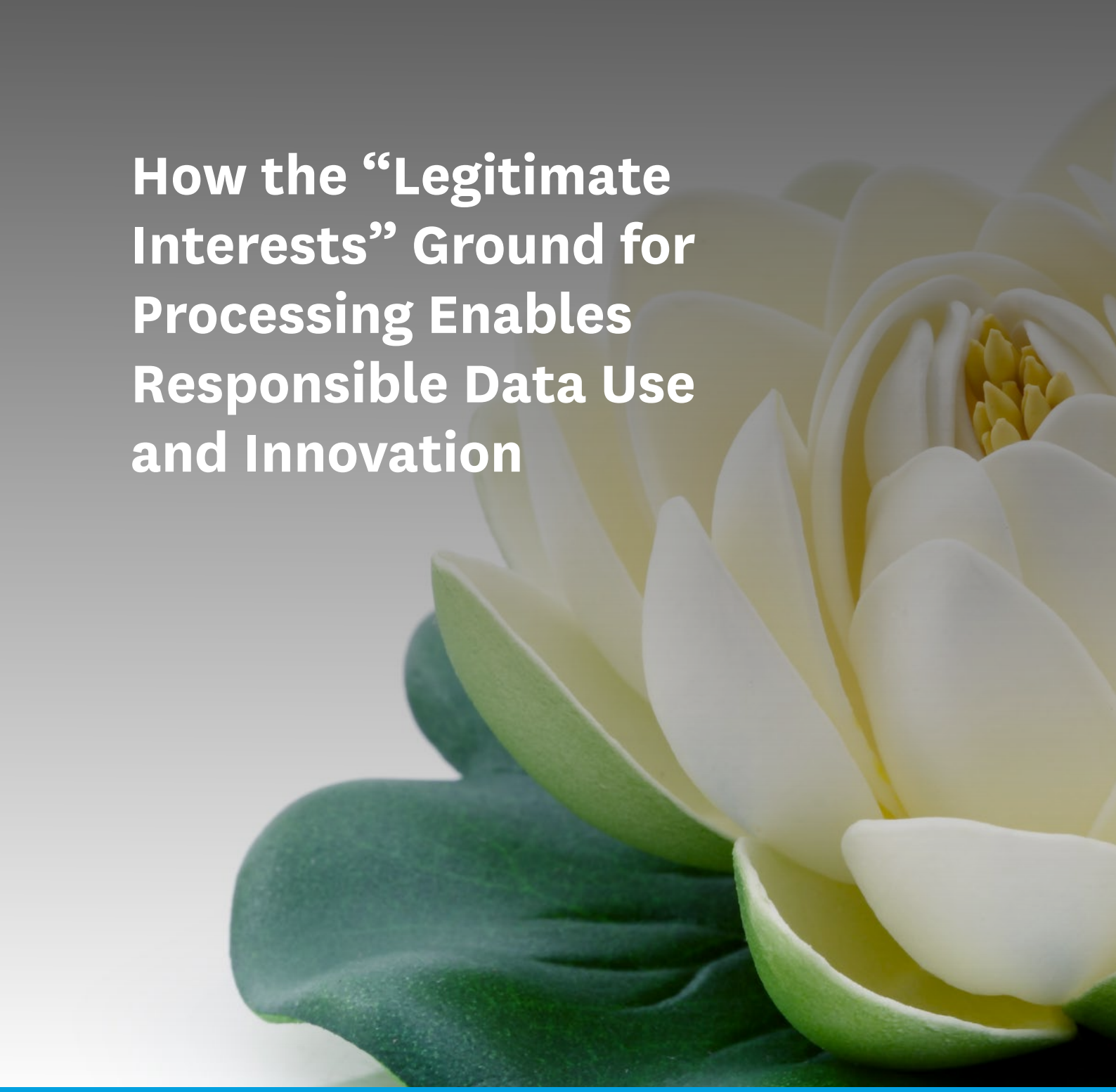
How the "Legitimate Interests" Ground for Processing Enables Responsible Data Use and Innovation



July 2021

CIPL AT 20 — SHAPING DATA POLICY FOR TOMORROW

HUNTON ANDREWS KURTH

Table of Contents

SUMMARY OF RECOMMENDATIONS FOR THE EDPB, DATA PROTECTION AUTHORITIES AND POLICY MAKERS

In their interpretation of the legitimate interests concept, these authorities should:

- Acknowledge that there is no hierarchy among the legal bases;
- Encourage and enable consistency in the data protection authorities' (DPAs) interpretation and application of the legal bases in the EU;
- Emphasise that the key consideration with respect to legal bases is that organizations must rely on a legal basis that is appropriate for the data processing activity at hand;
- Avoid adopting a narrow and overly restrictive interpretation of the legitimate interest legal basis;
- Acknowledge that the legitimate interests legal basis relies on and promotes risk-based organisational accountability enabling a robust level of protection for individuals;
- Avoid assuming that certain types of data processing activities are automatically excluded from the legitimate interests legal basis;
- Acknowledge that the examples of legitimate interests provided by the GDPR are non-exhaustive;
- Provide further examples of activities that may be carried out based on the legitimate interests legal ground;
- Clarify the applicability of the right to object to legitimate interests-based processing, including why the right to object is unsuitable or inappropriate in certain situations;
- Acknowledge that the legitimate interest legal basis is likely to be increasingly used to justify growing societal needs for beneficial and responsible uses and sharing of data;
- Acknowledge the elements that form part of the legitimate interests assessment and provide examples of these elements;
- Provide examples of outcome-based and non-prescriptive frameworks or methodologies that organisations can use for undertaking legitimate interests assessments;
- Acknowledge that weighing the legitimate interests of the controller or third party against the interests or rights and freedoms of individuals requires taking into account mitigating measures that would reduce or eliminate any harmful impacts on individuals;
- Refrain from recommending that organizations publish their completed legitimate interests assessments; and
- Clarify that accountability measures implemented in connection with legitimate interests-based processing operations can serve as mitigating factors in potential enforcement cases.

Following the European Data Protection Board's (EDPB) Stakeholder Workshop on Legitimate Interests on 27 November 2020,[1] the Centre for Information Policy Leadership (CIPL)[2] published this white paper (Paper) as input for the EDPB's future update of the guidelines on the legitimate interests legal basis (Guidelines). This Paper is also relevant for any jurisdiction where data protection law includes legitimate interests as a legal basis for processing personal data, as well as for policy makers in countries looking to adopt a data protection regime.

This Paper explains the growing importance of the legitimate interests legal basis for organisations' data processing activities and examines how it should be interpreted, used and applied to unlock the value of data in today's global data-driven and connected world. The Paper also includes an Appendix which summarizes case studies on how organisations currently rely on the legitimate interests legal basis for both (i) routine data processing activities, and (ii) more complex, unique, or new data processing activities that are key for innovation and for the development of the EU digital economy).[3]

There are still many challenges and legal uncertainties that prevent organisations from relying on legitimate interests as a legal basis for processing personal data. With the update of the Guidelines, the EDPB has an opportunity to clarify these issues, and make the legitimate interests basis a catalyst for accountable data practices that drive economic development and innovation in a privacy-preserving manner. One of the ways the EDPB can accomplish this is to acknowledge that organisations may rely on this legal basis for a wide variety of data processing activities, ranging from routine, operational data processing, to more complex and innovative data processing involving new technologies and business models. The EDPB should provide additional and non-exhaustive examples and use cases of such data processing activities of what the EDPB views as an appropriate legitimate interests assessment to help organisations of all sectors confidently rely upon this legal basis when appropriate.

1 EDPB Stakeholder Workshop on Legitimate Interest, published on 16 November 2020.

2 CIPL is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 80 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 that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

3 This paper updates the following CIPL 2017 papers: CIPL Examples of Legitimate Interest Grounds for Processing of Personal Data and Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR.

1. PRELIMINARY CONSIDERATIONS ON THE LEGAL BASES FOR PROCESSING UNDER THE GDPR

CIPL welcomes the EDPB's initiative to update the Article 29 Working Party's 2014 opinion on the legitimate interests legal basis and its dialogue with stakeholders on this important issue.[4] Applying the data protection principles outlined in Article 5 of the General Data Protection Regulation (GDPR) and selecting the relevant legal basis for processing personal data under Article 6 GDPR are among the most important obligations for organisations. Non-compliance with these provisions can potentially give rise to the highest fines under the GDPR, i.e., up to 20 million EUR or up to 4% of the total annual worldwide turnover.

All legal bases for processing are on equal footing with one another, meaning that there is no "default" legal basis, no hierarchy between them, and none should be privileged over the other.

1.1 Legal bases for processing have the same weight

The GDPR provides organisations with a range of legal bases for processing and organisations can choose a basis that is appropriate to their particular processing activity. All legal bases for processing are on equal footing with one another, meaning that there is no "default" legal basis, no hierarchy between them, and none should be privileged over the other. At the same time, they are intended to complement one another. However, there are still a number of general misconceptions about the legal bases for processing:

- Some DPAs still give more weight to consent over other legal bases. This approach disregards the fact that there are many instances where consent is an inappropriate legal basis, and that individuals increasingly express "consent fatigue." This approach also overlooks the benefits to individuals and controllers associated with relying on other legal bases (see Section 1.4 below);
- Outside of specific circumstances, such as those created by the COVID-19 pandemic, organisations still lack clarity about when they can rely on less commonly used legal bases, such as vital interests and public interest; and
- The legitimate interests basis is sometimes considered a processing ground of last resort that should be reserved for exceptional cases.

