects to whom aggregated personal data refers

To limit the risk that data subjects may be re-identified, first and foremost we have verified whether the personal data to be aggregated can be previously anonymized. Indeed, as specified above in para. 2.4.1, where the information to be aggregated is not of a personal nature, the data protection regulations are not applicable.

If anonymization is not possible, before proceeding to aggregate the personal information, the data controller must take the following precautions:

- give due consideration to the nature, scope of application, context and purpose of the aggregation, as well as the risks to the rights of freedoms of the data subjects that differ in terms of probability and severity, and implement appropriate technical and organizational measures in compliance with article 5, para. 2, 24, 25 and 32 of the Regulation;
- assess the need for a data protection impact assessment (DPIA) as per art. 35 of the Regulation;
- Seek the advice of the data protection officer in accordance with art. 35, para. 2 and 39, para. 1, point c) of the Regulation.

3. DPIA, Risk Analysis and Risk matrices

A DPIA is strongly recommended as a means for determining the potential risks underlying any the processing of personal data that could compromise the rights and freedoms of natural persons contemplated by the GDPR.

In this sense the risk analysis element is fundamental. Hence the need for a DPIA to include a Risk analysis assessment with a view to: i) determining the categories of risk; ii) evaluating their impact and probability of occurrence associated with elements of vulnerability in a given context; iii) identifying countermeasures able to reduce the level of residual risk to acceptable levels. These elements are specified in section 3.1.

Lastly, section 3.2 presents the risk analysis web tool given in this white paper. Compiling the tool gives an example of the methodology described above.

3.1. Data Protection Impact Assessment (DPIA)

Data protection impact assessment is necessary when describing a given type of processing with a view to evaluating necessity, proportionality, and related risks.

It is important to note that the GDPR refers to the obligation of the controller and/or processor to consider the risks that certain types of processing present to the rights and freedoms of data subjects, in two different articles:

- art. 24 includes risk analysis among the processing characteristics to consider for the implementation of all the necessary technical and organizational measures. The article requires that the controller must always prove to have adopted all the necessary risk mitigation measures, to render the processing compliant.
- art. 35 on the other hand, requires a specific impact assessment if the processing represents a high level of risk to data subjects, considering the circumstances indicated by the Regulation. In addition to this, the article provides the guidelines and lists the elements to consider in an impact assessment, as well as defining the significant role of the Supervisory authority.

Given that the technologies examined here process personal data in a variety of ways, as a consequence they could represent a high level risk to the rights and freedoms of natural persons, especially in such a delicate area as people “counting”. If these risks are effectively present, art. 35 of the GDPR details how the data controller is obliged to conduct a prior data protection impact assessment (DPIA) on the types of processing involved, if the processes involve at least one of the following elements:

1. Evaluation or attribution of a score, including profiling and prediction (Recitals 71 and 91);
2. automated decision processes with legal or similar effects;
3. systematic monitoring (article 35, paragraph 3, point c);
4. special category data (art. 9) or data of a highly personal nature (art. 10);
5. large scale data processing (Recital 91);
6. creation of correspondences of combinations/aggregations of datasets;
7. data concerning vulnerable natural subjects (Recital 75);

8. Innovative use of application of new technological or organizational solutions (article 35, paragraph 1 and Recitals 89 and 91).
9. impossibility for the data subject to exercise a right or to use a service or a contract (article 22 and Recital 91).

An impact assessment may concern an individual process or several processes with similarities in terms of nature, scope, context, purpose, and risk.
Impact assessment is therefore an instrument that allows the data controller to analyze the risks and impact of the present (and other) cases on the rights and freedoms of the data subjects involved.

"Carrying out a DPIA is a continual process, not a one-time exercise"

3.1.1 Methodology for the implementation of a DPIA

Although the GDPR does not define a standard method for conducting a DPIA (but only a set of mandatory content), a variety of frameworks and templates are available for this type of analysis. This section offers a brief description of the fundamental elements involved in a DPIA:

1. **Context analysis**
   The first phase of the DPIA involves the analysis and description of the context and the purpose of each type of processing, specifying the responsibilities associated with the processing.
   The context is considered as consisting of:
   - *Data processed:* data categories (Common, Special,), data groups (personal details, …);
   - *Process life cycle:* the functional description of the processing;
   - Data support resources: description of the Hardware and Software used (for example: Antennas, Cloud, ...).

