Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

CIPL Response to the European Data Protection Board's Public Consultation on Draft Guidelines 1/2024 on the processing of personal data based on Article 6(1)(f) GDPR

Centre for Information Policy Leadership (CIPL)

20 November 2024

CIPL Response to the European Data Protection Board's Public Consultation on Draft Guidelines 1/2024 on the processing of personal data based on Article 6(1)(f) GDPR

The Centre for Information Policy Leadership (CIPL)[1] appreciates the opportunity to comment on the European Data Protection Board (EDPB) Draft Guidelines 1/2024 on the use of Article 6(1)(f) of the GDPR as a legal basis for processing personal data. CIPL commends the EDPB's efforts to enhance regulatory clarity and foster consistent application of data protection principles across the EEA.

CIPL welcomes the EDPB's explicit recognition that legitimate interest as a legal basis for processing personal data is on an equal footing with the other five legal bases of Article 6 GDPR, without any hierarchy between them.[2] This is consistent with CIPL's position advocating for a balanced approach to the GDPR's legal basis framework.

CIPL also supports the Guideline's acknowledgement that there is no exhaustive or finite list of legitimate interests and that a wide range of interests may qualify. This is in line with recent CJEU decisions, and we appreciate the EDPB's timely inclusion of this reference in the Guidelines.

The Guidelines provide a helpful structure for assessing the three cumulative conditions that must be met for processing to be lawfully based on legitimate interest:

1) Determining the legitimate nature of the interest pursued;
2) Analysing the necessity of the processing to pursue legitimate interests and;
3) Conducting a balancing test.

This methodology is practical and consistent with the practices already adopted by accountable organisations.

The Guidelines highlight the importance of a thorough assessment and documentation of the balancing test to demonstrate organisational accountability. Through our many years of work on organisational accountability, CIPL has been urging organisations to ensure that these tests are well-documented, updated regularly, and conducted meaningfully.

CIPL has identified several areas of concern and offers targeted recommendations to refine and strengthen these important Guidelines. Our comments are divided into two main sections: fundamental issues, which highlight overarching concerns throughout the Guidelines, and substantial issues, which address specific elements requiring further consideration and improvement. In addition, our response contains an Annex which includes various use case examples of legitimate interest legal basis being applied in practice.

---

[1] The Centre for Information Policy Leadership (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 85+ member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices to ensure the responsible and beneficial use of data in the modern information age. CIPL's work facilitates constructive engagement between business leaders, data governance and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at https://www.informationpolicycentre.com/. Nothing in this document should be construed as representing the views of any individual CIPL member company or of the law firm Hunton Andrews Kurth LLP. This document is not designed to be and should not be taken as legal advice.

[2] EDPB Guidelines 1/2024, p. 4.

In the context of the EDPB Draft Guidelines 1/2024, CIPL recommends the EDPB to:

