Centre for Information Policy Leadership
Hunton & Williams LLP

16 March 2017

CIPL Examples of Legitimate Interest Grounds for Processing of Personal Data

Discussion Draft

In preparation for CIPL GDPR Project Madrid Workshop III, CIPL has asked the GDPR project members for examples where a) legitimate interest is the appropriate ground for processing personal data, and b) in some cases the only legal ground for processing.

The purpose of the exercise was to establish current practices and instances of organisations using legitimate interest processing under the current law and to inform all the stakeholders involved in the GDPR implementation of the broad application of this ground of processing today.

Part I of this document is a summary of the examples we received, organised in broad categories of processing purposes. Part II are specific case studies from different industry sectors that provide an in-depth discussion of the rationale for legitimate interest processing, and the balancing of interests and risk mitigation undertaken by the controller to ensure accountability and to meet the reasonable expectations of the individual.

The examples we received demonstrate the following:

a) organisations in all sectors currently use legitimate interest processing for a very large variety of processing personal data and this trend is likely to continue under the GDPR.
b) in many cases, legitimate interest processing is the most appropriate ground for processing, as it entails organisational accountability and enables responsible uses of personal data, while effectively protecting data privacy rights of individuals.
c) in some cases, organisations use legitimate interest as the only applicable ground for processing, as none of the other grounds can be relied on in a particular case.
d) organisations using legitimate interest always consider the interest in case (of controller or a third party / parties); they balance the interest with the rights of individuals; and they also apply safeguards and compliance steps to ensure that individuals rights are not prejudiced in any given case.
e) the current use cases of legitimate interest tend to form a pattern, with most common examples being prevalent in many organisations and all the cases broadly falling in several wide categories outlined below. The most prevalent category of legitimate interest cases across all industries is i) fraud detection and prevention and ii) information and system security.

PART I:

Summary of categories and examples of legitimate interest processing

1. Fraud detection and prevention (crime prevention)

Many companies need to process certain personal data to comply with industry standards, regulators' requirements and other requirements related to fraud prevention and anti-money laundering. These are often financial institutions such as banks, credit card issues and insurance companies, but also other organisation in consumer-facing businesses and they often need to process data in a global context. Specific examples are:

- Fraud and financial crime detection and prevention
- Anti-money laundry (AML) Watch-lists
- Know-your-customer (KYC)
- Credit checks and risk assessments
- Politically Exposed Persons (PEP)
- Terrorist financing detection and prevention
- Anti-fraud purposes - using information gathered from various sources, such as public directories and publicly available online personal or professional profiles, to check identities when purchases are deemed as potentially fraudulent
- Defending claims, e.g. sharing CCTV images for insurance purposes

2. Compliance with foreign law, law enforcement, court and regulatory bodies' requirements

Organisations in all sectors are subject to a multitude of laws and regulations; to reporting obligations to regulators; to regulators', law enforcement and judicial requests and regulations, including from specific industry regulatory bodies, such as health or financial regulators, both within EU and abroad. Global companies are often subject to many competing laws, which sometimes appear to be in direct conflict with data privacy laws elsewhere. Organisations are often compelled to use legitimate interest processing in some of these instances to base processing and sharing of some personal data where they are sufficiently able put in place mitigations and safeguards for rights of individuals. Specific examples are:

- Operation of Business Conduct and Ethics Line and Reporting under the Sarbanes-Oxley Act (SOX)
- Economic sanctions and export control list screening under economic sanctions and export control laws
- Data loss prevention software and tools for compliance with data protection laws and client contractual requirements

- Compliance with requests for disclosures to law enforcement, courts and regulatory bodies, both EU and foreign

3. Industry watch-lists and industry self-regulatory schemes

Organisations in credit industry, banking, finance, insurance, retail often need to process certain personal data to protect and develop industry standards; share intelligence about individuals or concerns that may have a negative or detrimental impact; to set pricing; and to follow industry best practices. Specific examples are:

- Industry watch-lists – non-payment, barred customers, etc.
- Relations with insurers – information to process insurance claims
- To comply with industry practices (issued by the Financial Action Task Force (FATF), Wolfsberg AML Principles, etc.)