2. **Compliance of processing**
   In the second phase the DPIA must demonstrate and ensure:
   - that the purposes of the processing are transparent, explicit, and lawful (to this regard, see section 2.1 of this chapter);
   - that the processing is lawful, and the data process is adequate, pertinent, complete, and limited to the purposes described in the context;
   - that the data retention period and methods are defined;
   - that the data subjects are adequately informed of the processing carried out and the rights they are entitled to exercise.

3. **Risk analysis**
   The third phase of the DPIA involves identifying the risks with impact on the personal freedoms of the data subjects and the appropriate countermeasures for mitigating the risk and demonstrating the compliance of the processing.

After this, the output of the analysis will be in the form of a level of risk exposure related to the use of a given technology (or combination of technologies) based on the probability of occurrence, the potential impact (severity) and the countermeasures that certify (or otherwise) the adequacy of the processing.

3.2. Methodology for conducting a privacy risk analysis assessment

The methodologies and criteria applied in the general analysis are described below.

Assumption: *The analysis concerns the protection of the data subject's personal freedoms, specifically, in terms of the Integrity, Availability and Confidentiality of the personal data, mitigating any risks inherent to the technology in question through the implementation of countermeasures.*

1. Context and technological description

The first element to consider is how the technology works and the context in which it operates. To this regard, the following must be identified:

- the categories of personal data processed;
- the purposes of the processing;
- the description of its function.

For more information on these subjects, see chapter 1.

2. Risk identification

The second element concerns the categories of risk to the integrity, availability, and confidentiality of the personal data. Several guidelines are provided to help in identifying macro categories

Assumption: The risks to each category of data for each technology analyzed are the same

The risk categories identified are:

- *Unlawful access to data*: partial or total loss of data confidentiality. Confidentiality is understood as rendering the data accessible exclusively to duly authorized users.
- *Unlawful modification of data*; partial or total loss of data integrity. Integrity is understood as the prevention of undue alteration or manipulation of the data;
- *Loss of data*; partial or total loss of data availability. Availability is understood as the property of being accessible and usable on demand by an authorized user.

3. Identification and attribution of threat value

Each category of risk can be related to a series of events (or threats). In any risk analysis assessment is therefore essential to draw up an exhaustive list of the potential threats, and attribute each of them a “weight” (or value), in terms of the impact they could have on the confidentiality, integrity and availability of the information.

***Assumption:** Each of the technologies examined in subject to the same risks and consequently the same threats*

***Assumption:** To simplify the analysis model, these guidelines do not identify and consider the vulnerabilities associated with each threat.*

Identification: the categories of threats to compliance of the processing are as follows:

- *Software - Malicious intrusion:* understood as malware or any other form of malicious (damaging) software, regardless of the methods used to spread it. This kind of software is usually designed to retrieve confidential data and cause damage to the systems it attacks;
- *Software - Execution error:* understood as any error in software, software components or applications caused by an incomplete or damaged code
- *Infrastructure - No connectivity:* understood as the incapacity of systems to connect and exchange information in a normal manner
- *Infrastructure - Electrical power outage* understood as the absence of a normal mains power supply
- *Infrastructure - Natural disaster:* understood as damage due to a sudden and violent natural event
- *Hardware – Damage:* understood as a partial loss of function or integrity of the unalterable physical elements of a data processing system
- *Hardware - Failure:* understood as the total loss of function or integrity of the unalterable physical elements of a data processing system
- *Persona - Malicious behavior:* understood as a series of actions with the intention of causing damage through actions in contrast with internal regulations or legal obligations

Valorization: impact and probability of occurrence are evaluated for each category of threat according to criteria able to offer an initially risk value prior to mitigation by countermeasures. Impact is given a score between 1 and 5 as illustrated in the tables below:

- *Impact on Confidentiality:* understood as the partial/total unauthorized distribution of the personal data of one or more data subjects;

Description of impact level	**Evaluation**
Negligible loss of data controller internal confidentiality	1
Limited loss of data controller internal confidentiality	2
Widespread loss of data controller internal confidentiality	3
Limited loss of external confidentiality	4
Widespread loss of external confidentiality	**5**