The legitimate interests basis may be an appropriate legal basis in circumstances where there is a legitimate interest in the processing that is not overridden by the individuals' interests or fundamental rights or freedoms. Another element of the test for "legitimate interests" may be whether individuals would reasonably expect the data processing activities at hand, as suggested by Recital 47 of the GDPR. However, organisations are still hesitant to apply this legal basis and often instead rely on other legal bases (including consent) that are less controversial in the belief that they give individuals more control and provide for more legal certainty, even where these legal bases are less suitable to the processing at hand and result in lower privacy outcomes when compared to the legitimate interests basis.

4 Article 29 Working Party's Opinion 06/2014 on the Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC.

The EDPB Guidelines should therefore underline that there is no hierarchy among the legal bases under the GDPR, and that the legitimate interests legal basis is not a basis of last resort. This will accommodate the growing frequency of data processing and complexity of modern data uses, as well as enable organisations to more confidently select any relevant and appropriate legal basis for a wide range of processing activities.

1.2 Organisations may be reluctant to rely on the most appropriate legal basis

If the EDPB applies a restrictive interpretation to the legitimate interests legal basis, it may result in organisations choosing to rely on consent and contractual necessity even where it would be more appropriate to rely on legitimate interests. Contractual necessity, however, has been interpreted very narrowly by the EDPB, and the requirements for consent may not be achievable or even be suitable in certain contexts. This may render these two bases inapplicable in a wide range of cases, including cases that involve innovative data uses with little or no risks to individuals. As a result, organisations may be reluctant to progress projects that may be beneficial to individuals and society due to a lack of clarity around the legal bases available for processing. For instance, during the COVID-19 pandemic, private organisations were unclear on whether they could rely on legitimate interests to conduct related data analytics and research.

The Guidelines should avoid applying a narrow and overly restrictive interpretation to the legitimate interests legal basis and clarify that organisations should be able to rely on any legal basis that is appropriate for a particular data processing activity.

This reluctance to rely on the legitimate interests legal basis may impact the ability of organisations to develop and innovate within the EU while relying on legitimate interests to process data and could, therefore, limit the practical use of a legal basis expressly provided for by the GDPR. The Guidelines should therefore avoid applying a narrow and overly restrictive interpretation to the legitimate interests legal basis and should clarify that organisations should be able to rely on any legal basis that is appropriate for a particular data processing activity.

EU DPAs must align their interpretations of the legal bases for processing. To date, it appears that EU DPAs have applied different interpretations of the legal bases for processing. The Dutch DPA, for example, has recently provided an opinion[5] that processing for "purely commercial interests" cannot be justified under a legitimate interests assessment, in contradiction with Recital 47 of the GDPR and the Article 29 Working Party's opinion on legitimate interests.[6] The Dutch District Court of Midden-Nederland has overturned the DPA's interpretation and confirmed that "any one interest should not categorically be excluded," i.e., all interests should have the opportunity to be recognised.[7]

Given that organisations conduct a growing number of data processing activities across several countries, consistent interpretation of the GDPR requirements by DPAs is critically important, and its importance will only increase as the EU data economy further develops.[8]

The Guidelines should therefore provide consistency in the interpretation and application of the legal bases and, in particular, of the legitimate interests legal basis.

1.3 The legitimate interests legal basis may be the most appropriate legal basis

In many instances, the legitimate interests basis may be the only possible legal basis upon which an organisation can rely. In others, it may be the most appropriate one. This might arise where private organisations are not processing personal data for purposes of performance of a contract, compliance with a legal obligation, or to protect the vital interests of individuals. The only legal bases they may be left with are consent and legitimate interests. In many cases, obtaining consent is impracticable,

5 Autoriteit Persoonsgegevens (Dutch DPA)'s Standard explanation of the 'legitimate interest' basis, November 2019 (in Dutch).
6 See footnote 4.
7 Hunton Andrews Kurth Privacy and Information Security Law Blog, Dutch Court Overturns DPA Fine on Legitimate Interests Legal Basis, 1 December 2020.
8 See, for reference, the European Commission's EU Data Strategy.

counter-productive and not meaningful (for example, as mentioned above, when it clashes with "consent fatigue" that could render an individuals' consent meaningless, or where the possibility of upholding consent could negatively impact the public interest or the legitimate rights of others).

In many instances, the legitimate interests basis may be the only possible legal basis upon which an organisation can rely. In others, it may be the most appropriate one.

Section 4 of this Paper provides several examples where consent is not the appropriate legal basis for processing, such as in the context of employment, where consent would not be recognised as freely given (case study 4); in the context of mergers and acquisitions (M&A), where consent would break the necessary confidentiality (case study 8); in cases involving imagery collection to improve mapping applications and audience measurement where controllers do not have a direct relationship with individuals (case studies 10 and 14); in fraud monitoring cases, where fraudsters would likely not provide their consent for data processing to combat fraud (case study 1); in the improvement of voice assistants based on machine-learning technology, where consent would limit the range of data used to train the algorithm in a fair manner and affect user experience (case study 11); and, in cases of product offers that clearly involve targeted advertising or content personalisation as part of the offer, where obtaining consent could be impractical and would negatively impact the online experience (case studies 13 and 16).

In all of these cases—which represent routine, daily data processing activities that organisations undertake in order to conduct their businesses—organisations are left with legitimate interests as the most appropriate legal basis to rely upon. Any narrow construction of the legitimate interests legal basis would undermine its usefulness and render these processing operations impossible, ultimately unduly restricting the ability of organisations to conduct business.

The EDPB should provide an interpretation of the legitimate interests legal basis that is sufficiently broad and flexible, as it may be the most relevant legal basis for many basic, essential and beneficial processing operations.

2. KEY FEATURES OF THE LEGITIMATE INTERESTS LEGAL BASIS

2.1 The legitimate interests legal basis is grounded in organisational accountability

As the legitimate interests legal basis relies on a balancing test that involves assessing the risks relating to the data processing activities and defining measures to mitigate these risks, it is effectively grounded in risk-based organisational accountability.[9] Under the GDPR, the principle of accountability means that organisations:

As the legitimate interests legal basis relies on a balancing test that involves assessing the risks relating to the data processing activities and defining measures to mitigate these risks, it is effectively grounded in risk-based organisational accountability.

i. Take steps to translate data privacy legal requirements into risk-based, concrete, verifiable and enforceable actions and controls; and

ii. Are able to demonstrate the existence and effectiveness of such actions and controls internally and externally.

The GDPR also requires (i) enhanced transparency when organisations rely on the legitimate interests legal basis (Article 13 (1)(d)), and (ii) documentation of the outcomes of the legitimate interests assessment to demonstrate accountability (Article 35 (7)(a)). Finally, it provides individuals with a right to object to the processing that the controller can override if it demonstrates compelling legitimate grounds (Article 21 (1)).

Organisations that have an accountability-based privacy management programme in place are already familiar with risk assessments, which would enable them to perform the legitimate interests balancing test and to mitigate the risks in an effective manner. The legitimate interests assessment is not a self-standing and isolated exercise conducted only at the outset of the processing. Rather, the process and outcomes of the legitimate interests assessment, which include devising mitigating measures, are fully operationalised and integrated as part of the organisation's wider accountability programme that is continuously subject to monitoring, updating and improvement. This enables real-time accountability throughout the life-cycle of a particular processing operation, contradicting the common, but unfounded perception, that the legitimate interests basis might be misused as a *"carte blanche"* for questionable data processing. **The Guidelines should acknowledge that the legitimate interests legal basis relies on, and promotes, organisational accountability.**

Furthermore, accountability mechanisms such as codes of conduct and certifications may help clarify and facilitate the use of the legitimate interests legal basis, particularly in a given industry sector. They may establish consistent practices concerning legitimate interests assessments, the risks and harms to be weighed against the legitimate interests of the controller and third parties, and relevant mitigating measures.

9 See the CIPL Accountability Framework for the elements of accountability. CIPL has written extensively on the principle of accountability. See CIPL White Paper What Good and Effective Data Privacy Accountability Looks Like: Mapping Organizations' Practices to the CIPL Accountability Framework, 27 May 2020. For the other CIPL accountability papers, see CIPL's website.

