Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR

Centre for Information Policy Leadership GDPR Implementation Project
19 May 2017

CIPL's TOP TEN MESSAGES ON THE PRINCIPLES OF TRANSPARENCY, CONSENT AND LEGITIMATE INTEREST

1. **Transparency is intended to be user-centric and should not primarily envisage legal compliance.**

2. **Transparency should be context-specific, benefit from the possibilities of new technologies and avoid information overload.**

3. **Transparency should be provided contextually by different methods and at different appropriate times throughout the lifecycle of processing operations.**

4. **Algorithmic transparency should focus on the broad logic involved instead of attempting full transparency to the individual. Most important may be transparency about the inputs to which algorithms are applied.**

5. **Consent should be used as a legal ground for processing in situations where it is possible to provide clear and understandable information at the right time and individuals have a genuine choice concerning the use of their personal data.**

6. **Member states should take a harmonised approach vis-à-vis the age of consent for children. The age should be 13. The practical difficulties and privacy issues arising from seeking to verify parental/guardian rights over the child must be recognised.**

7. **There are concerns about the predominance of consent in the ePrivacy rules. The EU legislator should introduce legitimate interest into the ePrivacy Regulation.**

8. **Legitimate interest may be the most accountable ground for processing in many contexts, as it requires an assessment and balancing of the risks and benefits of processing for organisations, individuals and society.**

9. **Legitimate interest places the burden of protecting individuals on the organisation, which is in the best position to undertake a risk/benefits analysis and to devise appropriate mitigations.**

10. **The legitimate interests to be considered may include the interests of the controller, other controller(s), groups of individuals and society as a whole.**

1. INTRODUCTION

1.1 The GDPR requirements on transparency, consent and legitimate interest

The GDPR recognises transparency as a core principle of data protection. Transparency is related to the fair processing principle. Processing can be fair only if it takes place in a transparent manner.

However, transparency can serve its purpose only if it is meaningful. There currently is a growing gap between legal transparency and user-centric transparency. Concise and intelligible privacy notices focusing on truly informing users by providing meaningful information are at the center of user-centric transparency.

Transparency in the GDPR is intended to be user-centric. It should be an effective instrument for the empowerment of the individual, one of the main objectives of the GDPR. This is why CIPL's recommendations focus on user-centric transparency. Transparency should be context-specific, flexible, dynamic and adaptable to constantly evolving and changing uses to provide clear and understandable information to individuals and to enable a genuine choice where it is possible about the use of their personal data. However, even where consent is not available, transparency is still necessary to provide relevant information about the processing activities, how the organisation has mitigated the risks, the rights of individuals and any other relevant information demonstrating that the organisation is fully accountable for its processing activities.

Further, in situations where consent is deemed impractical or ineffective and does not appear to be the most appropriate legal basis, if only because of the complexity of modern information uses, other legal bases, including the legitimate interest ground for data processing,[1] can be relied upon. Legitimate interest requires an assessment and balancing of the risks and benefits of processing for organisations, individuals and society. It also requires the implementation of appropriate mitigations to reduce or eliminate any unreasonable risks. This places the burden of protecting individuals on the organisation and shifts it away from individuals. Organisations are in the best position to undertake a risk/benefits analysis and to devise appropriate mitigations, and individuals should not be overburdened with making these assessments and informed choices for all digital interactions and processing of their personal data.

1.2 The CIPL GDPR Project

This paper by the Centre for Information Policy Leadership at Hunton & Williams LLP ("CIPL")[2] is a part of its project on the consistent interpretation and implementation of the GDPR ("CIPL GDPR Project").

The CIPL GDPR Project—a multiyear project launched in March 2016—aims to establish a forum for dialogue amongst industry representatives, the EU DPAs, the European Data Protection Supervisor, the European Commission, the ministries of the member states and academics, on the consistent

[1] There are additional grounds for processing (e.g. contractual necessity) not discussed in this paper but also applicable in many circumstances and important for organisations as a legal basis for processing.

[2] CIPL is a privacy and data protection think tank in the law firm of Hunton & Williams LLP and is financially supported by the law firm and more than 50 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices to ensure effective privacy protections and the effective and responsible use of personal information in the modern information age. For more information, please see the CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm Hunton & Williams.

interpretation and implementation of the GDPR through a series of workshops, webinars, white papers and comments.

CIPL aims to provide input to the Article 29 Working Party ("WP29") on a number of priority areas, identified in CIPL's GDPR Project work plans for 2016 and 2017. This is the fifth white paper in this series, following earlier CIPL papers on DPO, Risk, OSS and Lead Authority, and Certifications.[3] CIPL also submitted comments to the WP29 on its Guidelines on the right of data portability, OSS, Lead Authority and the DPO and DPIAs and "high risk".[4]

1.3 CIPL's White Paper

In this white paper, CIPL aims to provide the WP29 and data privacy practitioners with input on transparency, consent and legitimate interest—three core concepts of the GDPR. Accordingly, the paper sets forth CIPL's recommendations on how to apply and implement these concepts. It also notes certain open questions that might be further explored. The relevant GDPR provisions on each of these items are summarised at the end of this paper.

The items were discussed during a workshop organised by CIPL in Madrid on 7 March 2017. The input received at the occasion of this workshop is taken into account in this paper.

[3] See
https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/final_cipl_gdpr_dpo_paper_17_november_2016.pdf;
https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_the_gdpr_one-stop-shop_30_november_2016.pdf;
https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf.
PM.

[4] Available on www.informationpolicycentre.com.