4. Information, system, network and cyber security

All organisations need to monitor, detect and protect the organisation, its systems, network, infrastructure, computers, information, intellectual property and other rights from unwanted security intrusion, unauthorised access, disclosure and acquisition of information, data and system breaches, hacking, industrial espionage and cyberattacks. Organisations will inevitably process personal data as part of the purposes stated above, including of direct clients and customers, third parties, employees and any other people who may have access to company systems and networks. Legitimate interest processing is often the only ground that organisations can rely on for this type of processing.

These type processing are conducted by all organisations, in both public and private sector and all lines of industry. Specific examples are:

- Overall information security operations of an organisation to prevent unauthorised access, intrusion, misuse of company systems, networks, computers and information, including prevention of personal data breaches and cyber attacks
- Piracy and malware prevention
- IP rights protection and IP theft prevention
- Website security
- Monitoring access to systems and any downloads
- Use of information gathered form physical access control systems for investigating incidents
- Detection and investigation of security incidents – processing of personal data of individuals involved in an incident, as well as the underlying compromised data
- Investigation and reporting of data breaches
- Product and product user security

5. Employment data processing

Irrespective of industry, organisations process employees' data for legitimate and common business purposes, in situations which are not necessary for the performance of employment contract, but are nevertheless customary, or necessary for operational, administrative, HR and recruitment purposes and to otherwise manage employment relationship and interaction between employees. Specific examples are:

- Background checks and security vetting in recruitment and HR functions
- Office access and operations
- Disaster and emergency management tools and apps
- Internal directories, employee share-point sites, internal websites and other business cooperation and sharing tools.
- Business conduct and ethics reporting lines
- Compliance with internal policies, accountability and governance requirements and corporate investigations
- Call recording and monitoring for call centre employees' training and development purposes
- Employee retention programs
- Workforce and headcount management, forecasts and planning
- Professional learning and development administration
- Travel administration
- Time recording and reporting
- Processing of family members' data in the context of HR records – next of kin, emergency contact, benefits and insurance, etc.
- Additional and specific background checks required by particular clients in respect of processors' employees having access to clients' systems and premises
- Defending claims - sharing CCTV images from premises with insurers when required for processing, investigating or defending claims due to incidents that have occurred on our premises
- Intra-corporations hiring for internal operations

6. General Corporate Operations and Due Diligence

All organisations, irrespective of the sector, use personal data to operate the day-to-day running of the business and plan for strategic growth. This includes management of customer, client, vendor and other relationships, sharing intelligence with internal stakeholders, implementing safety procedures, and planning and allocate resources and budget. Specific examples are:

- Modelling – develop or operate financial/credit/conduct and risk models
- Internal analysis of customers – plan strategy and growth
- Reporting and management information – support business reporting

- Sharing information with other members of the corporate group
- Back-office operations
- Monitoring physical access to offices, visitors and CCTV operations in reception and any other restricted areas
- Processing of personal data of individuals at target company or related to the transaction in M&A transactions
- Corporate reorganisations
- Producing aggregate analytics reported to third party content owners, especially when it is to fulfil licensing obligations
- Business intelligence
- Managing third party relationships (vendors, suppliers, media, business partners)
- Processing identifiable data for the sole purpose of anonymising/de-identifying/re-identifying it for the purposes of using the anonymised data for other purposes (product improvement, analytics, etc.)