Finally, there may be situations where organisations voluntarily choose to go beyond the GDPR requirements regarding the legitimate interests legal basis—e.g., by proactively providing enhanced transparency, publishing a summary of their legitimate interests assessment, or providing differentiated tools to facilitate the right to object to processing based on legitimate interests. **The EDPB should take these practices and the overall robustness of an organisation's data privacy accountability programme into account as possible mitigating factors in potential enforcement cases.**

2.2 The legitimate interests legal basis is a manifestation of the GDPR's risk-based approach

The legitimate interests assessment is intrinsically linked to the GDPR's risk-based approach (see Section 3 for a detailed discussion of the legitimate interests assessment). It enables processing of personal data when it does not result in a risk of harm to individuals. It also promotes the protection of individuals, because it requires organisations to undertake the necessary risk assessments, define the mitigation measures, train employees on risks and mitigation measures, monitor the continued effectiveness of the mitigations, identify potential compliance gaps, fix them and continuously improve the level of protection. Of course, this does not mean that organisations do not apply accountability measures when relying on other legal bases for processing, but that accountability is inherent to the legitimate interests legal basis.

Accountable organisations may integrate the legitimate interests assessment with their overall risk assessment practices.

Accountable organisations may integrate the legitimate interests assessment with their overall risk assessment practices. For example, they may apply a similar approach or methodology to data protection impact assessments (DPIAs), the test for further processing for compatible purposes (see Article 6 (4) GDPR), and international transfers assessments. They may also link their risk assessments to internal and external triggers such as changes resulting from new business activities, new technologies, new regulatory requirements, or external scenarios like the COVID-19 pandemic.

The EDPB Guidelines should acknowledge the inherent risk-based and accountability dimensions of the legitimate interests legal basis.

2.3 The legitimate interests legal basis is contextual and relies on a case-by-case analysis

The legitimate interests assessment is linked to a processing activity in a specific context. Thus, its results are not set in stone and may vary according to the nature of the processing activities, the likelihood and severity of harm to individuals, the mitigation measures implemented by organisations, and individuals' reasonable expectations. Therefore, it is important that **the Guidelines do <u>not</u> pre-suppose that certain types of personal data and data processing activities would be inherently unfit for the legitimate interests legal basis without undertaking a concrete risk analysis as part of its assessment.**

The CJEU confirmed in the ANSEF (2011) and Breyer (2016) cases (under Directive 95/46, which already included the legitimate interests legal basis), that member states cannot definitively prescribe, for certain categories of personal data, the result of the legitimate interests assessment without allowing a different result by virtue of the particular circumstances of an individual case.[10] A similar approach should apply to DPAs and the EDPB.

Pre-supposing that certain data processing activities or data types would not pass a legitimate interests assessment could impose significant opportunity costs and lower privacy outcomes for individuals as a result of the unnecessary limitation on processing. That is, it could prevent organisations from even starting to undertake a legitimate interests assessment, thereby potentially excluding processing activities that may be both beneficial and harmless in their specific context, or that do not negatively impact the fundamental rights of individuals in their specific context. For example, due to the possible impacts of

10 Joined Cases C-468/10 AND C-469/10, Asociacion Nacional de Establecimientos Financieros de Credito (ASNEF) and Federacion de Comercio Electronico y Marketing Directo (FECEMD) v. Administracion del Estado, 24 November 2011 ("ASNEF"); and Patrick Breyer v. Bundesrepublik Deutschland / C-582/14, 19 October 2016.

Pre-supposing that certain data processing activities or data types would not pass a legitimate interests assessment could impose significant opportunity costs and lower privacy outcomes for individuals as a result of the unnecessary limitation on processing.

new technologies on individuals, the GDPR instructs organisations to undertake a DPIA to assess the risks of their data processing activities involving the use of new technologies (Article 35 (3)(a)). Indeed, new technologies can be used for legitimate purposes that benefit individuals and society, such as new tools that improve means for detecting and preventing fraud or child sexual abuse imagery. In both cases, there is a risk that false positives could prevent an individual from having access to a service. In such cases, a legitimate interests assessment provides the adequate means to assess the actual risks involved as well as relevant mitigation options.

2.4 The legitimate interests legal basis covers a non-exhaustive and growing list of processing activities

Recital 47 of the GDPR provides some insight into the types of cases in which organisations may be able to rely on the legitimate interests legal basis, including prevention of fraud and direct marketing. These examples are non-exhaustive. CIPL has identified many other cases where it may be more appropriate for organisations to rely on the legitimate interests legal basis than on other legal bases (see Section 4 for further details), and grouped them as follows:

- **Every-day, routine and established business purposes.** In these cases, it is important to preserve the flexibility of the legitimate interests basis in a way that is more streamlined and not unduly burdensome for organisations of all sizes. These cases:
  - Are clearly in the legitimate interests of the processing organisation or of third parties;
  - Represent data processing activities that are customary, and thus would be "reasonably expected" by individuals;
  - Are likely to represent a low-risk for individuals; and
  - Are likely not to be overridden by the interests or fundamental rights and freedoms of individuals in the legitimate interests assessment.
- **More complex, unique, innovative, original or new data processing activities that are key for innovation and for the development of the EU digital economy.** Examples include algorithmic training for machine-learning and Artificial Intelligence (AI) purposes, processing for unanticipated research and statistical purposes that do not meet the test of Article 89 of the GDPR, or the use of "data for good" to address a societal need or a crisis.

The EDPB Guidelines should therefore acknowledge that the examples of legitimate interests provided by the GDPR are non-exhaustive.

2.5 The legitimate interests legal basis offers the flexibility necessary for complex data use

The legitimate interests legal basis is essential for organisations of all sizes and industry sectors to operate in the modern and ever more complex information age. It is instrumental in a period of rapidly advancing technologies and changes in business models where processing activities are constantly evolving and business processes are increasingly digitised.

In particular, the legitimate interests legal basis is instrumental for algorithmic training in the context of developing new technologies such as AI and machine-learning and, in many cases, may be the only available legal basis for algorithmic training. Generally, using data for algorithmic training will involve further processing of personal data, which will also require organisations to undertake the compatibility test under Article 6 (4) of the GDPR. Organisations may carry out this test as part of the legitimate interests assessment. A study published by the EU Parliament has recognised that individuals' rights

The legitimate interests legal basis is essential for organisations of all sizes and industry sectors to operate in the modern and ever more complex information age.

and freedoms would generally not be impacted by the processing of personal data for algorithmic training, except if personal data is misused (which can be prevented, for instance, by robust security measures).[11]

One of the key concerns related to algorithmic training is ensuring that the variety of data types and sets used sufficiently represent society so that the machine-learning process will not result in biases. In the context of algorithmic training, therefore, organisations would not be able to rely on consent, as doing so could undermine the goal of having representative data sets if members of certain groups that are more likely to provide consent are over-represented in the data set, thereby creating data sets that do not accurately reflect the composition of the population.

Another concern relating to algorithmic training and to complex data uses relates to the fact that the GDPR does not allow organisations to rely on legitimate interests for processing special categories of personal data. This is an issue, as such categories of data are often necessary in order to appropriately train algorithms and to ensure bias monitoring.[12]

Finally, regulators and policy-makers expect organisations to undertake robust risk assessment and risk management when processing personal data in the context of AI and new technologies[13] to ensure that appropriate protective measures are implemented and weighed. For example, in its guidance on AI and Data Protection, the UK Information Commissioner's Office (ICO) provides an auditing framework for AI compliance that includes a roadmap for individuals designing, building and implementing AI systems that is heavily based on risk assessments.[14]

Therefore, the flexibility provided by the legitimate interests legal basis, coupled with organisational accountability and its inherent risk-based approach, makes the legitimate interests basis a key enabler of responsible innovation and an accountable digital economy. Specifically, it enables the GDPR to remain future-proof and technology-neutral, to allow for beneficial data uses that are in the public interest by both the private and public sectors, to provide ongoing delivery and improvement of products, services, systems and technologies, and to foster new and innovative uses of data in a privacy-preserving manner.

The legitimate interests legal basis will also be crucial for data sharing activities under the proposed Data Governance Act.[15] Such data sharing activities will be important to unlock the value of data, enable efficient cross-border business operations, promote innovation, and enhance greater business opportunities to better serve consumers in a responsible manner. GDPR and its interpretation must be aligned with and work together with the other digital laws and policies of the EU, and DPAs should take into account these initiatives as well.

The EDPB Guidelines should acknowledge that the legitimate interests legal basis is likely to be increasingly used in the modern digital age to justify growing societal needs for beneficial and responsible uses and sharing of data, including "data for good" initiatives.

11 See, for example, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence by Professor Giovanni Sartor of the European University Institute of Florence, published on the European Parliament Think Tank website, 25 June 2020, which provides that legitimate interests can be a legal basis for algorithmic processing. See also the UK ICO Guidance on AI and Data Protection, July 2020, which recognises that the controllers can process personal data for both development and ongoing use of AI based on legitimate interests.

12 See the Draft EU AI Act. Article 10 (5) provides that "To the extent that it is strictly necessary for the purposes of ensuring bias monitoring, detection and correction in relation to the high-risk AI systems, the providers of such systems may process special categories of personal data referred to in Article 9 (1) of Regulation (EU) 2016/679."

13 See the Hunton Andrews Kurth post on the Privacy & Information Security Law blog European Commission Publishes Proposal for Artificial Intelligence Act, 22 April 2021.

14 See the UK ICO Guidance on AI and Data Protection, July 2020.

15 See Recital 11 and Article 5 (6) of the European Commission's Proposal for a Regulation on European data governance (Data Governance Act).