2. TRANSPARENCY

2.1 Starting points

- **Transparency is key to ensuring that processing is fair.** The GDPR firmly links transparency to fair processing. It states in its first principle that personal data must be "processed lawfully, fairly and in a transparent manner".[5]

- **Transparency is a business consideration and priority**. It is critical for trust and digital confidence, and goes beyond pure legal compliance. By effectively informing individuals about the protection and use of their personal data, including benefits of data processing, and by addressing the concerns of regulators, transparency will have the effect of raising the level of digital education, broadening individuals' expectations, increasing their acceptance of and support for certain data uses, and generally deepening individuals' and regulator trust. This in turn will enable organisations to use data for wider and more beneficial purposes, and also encourage competition around the most effective transparency. All of this benefits individuals, organisations, society and the Digital Single Market.

- **Transparency in the GDPR is broader than privacy notices** provided at the time of data collection and privacy policies provided in general on organisations' websites. Transparency includes all mechanisms and instances used by organisations to communicate with an individual. For example, transparency also includes product and service descriptions that explain how personal data will be used, communications in respect of the exercise of individuals' rights and notification to individuals of data breaches.

- **Effective transparency requires a new multidisciplinary approach, innovative delivery and tools, and robust resourcing and investment.**

2.2 Transparency delivers effective compliance with other GDPR requirements

- **Transparency will have a role in defining and supporting the purposes for which personal data may be used** (including compatible uses for further processing), as well as for specifying the grounds for processing.

- **Transparency is an intrinsic part of any consent**, as consent must be informed in order to be valid. Transparency concerning the uses (including unexpected and future uses) of data, the benefits of processing and the organisation's accountability measures are all important to enable individuals to make choices.

- **Privacy notices of Articles 13 and 14 must be provided, irrespective of the ground for processing.** Transparency also offers benefits to the individual in situations where individuals do not have a choice on data use, or where consent is not feasible, impracticable or ineffective and/or where other legal bases are used. Transparency requires that organisations should be transparent about the data uses based on a legitimate interest ground. It is also important in respect of the legal basis for contractual necessity, by precisely defining the services within the contract.

- **Transparency has a role in setting the reasonable expectations of individuals** regarding the use of their personal data. For example, in the context of legitimate interest processing, the

[5] Art. 5 (1) GDPR. Indeed, fair processing is at the core of EU data protection. See also Art. 8 of the EU Charter on Fundamental Rights.

reasonable expectations of the individual are one element that a controller must take into account as part of the legitimate interest balancing test. Transparency and notices to individuals can shape the expectations of individuals as to how their personal information might be used.

2.3 Transparency as an element of organisational accountability

- **Transparency is an essential element of accountability.** Together with other accountability elements, transparency ensures responsible data use.

- **Transparency is complemented by other accountability elements, such as risk assessments, data protection management (e.g. DPO, CPO) and individual rights (access, portability, correction, objection).** Sometimes, organisations without a direct relationship with individuals will need to rely on other mechanisms to ensure they are fulfilling their accountability obligations and to compensate for the possibility that it will be challenging to fully satisfy all transparency requirements. Under those circumstances, these other accountability measures become important for delivering effective data protection for individuals and ensure responsible data use.

2.4 User-centric transparency is key

- **There is a perceived growing gap between legal transparency and user-centric transparency**. Legal transparency, T&Cs and privacy notices are necessary to comply with data protection law, but arguably they do not always effectively deliver transparency or understanding to individuals. In fact, perhaps the reverse is true, as they must follow specific legal mandates. This is even more complicated where the organisation operates in multiple jurisdictions and must try to tailor legal notices to numerous and sometimes competing legal requirements. User-centric transparency is about delivering transparency as part of the customer relationship and digital trust. It is also about building understanding and explaining the benefits of data use and the value of the product or service, organisational accountability, and the choices that are available.

- There is a tension between the legal requirement to provide detailed notices to individuals for each data processing with a long list of prescribed content and the requirement that notices be clear and concise. Thus, where the goal is to provide understandable and actionable information to individuals, it may be challenging to systematically communicate every complex detail. **There needs to be an effort to find a balance between clarity and completeness and to resolve this balance in favour of clarity through innovative ways of delivering required content of notices.**

- **GDPR transparency is intended to be user-centric.** This is why Article 12(1) GDPR requires that information is provided to the individual in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

- **Transparency should be designed to effectively provide relevant, timely and digestible information** to individuals when and where it is most meaningful to them. This can be done both based on the “push” model (proactively providing just-in-time transparency) and the “pull” model (making information available to individuals at their convenience, e.g. permission management, transparency dashboards and “learn more” tutorials).

- **The possibilities of a pull model should be further explored** to allow provision of information to individuals who desire it. Some information must always be provided under

the GDPR, but that should be the most important information to enable choices or deliver user-centric transparency. The rest should be made available to individuals in an accessible location or manner. This approach is also in line with the layered notices approach.

- **Transparency should be driven** not only by the legal requirements but also **by the real needs**, **interests and concerns of individuals** with respect to data processing. These can be determined through researching and testing how people actually interact with services and what concerns they may have about the use of data.

- Organisations face **real practical challenges in complying with the strict letter of Articles 13 and 14** for every single processing purpose of data in the modern digital economy and society. Hence, it may be better for both organisations and DPAs to focus on achieving real and user-centric transparency that remains true to the spirit and objective of the law and that is more effective in protecting individuals and their data than the lengthy and legalistic privacy notices and policies that would follow from the strict interpretation of Articles 13 and 14.

- In practice, **transparency may have to be delivered by (a) actionable and targeted user-facing information** focused on individuals and their needs; **and (b) more detailed legal disclosures** (privacy notices and policies) that are designed to ensure legal compliance as well as to provide comprehensive and accountable information for those who seek it (general public, NGOs, DPAs), in a manner that remains as clear and concise as possible.