- **Recognise legitimate interest as a basis for innovative, emerging technologies like AI model training.**
- **Include positive, practical examples** accompanied by analysis that illustrates how legitimate interest can be applied constructively in various contexts, especially for smaller organisations.
- **Ensure guidelines are accessible, concise, and clear** and accompanied by tools like checklists to assist SMEs in assessing legitimate interests.
- **Acknowledge legitimate interest as a viable legal basis for processing children's data where it aligns with the child's best interests**, is coupled with appropriate safeguards such as enhanced transparency measures specifically designed for children, includes prior consultation with child protection experts to validate data processing practices, includes where appropriate robust age verification mechanisms to ensure age-appropriate interactions and clear and accessible tools for children to exercise their data subject rights.
- Reconsider the language in the guidelines regarding the three-step test, clarifying that mitigating measures are part of the comprehensive assessment and that **the three-step test does not have to be repeated anew after identifying mitigating measures**.
- **Eliminate the ambiguous concept of "more private information"** or provide a clear legal justification, ensuring consistency with the GDPR and case law.
- **Recognise Recitals 47 and 49 GDPR**. While the Guidelines do mention Recitals 47 and 49, the Guidelines provide an overly restrictive interpretation not in line with the actual text of Recitals 47 and 49 GDPR.
- **Acknowledge the Evolving Threat Landscape**: Fraud and cyber threats are constantly evolving, requiring organisations to continually adapt their security measures and data processing practices. The EDPB should recognise this dynamic landscape and ensure that its guidelines allow sufficient flexibility to both pre-empt threats where possible and speedily address emerging threats as they arise.
- **Clarify the Scope of Legitimate Interest in Security Contexts**: CIPL recommends that the guidelines provide more detailed examples of data processing activities that can be justified under legitimate interest for security purposes.
- **Recognize the Contextual Nature of Legitimate Interest**: CIPL urges the EDPB to emphasise the importance of a case-by-case assessment of legitimate interest, considering the specific circumstances of each processing activity reflecting the approach taken by organisations' privacy programs. Overly prescriptive guidelines could hinder the flexibility and adaptability of this legal basis, limiting organisations' ability to respond to diverse situations effectively.
- **Emphasize Proportionality and Safeguards**: The guidelines should offer practical advice on implementing data minimisation principles, ensuring adequate security measures, and providing mechanisms for data subjects to exercise their rights in relation to these processing activities.
- **Further clarify the interaction between GDPR and the ePrivacy Directive**: CIPL recommends that the EDPB further clarifies the interaction between the GDPR and the ePrivacy Directive in Section 4 on "Processing for direct marketing purposes", the paragraph on "Compliance with specific legal requirements that preclude reliance on Article 6(1)(f)" (4.2). Clear guidance and practical examples on how the legitimate interest legal basis under the GDPR can be reconciled with the requirements under the ePrivacy Directive, including for strictly necessary trackers, would help organisations navigate these overlapping frameworks and ensure compliance.

I. FUNDAMENTAL ISSUES

1. The draft Guidelines contain practically no positive examples of legitimate interests and use a negative tone throughout the Guidelines

CIPL has consistently advocated for a balanced interpretation of legitimate interest legal basis that benefits both organisations and individuals.[3] This legal basis is a cornerstone of GDPR's risk-based approach, promoting organisational accountability while safeguarding individuals' rights. Legitimate interest enables organisations to pursue data processing that is necessary for business needs, including innovative and emerging data processing, provided that the interests of data subjects are duly respected and protected.

Some of the legitimate interest legal basis benefits include:

- **Flexibility and support for innovation**: The legitimate interest legal basis offers organisations the flexibility they need to operate in today's data-driven world. It can cover everyday, routine and established business purposes like fraud prevention and cybersecurity, as explicitly also foreseen in Recitals 47 and 49 GDPR, provided that the specific processing can pass the requisite balancing test. At the same time, legitimate interest processing provides a sufficiently flexible legal basis for organisations developing new products and exploring new features or versions of their offerings. Legitimate interest may also cover more complex, unique, innovative, original or new data processing activities that are key for innovation and for the development of the digital economy. For example, the legitimate interest legal basis can be instrumental for AI training in the context of developing new large language models and may be the only reasonably available legal basis for algorithmic training.[4]

---

[3] CIPL Report - The GDPR's First Six Years: Positive Impacts, Remaining Implementation Challenges, and Recommendations for Improvement, May 2024, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/gdpr_six_years_on_cipl_may24.pdf; CIPL White Paper - How the "Legitimate Interests" Ground for Processing Enables Responsible Data Use and Innovation, July 2021, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_how_the_legitimate_interests_ground_for_processing_enables_responsible_data_use_and_innovation__1_july_2021_.pdf; CIPL - Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR, May 2017, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf; CIPL Examples of Legitimate Interest Grounds for Processing of Personal Data; April 2017, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/final_cipl_examples_of_legitimate_interest_grounds_for_processing_of_personal_data_27_april_2017.pdf; CIPL Response to the Article 29 WP Consultation Regarding Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller Under Article 7 of Directive 95/46/EC, July 2014, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_article_29_wp_opinion_on_the_notion_of_legitimate_interests__july_4_2014_.pdf.

[4] CIPL Response to ICO Consultation on the Lawful Basis for Web Scraping to Train Generative AI Models, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_-_ico_consultation_on_the_lawful_basis_for_scraping_data_for_generative_ai__mar_2024_.pdf, p.4; CIPL Response to CNIL How-To Sheets on the Development of Artificial Intelligence Systems, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_cnil_consultation_on_ai_-_second_series-c.pdf.