The flexibility provided by the legitimate interests legal basis, coupled with organisational accountability and its inherent risk-based approach, makes the legitimate interests basis a key enabler of responsible innovation and an accountable digital economy.

2.6 Individuals may object to data processing unless the organisation demonstrates compelling legitimate grounds

Individuals may object at any time to processing of their personal data based on legitimate interests, unless the controller demonstrates compelling legitimate grounds for the processing that override the interests or fundamental rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims (Article 21 GDPR). **The EDPB Guidelines should clarify the following:**

- Organisations may not always be able to act upon the right to object as it depends on the legitimate interests assessment performed by the controller (except where explicitly provided by the GDPR, for example, for direct marketing purposes);
- The right to object may be overridden in some cases where there are compelling legitimate grounds for processing the data, for example, for fraud prevention purposes or where the processing is necessary for the defence of legal claims, following a case-by-case assessment by the controller in view of the rationale for the objection;
- Organisations that handle objections at scale should be able to implement internal guidelines and processes to streamline the consideration of objections rather than having to analyse similar and repetitive objections on a case-by-case basis; and
- Organisations should have the flexibility to provide information on the right to object and facilitate the exercise of this right in a manner that is most appropriate to the context of the processing activities whilst aligning with the requirements of the GDPR—e.g., by providing individuals with an online contact form, with an email/postal address to which any objection may be sent, via an opt-out option, or via a setting allowing the data subject to effectively "self-serve" by turning off any legitimate interests-based data processing.

3. SPECIFIC CONSIDERATIONS REGARDING THE LEGITIMATE INTERESTS ASSESSMENT

In practice, the legitimate interests assessment consists of a risk assessment in which organisations take into account and balance a set of key elements.

3.1 Key elements of the legitimate interests assessment

In practice, the legitimate interests assessment consists of a risk assessment in which organisations take into account and balance a set of key elements listed below. **The EDPB Guidelines should acknowledge that these elements form part of the legitimate interests assessment and should provide examples, whenever possible, of these elements:**

1. The context, purpose and benefit of the data processing activities, as well as the reticence risk (loss of opportunity/benefits) of not carrying out the processing;

2. The legitimate interests of the controller, third parties, groups of individuals or society, as well as their rights and freedoms other than data protection rights (see point 3.2 below);

3. The interests, rights and freedoms of individuals taking into account their reasonable expectations that are based on the relationship with the controller (see point 3.3 below);

4. The risks and harms that may result from the processing activity or from the absence of the processing activity (i.e., reticence risks), including the likelihood and possible severity of harms to the individuals;

5. Any mitigating measures/safeguards that can be used to mitigate those risks, including existing technical and organisational measures, additional specific measures, and privacy enhancing technologies; and

6. Other factors, including the regulatory landscape.

In this Paper, CIPL provides a number of case studies demonstrating how organisations undertake legitimate interests assessments. There is not, however, a one-size-fits-all methodology, template or mechanism for these assessments. Organisations should be able to address the elements outlined above and document their assessments in a context-specific manner that is most appropriate to their business and operational activities. Nevertheless, **there is an opportunity for the EDPB to promote consistency and to help streamline legitimate interests assessments by recommending certain outcome-based frameworks or methodologies that are not overly prescriptive.**[16] This is due to the fact that there has been some industry feedback on the complexity of such assessments, and uncertainty about their correct or defensible application, especially among SMEs and start-ups. The recommended and non-prescriptive broad frameworks or methodologies from the EDPB would help to provide greater clarity/simplicity on these assessments, confer more confidence and promote their usage by organisations.

3.2 Legitimate interests of the controller or third parties

Article 6(1)(f) of the GDPR allows organisations to process personal data when such processing is necessary for the purposes of the legitimate interests pursued "by the controller or by a third party." This possibility is closely connected to the fact that

16 See, for instance, the UK ICO's guidance and legitimate interest assessment template.

Organisations often pursue objectives that directly or indirectly serve the public interest and benefit third parties and society.

an individual's right to data protection is not absolute, as recognised by Recital 4 of the GDPR, and that there may be other fundamental rights, including those held by other stakeholders, against which that right should be balanced in the legitimate interests assessment—such as freedom of expression, right to engage in economic activities, or right to ensure protection of IP rights.[17]

"Third parties" refers to any stakeholders involved in, or impacted by, the processing activities. These include other public and private organisations, individuals other than data subjects, groups of individuals, and society as a whole that can benefit from processing activities. These activities can be purely commercial or involve the processing of data in the public interest. The latter became particularly relevant during the COVID-19 pandemic, as processing and sharing of data became indispensable to effectively fighting the virus, which is in the interest of society not only in the EU but globally. Organisations often pursue objectives that directly or indirectly serve the public interest and benefit third parties and society.

3.3 Reasonable expectations of individuals

Recital 47 of the GDPR provides that "The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller."

The "reasonable expectations of individuals" is a subjective factor and can greatly vary depending on each individuals' knowledge of the product or service they are using or their specific situation

The "reasonable expectations of individuals" is a subjective factor and can greatly vary depending on each individuals' knowledge of the product or service they are using or their specific situation. In addition, this concept has to be read together with the notion of transparency, as individuals' expectations may be impacted by the level of information they receive on the data processing and how easily they understand such information. Their expectations also vary depending on whether the product or service offered and the related data processing is well-established and known in the market. What constitutes "reasonable expectations" of individuals should therefore not be set in stone or pre-determined at the outset because the notion of "reasonable expectations" is inherently linked to a contextual assessment and societal evolutions.

When assessing individuals' reasonable expectations in the context of a commercial relationship, organisations generally believe that the average individual (consumer) expects to receive the best service or product quality possible, that this service or product works as advertised, and that it is safe. Individuals also trust that the corresponding data processing occurs in accordance with organisations' representations. However, if individuals would not reasonably expect processing to occur at a particular time or in a specific context, or if the processing might cause harm to individuals, the interests of the individuals will likely outweigh those of the controller or of third parties taking into account the reasonable expectations of the data subject. Similarly, processing the data of individuals who have no direct or indirect relationship with the controller may shift the balance towards the interest and rights of these individuals.

It is important to note that individuals' reasonable expectations as well as the context related to the data processing activities may change over time. For instance, until recently, individuals did not expect that buying a refrigerator would entail any type of data processing. However, with the advent of the Internet of things, individuals who buy smart fridges understand that they are connected devices and that some type of data processing must occur for this device to work as intended. The legitimate interests assessment must be capable of taking these changes into account. Finally, when considering the "reasonable

17 Charter of Fundamental Rights of the European Union, 26 October 2012.

expectations" of individuals, it is important not to require very specific expectations regarding very specific processing operations, but to consider whether the processing falls into a general category of processing that individuals might expect.

When processing creates risks to individuals that outweigh the interests of the controller or of third parties, the organisation may apply mitigating measures to reduce such risks. These measures could shift the balance towards the legitimate interests of the controller.

3.4 Mitigating measures

When processing creates risks to individuals that outweigh the interests of the controller or of third parties, the organisation may apply mitigating measures to reduce such risks. These measures could shift the balance towards the legitimate interests of the controller.

In many cases of routine data processing activities, mitigating measures are already well established as good practice (e.g., only installing CCTV cameras in areas of higher-risk with appropriate transparency, and avoiding privacy-invasive and unexpected locations). For higher-risk data processing activities, organisations recognise that there is a need for more scrutiny and organisational accountability. In those cases, organisations undertake more detailed risk assessments and implement more advanced mitigating measures (e.g., enhanced transparency and controls to individuals, using aggregated and pseudonymised data sets to improve digital voice assistants through machine learning). Privacy Enhancing Technologies (PETs), in particular, have made important strides in recent years and have enabled novel and effective protection to individuals. Such technologies are constantly under development. For example, Google is currently developing technology to replace the use of third party cookies for advertising purposes with technologies focused on privacy by design and data minimisation.[18] Similarly, Apple has introduced Privacy Nutrition Labels and is rolling out a new App Tracking Transparency feature for users, consistent with their commitment to privacy.[19]

The EDPB Guidelines should acknowledge that effective mitigating measures and, in particular, PETs, may impact the legitimate interests balancing by reducing or eliminating risks to individuals and thus weighing in favour of the data processing. This would encourage organisations to implement more privacy protective measures and privacy enhancing technologies.

3.5 Confidentiality of the legitimate interests assessment

Although Article 13 (1)(d) requires controllers to provide the data subject with information about the legitimate interests pursued by the controller or a third party, the GDPR does not mandate that the controller publish the actual legitimate interests assessment or elements of its balancing test. The Guidelines should thus not require this practice. Doing so could lead to revealing confidential business information or IP/trade secrets, raising competition issues. This information may also be too technical and not meaningful to individuals. Equally, there may be cases where full transparency to individuals is inconsistent with public interest considerations and may prejudice organisations' ability to conduct essential and common data processing operations, such as fraud prevention, corporate investigations, or implementing information and network security measures.