2.5 Specificity of and exemption from notices

- **Transparency means that organisations need to provide the following key information** in a concise and intelligible manner: a) all purposes of processing; b) reliance on the legitimate interest processing ground; c) the logic in automated decision making; d) use of third parties to process data; e) cross-border data transfers; f) data retention period; and g) individuals' rights (access, rectification, objection, etc.).

- It should be acceptable to **provide the full list of required elements of a privacy notice under Articles 13 and 14 in a generic privacy policy**, instead of providing this notice for each single collection and use of data. Presenting all this information to users at the time of collection will only undermine the very transparency the GDPR is seeking to achieve by overwhelming a user with information that in many cases they simply do not wish to actively consume.

- **Specific or just-in-time privacy notices** should be reserved for actionable information and limited to cases where provision of such privacy notices is warranted, such as where there is a higher risk of processing, or where there are unexpected uses of data, or in cases of sharing with third parties that is outside the normal provision of the services. Also, these methods are generally more applicable and viable for the online and mobile environment, and where there is real-time interaction (online or call-centre situations, for example).

- It must be possible for a controller to **rely in certain cases on the exception for disproportionate effort (Art. 14(5))** as an exemption to providing notice under Article 14. Moreover, this exemption must be possible of being interpreted broadly, especially where organisations do not have direct relations with the individuals and in cases where the provision of a notice would prejudice the very purpose of processing and the legitimate rights of organisations and other parties (e.g. fraud prevention, information and system security, corporate investigations).

2.6 Gap between industry practices and understanding of consumers

- **Transparency must go hand in hand with broader consumer education and digital literacy initiatives**. This is essential to address the growing gap between the technology and business processes on the one hand and the general understanding of the public about data uses and the digital ecosystem on the other. This is the responsibility not only of organisations using data and technology, but also of the media, the DPAs, NGOs and other relevant organisations. It is part of the task of the DPAs to promote public awareness (Article 57(1)(b) GDPR).

2.7 Transparency where there is no direct relationship with individuals

- Transparency is increasingly difficult in complex data ecosystems where organisations do not have a direct relationship with individuals, or where they just process pseudonymous data and do not have the ability to identify individuals themselves.

- Where data is **pseudonymised** or relates to individuals who cannot be identified from the information in the possession of the organisation, **organisations should not obtain additional data in order to provide a data privacy notice** to such individuals, or to answer an access/portability/erasure request with respect to them. This raises questions about the definition of pseudonymisation and how the GDPR requirements apply to these data categories.

- There should be **flexibility in interpreting** the requirement of transparency in practice and in addressing the above challenges, especially **the strict and long list of requirements of data privacy notices in Articles 13 and 14**. The interpretation should allow for more creative and distributed ways of providing necessary information to individuals.

2.8 Algorithmic transparency should be focused on the broad logic involved

Algorithmic transparency vis-à-vis individuals and the general public must be achieved in a manner that is realistic and effective in practice. As the GDPR recognises, there is no obligation to provide detailed information about the algorithm itself, merely the logic behind it. Individuals will not have the time or inclination, and most likely not the ability, to understand the algorithms behind big data and machine learning applications. To illustrate the issue: individuals rely on brakes in cars without understanding how they work. However, there is certainly a place for regulators to understand brakes. It should be the same with algorithms and data processing—algorithmic transparency may be more appropriate vis-à-vis DPAs in connection with their oversight and enforcement roles.

Algorithms are not static and defy real-time explanation. To complicate things further, algorithms cannot be understood in a static manner. It is inherent in all algorithms and machine learning techniques that they constantly change based on accumulated knowledge and insights. This makes it difficult to deliver real-time and detailed transparency on the workings of algorithms.

- **Focus on objectives and outcomes of algorithmic transparency.** Providing the "logic behind" algorithms means that there is an obligation to consider the intended objectives of algorithmic transparency vis-à-vis individuals, and then deliver the desired outcomes through appropriate means.

- **Algorithmic transparency should be focused on the broad logic involved** and not the detailed workings of algorithms. A key element **is to be transparent about the type of inputs to which algorithms are applied as well as on the outputs, and to ensure that they are both accurate and correctible.**

- **Other internal accountability mechanisms and tools are essential.** This includes DPOs who exercise oversight and advice in respect of the use of algorithms and machine learning. Accountability should also include the safeguards, as articulated in Article 22 GDPR. Also, as mentioned above, more details concerning algorithmic transparency may be part of transparency vis-à-vis DPAs in the event of a complaint, investigation and enforcement action or on request, respecting the confidentiality of trade secrets.

- **GDPR certification could be a useful instrument to increase transparency of algorithms.** Certification does not necessarily increase transparency of algorithms to individuals directly, because the GDPR provisions on certification[6] only require transparency to a DPA or a certification body. However, certification can provide assurances to individuals that a DPA or a certification body has reviewed and approved the processing at issue.

2.9 Limitations on transparency

- **Transparency cannot be absolute.** Transparency is an essential element of effective data protection, but is subject to limitations imposed by the complexities of the modern digital economy and the other rights and freedoms. This must be recognised. There should be a number of factors that define the limits.

- Transparency **may be limited by trade secrets, commercial and competition considerations, other intellectual property rights, as well as by rights of other individuals.** Equally, there may be cases where full transparency to individuals may be inconsistent with public interest considerations and prejudice organisations' ability to conduct essential and common data processing, such as fraud prevention, or corporate investigations, or to implement information and network security measures.