- **Promotes responsible data use and protection of fundamental rights**: The legitimate interest legal basis encourages organisations to implement strong data protection measures and organisational controls. As outlined above, in order to rely on it, organisations have to conduct a balancing test assessing the potential risks and competing individual interests, rights and freedoms related to a processing operation and define measures to mitigate the risks. Moreover, organisations have to document such assessments and be able to demonstrate the outcomes.
- **Promotes risk-based approach**: Legitimate interest legal basis 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. The legitimate interests assessment can form part of the overall risk assessment practices
- **Right to object**: Individuals have the right to object to the processing of their data based on legitimate interests. This provides individuals with a level of control over their personal data.

Considering these evident benefits, CIPL finds it concerning that the Guidelines adopt a restrictive and negative tone regarding the use of legitimate interest as a legal basis, providing practically no positive examples that would demonstrate its practical applicability. While the EDPB recognises that: "GDPR does not establish any hierarchy between different legal bases laid down in Article 6(1)",[5] The approach taken in the Guidelines may inadvertently discourage organisations from considering legitimate interests as a viable processing ground. By contrast, the WP29 previously recognised the significance and usefulness of the Legitimate Interest under Article 7(f) of the previous Directive, which, subject to adequate safeguards," may help prevent over-reliance on other legal grounds."[6]

CIPL includes a list of numerous real-world examples of legitimate interest use cases based on our research. Below, we also provide a case study for using legitimate interest for training AI models for consideration.

Case study 1. Processing of Personal Data for AI Model Training

Legitimate interests of the controller, third parties and/or society	**Individuals' rights and freedoms and reasonable expectations**
Beyond commercial interests, there are broad societal benefits for EU users in training AI on personal data: - advancing AI innovation for all users, - easing information access, - improving AI's quality (non-discrimination, non-bias, fairness. and Article 10 (5) of the AI Act) as well as more diversity of data, e.g. local languages, cultures, etc.)	Individuals can reasonably expect that their personal data could be processed by companies to understand their business better, ensure efficiency and enhance their products and services through various methodologies such as model development. Provided the processing of personal data is limited to training, operating, building and improving the model and the individuals have the right to object to the use of their personal data for such purpose at any time, the impact on the individual's freedoms and privacy will be minimal.

[5] Guidelines 1/2024, p. 4.
[6] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

- improving AI's accessibility (data subjects can interact in their own language). - avoiding EU users being excluded or benefiting less from global AI innovation	Consistent with the 2013 opinion of Advocate General Jääskinen in the context of search engines, which informed the landmark CJEU Costeja decision, it would seem appropriate for controllers developing AI models to also rely on legitimate interests as their legal basis for processing personal data given the broad capabilities that AI brings such as search, language, vision, reasoning or human interaction that can serve as the base for use-specific applications which bring broad benefits to information access, dissemination, and the advancement of new technological development. The reasoning potentially holds even more true for AI training models, which work with both structured and unstructured data, than for search engines – where the data is, after all, indexed and thus somewhat structured.
Mitigating measures (non-exhaustive and non-cumulative list): - Implement an opt-out mechanism that allows individuals to object to the use of their personal data for model operation, development, and improvement at any time. - Provide transparency through privacy notices and model documentation, such as model cards or other best practices for information sharing. - Implement strong technical and organisational measures to protect data, ensuring it is processed securely for its intended purposes, with safeguards such as encryption and pseudonymisation. - Utilize measures to de-identify personal data, such as the use of Privacy-Enhancing Technologies (PETs) and Privacy-Preserving Techniques (PPTs). - Conduct adversarial red teaming to identify any potential vulnerabilities. - Scrub datasets before they are transmitted to the training area. - Train models with fine-tuning to prevent the unintentional disclosure or regurgitation of personal data. - Apply exclusions based on factors like age or specific types of content and exclude unauthenticated entries.	

Member state DPAs have also been considering legitimate interest a valid legal basis in the context of AI, subject to sufficient safeguards.[7]

We urge the EDPB to include practical examples that illustrate how legitimate interest can be applied constructively in various contexts to provide actual guidance, especially for smaller organisations. A more balanced perspective would better align with the GDPR's objective of facilitating the free flow of personal data within the Union while ensuring a high level of protection of personal data.[8]

[7] See for example the CNIL Focus Sheet, The legal basis of legitimate interests: Focus sheet on measures to implement in case of data collection by web scraping, available https://www.cnil.fr/en/legal-basis-legitimate-interests-focus-sheet-measures-implement-case-data-collection-web-scraping.