- *Impact on Integrity: understood as the portion of the total personal data of one or more data subjects that have has suffered an irreversible alteration;*

Description of impact level	**Evaluation**
Limited portion < 5%	1
Limited portion < 10%	2
Consistent portion < 33%	3
Very consistent portion < 66%	4
Total □ 66%	**5**

- *Impact on availability:* understood as the time between the need for the personal data of one or more data subjects and its availability (permanent unavailability is considered as total loss of integrity);

Description of impact level	**Evaluation**
Less than 1 hour	1
Less than 4 hours	2
Less than 2 days	3
Less than 5 days	4
Less than 10 days	**5**

The “security impact” is thus the result given by the aggregation algorithm applied to the impacts described above, as follows:

$$\textbf{Security Impact}_{\textbf{(xm)}} = \text{AVERAGE[MAX(Impacts)}_{(mx)} + \text{AVERAGE(Impacts)}_{(mx)}\text{]}$$

4. Attribution of threat occurrence probability

Occurrence Probability: the probability of occurrence of each category of risk is determined according to the criteria below:

Description of occurrence probability	**Evaluation**
Threat that occurred on a five-year basis	0.1
Threat that occurs on an annual basis	0.25
Threat that occurred every six months	0.5
Threat that occurred monthly	0.75
Threat occurring weekly	1

5. Threat risk calculation

At this point the risk can be calculated, understood as the index corresponding to the uncertainty of achieving an objective; in this context, risk can be defined as the uncertainty associated with compliance of the data controller's processing of personal data belonging to one of more data subjects, using determined technologies.

The algorithm for calculating risk as a function of impacts and probability but without implementation of countermeasures, is as follows:

$$\boldsymbol{Risk}_{\boldsymbol{(xm)}} = \textit{Security Impact}_{(mx)} * \textit{Occurrence Probability}_{(xm)}$$

Given that risk is assessed on a scale from 1 to 5, the aim is to mitigate the risk to achieve a risk value of less than 2.

6. Countermeasure identification and evaluation

Having determined the risk index of each of the identified threats (through occurrence probability and impact calculation), the technical and organizational measures for mitigating them can be identified. A few examples of the possible types of mitigation are given below:

- *Password:* understood as a series of at least 8 upper- and lowercase alphanumeric characters used as the key to access systems, networks, and databases;
- *Access rights:* understood as the control process for physical and logical access to information processing systems;
- *Backup:* understood as the set of information duplication operations (periodicity, methodology,) aimed at ensuring the availability and integrity of personal data, as well as its confidentiality;
- *Asset positioning:* the physical or virtual place where information is stored, processed;
- *Anonymization:* the process by which an identified dataset loses at least the capacity to be relatable, identifiable, and deducible, thereby becoming a set of anonymous data*;*

- *Data partitioning:* the process to reduce the possibility of correlation between the personal data and total data compromise (by the logical separation of the environments);
- *Logic access control:* this involves limiting the risk of unauthorized access to personal data in digital form, for example by defining authorization profiles in systems;
- *Archiving:* the storage of data no longer in current use but for which the retention period has not yet expired;
- *Hard copy document security:* policies to define how and where documents must be managed (printed, archived, destroyed, and shared);
- *Data minimization:* understood as limitation of personal data processing to the minimum necessary for achieving the purpose;
- *Vulnerability assessment:* the process of researching vulnerabilities and threats present in systems;
- *Firewall system:* a perimeter defense system for one or more networks;
- *Management of responsibilities associated with processing:* organizational countermeasures for defining the various data processing responsibilities*;*
- *Physical access control:* understood as the establishment of physical controls to areas where processing is carried out;
- *Hardware / asset security:* the securing of processing equipment (cabinets, workstations, ...);
- *Nominal users:* users assigned to a given resource (usually identified by name and surname of the resource)
- *System administrator appointment and audit;* certification of the competence and professionalism of resources appointed with the tasks and privileges of administrators of personal data processing systems*;*
- *Security & privacy incident management processes;* processes defined and implemented for the linear management of processing-related problems;
- *Personnel training and management:* personal undergo periodic training through specific awareness courses and competence tests;
- *Management of data access by third parties:* implementation of control systems for access by external resources to processing systems;
- *Monitoring system:* a preventive countermeasure for identifying processing problems data subjects are not yet aware of, and reporting them to the resources tasked with remedying them;
- *Encryption:* the process to render any given data incomprehensible, to ensure its confidentiality
- *Pseudonymization:* the process by which the processing of the personal data cannot be used to identify the data subjects themselves;
- *Authentication:* the process to certify the identity of a resource duly authorized to carry out data processing;
- *Redundant connectivity (provider diversification):* the possible use of two different connectivity providers to ensure data availability;
- *Genset:* a machine consisting of an internal combustion engine and an alternator to generate electrical energy;
- *Logging:* the mechanism that permits the registration of the operations carried out on an IT system to identify any unauthorized access, record events, and ensure data inalterability;