2.10 Contextual means for delivering transparency

- **The means of delivering transparency and its content must be contextual and allow for appropriate discretion to organisations.** Transparency must take into account the nature of services being provided and the relationship between the organisation and its customers/individuals. It must give individuals understanding and clarity about the products and services they are obtaining and the use of their personal data in that context.

- **Transparency must be provided by different methods and at different appropriate times throughout the lifecycle of the data** and the related products or services used by the individual. Transparency should make it possible to understand the processing of personal data *ex ante* and *ex post,* enabling individuals to exercise their rights at the appropriate time. One way to provide ongoing transparency and control would be periodic reminders about data and privacy settings, while also retaining the organisation's flexibility to adjust to the specificities of a given service, circumstance and user expectation.

- **Transparency mechanisms and tools must change with and adapt to technological changes.** They should not be too technology specific, stifling innovation.

[6] In particular Article 42 GDPR.

- **Transparency mechanisms must be embedded as much as possible within the relevant product, service, process or technology.** They should not be at the expense of usability and functionality of any given technology or create burdens for individuals as they use technology in their daily lives and work.

- Effective mechanisms for transparency may include **push and pull mechanisms**, and can be delivered via a combination of tools, such as privacy policies, layered notices, just-in-time notices for websites, dashboards, control panels, custom-built apps, tutorials, user guides, interfaces, etc.

2.11 Icons: not in all cases and not top down

- Standardised icons are presented in Article 12(7) of the GDPR as a specific transparency tool and the Commission is empowered to adopt delegated acts to specify the use of this tool.

- **The feasibility of employing icons** and standardised policies as effective transparency mechanisms should be based on research and evidence. The views and experiences of privacy practitioners and experts regarding their usefulness are split, ranging from extremely skeptical to somewhat optimistic in limited contexts.

- Icons might be able to provide useful information and create market value in some cases, but they are also considered to be static and thus inappropriate for modern ways of processing data that are constantly evolving with innovation and cannot be captured by simplistic and fixed icons. Icons represent the state of play at a certain moment and do not take account of changes in technology and business practices. Also, if there are too many icons, they will not simplify or promote user-centric transparency for individuals. Instead, having to learn icons may be perceived as burdensome.

- For **icons** to be useful, they **should not be created and imposed "top down".** To the extent possible, they should be developed initially by industry and then vetted, refined and potentially harmonised in collaborative stakeholder processes. However, organisations must also have the flexibility to create and deploy their own icons to suit their brand, products and services.

- **Encourage harmonisation, not standardisation.** Icons should not be standardised across different subject matters and applications, suiting all categories of individuals (customers, employees, citizens) and all different data uses and alternative platforms. However, harmonisation should be encouraged so as to avoid confusion of individuals having to learn the differences between different icon systems.

- **Interactive tools are in many cases a better alternative**. Rather than force users to understand icons, we should develop transparency technology that understands the user and that reacts to the user. Examples are user-friendly chatboxes or chatbots. Machine-learning should play a role; human interfaces should also play role.

2.12 Develop effective transparency tools by multidisciplinary teams

- Organisations will be the ones that will have the best sense of what may work and the individuals they interact with may be best placed to determine how any transparency tools may fit into user interfaces, experiences and the organisation's brand and design standards.

- The most successful transparency tools and methodologies will be those not built only by lawyers, but that are built **by multiskilled/multidisciplinary teams** that include behavioral economists, user interface and design scientists who are expert in human factors or ergonomics, social scientists, psychologists, technologists and communication experts. DPAs could be included in the process as well at their own discretion.

2.13 Transparency and DPAs

- **Accountability** includes the obligation to demonstrate compliance, which by definition **requires some transparency to DPAs**. Transparency vis-à-vis DPAs is also an objective of consultations between businesses and DPAs and of responding to information requests in the context of regulatory oversight matters and investigations.

- **DPAs should recognise organisations that have developed innovative and effective user-centric transparency as accountable organisations**. Positive and reinforcing messages and showcasing "what the good looks like" by DPAs can be a way to deliver such recognition, in addition to the methods mentioned below.

- **DPAs should incentivise diverse user-centric transparency and showcase best practices**. They should not impose on organisations one-size-fits-all solutions and tools, but take into account differences between industry sectors and user expectations.

- DPAs may also incentivise and recognise transparency by giving **significant weight to effective and user-centric transparency in investigations and enforcement actions**.

- **Enforcement by the DPAs** should **not** be based primarily **on failure to comply with the precise letter of Articles 13 and 14**, but rather on how effective organisations are in delivering user-centric transparency.

3. CONSENT

3.1 Starting points

- **The GDPR places all processing grounds on an equal footing.** Consent is one of the grounds for processing personal data in the GDPR. It is neither the only ground nor the most important one.[7]

- **Consent should be used as a legal ground for processing where:** a) it is possible to provide clear and understandable information; b) individuals have a genuine choice to decide whether to use a service or not; and c) consent can be withdrawn without any detriment to individuals (although this may result in inability to use a service). Organisations should not be expected to offer a "shadow service" without personal data if the very service itself relies on personal data to provide the very best user experience.

- **Overreliance on consent undermines its quality and creates consent fatigue.** Overreliance on consent or use of consent in contexts other than the situations described above will undermine the quality of the consents that are obtained. Equally, it will not achieve the

[7] Art. 4(11) GDPR defines consent as: "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."

desired purpose of putting individuals in control, but instead create a consent fatigue with people using services and technology in their daily life and work.[8]

- **Other processing grounds may be more appropriate in some instances.** In many situations it may, for a variety of reasons, be more appropriate for organisations to use other legal grounds for processing, such as legitimate interest, necessity for fulfilling a contract or a legal obligation. If individuals do not have a real choice, or cannot be provided the necessary information as a result of the complexity of modern data uses, or if the withdrawal of consent is not possible for the organisation, legitimate interest or contractual necessity may be the most appropriate or most effective and accountable tool for protecting individuals.