However, this does not prevent organisations from proactively publishing their legitimate interests assessment or a summary of it. Organisations could do so in response to a specific request from a regulator or choose to provide them to third parties voluntarily, to enhance transparency and client trust.20 This enhanced transparency could also serve as a mitigating factor in enforcement cases.

18 Google Ads and Commerce Blog, Charting a course towards a more privacy-first web, 3 March 2021.
19 See Apple's User Privacy and Data Use and Apple's Privacy Features, section App Tracking Controls and Transparency.
20 See Twitter's webpage on Additional information about data processing, section Legitimate interests analysis summary.

4. CATEGORIES OF COMMON PROCESSING ACTIVITIES BASED ON LEGITIMATE INTERESTS

Below are non-exhaustive categories of data processing activities that organisations may undertake based on the legitimate interests legal basis. The purpose of this list is to provide some common examples across various industries, as well as use cases illustrating the key considerations of organisations when undertaking the legitimate interests assessment. Note that many of the data processing activities below may be undertaken based on AI and machine-learning, in which case the training of algorithms related to these technologies may also be considered in the legitimate interests assessment.

4.1 Fraud detection and prevention

Financial institutions, such as banks, credit card issuers and insurance companies, as well as consumer-facing organisations, often need to process data to comply with industry standards and regulators' requirements related to fraud prevention in a global context. In many circumstances, consent is an inappropriate legal basis as fraudsters could potentially withhold or withdraw their consent with the intent of circumventing the system.[21]

The majority of anti-fraud activities are performed under regulatory and sectoral obligations, rather than EU or Member State law. Payment networks and financial institutions are subject to the oversight of the European Central Bank and relevant National Banks and, as such, must comply with certain recommendations and standards to ensure an adequate degree of security, operational reliability and business continuity. Moreover, the EU, national governments and policymakers increasingly expect all parties in the payment ecosystem to be more active in this space, as the effective fight against fraud is key to boosting individuals' trust in the digital economy.

Specific examples include:

- Fraud and financial crime detection and prevention, including 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;
- Anti-Money Laundering (AML) watch-lists;
- Know-Your-Customer (KYC);
- Credit checks and risk assessments;
- Politically Exposed Persons (PEP);
- Terrorist financing detection and prevention;
- Defending claims, e.g., sharing CCTV images for insurance purposes; and
- Preventing online sales and purchases of illicit goods and services, goods and services that may damage business/brand reputation or otherwise prohibited activities.

21 Depending on the specific context, some organisations may choose to rely on Article 6(1)(c), which relates to processing necessary for compliance with a legal obligation.

CASE STUDY 1. FRAUD MONITORING, DETECTION AND PREVENTION BY PAYMENT NETWORKS

Payment networks are in a unique position to monitor and detect signs of fraud across the entire payment eco-system. They can alert financial institutions that a payment transaction is likely to be fraudulent in real-time, so that the affected individual can make a decision whether to approve or deny a payment transaction.

Legitimate interests of the controller, third parties and/or society	Individuals' rights and freedoms and reasonable expectations
Organisations have a legitimate interest to protect their network and brand. All parties in the payment eco-system, including financial institutions and merchants, have a legitimate interest to prevent and minimise fraud impact and losses. Clients, individuals and society as a whole have a legitimate interest to reduce fraud in the financial system.	Individual cardholders expect their payment transactions to be processed in an efficient, safe and secure way.
Mitigating measures: • Strict data access rules; • Data use limitations.; • Security measures; • Retention schedules; and • Data minimisation including, as appropriate, data anonymisation and pseudonymisation.	

CASE STUDY 2. CREATION AND/OR USE OF WATCH LISTS TO MEET ANTI-MONEY LAUNDERING (AML), POLITICALLY EXPOSED PERSONS (PEP), ANTI-FRAUD OR DILIGENCE OBLIGATIONS

To protect the international financial system, financial institutions must screen new and existing customers or vendors against watch lists to determine if a business relationship might result in financial risk or crime. Watch lists include personal data that is publicly available or extracted from sanctions published by national or international organisations.

Legitimate interests of the controller, third parties and/or society	Individuals' rights and freedoms and reasonable expectations
Financial institutions and society, in general, have a legitimate interest in preventing and combating money laundering, and ensuring the stability of the financial system. Organisations that perform checks against the officially published watch lists and conduct the screening activities have a legitimate interest in processing the data of the individuals on the lists.	Individual cardholders expect their payment transactions to be processed in an efficient, safe and secure way. Individuals also reasonably expect that organisations process their personal data for the purpose of meeting regulatory requirements, such as in relation to AML, according to market standards.
Mitigating measures: • Appropriate purpose and storage limitation controls on watch lists data; • Data minimisation, including as appropriate anonymisation and pseudonymisation; • Verification mechanisms to ensure no decisions are made on the basis of inaccurate data; • Enhanced transparency to individuals on data processing for AML and fraud prevention purposes; strict data access rules; • Retention schedules; and • Periodic review of the legitimate interests.	

4.2 Compliance with requirements of foreign law, law enforcement, courts and regulatory bodies

Organisations are subject to a multitude of laws and regulations, from reporting obligations to regulators (including sectoral regulators such as health or financial), to law enforcement and judicial requests within the EU and abroad. Organisations often rely on the legitimate interests basis to share personal data when responding to these mandatory requests as reliance on the "compliance with a legal obligation" legal basis is not always possible. Specific examples of data sharing obligations include:

- Operation of ethics lines and reporting under the US Sarbanes-Oxley Act (SOX) and equivalent legislation;
- Economic sanctions and export control list screening under economic sanctions and export control laws;
- Compliance with requests for disclosures to law enforcement, courts and regulatory bodies, both from the EU and from outside the EU, served on the group of companies; and
- Use of data loss prevention software and tools for compliance with data protection laws and client contractual requirements.

4.3 Information systems, network and cyber-security

All organisations (including those in the public sector) need to monitor, detect and protect themselves, their systems, networks, infrastructure, and computers from unwanted security intrusion, unauthorised access and disclosure of information, industrial espionage, and cyberattacks. Organisations inevitably process personal data for monitoring and detection, including the data of customers, third parties, employees and any others who may have access to company systems and networks. The legitimate interests legal basis is the most appropriate ground organisations can rely on for these types of processing activities. Specific examples include:

- Overall information security operations to prevent unauthorised access, intrusion, modification, exfiltration or other misuse of company systems, networks, computers and information, including prevention of illegal access to and interference with data and computer systems;
- Piracy and malware prevention;
- IP rights protection and IP theft prevention;
- Website security;
- Access to systems and download monitoring;
- Prevention, detection and investigation of security incidents (processing of data of individuals involved in an incident, as well as the underlying compromised data);
- Investigation and reporting of data breaches (including use of information gathered from physical access control systems);
- Product and product user security;
- Video surveillance for ownership protection, preservation of evidence; and
- Data sharing to ensure and promote network and system security.

CASE STUDY 3. PROCESSING OF INTERNET PROTOCOL ADDRESSES FOR DELIVERY OF ONLINE CONTENT AND SECURITY

IP addresses are used to deliver web pages and content, for cybersecurity purposes, and to measure website traffic. Internet Service Providers (ISPs) have information linking IP addresses to individual subscribers in order to provide services such as technical support, fraud prevention and billing.

Legitimate interests of the controller, third parties and/or society	Individuals' rights and freedoms and reasonable expectations
ISPs have a legitimate interest in processing IP addresses linked to the routine performance of their services. Internet content owners and users have a legitimate interest in having content and services protected from bad actors.	Individuals have a reasonable expectation that their IP addresses will be used for delivering these services.
Mitigating measures: · Strong technical and organisational measures ensuring that IP addresses are strictly used for the purposes of delivering online content and ensuring security.	

4.4 Customers' physical safety

Organisations are expected to ensure the physical safety of their customers and users. This is particularly relevant for online services that encourage users to meet in person (such as dating apps), and social media that enable live-sharing of real life events. Specific examples include:

- Age verification to ensure users are old enough to use the services;
- Content moderation on services and platforms;
- Retaining personal information as necessary to prevent users banned from the platform from creating new accounts or otherwise abusing their network usage rights or privileges;
- Algorithmic training and deployment to detect unsafe and harmful behaviours; and
- Preventing recurring access to systems by repeat offenders (e.g., who publicise their offenses online).

4.5 Employment data processing

Organisations process employees' personal data for legitimate and common business purposes, sometimes in situations that are not strictly necessary to the performance of the employment contract. In these cases, the EDPB provided that it is not possible to obtain valid consent due to the imbalance in the employment relationship.[22] Processing of employee data is necessary to manage the employment relationship and interaction between employees. Specific examples include:

- Background checks and security vetting in recruitment and HR functions;
- Office and data centre access and operations—cards and badges, entry and exit records, CCTV;
- 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, corporate investigations and disciplinary processes;
- Call recording and monitoring for call centre employees' training and development purposes;
- Employee retention programmes;
- Workforce and headcount management, forecasts and planning;
- Professional learning and development administration;

22 See Guidelines 05/2020 on consent under Regulation 2016/679, version 1.1, adopted on 4 May 2020.

- 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;
- Additional and specific background checks required by particular clients in respect of processors' employees having access to clients' systems and premises;
- Hiring and moving jobs within the same corporations/group of companies;
- HR analytics tools for statistic evaluation to strengthen employee collaboration and self-organisation; and
- Processing of publicly available online information in connection with scouting and recruitment prior to engagement with an applicant.