How do we attribute a value to the countermeasures listed so far? To keep the proposed model as simple as possible, we can distinguish between **preventive** measures and **mitigating** measures.

Preventive measures mitigate risk by acting on the probability of occurrence of a given event, or the probability of a threat.
Each of the countermeasures listed has been attributed a "preventive mitigation" value based on the following criteria:

Preventive measure level	**Evaluation**
Application of the countermeasure reduces the possibility of threat by approx. 10%	0.1
Application of the countermeasure reduces the possibility of threat by approx. 25%	0.25
Application of the countermeasure reduces the possibility of threat by approx. half	0.5
Application of the countermeasure reduces the possibility of threat by approx. 75%	0.75
Application of the countermeasure reduces the possibility of threat to zero	1

The purpose of mitigation countermeasures on the other is to contain the impact of a given event that has occurred.
Each of the countermeasures listed has been attributed a "preventive containment" value based on the following criteria:

Preventive measure level	**Evaluation**
Application of the countermeasure reduces the possibility of threat by approx. 10%	0.1
Application of the countermeasure reduces the possibility of threat by approx. 25%	0.25
Application of the countermeasure reduces the possibility of threat by approx. half	0.5
Application of the countermeasure reduces the possibility of threat by approx. 75%	0.75
Application of the countermeasure reduces the possibility of threat to zero	1

After attributing a value to the preventive and mitigation countermeasures, they can be combined to determine the single value associated with risk in question, using the algorithm:

$$\textit{Countermeasure value}_{(xm)} = \textit{Security Impact}_{(xm)} * \textit{Occurrence Probability}_{(xm)}$$

7. Residual risk calculation

Residual risk, in the contest of this analysis, is the uncertainty associated with compliance of the personal data processing of one or more data subjects conducted by the data controller using any given technology.

$$\textit{Res. risk}_{(xm)} = (\textit{Security Impact}_{(xm)} * \textit{Occurrence Probability}_{(xm)}) - \textit{Countermeasure value}_{(xm}$$

After calculating the Residual risk for the category of threat under analysis, the process must be repeated for all the other threats to the risk categories identified for the technology under analysis. As we explain at the start of this chapter (3. Threat value identification and attribution) each threat acts on one or more of the identified risk categories. After analyzing all of them, the residual risk for each category can be determined:

$$\textit{Residual risk}_{(R)\ \textit{Data loss}} = \textit{Mean }(\textit{Residual risk}_{(m)})$$

$$\textit{Residual risk}_{(R)\ \textit{Unauthorized alteration of data}} = \textit{Mean }(\textit{Residual risk}_{(m)})$$

$$\textit{Residual risk}_{(R)\ \textit{Unauthorized access to data}} = \textit{Mean }(\textit{Residual risk}_{(m)})$$

The result of this analysis gives the Residual Risk for the technology in question

$$\textit{Residual risk }(_{x}) = \textit{Residual risk}_{(R)\ \textit{Data loss}} + \textit{Residual risk}_{(R)\ \textit{Unauthorized alteration of data}} + \textit{Residual risk}_{(R)\ \textit{Unauthorized access to data}}$$

m = Threat Category
R = Risk Category
X = Technology

X < 1	Minimum risk	The risks presented by technologies at this level can be ignored. No further preventive or mitigation measures are required, just information activities
1 ≤ X < 2	Partial risk	The risks presented by technologies at this level require management. The adequacy and effectiveness of the chosen countermeasures must be constantly monitored.
2 ≤ X < 3	Considerable risk	The risks presented by technologies at this level require management. The implementation of further countermeasures must be assessed, in addition to continually monitoring those already adopted.
3 ≤ X < 4	Significant risk	The risks presented by technologies at this level require management. Appropriate countermeasures must be implemented immediately