7. Product development and enhancement

All organisations process personal data to deliver and improve their products or services. Many technology companies need to process data collected from their services or products in order to deliver that service, or to instruct their products how to work and to continuously keep on improving them. Specific examples are:

- Processing of personal data for research, product development and improvements – such as integrity and fairness of a process/service; or data collected by voice recognition tools, or translation tools, which all depend on ability to collect a lot of data of direct customer and other individuals to be able to create and improve the actual service
- Processing of most device data (including the hardware model, operating system version, advertising identifier, unique application identifiers, unique device identifiers, browser type, language, wireless network, and mobile network information) to improve performance of the app, troubleshoot bugs, and for other internal product needs.
- Information from GPS on smartphones where the chip in the phone needs to provide location data in order to pick up satellite information
- Collection of IP addresses and similar by telecommunication companies that may need to use several unique identifiers to enable them to provide connectivity as well as charge the appropriate person.
- Log files/actions within apps for product use analysis, product performance enhancement and product development
- Monitor use and conduct analytics on a website or app use, pages and links clicked, patterns of navigation, time at a page, devices used, where users are coming from etc.
- Monitor queues at call centres

8. Communications, marketing and intelligence

Organisations across all the sectors process certain personal data to gather market intelligence, promote products and services, communicate with and tailor offer to individual customers. In addition to B2C, many organisations also use legitimate interests in the context of marketing and communications with B2B customers and contacts. Specific examples are:

- Discretionary service interactions - customers are identified in order for them to receive communications relating to how they use and operate the data controllers' product
- Personalised service and communications
- Direct marketing – of the same, or similar, or related products and services; including also sharing and marketing within a unified corporate group and brand;
- Targeted advertising
- Analytics and profiling for business intelligence – to create aggregate trend reports; find out how customers arrive at a website; how they use apps; the responses to a marketing campaign; what are the most effective marketing channels and messages; etc.
- Ad performance and conversion tracking after a click
- Audience measurement – measuring audiovisual audiences for specific markets
- Mapping of publicly available information of professional nature to develop database of qualified professionals/experts in relevant field for the purpose of joining advisory boards, speaking engagement and otherwise engaging with the company
- B2B marketing, event planning and interaction

PART II: Specific case studies

The following case studies have been contributed by CIPL GDPR Project members and selected to illustrate the breadth and scope of legitimate interest as the legal processing ground across industry sectors. The cases follow a similar pattern, but with some variance in format to highlight the various issues and topics that each individual example addresses.

1. Case: Creation and/or Use of Watch Lists to Meet Anti-Money Laundering (AML), Politically Exposed Persons (PEP), Anti-Fraud or Diligence Obligations

Rationale for legitimate interest processing: To protect the international financial system from abuse, financial institutions and other companies must often screen new and existing customers or vendors against watch lists. The lists are designed to help financial institutions determine if a business relationship might carry a risk of financial or other crime. The source of this obligation must be either Member State law, laws of non-EU countries; or even just good business practices designed to reduce regulatory or financial risk.

The source of the information that goes on the watch list may for example be private entities using publicly available information of Politically Exposed Persons (PEPS) or sanctions

published by national or international organisations. Given the nature of such lists, it is not feasible for the creator to obtain consent from the individual regarding the inclusion of their personal data, so the creator must use legitimate interest as their processing ground. Note the Fourth AML Directive explicitly authorises financial institutions to use third party service providers to provide watch lists, as it may be the only way an institution can meet its AMLs obligations. Equally, for some instances, controllers that perform checks against the officially published watch lists and conduct the screening activities themselves also must rely on legitimate interest in order to process personal data of people on the lists.

GDPR legitimate interest balancing: The data processing should be relevant, adequate and limited to what is necessary for its purpose. The public and private interests served by such diligence meet the legitimate interest requirements as long as the interests or the fundamental rights and freedoms of the individual are not overriding. Those public or private interests may include fraud prevention, stability of the financial system, preventing market abuse, investor protection, combatting money laundering and combatting terrorism.

Mitigation and reasonable expectation: Satisfying the legitimate interest basis for processing also requires accurate and fair procedures in the creation and use of the lists. It is imperative that the processing parties have applied the necessary safeguards under the GDPR for the processing of this data. For example, the vendor of a list must have a DPO and the individual must have the opportunity to correct inaccurate information. However, the right to correct inaccurate information is not absolute, as EU and Member State law can impose limitations in the context of public good or national security or defence interests in the public good. For example, this may also cover the obligations of public or private entities as publishing a list of potentially fraudulent IP addresses might inform criminals by omission of IP addresses that may still be used for fraud.