CASE STUDY 4. PROCESSING OF PERSONAL DATA RECEIVED IN THE CONTEXT OF AN EMPLOYEE INVESTIGATION OR DISCIPLINARY PROCESS

In some cases, organisations need to process personal data of individuals who are not their employees in the context of an employee investigation or disciplinary process—e.g., text messages exchanged by an employee with another individual outside of work which may violate an employer policy.

Legitimate interests of the controller, third parties and/or society	Individuals' rights and freedoms and reasonable expectations
The employer has a legitimate interest to uphold its business policies, to ensure that any breaches of its policies are appropriately investigated, to investigate alleged breaches of the law, to protect its employees, and to protect its products and brand reputation. Society has a legitimate interest in the prevention and detection of crimes.	Employees have a right to privacy in relation to messages they exchange with another individual outside of work, and have a right to express their opinions freely. Employees may not reasonably expect that their personal data in such a case would be processed in the course of an employment investigation or disciplinary process. Individuals who are not an organisation's employee may not realise that their personal data will be processed in the context of the investigation/disciplinary process. Individuals can exercise the rights related to the processing of their personal data and have a right to complain to the DPA and seek redress before courts.
Mitigating measures: · Limitation of the use of material that includes personal data to only that which is strictly relevant to the investigation or disciplinary measure; and · Redaction of the personal data of any third parties.	

4.6 General corporate operations and due diligence

Organisations use personal data to run their day-to-day business and plan for strategic growth. This includes management of customer, client, vendor and other relationships, sharing intelligence, implementing safety procedures, and planning and allocating resources and budget. Specific examples include:

- Modelling (developing or operating financial/credit/conduct and risk models);
- Managing relationships with prospects and customers (customer relationship management or CRM);
- Internal analysis of customers including measuring customer satisfaction, purchasing data, segmenting data, and augmenting it based upon customer interactions to support strategy and growth;
- Managing prospects, including proactive collection of contact details by business development teams;
- Reporting and information management;
- Sharing information with other members of the corporate group;

- Back-office operations;
- Monitoring physical access to offices, visitors and CCTV operations in reception and other restricted areas to ensure the physical security of employees and protect confidential and personal information from unauthorised access;
- 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 to fulfil licensing obligations;
- Business intelligence; and
- Managing third party relationships (vendors, suppliers, media, business partners).

CASE STUDY 5. BUSINESS-TO-BUSINESS CRM IN THE HEALTHCARE SECTOR

In the pharmaceutical sector, business-to-business CRM activities include documenting face-to-face visits with health care professionals (HCPs), providing scientific and promotional information to HCPs about medicines that can help their patients, and inviting them to attend events. To do so, the company may process some of the HCP's personal data. It may also combine data directly obtained from the HCPs with publicly available data taken from medical societies' websites, hospitals' websites or medical publications. Pharmaceutical companies may classify data stored in their CRMs into pre-determined categories and use such data to identify specific actions that the company should take with respect to these categories, such as sending timely informational emails about the efficacy of certain medicines, which may help HCPs when treating patients.

Legitimate interests of the controller, third parties and/or society	Individuals' rights and freedoms and reasonable expectations
Pharmaceutical companies have a legitimate interest in processing data for CRM purposes in order to facilitate their business. HCPs have a legitimate interest in obtaining information from pharma companies about new diseases and available treatments. Patients of HCP (third parties) have a legitimate interest in having access to the most efficient treatment and medicines.	There is limited intrusion into privacy since data processed is primarily related to the professional activities of the HCP (and no special categories of data are processed). Interactions between pharmaceutical companies and HCPs are a well-established market practice and are regulated. HCPs expect pharmaceutical companies to process their data (including data that they have made public) to provide them with information on medicines and medical innovation that would better enable them to care for patients.
Mitigating measures: · Providing HCPs with clear and direct information about the processing of their personal data for CRM purposes and the means to opt out at any time; · Internal governance measures to prevent non-expected uses (including role-based access restrictions); · Retention policies; and · Adherence to contractual protections on purchased data and inclusion of contractual protections on data transferred to third parties.	

CASE STUDY 6. PUBLIC DISCLOSURE OF TRANSFERS OF VALUE (TOV) TO HCPS

Industry and HCPs collaborate in a range of activities from clinical research, to sharing best clinical practices and exchanging information on how new medicines fit into the patient pathway. As part of these activities, HCPs may receive a direct or indirect TOV, whether in cash, in kind or otherwise, made for promotional purposes or otherwise. Although disclosing TOVs may include disclosing compensation data of HCPs, such disclosure relates only to specific activities that should in principle be a small portion of the HCP's total income and therefore is of limited impact to the HCP.

Legitimate interests of the controller, third parties and/or society	Individuals' rights and freedoms and reasonable expectations
Pharmaceutical companies, HCPs, and the general public have a legitimate interest to process personal data related to TOV and to disclose such data as it provides transparency into the relationship between pharmaceutical companies and HCPs. This, in turn, fosters trust between the pharmaceutical industry and the medical community, and strengthens patients' trust in the healthcare industry and its practices. Pharmaceutical companies and HCOs also have a legitimate interest in the processing of personal data related to TOV per se, as the processing promotes innovation and research in the pharmaceutical market in an ethical manner, and reinforces the independence and professional integrity of stakeholders involved. Patients have a legitimate interest in the processing of personal data related to TOV as it is a form of collaboration between industry and HCPs, which benefits them by making available innovative medicines and treatment.	The amount of personal data processed in the context of the TOV disclosure is limited to professional data and does not include special categories of personal data. HCPs reasonably expect disclosures of TOV to happen, as these are a common and global practice (and mandatory in some Member States), done in compliance with laws, regulations, standards and codes of conduct (such as European Federation of Pharmaceutical Industries and Associations Disclosure Code).
Mitigating measures: • Adopting strict destruction procedures for outdated data; • Disclosing only data processing practices regarding TOVs; and • Publishing the TOV in an aggregate form if the HCP has objected to its publication.	

CASE STUDY 7. MEASURING CUSTOMERS' SATISFACTION

Measuring consumers' satisfaction on a product or service provides high value to businesses and is seen as a key performance indicator. In a competitive marketplace, customer satisfaction is considered a key differentiator.

Legitimate interests of the controller, third parties and/or society	Individuals' rights and freedoms and reasonable expectations
Companies have a legitimate interest to ask their customers for their opinions, and to contact them for the purpose of conducting surveys (in product or by other means such as emails) to measure their satisfaction with a product or service. Other customers have a legitimate interest to receive products or services that have been improved on the basis of feedback provided to the provider.	The severity and likelihood of risk of harm is very low for the customer. The data processed is limited and customers can freely decide whether to respond to surveys and share additional personal data. Customers have reasonable expectations that they may be contacted for the purpose of providing their level of satisfaction with a product or a service's performance. Customers may have a self-interest to provide feedback (e.g., on the interface or functionality of a certain service so that it is improved).
Mitigating measures: · Transparency about surveys provided in online privacy notices and in emails to customers; · Internal governance measures to prevent unexpected uses of personal data (including role-based access restrictions); preventing any use of survey responses in the employment context (e.g., not relying on customer un-satisfaction to sanction responsible employee); · Retention policies; and · Adherence to contractual protections on purchased data and inclusion of contractual protections on data transferred to third parties.	

CASE STUDY 8. USE OF CCTV FOR SECURITY PURPOSES

Use of security cameras is a common practice. This may involve monitoring employees.

Legitimate interests of the controller, third parties and/or society	Individuals' rights and freedoms and reasonable expectations
Organisations have a legitimate interest in securing their premises. Employees and customers have a legitimate interest in having their physical safety protected. Society has a legitimate interest in the prevention and detection of crime.	Employees have reasonable expectations that their privacy will not be intruded upon disproportionately by the installation of CCTV. Employees may also expect employee monitoring to take place where labour laws allow for it.
Mitigating measures: · Clearly informing individuals about the use of CCTV (such as through posts and signs); · Avoiding the installation of CCTV in areas where employees have an increased expectation of privacy such as break rooms or changing rooms; · Retention policies; and · Restricted access to images and recordings.	

CASE STUDY 9. PROCESSING OF DATA IN RELATION TO MERGER AND ACQUISITION (M&A) TRANSACTIONS

M&A transactions may require the potential acquirer and their advisors (lawyers, IT consultants, financial auditors) to review various types of documentation containing personal data of various individuals in order to determine the initial and final scope of the subject-matter of the acquisition.

Legitimate interests of the controller, third parties and/or society	Individuals' rights and freedoms and reasonable expectations
Controllers have a legitimate interest to process personal data in the context of M&A transactions to ensure that they have an accurate and thorough understanding of the risks, scope and purpose of the transaction.	Individuals involved reasonably expect their personal data to be processed as this is in line with market practice.
Mitigating measures: · Signing non-disclosure agreements to protect the exchange of information, including personal data; and · Making documentation available in secured platforms held by third parties in "view only" as a general rule (upon request, the reviewers may ask to have copies of specific documents with no personal information).	