4 ≤ X ≤ 5	Critical risk	The modalities and purpose of the processing must be examined by the Supervisory Authority

3.3. Web Tool

The analysis described in section 3.1 is available in an automatic, digital format to readers via the link below or the QR code given here.

https://is.gd/audiencetech_riskanalysis

SCAN ME

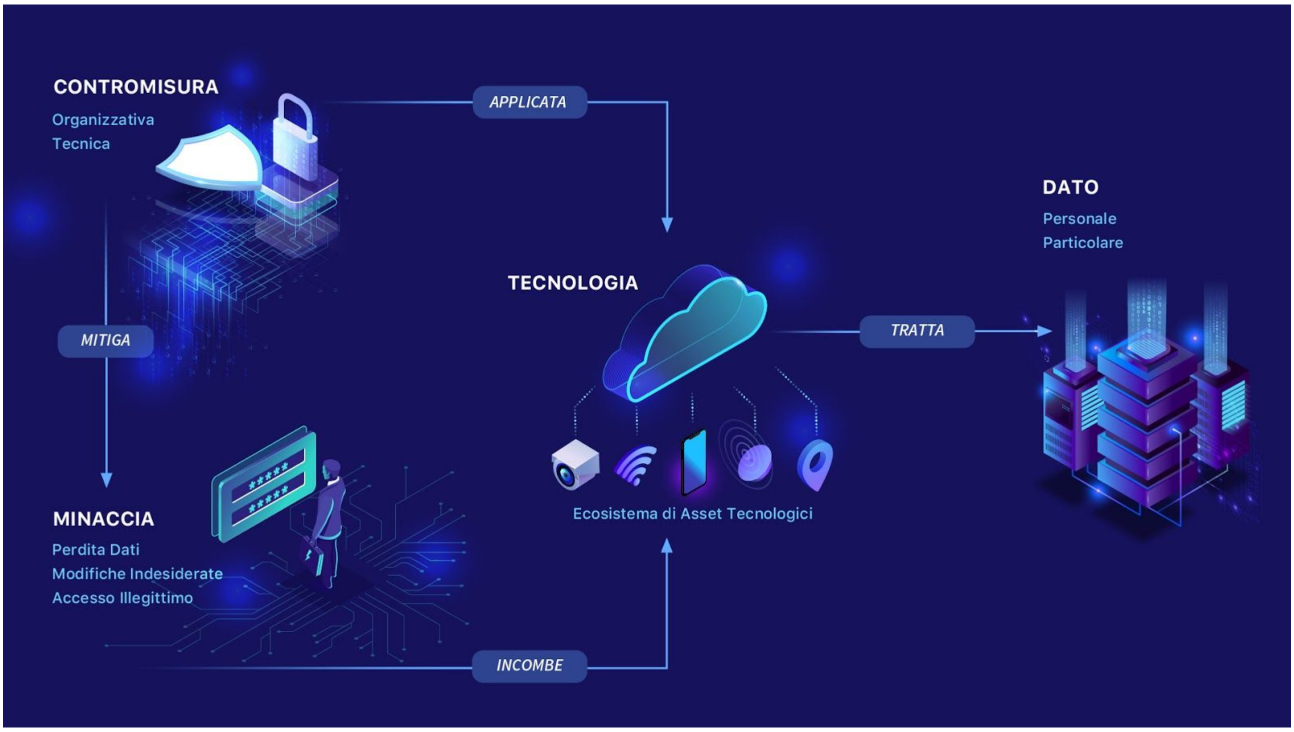
The link connects to a web tool that summarizes the text and the analysis for each technology.

3.4. Data Security

Art. 5(1) point f) of the GDPR indicates that personal data must be processed in a manner that ensures: appropriate security [...] including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.

It is therefore necessary to ensure “appropriate” levels of personal data integrity, availability, and confidentiality; the level of adequacy is expressed in concrete form in the criteria applied to the risk analysis.