2. Case: Fraud monitoring, detection and prevention

Rationale for legitimate interest processing: Financial institutions, payment networks and other companies must process personal data of individuals in order to monitor, detect and prevent fraud. In particular, payment networks are in a unique position to monitor and detect signs of fraud across all participants in the payment eco-system. They can alert financial institutions that a payment transaction is likely to be fraudulent in real-time, so that the financial institutions can notify the affected individual cardholders and/or make a decision as to whether to approve or deny a payment transaction.

The EU Payment Services Directive 2007/64/EC sets out that "*Member States shall permit the processing of personal data by payment systems and payment service providers when this is necessary to safeguard the prevention, investigation and detection of payment fraud*"". However, the majority of anti-fraud activities are performed under regulatory and sectorial obligations, rather than EU or Member State law. Payment networks and financial institutions are indeed subject to the oversight of the European Central Bank and relevant National Banks and, as such, must comply with recommendations and standards to ensure an adequate degree

of security, operational reliability and business continuity. This includes the implementation of robust measures to combat fraud. Moreover, EU and national governments and policymakers increasingly expect all parties in the payment eco-system to be more active in this space. The effective fight against fraud is indeed key to boost individuals' trust in the digital economy.

GDPR legitimate interest balancing: The legitimate interest of the payment network to protect its network and its brand meets the interests of all parties in the payment ecosystem, namely financial institutions and merchants to minimize the fraud impact and losses, as well as individual cardholders to be protected against fraud. Individual cardholders actually expect their payment transactions to be processed in a safe and secure way.
The outcome of the balance of interests test is properly documented and, where appropriate, a full Data Protection Impact Assessment is conducted to ensure adequate and effective data protection.

Mitigation and risk assessment: Prior to launching a new anti-fraud tool, the payment network assesses whether there are less invasive means to achieve the same purpose. To further mitigate the potential risks and enhance the protection of the individuals' interests and fundamental rights and freedoms, additional safeguards and controls are implemented by the payment network as needed, such as strict data access, data use limitations, security measures, retention schedules, as well as data minimization including as appropriate data anonymization and pseudonymization.

Limits of consent: Obtaining consent from individuals for collecting and using their data for anti-fraud purposes would not be workable or meaningful. Indeed, all good faith individuals would agree to provide their consent while fraudsters would withhold their consent. This would result in missing information making fraudulent activity increasingly difficult to monitor and/or to detect. Ultimately, this would jeopardize the financial stability, reliability and integrity of the payment network, thereby harming all legitimate parties in the payment ecosystem including individuals themselves.

3. Case: Processing of data in relation to M&A

Rationale for legitimate interest processing: In the context of an M&A transaction, there may be a need to make available and review documentation containing personal data, and to prepare transaction documents based on these. The documentation may contain personal data (i) incidentally, such as names and other details of those executing agreements and notarial deeds, the proxyholders, the identity of the members of the corporate management bodies, the identity of individuals involved in litigation actions initiated by or against the relevant company, etc. or (ii) purposefully, such as the employment documentation that must be reviewed, particularly to determine the appropriate conditions of the transfer of the workforce and, if transferred, whether the documentation appropriately evidences the compliance with the applicable requirements that the "buyer" may inherit (e.g. social security payments).

M&A transactions (with third parties or intra-group) may be structured, as a general rule, either through share deals or asset deals. Asset details may entail a universal succession of rights and liabilities (e.g. a merger or a split off) or transfers "uti singuli" (e.g. a sale and purchase agreement. Some may entail a transfer or undertaking from an employment law point of view, and some may entail the transfer of a business unit from a tax law point of view. What is common in all of these transactions, for the purposes of legitimate interest, is that the potential acquirer is interested in pursuing the same activity as the seller (if not, other legal grounds would not need to be assessed).