3.2 Consent iscontext-specific and must be adapted to the information society

- The implementation of consent should align with the underlying policy goals behind consent: (a) **individuals have the information they need to make informed choices** about their data; (b) **individuals can make those choices before their personal data is being processed**; and (c) **individuals can withdraw their consent any time thereafter but should understand that this may mean that a specific service may no longer be offered**.

- **The GDPR sets out some new requirements for valid consent**. Not only must consent be informed, specific and freely given, but the GDPR also requires consent to be a) distinguishable from other terms and conditions; b) separate for each processing operation; c) not conditional on the performance of a contract; d) not used in situations of clear imbalance of relationship between the organisation and individuals, e.g. in an employment relationship; and e) able to be withdrawn at any time. This will require organisations to consider carefully how to organise and deliver consent in a way that is appropriate for the circumstances, does not overburden individuals and creates legal certainty to allow them to rely on consent.

- **The implementation of consent must be adapted to the modern information age.** This is not only because of the complexities and volume of data processing, but also because of the effect on individuals of actively providing consent as they interact with technology in every aspect of their lives and their work. Individuals will not expect to have to legitimise every single use of data, or every single processing operation, technology and the provision of products and services they want to use. In fact, individuals will expect organisations to use data and develop products, services and technology in a responsible manner and to use consent as a means to legitimise data use in situations where there is a clear and easy choice for individuals.

- **Normally, the GDPR does not require "explicit consent" and organisations have flexibility in how they obtain consent in accordance with Article 7 GDPR. Thus, clear affirmative action or statements as modalities of consent should be interpreted flexibly.** The validity of consent mechanisms should be examined in context, avoiding strict or static interpretations of consent requirements and evaluating consent flows based on user expectations in a given situation. There will be circumstances where a valid consent will be given by a clear

[8] This is also the practical approach taken by industry, as confirmed by the recent CIPL and AvePoint GDPR Readiness Survey Report. Some organisations heavily rely on consent today. Under the GDPR, they will continue to use consent in situations where organisations are able to obtain valid consent, or where local law imposes a consent requirement.

affirmative action that indicates the individual's agreement with the use of personal data. For instance, when an individual fills out an online form provided by a service provider, he consents to the use of his personal data in relation to the requested service by submitting the completed form. Another example of a consent by an affirmative action is a request of an individual for an individualised service, or an employee who has a choice to take part in her company's diversity survey and after a full notice about the use of her data clicks the link to take the survey. This consent extends to all processing reasonably related to this service, or the survey, as stated in the notice.

- **Explicit consent is only required for certain processing.** Explicit consent is a higher and stricter level of consent required by the GDPR for processing of special categories of data, automated decision taking where there is a legal effect/similarly significant effect, and as a derogation for the international data transfers prohibition. Explicit consent means that an individual states that he or she agrees with a specific use of his or her personal data, which requires such heightened consent.[9]

- **Further consideration is needed on contextual ways to express and revoke consent** under the GDPR. Especially, a) the provision of consent by "affirmative action" (e.g. recognising the completion of the online form explained above); b) an interpretation of the meaning of "revoke consent in the manner given"; and c) the relationship between the "right to object" and withdrawal of consent. CIPL recommends a flexible interpretation of points a) and b) above. Revoking or withdrawal of consent can certainly be made in multiple ways, depending on circumstances. For example, an individual who provides oral consent over the phone should be able to revoke consent on an online dashboard or a permission management portal/app at a later time. At a minimum, organisations should be able to satisfy the obligation to provide withdrawal of consent by offering individuals the ability to terminate their relationship with the organisation.

- **The notion of compatible use should be interpreted to include further processing of personal data that benefits the common good and society and does not create risks and harms for the individual**. There is a link between consent and further processing for compatible purposes. "Compatible" future uses or new uses do not require a new legal ground but may require organisations to provide notice to the individual in some cases. So-called incompatible future uses or new uses of personal data require a new legal ground for processing, such as consent. It is essential that in an information society and in the context of Digital Single Market the notion of compatible use is not interpreted in such a limited manner that it impacts or impedes the ability of organisations to engage in beneficial new data uses and data innovation, especially where these further data uses do not create risks and harms for individuals. In these situations, a new consent should not be required. Furthermore, any future use that does not undermine, contradict or in any way interfere with, or that can coexist with, the original use is, by definition, "compatible" with the original use within the common meaning of the word "compatible". Obviously, data sets that are de-identified or anonymised fall outside the scope of the definition of personal data and can be used for further and different purposes.

[9] The interpretation of explicit consent under the GDPR should not depart from that of Directive 95/46/EC, which also requests explicit consent for processing of special categories of data. Oral explicit consent is not excluded.

- **Pre-GDPR consents should continue to be valid if they have been obtained in compliance with the Directive and national law.** Organisations should not have to re-paper existing consent until there is a material change in processing and its purposes. The only exception are cases where existing consents do not comply with the GDPR's requirement that performance of a contract or service is not conditioned on consent to processing that is not necessary for the performance of a contract or, in connection with a child, the requirements of Article 8(1) have not been met.[10]

- **The GDPR consent should accommodate product development.** In some instances, certain data processing may be required to provide new features or functionality of a service or a product, and a user may need to decline to use the product if they do not want their data processed in that way.

  The concept of freely given consent under Article 7(4) should be interpreted to accommodate processing for product development, so that in instances where consent is required, there is no obligation to continue to support static, outdated versions of products if users do not wish to provide consent. The GDPR should not artificially constrain launching new functionality for users.