Ensuring security means protecting “containers” of information (assets) from incumbent threats though adequate countermeasures and, consequently, permitting compliance of the data processing



Source: www.fabbricadigitale.com

Note that countermeasures may vary in terms of content and intensity, mitigating the probability of occurrence and/or the impact of the risk, but are strictly dependent on the original risk assessment of the processing itself and any further risk assessments conducted by the Controller and/or Processor.

It is also important to stress how data security has implications that go beyond each process, directly concerning:

- *the technologies and systems used to conduct the activities*
- *the players involved in the processing itself*

Articles 25 and 32 of the Regulation also focus on organizational aspects, and suggest several functional countermeasures such as:

- *possession or acquisition of IT skills;*
- *use of products for data protection and classification;*
- *static and dynamic assessment of software vulnerability;*
- *verification of Open Source software compliance;*
- *review and communication of organization procedures;*

To adapt the organization to the Regulation, it must be managed according to the principles of privacy by default and design, in the following macro-categories:

1. *Production processes*
    a. *software development estimation and analysis*
    b. *software architecture design*
    c. *software production*
    d. *software testing*

    e. *software testing*
    f. *software release*

2. *Support processes*
    a. *detection of information loss and prevention;*
    b. *loss of information prevention;*
    c. *content monitoring and filtering;*
    d. *information protection and control;*
    e. *extrusion prevention system;*
    f. *intrusion prevention system.*

In general, to adapt the data management system in an organization to the Regulation, it must be subject to the following processes:

- classification: the process output must ensure confidentiality of the information. Appropriate output could be obtained, for example, by giving different values to different categories of data (metadata, data, and documents), attributing them distinct levels of confidentiality (public, internal, confidential, and reserved);
- protection: to ensure adequate levels of integrity and availability, it is necessary to implement authentication (for example, passwords, named users) and encryption systems, network protocols, remote access (VPN) and backup systems;
- monitoring: this involves conducting penetration tests and vulnerability assessments on software and systems, allowing the company to promptly detect the appearance of vulnerabilities and threats. Further monitoring activities include data logging and data log analysis.

4. Conclusions, best practices, and problems (still) open

In conclusion to this work, we feel it is important to offer a response to the original purpose of this white paper, that of better understanding the principal risks to the protection of personal data represented by the technologies we have examined.
It is equally important to attempt to define a number of guidelines based on our observations, with the caveat that all of the opinions given here are derived insofar as possible from the scrupulous analysis of the orientations of the Supervisory Authorities. Where this has not been possible (or where our opinions are based on the observations made during the months of research dedicated to this white paper) this will be duly indicated.
Any observations not effectively based on any given regulation are given solely for the purposes of the study. They shall in no way be considered binding nor as substituting any regulation in force.

Initial considerations on the lawfulness of processing data collected using audience measurement technology

In general terms, the lawfulness of data processing depends on the purpose of the processing in concrete terms. For the purposes of this white paper, we assume that purposes of data processing using audience measurement technology are normally associated with marketing and market research analytical surveys of audience for commercial purposes. In this case, we have seen how data controllers can invoke legitimate interest as per art 6.1.f) of the GDPR if, after legitimate interest assessment ("LIA"), they consider that the interests, rights and fundamental freedoms of data subjects do not override their legitimate interest, also considering the reasonable expectations of the data subjects depending on their relationship with the controllers themselves; where this is not the case, controllers cannot invoke legitimate interest and necessarily must obtain the consent of the data subjects as per art. 6.1.a) of the GDPR. In substantial terms, the weaker the LIA finds the legitimate interest, the more opportune it would be for the controller to request specific consent by the data subject.

An exception to the rule by which the legal basis depends substantially on the purpose of the processing is the case of "location data" as per art. 2, point c) of the e-Privacy Directive. Indeed, in this case the directive gives relevance to the nature of the data in question and in art. 9 specifies that the only suitable legal basis for processing is the effective consent of the data subjects.

1. Image and video stream analysis and acquisition systems

Image analysis and radio frequency systems have several aspects worthy of attention and protection.