In all of these transactions, the review of the documentation that may contain personal data must be undertaken by the potential acquirer (e.g. the buyer or the beneficiary of the company, the asserts or the business unit) and seller, as well as its external advisors (lawyers, IT consultants, financial auditors) in order to determine the initial and final scope of the subject-matter of the acquisition (which would need to be described in the transaction documents, the potential legal, financial and operational contingencies, the condition precedents for closing and the price of the transaction). Hence, all of these parties processing personal data would rely on the legitimate interest ground to be able to proceed with their tasks.

GDPR legitimate interest balancing: There is a clear legitimate interest in carrying out such review with appropriate safeguards in place to protect that there is no deviation of the legitimate purpose due to the NDA agreements. These may include information being made available to individuals with access rights on a need-to-know basis. To anonymise the data is not only a huge effort for the selling company (in terms of cost and time but will prevent the transaction from being properly designed (e.g. you need to identify the owners of the shares or the assets; who is an authorized signatory, etc. or jeopardize the review since many contingencies can only be detected if identifiers exist (e.g. labour contingencies, litigation, non-compete provisions regarding senior executives).

Mitigation and risk assessment: Before any M&A review, a non-disclosure agreement is always executed among all the involved parties in order to protect the exchange of information, which is by nature, commercially sensitive (irrespective of whether personal data are contained or not). The review could be made by marking available documentation in platforms held by third parties in "view only" as well as a general rule (upon request, the reviewers may ask to have copies of specific documents with no personal information).

Limits of consent: Informed consent is not an option. This is not only because it would involve disproportionate effort, but because confidentiality should be preserved until the transaction is closed (vis-à-vis employees, the clients or the capital markets). The closing of a M&A transaction cannot depend on the consent, or its withdrawal for data protection reasons (if specific groups must be protected, other laws would provide such protection, such as minority shareholders protected by corporate laws; employees protected by employment laws etc.

4. Case: Internet Protocol Addresses

Rationale for legitimate interest processing: Much like a house or apartment in the physical world, computers that are connected to the Internet are assigned an address called an "Internet Protocol Address" or "IP Address" for short. Those addresses can be "dynamic" which means they change each time the computer connects to the Internet, or they can be "static" which means that they are fixed. When a computer requests a web page or other content on the Internet, it sends its IP address to the computer hosting that content asking the server to return the content to its IP address. Without the address, the server would not know where to send the content. For most companies, that IP address is simply either (a) the computer requesting the content, or (b) the identity of the computer hosting the content. In addition to using the IP address for sending or receiving content, however, companies can also use the IP address for internal business purposes such as security (for example to detect and prevent "denial of service" attacks where an attacker can overload a server by sending superfluous requests for a web page), or to measure website traffic. The exception, however, is the Internet Service Provider (or ISP) who is providing the connectivity. ISP's often have information linking the IP address to the individual subscriber in order to provide technical support, billing, and other business purposes related to their service.

GDPR legitimate interest balancing: The data processing should be relevant, adequate and limited to what is necessary for its purpose. The public and private interests served by such use of the IP address meet the legitimate interest requirements as long as the interests or the fundamental rights and freedoms of the individual are not overriding. In this case, delivery of content on the internet would simply not be possible without the IP address just like sending or receiving physical mail in the real world. And internet content owners certainly have a legitimate interest in protecting their content and services from bad actors. Apart from the legitimate interest ground, none of the other Art. 6 processing grounds allowing for the lawfulness of processing of the IP address would be applicable in this case.

5. Case: Providing Location Through Terrestrial Wireless Signals

Rationale for legitimate interest processing: Location based services, or LBS, provide significant value to individuals and are a key feature of multiple products and services used today. But LBS loses its usefulness if wireless devices cannot readily determine location in urban environments or deep indoors. In such environments, using satellite positioning technology alone, such as GPS or Galileo, is slow and uses substantial power. One way to speed up location determination and save battery life is to determine location by detecting nearby wireless access points such as Wi-Fi routers and cell towers and comparing those access points to data stored on the device. Such data stored on the device is essentially a look-up table containing Wi-Fi routers' and cell towers' unique IDs and associated locations. Using Wi-Fi signals is particularly important because it enables indoor LBS services where accessing navigation satellites is limited or impossible.