3.3 Contexts where other legal bases may be more appropriate than consent

While consent has a role to play in data protection law and practice, CIPL believes that in many situations other data protection concepts and tools may be more appropriate. Indeed, in cases where consent may not be available, there are other tools that can protect the individual. The examples of such tools and concepts empowering the individual and ensuring focus on the individual are: transparency, risk assessments, legitimate interest, organisational accountability, data protection by design, security measures, exercise of individuals' rights, redress in case of an infringement, etc.

3.4 Children's consent should be valid from the age of 13

- **Member states should take a harmonised approach to the age of consent for children** to enable delivery of the same digital services, products and technologies across the EU. Differences of minimum age would create obstacles for seamless development and delivery of service across the EU, prejudice the functioning of the Digital Single Market and may also complicate the control by DPAs and their cooperation. Moreover, there is no reason why in some EU member states children should be treated differently than in others.

- Member states should be encouraged to provide through national law for **the age of consent at 13**. This is consistent with the latest research.[11] Any higher age of consent would prejudice the children's right to privacy and data protection, as their participation in the information society would be subject to parental knowledge and consent.

- **It should not be required under the GDPR to collect unreasonable amounts of additional information to verify parental/guardian rights over the child, or to verify the age of the**

[10] This is consistent with the September 2016 opinion of the German DPAs of the Duesseldorfer Kreis.

[11] See Janet Richardson, et al., "EU General Data Protection Regulation: teen access to internet services; 5 reasons why they shouldn't require parental consent above age 13", 3 March 2017, available at https://medium.com/@janice_richie/eu-general-data-protection-regulation-teen-access-to-internet-services-685cbef7aeab.

children. "Reasonable efforts" to confirm that the person consenting is a person holding parental responsibility would be sufficient. This approach would be in line with the regime in the United States under the Children's Online Privacy Protection Act (COPPA), which requires only that methods used to obtain verifiable parental consent be reasonably calculated in light of available technology to ensure that the person providing consent is the child's parent. This does not require organisations to collect additional information above and beyond the approved methods of parental consent, which serve as proxies for parental verification. Use of readily available consumer technologies, such as credit card transactions, should be allowed, and new technologies should be supported provided they meet the standard.

- **Further discussion is needed on how to best implement the children's consent requirements.** This would include analysis and development of best practices around consent verification, among other issues, based on relevant experience under COPPA. CIPL offers to facilitate such multistakeholder discussions to study these issues further.

3.5 Concerns about the predominance of consent in the ePrivacy Regulation

- **The proposed ePrivacy Regulation may have unintended consequences of undermining the application of the GDPR by requiring consent in a wide range of situations,** relating to electronic communications content or metadata, as well as the information stored in and related to terminal equipment. The proposal extends to all communications, including machine to machine and IoT outside the traditional telecommunications sector. Activities that would be legal under the GDPR would be made illegal because of the broad application of the ePrivacy Regulation and its strict consent requirements.

- **The ePrivacy Regulation risks undermining the usefulness/availability of other processing grounds, especially the legitimate interest processing ground in the GDPR**. As explained, the legitimate interest processing ground may in many situations be more appropriate. One should avoid any unintended consequence of excluding many new and future uses of electronic communication data (including metadata and content), which may be perfectly legitimate, customary and safe for individuals in the digital economy.

- The proposed ePrivacy Regulation is the subject of a forthcoming CIPL discussion paper which will be very critical about the heavy reliance on consent to the exclusion of other grounds for processing, highlighting not only the negative impact for individuals to benefit from data uses, but also the risks to the protection of their personal data. The paper will provide suggestions for limiting the scope of application of the ePrivacy rules and for **introducing the concept of legitimate interest into the ePrivacy Regulation** to align it more with the GDPR, possibly in combination with a risk-based approach.

- **The application and interpretation of consent under the GDPR and the ePrivacy Directive (and the proposed ePrivacy Regulation) must align.**

4. LEGITIMATE INTEREST

4.1 Starting points

- **Legitimate interest is an essential processing ground in the modern information age**. It ensures that the GDPR remains future-proof and technology neutral. It enables ongoing delivery and improvement of products and services, and new and innovative uses of data,

while ensuring organisational accountability and respecting data protection rights of individuals.

- **Legitimate interest is an element of and supports the controller's accountability.** It must not be considered as a processing ground of last resort. In many instances, it is a more accountable and effective tool for protecting individuals than other grounds, including consent.

- **The WP29 Opinion on legitimate interest of 2014[12] provides a useful and still relevant discussion of legitimate interest**. It provides useful examples and enables an understanding of possible practices of legitimate interest. The annex of this paper elaborates a number of examples of the legitimate interest ground for processing of personal data, based on the practices of the organisations participating in CIPL's GDPR project.

- **A general nonexhaustive "database" of legitimate interest processing cases may facilitate proper implementation of this requirement in the future.** We encourage the establishment of such a database by the EDPB with inputs from a multistakeholder group, including DPAs, industry and civil society.

4.2 Scope

- Legitimate interest is particularly useful because of the broad scope of application of the GDPR. Given this wide scope, **it is not possible to predetermine all contexts or processing activities where the legitimate interest ground may apply**. The basic purpose of the legitimate interest ground is to enable it to be applied contextually in cases where the conditions are right.

- **It is possible to articulate general categories of processing where legitimate interest typically does, or might, apply**. This approach is reflected in GDPR Recital 47 and demonstrated in CIPL's paper on legitimate interest case studies. Examples are: processing of customer or client data, including for direct marketing and advertising more broadly; processing of employee and customer data within a corporate family or group of undertakings for administrative purposes; processing payments/subscriptions to fulfill financial commitments and contracts; processing of data necessary for network and information security, processing for fraud prevention and investigation; certain data transfers.