From a legal standpoint (legal precedent) the Supervisory Authorities have:

- imposed the need to verify respect of the principles of necessity, proportionality, purpose, fairness, and lawfulness;
- clarified that personal data processing is present, even if only for a few seconds;
- clarified that if the images are erased by the system almost immediately, no personal data is permanently stored by the system and the system only uses face detection algorithms, the data processing itself would be compliant with the principles of the Code.
- prescribed a simplified privacy notice, to supplement with more complete information on a website or through the QR code present on the window banner, near the acquisition device;
- allowed, providing adequate precautions are taken to mitigate risks to fundamental rights and freedoms, "the use of cameras as mere sensors, the use of processing software

capable of extracting statistical data from images taken almost immediately, without biometric processing, image recordings or live access";

- ruled that image recording must be excluded and display of images limited solely to persons responsible for processing and the maintenance of the equipment in real time, and that data subjects must be able to exercise their rights;
- clarified that, with respect to consent, that balance of interests (now legitimate interest) can be taken as the legal basis for the use of these technologies;
- required that the image and video stream acquisition/analysis equipment undergo periodic monitoring, at intervals of at least six months.

Regarding these aspects, manufacturers of this category of equipment must:

- Ensure that the raw data is processed in the place and at the moment the image is acquired (and that the image remains in the volatile memory of the equipment only for the time necessary for its processing and subsequent erasure)
- Implement to appropriate *data security* measures to prevent incidents, *data breaches* or *data leaks*;
- Ensure that images and video cannot be saved or externally accessed, except by authorized personnel;
- Ensure that such personnel are duly appointed and authorized to process personal data;
- Provide a brief privacy notice in the area in which systems of this category are operating, linked with more complete information (by means of web link or QR code).
- Establish an equipment monitoring plan, combined with an *auditing* system to prevent tampering and malfunction.

Other aspects to consider:

- Systems in this category do not permit the exercise of data subject rights due to their intrinsic technical nature. In effect, the images or videos are erased almost immediately. This means that operations like erasure, correction, opposition and so on are physically impossible.
  The European Supervisory Authority has strictly indicated that the impossibility of data subjects to exercise their rights is one of the fundamental reasons for conducting a *Data Protection Impact Assessment* (DPIA). Moreover, as specified in art. 35, the fact that a system is capable of measurements in public space (with potential interaction with a significant number of natural persons) is another significant reason for conducting a DPIA. For these reasons we strongly recommend conducting a DPIA.

2. Radio frequency systems

Radio frequency systems have several aspects worthy of attention and protection. From a legal standpoint (legal precedent) the Supervisory Authorities have:

- clarified that RFID systems must be configured such as to avoid the use of the data subject's personal data or identity, where not strictly necessary for the declared purpose;
- determined that the location tracking of mobile terminals to trace the physical movements of people (for example "Wi-Fi" or "Bluetooth" tracking) could be conducted only after anonymization of the data and obtaining the valid consent of the data subjects; in this case

the use of legitimate interest as the legal basis for the use of the data for marketing or market research purposes is not considered as valid

- In the case of use for medical purposes, personal data may be processed exclusively by subjects operating in the health sector and with the prior, informed consent of the data subject, even without authorization by the Supervisory Authority.

Other aspects to consider:

- **Rights of Data subjects**
  Radio frequency systems effectively permit the exercise of data subject rights given that there are no technical-organizational impediments to their potential exercise. These rights can be exercised by data subjects through the usual channels (mail, Certified mail, Service desk portal, ...)**.**

- **DPIA**
  We recommend conducting a DPIA because these technological systems are generally used to process a significant quantity of information and data (interacting with a significant number of physical persons), some of which personal (MAC address).[2]

3. Cell network data acquisition systems

The aggregated data sold by mobile phone companies is obtained by processing the personal data of the natural persons they collect and retain for administrative and operational purposes, as well as for compliance with legal obligations.

The data sold to the public by mobile phone companies is always aggregated. In this context, the risk to the natural persons to whom the data refers derives from the depth, veracity and accuracy of the level of aggregation implemented by the company, and the technical means by which the processing is carried out.