Limitations of consent: Maintaining an up-to-date list of locations of Wi-Fi routers is a continuous process because Wi-Fi routers are frequently added or removed from the internet. Thus, companies frequently collect this information through a variety of sources, including from individual smartphones as they move about the environment. Getting consent from the smartphone owner is certainly possible for the service provider, operating system provider, or device provider because of the direct relationship between the smartphone owner and these companies. . These companies, however, often do not have a direct relationship with the owner of the Wi-Fi access point, thereby making obtaining their consent impracticable and unfeasible. According to the WP29, the owner of the Wi-Fi router has a privacy interest in their router's unique ID in combination with its location. But because of the lack of a relationship with router's owner, the only lawfulness mechanism applicable to collect such information is legitimate interest.

6. Case: Processing for Targeted Advertising and Service Personalisation (Recital 47)

Rationale for legitimate interest processing: Direct marketing may be a legitimate interest in accordance with GDPR Recital 47. Equally, the WP29 has stated in its guidance on legitimate interests that: "controllers may have a legitimate interest in getting to know their customers' preferences so as to enable them to better personalise their offers and ultimately, offer products and services that better meet the needs and desires of the customers."

The same rationale should apply to other forms of targeted marketing, including advertising based on a person's online activity. Targeted advertising should be deemed to fall within the controllers and third parties' legitimate interests and not be outweighed by the individual's rights, provided the data are used in accordance with the specific requirements, the individual receiving the advertising is given information about how their data will be used for targeting and has meaningful controls over those uses. The controller must also be accountable for honouring the choices individuals have made regarding how their data are used for ads.

Advertising is one of the primary business models of free services, a fact all users of free services are well aware of. Personalisation of content and offering is a core feature of many services – it makes the service what it is. Without personalisation, many services would lose business as their customers and users rely on personalisation as one of the value propositions of the service. Therefore, controllers should be able to rely on legitimate interest as the basis for processing of the personal data of their users for personalisation of content and offerings.

GDPR legitimate interest balancing: In considering targeted advertising through the lens of the legitimate interests balancing test, this test should take into account interests of multiple actors. The growing evidence shows both the importance of targeted ads to the business models of many online publishers and advertisers and the fact that relevant ads can create real value for individuals by helping them discover new products, services, and causes, and by helping to avoid subjecting individuals to discriminatory advertising. Businesses clearly have legitimate interests in providing targeted advertising for these purposes.

Mitigation of risk: For similar reasons, personalisation has become the hallmark of many of the world's most popular online services, which has led individuals not only to expect, but to demand that websites and apps use their personal data to personalise their experience. The value personalisation creates for people and for businesses (which benefit from increased engagement) is clear. To mitigate privacy risks, organisations put in place measures to ensure that service personalisation usually does not involve sharing personal data with third parties, or making decisions about the individual that could have an adverse effect and create harms to individuals.

The widespread availability of controls around targeting advertising (such as controls offered by the European Interactive Digital Advertising Alliance) have helped address individuals' privacy interests, as have the enhanced commitment of commercial players to educate consumers regarding how advertising works on their services and how individuals can make relevant choices about their advertising experiences. Moreover, some companies have gone ever further in giving users more transparency and more granular controls over how their data is used to show them relevant ads. Coupled with internal safeguards and compliance measures employed by organisations, these efforts should mitigate any privacy risks to the individuals that receive targeted ads.

Reasonable expectations of the individual: Individuals have come to expect and understand that they will receive targeted advertising based on their personal data and preferences, particularly when using free online services. These expectations are clearest where the consumer has a direct relationship with the company that provides the advertising. Third-party providers can also enable this understanding by providing improved transparency themselves, or through the first parties with which they work.