[8] GDPR Recital 6.

2. The draft Guidelines are repetitive, lengthy and lack readability

The EU is at a critical juncture, navigating a rapidly changing global landscape with new challenges on the horizon. To remain resilient and uphold its robust system of rights, values, strong institutions, economic stability, and global leadership, the EU must foster an environment where businesses can innovate and thrive, ultimately supporting broader economic and societal progress.[9]

In this context, the European Data Protection Board (EDPB) has a significant role to play. To ensure legal clarity, reduce regulatory complexity, Guidelines should strive to be accessible and easy to understand, particularly for SMEs.

The present Guidelines are lengthy—spanning 37 pages—and often appear repetitive . It is unlikely that smaller organisations, already resource constrained will find these Guidelines accessible or easy to interpret.

We kindly suggest that the EDPB consider developing more streamlined and practical guidelines and tools (such as a checklist) that succinctly outline the key elements for assessing the legitimate interest legal basis and provide positive examples for doing so. This would significantly enhance clarity and utility for businesses, especially SMEs, while supporting the EU's commitment to competitiveness and innovation.

II. SUBSTANTIAL ISSUES

1. Contextual Application of Article 6(1)(f) GDPR: Processing of Children's Personal Data

CIPL acknowledges the critical importance of protecting privacy and safety online, including safeguarding children's personal data. Children deserve special safeguards in data processing activities.[10] To that end, the *Best Interest of the Child*, as outlined in Charter Article 24(2), the UN Convention on the Rights of the Child (UNCRC), must be a primary consideration.[11]

The UNCRC highlights the significance of empowering children as digital citizens, emphasising their right to access, seek, and share information across any media of their choice. Furthermore, the UN Committee on the Rights of the Child's General Comment No. 25 specifically emphasises the need to support children's full participation in social, cultural, and educational activities in the digital realm, advocating for states to foster their engagement as active digital citizens.[12]

Given these considerations, a balanced approach, avoiding one-sidedly hindering children's participation online and the development of beneficial services for children. CIPL believes that a categorical exclusion of legitimate interest as a legal basis for processing children's data is not justified. Article 6(1)(f) of the GDPR explicitly calls for a careful balancing test "in particular where the data

---

[9] European Commission, EU Competitiveness: looking ahead, available at https://commission.europa.eu/topics/strengthening-european-competitiveness/eu-competitiveness-looking-ahead_en

[10] EDPB Guidelines 1/2024, p 26.

[11] See also WP29 Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools), available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp160_en.pdf.

[12] United Nations, Committee on the Rights of the Child, General Comment No. 25 (2021) on children's rights in relation to the digital environment, available at https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation.

subject is a child," which implies that legitimate interest is not inherently incompatible with all processing of children's data. Relying exclusively on consent will not necessarily provide the desired level of protection for children's data.

Additionally, while the EDPB rightly points out that the Digital Services Act (DSA) restricts targeted advertising based on children's data, it is essential to recognise that the legislator has consciously chosen, both in the DSA and AI Act process, to not prohibit personalised services by law. These services can actually enhance the online experiences of children. Profiling can be leveraged to ensure that children receive content appropriate to their age, development level, and interests while also shielding them from inappropriate materials, which can, therefore, be part of mitigating measures. This requires a nuanced assessment of whether profiling, aimed at curating child-friendly content, can be conducted in a manner that upholds their privacy and well-being.

2. Processing for the purpose of preventing fraud and ensuring network and information security

In today's digital environment, the increasing prevalence of fraud and cyber threats demands robust measures to safeguard individuals, organisations, and society at large. An overly restrictive interpretation of legitimate interest in these contexts can severely impede efforts to counter these threats, ultimately putting individuals at greater risk. Fraud prevention, data security, and cybersecurity frequently necessitate processing personal data in ways that do not easily align with other legal bases, such as consent, contractual necessity or compliance with a legal obligation.[13] Statutory obligations may only apply in certain sectors, such as the financial sector, and requiring consent in fraud detection scenarios would be both impractical and ineffective. Malicious actors would simply decline to provide it. Requesting consent for fraud prevention measures might also create a 'tip-off' around certain approaches an organisation is setting up or may, in fact, be contrary to confidentiality obligations. For fraud prevention to function well, it is necessary to be able to draw trends, patterns, and insights based on a sufficiently representative sample of users, which cannot be obtained through consent alone. Similarly, stringent security measures often involve analysing data to identify and address vulnerabilities, which may not always have a direct link to a specific contractual obligation.