Regarding the regulatory aspects of using this technology, the Supervisory Authorities have listed a series of conditions mobile phone companies must meet in order to use aggregated personal data:

- use of aggregated personal data from which **it is not immediately possible to gather detailed information on the individual data subjects**;
- use of a **range** of values in the creation of the *clusters* (e.g. using age groups such as 20-30 or 30-40, or geographical areas larger than the single municipality the users belong to), or implementation of equivalent measures with the purpose of reducing the risk of reaching a level of detail sufficient to permit the identification of users, even indirectly;
- *ex post* checks on each *cluster* extracted, to prevent the creation of *clusters* of users containing less than 100 units and thereby significantly reduce the capacity of the data to identify users after processing;
- storage of the aggregated personal data subject in specifically dedicated systems, functionally separate from the original system source of the aggregated data and any other systems used by the data controller for other purposes;

[2] Provvedimento n. 370 del 29 novembre 2012

- data processors carrying out aggregated personal data processing must be assigned limited authentication profiles, different to those who perform any further processing;
- the aggregated personal data must be stored for a limited period, after which it must be erased or rendered anonymous in an irreversible and permanent manner;
- issue of a privacy notice concerning the processing of the personal data specifying that the processing is conducted using aggregated personal information and therefore does not require the prior and specific consent of the data subjects.

As previously mentioned, to conduct profiling activities using “aggregated” personal data, mobile phones companies must implement the measures required by the Supervisory Authority.

The purchase and subsequent use of aggregated data is not considered as personal data processing, in the sense that the level of aggregation implemented by the companies does not permit the identification of an individual data subject.

Operators that purchase this kind of data can protect themselves against any dispute with the data subjects involved in the processing by verifying that the mobile phone companies have implemented all of the measures required by the Supervisory Authority and the principles of the GDPR. However, in most cases this kind of verification is virtually impossible. For this reason, we recommend including guarantee and indemnity clauses on the correct implementation of the required measures in both the original personal data processing and the subsequent personal data aggregation process, in all contractual relations with the mobile phone companies.

4. SDK, Beacon, bidstream

Personal data acquisition systems based on SDK, BidStream and Beacon technology pose problems due to the sheer number of subjects to whom this data is communicated,

For this reason, any time apps containing SDK or other codes able to access BidStream for data transfer to advertiser networks, users must:

- be specifically informed of this additional processing (with respect to the “standard” processing by the SDK “carrier” app) by the app;

- be specifically informed about the series of subjects who will process the data collected by SDK (companies developing the technology and networks of subjects acquiring the data);

- provide a series of consents, both to the use of their location data for further purposes, and to the transfer of their location data to the subjects indicated in the privacy notice, who process the data as independent data controllers;

- be informed about the retention times of the data collected (since the term of 13 months indicated by Fidzup was considered excessive, the term of 3 months was considered sufficient.

Other aspects to consider:

The identification of a network of advertisers would be a complicated matter a priori, given that by nature the list of subjects would be susceptible to frequent changes.

To ensure that you provide correct and complete privacy information, we recommend including links to lists of advertisers that are continually updated, and the corresponding privacy notices.

However, the specific consent requirement may not be fully satisfied in the case of consent given to the entire network of advertisers.

- **Rights of Data subjects**
  The exercise of data subject rights remains applicable even with regard to personal data collected by the above methods, with the complication that they may only be exercised against the company that developed the App integrated into the aforementioned systems.

- **DPIA**
  While this is type of data processing is not based on the use of "new" technology, but rather on a now widespread market practice, we feel that conduction of a DPIA would be appropriate also, and especially, in the case of a decision to use a different legal basis (e.g.) Legitimate Interest) for the processing of personal data collected using the above technologies.
  In specific terms, if legitimate interest is taken as the legal basis for providing data to the network of advertisers, a Balancing Test would be necessary, in addition to the DPIA, to demonstrate that the processing does not represent risks to the freedoms and rights of the data subjects and to justify the legal basis of this operation.

5. Occupancy Detection Systems

The Supervisory Authority has not made any specific provisions regarding the use of *Lidar* systems and occupancy sensors.

The functions of the technology imply limited privacy problems since it does not permit recognition of the unique personal features and does not involve the processing of personal information. Consequently, it does not present significant risks.

Other aspects to consider:

- **Rights of Data subjects**
  The systems in this category do not allows for the exercise of data subject rights since they do not permit recognition of unique personal features and do not involve the processing of personal information.

- **DPIA**
  Due to their technical nature, occupancy detection systems do not permit the exercise of data subject rights. We therefore recommend conduction of a DPIA.
  Moreover, given that this technology is not widely used yet for personal data processing, a

DPIA would be especially useful for assessing the impact of any future technical innovations