- **Legitimate interest facilitates low-impact data processing**. Legitimate interest is particularly useful because of the broad scope of application of the GDPR, which includes a wide range of situations of personal data that is collected, used or shared that has little to no impact on the private life of individuals and does not create any risks for individuals. Legitimate interest facilitates the evaluation of this type of processing and the implementation of necessary controls, if any, with respect to this data, thereby enabling use of the data without resort to consent. Appendix II provides useful examples.

- **The legitimate interest to be evaluated may be the commercial or other interests of a controller but also may be the interests of other controller(s), groups of individuals and society as a whole.** Examples of the interests of society include: spam and fraud prevention,

[12] Article 29 Data Protection Working Party, 844/14/EN, WP217, Opinion 06/2014, on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, adopted on 9 April 2014.

improvements in health provision and prevention, environmental protections, infrastructure, scientific advancement, timely payment processing and invoicing, cybersecurity, tax collection, etc. In that connection, it should be recognised that commercial organisations often work in the public interest and that their own legitimate business interests may also involve benefits to third parties and society.

- **The legitimate interests of the controller or a third party may also include other rights and freedoms.** The balancing test will sometimes also include consideration of other rights and freedoms, such as freedom of expression, right to engage in economic activity, right to ensure protection of IP rights, etc. These rights must also be taken into account when balancing them against the individuals' right to privacy.

- **CIPL proposes to identify and further develop lists of general criteria that can help establish a potential legitimate interest**.

4.3 The limitation for special categories of sensitive data

- **Special categories of data (or sensitive data) may not be processed on the basis of legitimate interest.** This raises problems, particularly in relation to processing in which the controller or processor does not have direct contact with the individual and cannot ask for consent and also given the growing use of biometrics, for security, verification and authentication purposes. Examples include CCTV, or facial recognition by retailers to identify known shoplifters, or use of fingerprints for payment ID.

- **Anonymisation and pseudonymisation could be solutions and should be further developed**. First, anonymisation may resolve the problem in contexts where full anonymisation is possible and subsequent re-identification is not possible or needed. Second, pseudonymisation is an instrument that allows for transforming sensitive data into "ordinary" personal data, representing low risks for the individual. Pseudonymised data may be processed on the basis of the legitimate interest ground, which is particularly attractive in view of the low risk for the individuals after pseudonymisation.

- Pseudonymisation should also be further developed for specific contexts where additional safeguards apply. An example is clinical research where legal, ethical and contractual safeguards must be applied in addition to a very specific codification process.

4.4 The balancing test

- **The legitimate interest ground is no carte blanche for processing.** Instead, the balancing test under legitimate interest requires a context-specific risk/benefit assessment and implementation of potential mitigations as part of organisational accountability.

- **Each controller is responsible to ensure that the application of the legitimate interest ground for a new processing purpose meets the relevant balancing test**. Moreover, each new or changed proposed processing purpose must be reviewed de novo under the legitimate interest balancing test.

- **DPAs should be available and accept informal consultations** when businesses conduct the relevant risk analysis or balancing test.

- **Industrialise risk assessments, but accept that they are context-specific.** The weighing of legitimate interests and benefits of controllers or third parties against competing individual rights and freedoms and the outcomes of risk assessments are **context-specific**. Organisations will have to become proficient in conducting risk assessments in the context of applying the legitimate interest ground.

- However, this **does not preclude a general framework or guidance** that would enable businesses to identify processing activities that are likely to meet the legitimate interest requirements (subject to verification) or to consistently identify/assess potential risks or harms to individuals. The WP29/EDPB should play a role in developing a general framework or guidance on this issue, as a follow-up of the "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679".[13]

- Given that **organisations must take into account the reasonable expectations of individuals** in determining the legitimate interest and performing a balancing test, it may be possible to identify generally accepted examples of "reasonably expected" processing, i.e. activities that are customary and reasonable and thus should be "reasonably expected". This should include services where advertising is a normal feature related to the service. In addition, it should be reasonably expected that organisations will analyse their customers' data to make improvements to their products and services or to develop new products and services.

  However, even where a proposed data use was not within the reasonable expectations of a data subject, it should still be possible to rely on the legitimate interest balancing test to authorise that use. While it is essential that organisations take into account the reasonable expectations, the public interest or other factors considered in the balancing test may support an unexpected use.

- **The test for legitimate interest must be flexible.** The "reasonable expectations" of individuals change over time and the legitimate interest balancing test must be capable of taking these changes in reasonable expectations into account.

4.5 Transparency

- The requirement to **provide the legitimate interest pursued by the data processing in privacy notices to individuals must be implemented with flexibility.** DPAs should recognise practical challenges in delivering this information in every single case of legitimate interest processing. Organisations should be allowed to provide general information about the legitimate interests pursued in their privacy policies. In some instances, it may be actually prejudicial to provide a detailed notice about a processing based on legitimate interest, where that may prejudice the purpose of processing, such as in respect of information and system security or fraud prevention processing.

4.6 Legitimate interest and cross-border transfers

[13] Adopted by the WP29 on 4 April 2017. See also CIPL's December 2016 white paper on "Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR", which provides guidance on devising such a framework to identify and assess the risks and benefits associated with processing, including in the context of establishing a legitimate interest ground for processing. See https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf.

- **The WP29 should develop guidance (including examples) for use of legitimate interest as a ground for cross-border data transfers**, given the higher threshold for legitimate interest as a basis for data transfers in the GDPR (see Article 49(1)(g). The GDPR refers to notification to individuals and DPAs and to the assessment of all circumstances surrounding the transfer, as additional elements of a legitimate interest test.