It is also crucial to highlight that fraud prevention benefits not only organisations but also individuals, who derive significant advantages from a safer digital ecosystem. The European Commission's study on "Scams and Fraud Experienced by Consumers" stresses that online fraud represents a significant portion (43%) of fraud cases, a finding also referenced in the Commission's recent Digital Fairness Fitness Check. Given that combatting online fraud is a key focus of the EU's agenda, a restrictive application of the legitimate interest legal basis would be counterproductive to these efforts.[14] There

[13] Centre for Information Policy Leadership, Limiting Legal Basis for Data Processing Under the DMA: Considerations on Scope and Practical Consequences, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_dma_limiting_legal_basis_may2023.pdf, p. 14.

[14] European Commission, Survey on "Scams and fraud experienced by consumers", available at https://commission.europa.eu/system/files/2020-01/factsheet_fraud_survey.final_.pdf; European Commission, Staff Working Document Fitness Check on EU consumer law on digital fairness, available at https://commission.europa.eu/document/707d7404-78e5-4aef-acfa-82b4cf639f55_en.

is a general public interest in fighting fraud in the interest of the payment ecosystem or combatting cybercrime in the interest of society at large. The EDPB should recognise this in these Guidelines.

Additionally, we disagree with the EDPB in its interpretation of GDPR Recital 47.[15] Whereas EDPB proposes that such processing "may" constitute a legitimate interest, Recital 47 affirmatively states that: "processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned". The same applies to legitimate interest in the context of network and information security as set in Recital 49 GDPR. These are both imperative for the continued function of the digital environment, the safeguarding of all users' data, and the integrity of organisations' IT environments. Therefore, we urge the EDPB to improve the Guidelines' Chapter IV parts 1 and 6 to reflect the legislator's clear intention.

To that end, we would like to respectfully point out that detection is a fundamental aspect of the fraud prevention process—without sufficiently robust detection measures, prevention will be limited to accidental findings or user reporting. We recommend that the EDPB reconsider the distinction between fraud prevention and detection or provide a more substantial justification for maintaining such a separation.

Furthermore, it would be useful to clarify that fraud prevention covers processing aimed at monitoring and detecting fraud-related activities, such as money laundering, money mule schemes, or identity theft.

Indeed, fraud detection and prevention are essential elements of providing a service. CIPL has previously provided input on EDPB Public Consultation on Draft Guidelines 02/2023 on the Technical Scope of Art. 5(3) of ePrivacy,[16] and we regret the further restriction of lawful bases for subsequent processing, which departs from earlier WP29 and EDPB opinions.[17] Particularly, we are concerned with the language in paragraph 115 of the draft Guidelines. CIPL emphasises that the legitimate interests of controllers and third parties must be thoroughly evaluated in the balancing test, as substantial interests are at stake, including safeguarding the financial system, protecting critical infrastructure, and ensuring the security of individuals.

3. Expansion of the Scope of the Concept of Sensitive Data

CIPL agrees with the EDPB that data controllers must carefully assess the nature of the data they process, recognising that special categories of data warrant enhanced protection under Article 9 of the GDPR. However, CIPL seeks further clarification on the EDPB's reference to the notion that certain "types of data that data subjects generally consider more private" require special consideration and

---

[15] Para 100 of the draft Guidelines.

[16] CIPL Response to the EDPB Public Consultation on Draft Guidelines 02/2023 on the Technical Scope of Art. 5(3) of ePrivacy Directive, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_public_consultation_on_edpb_guidelines_2_2023.pdf.