4.7 Product development and enhancement

All organisations process personal data to deliver and improve their products or services,[23] for example:

- Data processing for research, product development and improvements, such as integrity and fairness of a process/service, imagery collection for mapping applications, data collected by voice recognition tools, and data collected by translation tools;
- Processing of device-generated data to improve app performance, troubleshoot bugs, and for other internal product needs such as updates relating to hardware model, operating system version, unique application identifiers, unique device identifiers, browser type, language, wireless network, and mobile network information;
- Developing new services;
- Measuring the performance of products and services;
- Training of algorithms to maintain and improve AI and machine-learning technologies;
- Processing identifiable data for the sole purpose of anonymising/de-identifying/re-identifying it to use the anonymised data for other purposes (product improvement, analytics);
- Processing of log files/actions within apps for product use analysis, product performance enhancement and product development;
- Monitoring an individual's usability of websites or apps and conduct analytics regarding this usability, such as number of clicks on pages and links, patterns of navigation, time at a page, devices used, where users are coming from; and
- Monitoring queues at call centres.

23 Whilst reliance on legitimate interests as an appropriate lawful basis for product improvement is generally well accepted, organisations may decide to rely on another lawful basis where appropriate, such as contractual necessity, depending on the nature of the service provided. This is the case, for instance, of innovative services that need to be improved over time to work as intended as per the customer contract (e.g., trouble-shooting).

CASE STUDY 10. IMAGERY COLLECTION TO IMPROVE MAPPING APPLICATIONS

Mapping applications offer users digital and navigable representations that enable them to enjoy a reliable navigation experience. To provide state of the art applications, a service provider needs to collect the necessary imagery that enables it to reproduce accurate representations of physical environments, including multi-dimensional representations of streets and buildings. Imagery may be collected through, for example, vehicles and dedicated personnel tasked with collecting GPS traces (e.g., heading, latitude, longitude of road networks), still images (e.g., traffic signs, lane markings and speed limits), and other information based on radio signals that help identify the projected dimensions of building and other structures for multi-dimensional representation. The data collection is focused on stationary objects, but it may unavoidably capture items that could be classified as personal data, such as still images of individuals and vehicle license plates.

Legitimate interests of the controller, third parties and/or society	Individuals' rights and freedoms and reasonable expectations
Mapping application service providers have a legitimate interest in building and making improvements to offer the best product and user experience. To achieve this goal, the service provider needs to build the necessary mapping data to take advantage of innovation, to ensure the quality of the data and to allow the service provider to ensure the best privacy experience to meet its user's expectations.	Individuals have an expectation of privacy inside his/her car and arguably also in public spaces. Individuals also have a right to data protection that is not limited to private or public areas. Individuals reasonably expect that their images and license plates would not be made publicly available, or made available through a mapping application without the use of privacy-preserving tools.

Mitigating measures:

- Enhanced transparency through the creation of a website and launching other media outreach campaigns containing all relevant information about the imagery collection performed by the service provider;
- Ensuring that all vehicles used for collection of imagery are clearly identified;
- Applying blurring techniques automatically to any objects that are a by-product of the activity and could qualify as personal data by using proprietary technology specifically trained to recognise and blur faces and license plates;
- Storing the data collected on traceable secure systems;
- Securely deleting the data from the traceable security system after use;
- Encrypting data stored and ensuring that the encryption key is held by a service provider and renewed in regular intervals; and
- Using proprietary software to enable enhanced security.

CASE STUDY 11. USING REAL-WORLD CUSTOMER DATA AND MACHINE-LEARNING TO IMPROVE DIGITAL VOICE ASSISTANT SERVICES

The core function of a digital voice assistant is to accurately recognise and respond to customers' spoken requests. Some organisations use supervised machine-learning involving processing of real-world customer voice data to maintain and improve such services.[24] In these cases, a service provider may manually review a small fraction of customers' voice data, annotate the data, and use the annotated data to train a machine-learning model to correctly respond to a voice input and to ensure that the service works well for all customers.

Traditional computation methods relying on hard-coded logic are unable to accurately understand and respond to the varied, dynamic speech used by customers in the real world. Supervised machine-learning using real-world customer voice data is state of the art for making service improvements and new features possible for digital voice assistants such as improving the ability to "wake up" only when invoked, understand and respond to new types of requests (such as COVID-19 or digital certificates), play new music content, recognise innovative new smart home devices, and understand all users equally well.

Using real-world customers' voice data also makes some of these services commercially viable. For example, expanding to new languages would be extremely costly to customers if digital voice assistants could not learn and improve from real-world customer use. Customers would suffer from less usability, diminished improvement, fewer features, and fewer service options if service providers could not train digital voice assistants using real-world customer data.

Legitimate interests of the controller, third parties and/or society	Individuals' rights and freedoms and reasonable expectations
Digital voice assistant service providers have a legitimate interest in maintaining their service, and making improvements and service developments that meet users' expectations, such as improving the general accuracy of their services, improving existing features, accommodating population-based differences in speech and language, and developing new service features. This also benefits third parties and society more generally.	Individuals expect digital voice assistant services to perform well and to improve over time, including by adding new and desirable features. They expect the service to understand their requests and respond accurately, including by not "waking up" incorrectly. On the other hand, they may be concerned about employees of service providers listening to their voice recordings and accessing their personal information (e.g., reminders for doctor's appointments).
Mitigating measures: • Providing enhanced transparency, including informing customers of manual reviews of voice recordings and creating dashboards that allow users to see and hear the voice recordings; • Providing users with controls, including opting out of the manual review of their voice data for service improvement, deleting voice recordings; • Making privacy controls accessible and easy to use for customers such as via voice; • Offering automated scheduled deletions of voice recordings; • Making features that require processing of special categories of personal data optional; and • Implementing robust technical safeguards, including pseudonymising voice data, restricting the information available for manual review, using filters to restrict access to personal information, and internal access controls.	

24 Note that this case study does not apply to digital voice assistants that do not process personal data (e.g., that anonymise data at the outset).

CASE STUDY 12. RESEARCH AND DEVELOPMENT ACTIVITIES AIMED AT TRAINING AND PROTOTYPING MACHINE-LEARNING ALGORITHMS

Training and prototyping machine-learning algorithms can help organisations create more user-friendly software applications. Machine-learning technology supports improvement in areas such as task automation or contextual searches. The ultimate goal is to provide users with an optimised and more powerful user experience. In most cases, the data will have been collected for other purposes and, therefore, further processed for the purpose of training and prototyping machine-learning algorithms. In these cases, organisations may have to include a compatibility test in the legitimate interests assessment in order to determine whether they can lawfully further process such personal data in that particular context.

Legitimate interests of the controller, third parties and/or society	Individuals' rights and freedoms and reasonable expectations
Organisations have a legitimate interest in processing aggregated datasets for the purpose of training and prototyping machine-learning algorithms, as they want to ensure that their customers have access to new technologies that facilitate and improve user experience. Individuals also have a legitimate interest in such data processing given that they will benefit from improved services. Society has a legitimate interest in individuals being treated fairly.	Individuals have a right to dignity, including being treated fairly. Training machine-learning algorithms will involve collecting substantial amounts of individuals' personal data that represent various racial, ethnic, gender, societal and other groups to avoid biases in the technology and, therefore, ensure fairness.
Mitigating measures: • Using pseudonymised, anonymised and aggregated data sets.	

4.8 Communications, marketing, and advertising

Organisations process data to gather market intelligence, promote products and services, and communicate with and tailor offers to individual customers and business customers. The widespread availability of controls around targeted advertising (such as controls offered by the European Interactive Digital Advertising Alliance—EDAA[25]) have helped address individuals' privacy interests. It has also enhanced the commitment of commercial players to educate consumers about how advertising works on their services and how individuals can make relevant choices about their advertising experiences. Specific examples are:

- Discretionary service interactions—customers are identified in order for them to receive communications relating to how they use and operate the organisations' product;
- Direct marketing of the same, or similar, or related products and services, including sharing and marketing within a unified corporate group and brand;
- Targeted advertising, where it is clearly part of the product or service and the organisation provides individuals with an option to object;
- Analytics for business intelligence—to create aggregate trend reports, find out how customers arrive at a website, determine how customers use apps, collects responses to a marketing campaign, and determines what are the most effective marketing channels and messages;
- Ad performance and conversion tracking after a click—services such as Private Click Measurement to measure the effectiveness of advertisement clicks that navigate to a website while maintaining user privacy;
- Audience measurement;

25 EDAA has developed a European self-regulatory programme consisting of a certification process offered to entities engaged in data-driven advertising to clearly inform consumers about their data collection and use practices through enhanced notice, provided via the consumer-facing 'AdChoices Icon.'

- Developing databases of qualified professionals/experts via collection of publicly available information for the purpose of recruiting for advisory boards, speaking engagements and otherwise engaging with the company;
- B2B marketing, event planning and interaction; and
- Social media listening.