- **Legal requirements or legitimate administrative requests for data in non-EU countries should be considered as an example of a legitimate interest enabling data transfers in specific and limited instances.** There are numerous examples, such as a requirement of a third country to give tax authorities of third countries access to personal data, or a need to provide senior leadership data to a foreign client for the purpose of a public service tender, or a requirement to provide data for e-discovery and judicial proceedings purposes, or an export control law requirement to check against economic sanctions lists.

- **International data transfers necessary for global cyber threat intelligence and security should be considered to be based on legitimate interest,** consistent with Recital 49.

Appendix I
Relevant GDPR Provisions

GDPR Transparency Requirements

Transparency is now **explicit requirement** and part of 1st DP principle:

- Personal data must be processed fairly, lawfully and in a transparent manner (Art. 5(1)(a); Recital 39)

- Controller is responsible for demonstrating compliance with transparency (Art. 5(2))

- Controller must provide information and all communications to individuals in a concise, transparent, intelligible and easily accessible form, using clear and plain language (Art. 12(1)), in respect of:

    - Privacy notices when data is collected from data subject (Art. 13) or third parties (Art. 14)

    - Individual rights: right of access (Art. 15), right of rectification (Art. 16), right to erasure (Art. 17), right to restriction (Art. 18), notification re rectification, erasure or restriction (Art. 19), data portability (Art. 20), right to object (Art. 21), automated decision making, including profiling (Art. 22)

    - Notifications of personal data breach (Art. 34)

See also Recitals 39, 58, 60-63 - individuals must be made aware of processing, purposes, risks, rules, safeguards and rights

Transparency is further reinforced by and linked to GDPR requirements for consent, notice, legitimate interest, right of access, publicising DPO contacts.

- **Privacy Notice (Art. 13 & 14)**

  Controllers must provide the following information to individuals **when obtaining data from individuals** and **when obtaining data from third parties**:

    - Controller/representative identity

    - DPO identity/contact details

    - Purposes of processing and legal basis

    - If processing based on legitimate interests, an explanation of those interests

    - Whether provision of data is mandatory

    - Recipients

    - Data retention periods

    - All individuals' rights, including right to complain to DPA

    - Information on cross-border transfers

- Existence of automated decision taking and logic behind it
- Not necessary where individuals already have this information
- Further exemptions from notice when collecting data from third parties – impossible or disproportionate effort, legal obligation, confidentiality duty (Art. 14(5))
- Standardised machine readable policies and icons are encouraged and Commission can set the information provided by icons and procedure for standardised icons (Art. 12(7)(8))

GDPR Consent Requirements

- Consent is one of the grounds for lawful processing (Art. 6(1)(a)), key ground for processing of sensitive data (Art. 9), one of the basis for data transfers outside EU (Art. 49)
- Consent must be freely given, specific, informed and unambiguous indication by statement or clear affirmative action (Art. 4(11); Recital 32)
- Controller must be able to **demonstrate** consent, if a basis for processing (Art. 7(1); Recital 42)
- Request for consent must be intelligible and easily accessible using clear and plain language (Art. 7(2); Recital 42)
- DP Consent must be **distinguishable** from other consents and **separate for each processing operation** (Art. 7(2))
- Consent can't be used where there is **clear imbalance** between individuals and controller (Recital 43), in particular where controller is a public authority
- Consent must **not be conditional** – contract/ service must not be conditional on consent to processing not necessary for the contract/service (Art. 7(4); Recital 43)
- Individuals can **withdraw** consent any time (Art. 7(4); Recital 42)
- **Children's consent**: can be used if child is at least 16. If below 16, consent must be "given or authorized" by the parent (Article 8(1)) (Member States may lower the age 16 -13. Art. 8(1))

GDPR Legitimate Interest Requirements

- One of grounds for **lawful processing** of personal data (Art. 6(1)), as well as an exceptional basis for data **transfers outside the EU** (Art. 49(g))
- Processing is necessary for the purpose of the legitimate interests by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedom of the data subject, in particular where data subject is a child (Art. 6(1)(a), (f); Recitals 47, 51)
    - Controller must take into consideration individual's **reasonable expectations based on his/her relationship with controller** (Recital 47)
    - Controller must provide **notice** of legitimate interest to individuals.

- Examples of recognised legitimate interest in GDPR (Recitals 47-49):
    - Fraud prevention
    - Information and network security
    - Direct marketing
    - Processing by a group of undertaking for internal administrative purposes, including clients' and employees' data (but without prejudice to cross border data transfers requirements)
- Individuals have a broad **right to object** to processing based on legitimate interests, at any time and without justification, but the controller may demonstrate compelling interests overriding the right of the data subject (Art. 21)
- Legitimate interest processing not available for processing of special categories of personal data (Art. 9), or for automated decision making that produce legal effects or significantly impact individuals, or for data processing in the context of ePrivacy Regulation (*lex specialis* applies)
- Legitimate interest may be used exceptionally for data transfers outside the EU on a limited basis (Art. 49(g)(2)) - no other ground and derogation applies, not repetitive transfers, limited number of individuals' interests must be "compelling" and controller must assess all the circumstances and provide suitable safeguards
    - Controller must inform DPA and individual of the transfer and the use of the compelling legitimate interest

APPENDIX II:
CIPL Examples of Legitimate Interest Grounds for Processing of Personal Data

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 minimise 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 minimisation including as appropriate data anonymisation and pseudonymisation.

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 jeopardise 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 authorised signatory, etc. or jeopardise 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).