[17] *Opinion 5/2019, which states in paragraph 75 that: "For example, article 5(3) of the ePrivacy Directive contains a special rule for the storing of information, or the gaining of access to information already stored, in the terminal device of an end-user. It does not contain a special rule for any prior or subsequent processing activities (e.g., the storage and analysis of data regarding web browsing activity for purposes of online behavioural advertising or security purposes). As a result, data protection authorities remain fully competent to assess the lawfulness of all other processing operations that follow the storing of or access to information in the terminal device of the end-user."*

that: "this does not mean that seemingly less sensitive data may be regularly processed under Article 6(1)(f) GDPR."[18]

Given that these Guidelines are issued under Article 70(1)(e) of the GDPR, which mandates the EDPB to foster a consistent interpretation and application of the GDPR, we believe it is essential that any references align with established GDPR concepts within the EDPB's remit. It remains unclear how the term "more private information" fits within the existing framework of the GDPR, as no specific legislative provisions or case law have been cited to substantiate this concept.

There is a question of whether, if certain data were to be considered somewhat "more" private and require more scrutiny, other data would be somewhat "less" private. CIPL recommends that the EDPB either eliminate this ambiguous notion or provide clear legal justification for the inclusion of "more private information" within the context of the GDPR. Such clarity is crucial to ensure that the guidelines adhere to the principles of consistency and legal precision that the GDPR aims to promote and introduces the potential for sector-specific interpretations.

4. Expansion of the Scope of the Concept of Direct Marketing

The guidelines appear to broaden the definition of direct marketing without providing adequate justification. Specifically, the case law cited in paragraph 109 of the draft guidelines does not support the expansion of the 'direct marketing' concept to include personalised advertising. For instance, the referenced paragraphs 47-50 of case C-102/20 explain the Court's reasoning in the context of the ePrivacy Directive and advertisements delivered directly to an email inbox. It remains unclear how the EDPB connects this case to the expansion of the direct marketing concept to personalised advertising. Additionally, Case C-252/21 primarily cites Recital 47 of the GDPR to identify the types of commercial activities that could, in principle, constitute a legitimate interest under Article 6(1)(f) of the GDPR.

CIPL further notes that none of the GDPR's provisions suggest that online advertising qualifies as "direct marketing," despite the prevalence of online advertising (including personalised advertising) at the time the GDPR came into effect. Furthermore, Article 13(1) of the ePrivacy Directive clearly states that "direct marketing" applies only to communications through direct channels such as phones, faxes, and emails, excluding online personalised advertising.

We recommend that the EDPB clarify these paragraphs in the draft guidelines and refrain from expanding the definition of direct marketing.

5. The need to repeat the balancing test following the introduction of mitigating measures

Referring to our previous call concerning the streamlining of GDPR compliance, we would like to respectfully challenge the assertion made in paragraph 58, which indicates that following the implementation of mitigating measures, the controller must initiate the balancing test anew. This implication suggests that the balancing test will necessarily be conducted twice, resulting in two distinct sets of documentation to be processed.

CIPL believes that the comprehensive three-step test, which includes the balancing test, is inherently contextual and should incorporate the overall assessment of mitigating measures. These mitigating

[18] Guidelines 1/2024, para 40.

measures are integrated into the broader three-step approach and are not isolated or separate processes. Consequently, it is unclear why controllers would be required to repeat the same assessment after identifying mitigating measures that serve to minimise risks identified in the initial assessment. CIPL, however, agrees that part of accountability includes demonstrating the efficacy of the mitigating measures.

Therefore, we urge a reconsideration of the language used in this paragraph to reflect that mitigating measures form a part of the comprehensive three-step test and should be assessed within its context.

6. Reassessing processing for internal administrative purposes within a group of undertakings

The draft Guidelines may inadvertently impose limitations that do not align with the realities of modern companies. Today's organisations typically operate within complex, multidimensional HR structures that disrupt traditional, linear relationships between employees and their employers. In these matrix structures, employees often engage with multiple legal entities within a corporate group, participating in product teams and projects that transcend conventional boundaries. As a result, it becomes necessary to facilitate the internal transmission of personal data, as it not only supports the operational efficiency of the organisation but also enhances employee engagement and career development.

In many instances, the transmission of personal data within a corporate group is not just beneficial but necessary for fulfilling employment obligations and executing pre-contractual measures in accordance with Article 6(1)(f) GDPR. However, in addition to this legal basis, the importance of Article 6(1)(f) GDPR should not be underestimated, particularly in light of Recital 48. This provision allows for the legitimate interests of employers to be weighed against those of the employees, emphasising that data processing can serve shared interests, such as centralising payroll and HR functions to prevent the fragmentation of employee records.