CASE STUDY 13. TARGETED ADVERTISING THAT IS CLEARLY PART OF THE SERVICE PROVIDED

Some organisations offer products and services that clearly include targeted advertising as part of the experience of such product and service. Targeted advertising is a complex business model that mostly involves multiple parties and transactions.

Legitimate interests of the controller, third parties and/or society	Individuals' rights and freedoms and reasonable expectations
Organisations have legitimate interests in providing targeted advertising when it underpins their business model and where it is clearly part of the services provided. Some individuals may also have legitimate interests in receiving targeted advertising when they believe that they benefit from discovering new products, services, offers and causes, and it is clearly a part of the services requested by the individuals.	Individuals expect to see targeted advertising where they use services that are offered in a way that the provision of such advertising is clearly part of the experience.
Mitigating measures: · Providing an option for individuals to object to the data processing; · Providing enhanced transparency, such as just-in-time privacy notices when users see ads; · Ensuring that the targeted ads are not discriminatory or result in another adverse effect to individuals; and · Providing granular and meaningful controls to individuals concerning ads and the related use of their personal data.	

CASE STUDY 14. AUDIENCE MEASUREMENT (AM)

AM is a way to measure audiences for specific markets such as TV, radio, newspapers, and websites. 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 require the installation of a special box that measures viewing behaviour, based on a contractual relationship.

Legitimate interests of the controller, third parties and/or society	Individuals' rights and freedoms and reasonable expectations
Online service providers and media owners have a legitimate interest in undertaking AM as it helps the market to function more efficiently and competitively. A lack of effective AM would lead to opaque markets and leave advertisers in the dark, which would impact media funding negatively.	Risks to individuals' rights and freedoms are likely going to be low, as there is no identification and reports are aggregated.[26]
Mitigating measures: · Ensuring that no AM data is used for direct advertising to individuals; · Truncating IP addresses and subsequent one-way hashing/ pseudonymisation; · Aggregating data provided in AM reports; and · Providing contractual safeguards with suppliers and partners including prohibition to re-identify data.	

26 The Working Party 29 has recognised in its opinion on legitimate interests that web analytics pose minimal privacy risks to individuals. See supra note 4.

CASE STUDY 15. SOCIAL MEDIA LISTENING (SML) ON PUBLICLY AVAILABLE DATA RELATED TO HEALTHCARE PROFESSIONALS (HCPS)

SML means a process involving identifying, monitoring, or assessing what is being said about a company, brand, product, service, or other topic across the internet, including social media platforms and blogs, whether done in real-time or on a retrospective basis. In the pharma sector, organisations listen to HCPs to understand how they feel about patient journeys and patient responses to certain medicines, to support the development of new medicines and treatments, to identify and form relationships with key HCP stakeholders and influencers, and to foster trust with HCPs and patients. As organisations undertaking SML do not engage directly with the individuals who are being listened to, it is not feasible to obtain their consent. In addition, the European Data Protection Supervisor has opined that there seems to be no risk of breaching the internet users' privacy where data is used for "purely statistical purposes" and does not contain identifiable quotes.[27]

Legitimate interests of the controller, third parties and/or society	Individuals' rights and freedoms and reasonable expectations
Healthcare organisations have a legitimate interest in understanding their audiences and influencers to get better insights on these audiences and engage them more successfully. Society has a legitimate interest to access new medicines and health treatments that may be developed after SML.	The impact on HCPs is generally low. Although such SML covers health, it is focused on the interests and opinions of HCPs in their professional capacity, and does not involve the health condition of any identified individual. Professionals who post information on social media platforms, blogs, and other public internet platforms are generally aware that this information will be seen by the public and cannot expect confidentiality (particularly for those HCP who position themselves as thought leaders and influencers).
Mitigating measures: • Providing information on public websites about the processing of data for the purposes of SML; • Providing HCPs with clear and direct information about the SML practices and the means to opt out at any time; • Applying minimisation measures to limit the amount of personal data being processed, including relying upon aggregated data reports where sufficient to fulfil the company's purposes; • Internal governance measures to exclude unexpected uses (including role-based access restrictions); • Having retention policies in place; • Training business owners before initiating SML projects; • Adherence to contractual protections on processed data and contractual provisions ensuring it is not from closed groups; and • Inclusion of contractual protections on data transferred to third parties.	

4.9 Content personalisation

Organisations process personal data to provide services and content that is personalised to each individual who accesses their service where these experiences are clearly part of the product or service, therefore tailoring the service and the customer experience. Specific examples include:

- Personalised news feeds on social media;
- Personalised suggestions of video content; and
- Personalised suggestions of products/services.

27 EDPS Prior Checking Opinion on "Data processing for social media monitoring" at the European Central Bank (ECB), Case 2017-1052, page 8.

CASE STUDY 16. PROCESSING FOR CONTENT PERSONALISATION

Many online services include vast content inventories including thousands of products and content that customers cannot effectively navigate on their own. Content personalisation enables customers to navigate through such inventories in the most relevant manner. The Article 29 Working Party has acknowledged in their guidance on legitimate interests that controllers can rely on the legitimate interests legal basis for content personalisation.[28]

Legitimate interests of the controller, third parties and/or society	Individuals' rights and freedoms and reasonable expectations
Website/app service providers have a legitimate interest in providing the best and most relevant experience to their users. Third party businesses (e.g., sellers, app developers) have a legitimate interest in connecting their content to the most relevant audience. Some users will also have a legitimate interest as they will want to benefit from easier website/app navigation and access to the most relevant content.	Content personalisation is already a well-established market practice for online content providers, which individuals reasonably expect as part of a seamless and enhanced customer experience. This expectation is particularly strong in the context of services that are provided directly to customers, which is often accomplished via an online authenticated account. The act of creating an account, in particular, shows that the user wants a direct relationship with the service provider and even expects a degree of recognition, which includes content personalisation.
Mitigating measures: · Ensuring that personal data is only used for the purpose of tailoring content to the user; · Implementing controls that enable users to tailor their preferences; · Providing enhanced transparency, such as via just-in-time privacy notices, as well as language indicating that products are shown based on past purchasing behaviour and buying history; and · Adopting strict retention periods to minimize the risks to individuals.	

4.10 Processing "data for good"

Organisations may process data for purposes that go beyond their corporate-related processes and may result in wider societal benefits or benefits of groups of individuals (which is commonly known as "data for good").[29] The COVID-19 pandemic has made clear that individuals expect such data processing when appropriate protective measures are in place. Specific examples include:

- Data sharing between public and private sectors to address force majeure issues (such as a pandemic);
- Research activities to train machine-learning and AI algorithms (e.g., AI used during the COVID-19 pandemic to define which areas were more susceptible to the virus);
- Processing of personal data to prevent online harms, therefore protecting groups of individuals online (e.g., protecting children against sexual abuse and exploitation); and
- Processing of personal data to improve technological capabilities of energy-related products for the purpose of energy efficiencies that would result in benefits to the environment.

28 See supra note 4, page 25 of the guidelines.

29 In the case of "data for good," there may be an overlap with Article 6 (1)(e) of the GDPR on processing necessary for the performance of a task carried out in the public interest. However, this legal basis is interpreted narrowly and can lead to different interpretations among EU Member States.

APPENDIX
SUMMARY OF LIST OF ROUTINE DATA PROCESSING ACTIVITIEs

Fraud detection and prevention	• Anti-money laundering (AML) watch-lists • Politically Exposed Persons (PEP)
Compliance with foreign law, law enforcement	• Economic sanctions and export control list screening • Compliance with requests for disclosures
Industry self-regulatory schemes	• Industry watch-lists • Industry standards • Relations with insurers
Information, system, network and cyber-security	• Information security operations • Product and product user security
Customers' physical safety	• Age verification • Content moderation • Algorithm training to detect unsafe and harmful behaviours
Employment data processing	• Background checks • Time recording • Use of CCTV for monitoring employees
General corporate operations and due diligence	• Customer analysis • Back-office operations • B2B relationship mgmt • Data processing in M&A
Product development and enhancement	• Processing to improve performance • Monitor use and conduct analytics
Comms, marketing ads	• Direct marketing • Targeted ads • Audience measurement • Social media listening
Content personalisation	• Personalised social media feeds • Suggestions of content relevant to individual
Processing data for good	• Combating pandemic • Preventing online harms • Energy efficiencies

About the Centre for Information Policy Leadership

CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 90 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 that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at **http://www.informationpolicycentre.com/.**

If you would like to discuss this paper or require additional information, please contact Bojana Bellamy, bbellamy@HuntonAK.com; Nathalie Laneret, nlaneret@HuntonAK.com; or Giovanna Carloni, gcarloni@HuntonAK.com

CIPL AT 20 — SHAPING DATA POLICY FOR TOMORROW

HUNTON ANDREWS KURTH

DC
2200 Pennsylvania Avenue
Washington, DC 20037
+1 202 955 1563

London
30 St Mary Axe
London EC3A 8EP
+44 20 7220 5700

Brussels
Park Atrium
Rue des Colonies 11
1000 Brussels
+32 2 643 58 00