Limits of consent: Legitimate interests in some cases may be a more appropriate legal basis than consent because of the way the online advertising ecosystem works. In many, if not most, targeted advertising scenarios, multiple parties will be involved in serving the targeted advertisement. It often will be infeasible for each of these parties to obtain individuals' consent (and provide the mechanism for withdrawal) that the GDPR requires. More importantly, however, requiring each of these parties to obtain consent would result in the individuals being overwhelmed by consent requests and burdened by having to manage them all. Research has shown that in these scenarios, individuals are less likely to pay attention to notices and consents and more likely to simply click through, in order to receive a service or access information that they want. This leaves people in a position where they are actually less empowered.

7. Case: Audience Measurement ("AM")

Rationale for legitimate interest processing: Audience Measurement ("AM") is a way to measure audiences for specific markets (e.g. TV, radio, newspapers, or websites). It is distinct from advertising and cannot be used to target individuals for advertising. Different AMs (e.g. surveys, panels and online measurements) have distinct methodologies and rely on

different legal grounds. For example, TV measurement panels involve a large number of households and currently requires the installation of a special box that measures viewing behaviour, based on a contractual relationship. Surveys are carried out by fieldworkers and rely on consent, while online measurements require the content owner to include tag that allows the AM provider to place a cookie.

AM provides information regarding market size, business analytics and allows for the independent verification of viewing for billing purposes. AM also serves to ensure that copyright royalties are calculated precisely. The outcome of AM are reports that show aggregate data: they do not permit the identification of any individuals, but are usually grouped under relevant geodemographic headings (e.g. age-brackets, gender, geographical distribution, socio-economic parameters).

GDPR legitimate interest balancing: When conducting the balancing test under the legitimate interest ground one has to consider multiple rights and interests - the privacy right of the individual, the rights of media owners, the right to conduct a business, and AM providers' interests. In balancing how the right to conduct business and the AM provider's interest are pursued with the rights of individuals, the intrusion into privacy is minimal: WP29 has recognised that web analytics pose minimal privacy risks. This ought to be even more the case where the AM provider cannot link the data to an account or a registered user, which a website can do with web analytics. The objective of AM is to produce aggregate reports that consists of anonymous data. At an individual level, data are psedonymised and not retained beyond the original purpose.

AM helps market function more efficiently and competitive and also help fund free and quality media. A lack of effective AM would lead to opaque markets and leave advertisers in the dark, which would impact media funding negatively.

Mitigation and risk assessment: risk to the individual are limited by deploying privacy safeguards, including:

- Strict purpose limitation – no AM data is used to direct advertising to individuals
- Providing opt-outs
- Truncating IP addresses and subsequent one-way hashing/pseudonymisation
- Anonymisation - clients only receive aggregate reports
- Contractual safeguards with suppliers and partners and prohibition to re-identify data

AM providers draw a line between third party independent measurements and advertising. AM reports are not intended or suitable for advertising or to target individuals for marketing purposes. Instead, AM can provide verification that content has reached its intended demographic segment, whether that is for content or for advertising purposes. Any intrusion on privacy is minimal and individuals always have the opportunity to object to the processing or delete their cookies. AM cookies are not used to re-identify individuals or allow those users to be targeted for advertising or other marketing purposes.

Limits of consent: The legitimate interest ground is the cornerstone for enabling the benefits of AM activity in the ecosystem, both for media owners as much as for AM providers. Legitimate interest is the only practical available ground for processing because the data collected typically does not enable identification of the individual. Also, consent would generally be performed in such a way as to make obtaining user consent unduly burdensome. Indeed, the accuracy of the measurement in the digital and mobile areas would likely be greatly diminished if consent was required, due to typically low participation rates where opt-in is required.

AM companies, just like processors and IT service providers, are unknown to users and do not have a direct relationship with the individuals or provide a direct consumer benefit. Media companies are also very reluctant to request providers to collect consent individually, as this would pose a major disruption and favour companies that have those capacities in-house or have already obtained consent via different means (which would undermine the unbiased and neutral features of AM activities).