Furthermore, the legitimate interests of employees should also be taken into account. For instance, a centralised approach to HR management enables employees to maintain an overview of their career progression and the opportunities available within the organisation. This transparency not only helps employees understand how their personal data is processed but also enhances their ability to navigate their career paths within the corporate structure. Additionally, a robust cross-group data protection strategy can facilitate compliance with data protection regulations, offering clear mechanisms for employees to exercise their rights. By acknowledging these legitimate interests and adopting a more flexible interpretation of the guidelines, organisations can better support their operational needs while safeguarding employee rights.

The EDPB should recognise the complexities of modern corporate environments, recognising that effective data transmissions within a group of undertakings are not only necessary for operational efficiency but may also align with the interests of the employees involved. Acknowledging this in the Guidelines serves both the interests of the organisation and the rights of individuals, fostering a more cohesive and functional data governance framework.

7. Information Provided to Individuals about the Legitimate Interest Assessment

CIPL recommends that the EDPB explicitly confirm that organisations are not obliged to provide individuals with copies of legitimate interest assessments. The Guidelines' assertion that such access is "essential to ensure effective transparency and to allow data subjects to dispel possible doubts as to whether the balancing test has been carried out fairly" is unsupported by the GDPR.

The GDPR already includes detailed transparency requirements under Articles 13 and 14. These provisions ensure data subjects are informed of the legitimate interests pursued by the controller or third party when processing is based on Article 6(1)(f). However, they do not mandate disclosure of the balancing test itself. Similarly, while Article 15 grants a right to obtain a copy of the personal data undergoing processing, it does not extend to requiring a copy of any legitimate interest assessment.

Additionally, CIPL is concerned with the draft Guideline's assertion that: "reasonable expectations do not necessarily depend on the information provided to data subjects... the mere fulfilment of the information obligations set out in Articles 12, 13, and 14 GDPR is not sufficient in itself to consider that the data subjects can reasonably expect a given processing." We would like to highlight that the text of the GDPR does not support such an interpretation. Articles 12, 13, and 14 of the GDPR provide means for individuals to be informed, and as a result, this forms their reasonable expectations about a given processing activity.

Organisations make considerable efforts to comply with GDPR transparency obligations, ensuring individuals are informed about the personal data being processed, the purposes of processing, and its duration. Such disclosures are critical in shaping data subjects' reasonable expectations. The Guidelines should, therefore, recognise transparency information as a key factor in assessing reasonable expectations and list it among the relevant considerations.

III. ANNEX

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 ecosystem, including financial institutions and merchants, have a legitimate interest in preventing and minimising the impact of fraud and losses. Clients, individuals and society as a whole have a legitimate interest to reduce fraud	Individual cardholders expect their payment transactions to be processed in an efficient, safe and secure way.

and protect the integrity of the financial system.	

Mitigating measures

- Strict data access rules;
- Data use limitations;
- Security measures;
- Retention schedules;
- 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;
- Periodic review of the legitimate interest periodically.

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 as well as society 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; • Periodic review of the legitimate interest assessment and in cases where data is retained for longer than a predetermined period.	

Case study 3. Processing of Internet Protocol Addresses (IP 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.	

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 employees 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; • Redaction of the personal data of any third parties.	

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. Pharmaceutical companies 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 personal data (including data that they have made public) to provide them with information on medicines and medical innovation that 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; • 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	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).

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.	
Mitigating measures • Adopting strict destruction procedures for outdated data; • Disclosing only data processing practices regarding TOVs; • Publishing the TOV in an aggregate form if the HCP has objected to the publication of TOV.	

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;	

• 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 (such as CCTV) for security purposes 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; • 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; • 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).	

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;
- 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.[19] 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.	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;
- 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.

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.	

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.	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.

[19] 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).

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.	
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; • 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.[20]
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; • Providing contractual safeguards with suppliers and partners including prohibition to re-identify data.	

[20] The Working Party 29 has recognised in its opinion on legitimate interests that web analytics pose minimal privacy risks to individuals. See footnote 4 for source.

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.[21]

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;
- Inclusion of contractual protections on data transferred to third parties.

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.[22]

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; • Adopting strict retention periods to minimize the risks to individuals.	

Case study 17. Processing for loyalty program

A loyalty program can involve multiple key players, each with distinct roles:
(1) Loyalty Program Owner: The program owner could be a third-party company that designs the loyalty program and defines the program rules, structures the rewards and determines the eligibility criteria for the program participants. A loyalty program owner may be engaged by a Benefit Provider while exercising some level of autonomy; since the Loyalty Program Owner is not in direct contact with individuals, it may be difficult for them to rely on consent or contract performance as a lawful basis to process personal data.
(2) Benefit Provider: The benefit provider entity such as retailers offers rewards, benefits, or discounts to the program participants. Benefit providers might process personal data of the

[21] EDPS Prior Checking Opinion on "Data processing for social media monitoring" at the European Central Bank (ECB), Case 2017-1052, page 8.
[22] See footnote 4 for reference, page 25 of the guidelines.

program participants necessary to deliver specific benefits, often based on a contract they have in place with individuals.
(3) Loyalty Program Participant: Data Subjects who are eligible customers of the loyalty program. The participants can participate to the program for example by making purchases or engaging with the program to earn rewards, benefits or offers.

Legitimate interests of the controller, third parties and/or society	**Individuals' rights and freedoms and reasonable expectations**
Legitimate Interest: Loyalty Program Owners have a legitimate interest to process personal data that are strictly necessary in order to make sure that the loyalty program functions effectively and to optimize the loyalty program. This interest is real and present and effective at the date of the data processing and not speculative. **Necessity:** It is necessary for the Loyalty Program Owner to process adequate, relevant, and limited personal data of participants to fulfill such legitimate interest. This includes purposes such as managing the reward system, tracking eligibility for rewards, allocating benefits, and ensuring that participants can redeem points smoothly and receive benefits accurately.	Individuals may reasonably expect that their personal data will be processed to enhance the core purpose of a loyalty program relating to a product or service they've solicited. Importantly, this processing of personal data (e.g. calculation of rewards, tracking of points, analysis of purchase history) is entirely beneficial to individuals and individuals only obtain positive outcomes from this data processing, such as rewards, offers or cashback.
Mitigating measures • Ensuring compliance with data protection principles such as "data minimization" principle. • Ensuring that personal data is only used for the purpose of the Loyalty Program. • Providing transparency through privacy notices and Loyalty Program Terms and Conditions. • Providing opt-out option from the loyalty program.	

Case study 18. Processing for delivery of online content, security, and audience measurement via strictly trackers

Strictly necessary trackers, including cookies, may process personal data (e.g., IP addresses, user preferences and device information) to support essential website functions, including online content delivery, security and audience measurement purposes.

Legitimate interests of the controller, third parties and/or society	Individuals' rights and freedoms and reasonable expectations
Website owners and service providers have a legitimate interest in ensuring that web pages and digital content function properly to ensure the secure, reliable, and efficient delivery of online content, for load balancing and service optimization purpose. Ensuring security and fraud prevention also pursue a legitimate interest as it helps to maintain a secure online environment. There is also a legitimate interest in processing aggregated data via essential trackers to provide essential metrics on website traffic.	Individuals reasonably expect that their personal data will be used for essential functions such as delivering requested content, ensuring online security, and enabling service reliability. They also reasonably expect websites to measure aggregated usage patterns to enhance services. The use of strictly necessary trackers for audience measurement and security relies on processing of anonymized, aggregated or pseudonymized data, and may not necessarily involve direct personal identification of individuals. [23]
Mitigating measures • Ensuring personal data collected by strictly necessary trackers are used for the specific purposes of content delivery, security, and aggregated audience measurement. • Implementing strong technical and organizational measures to protect any personal data processed through these trackers and prevent unauthorized access, with safeguards such as anonymization of personal data or truncation of IP addresses where possible, and aggregation of audience measurement data to prevent identification of individuals. • Providing users with clear and accessible privacy notices about the collection and use of personal data through strictly necessary trackers, explaining their role in content delivery, security and audience measurement.	

[23] The Working Party 29 has recognized in its opinion on legitimate interests that web analytics pose minimal privacy risks to individuals. Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller Under Article 7 of Directive 95/46/EC, July 2014, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_article_29_wp_opinion_on_the_notion_of_legitimate_interests__july_4_2014_.pdf.