7 February 2024

info@informationaccountability.org

The following comments are pursuant to the European Commission's call for evidence for the report on GDPR (under Article 97) and the IAF welcomes the opportunity to provide its input.

1. Who We Are and the Scope of Our Comments[1]

The Information Accountability Foundation (IAF) is the preeminent global information policy think tank, creating collaborative scholarship and education on the policies and processes necessary to use data responsibly in an observational age, while enabling a trusted digital ecosystem that serves people. It is not-for-profit and independent. The IAF is the incorporation of the Global Accountability Dialog, the multi-stakeholder project that developed the "Essential Elements of Accountability." The IAF believes:

- It is critical that organizations are able to think with data and engage in knowledge creation to enable and achieve the benefits of a global digital ecosystem.
- To be trusted, organizations must be accountable, responsible, and answerable, and be prepared to demonstrate their accountability.
- Frameworks based on risk assessment and effective data governance enable beneficial, data-driven innovation while protecting individuals and society from the potential harms that may arise from data processing in the digital age.

Since 2014, the IAF has focused on public policy models and the governance of innovative uses of data pertaining to people in advanced analytics and artificial intelligence (AI).

2. Initial comments

Given the breadth of GDPR the IAF has not sought to provide comments on all areas of its implementation but has sought to focus on five key issues that intersect with the IAF's mission and objectives, as detailed above. The comments focus on:

- Research, knowledge creation and knowledge discovery
- Legitimate interests, accountability and responsible innovation
- The intersection between Artificial Intelligence (AI) and GDPR
- International Data Transfers
- The approach of Data Protection Authorities to GDPR implementation

The GDPR has now been in full force for six years, the IAF recognises the benefits that it has provided for data subjects in terms of greater awareness and engagement with their rights, and the improvements that many organisations have made to data governance. While there is still distance to be travelled in raising the strategic positioning of data governance, there is now better awareness at board level of the importance of governing risks related to personal data. In

[1] These comments were prepared by IAF staff and do not necessarily reflect the views of the IAF Board of Directors, funders, or members of the IAF extended community.

some organisations GDPR has played a role in driving investment into privacy management programmes and organizational-wide data governance strategies, which enable long term benefits in developing a culture of data stewardship and accountability, and greater trust in data use.

Focused on areas for improvement, the IAF respectfully calls for further steps to properly realise the potential of the GDPR as a risk-based system of regulation and that an effective balance between data protection and the other fundamental rights in the EU Charter is realised. In addressing this central issue, as part of a risk and harm-based approach, the costs and benefits of GDPR can be put into a fairer balance – for people, society and the economy. The IAF set out its thinking on a fairer approach to rights balancing in a 2022 paper: A Principled Approach to Rights and Interests Balancing Multi-Dimensional Proportionality.

EU Parliament Member Axel Voss identifies the necessity for risk differentiation in his paper "Fixing the GDPR: Towards Version 2.0," when he states:

> *The GDPR does not differentiate enough between low-risk and high-risk applications, determining – with a few exceptions such as prior consultation of the DPA for high-risk applications – largely the same obligations for each type of data processing. The possibility in the GDPR to define different risk classes of data processing, which require different legal bases, is not being used.*

While some of the issues raised by our comments may ultimately be best addressed by amendments to GDPR itself, the European Data Protection Board (EDPB) and the Data Protection Authorities (DPAs) could also address these issues in the approach they take to guidance and other regulatory activities.

3. Research, knowledge creation and discovery

The current approach in GDPR to research, knowledge creation and discovery has led to confusion about when advanced analytics may be used where there is no distinct legal basis for processing personal data for this purpose. Since the Commission's last report in 2020, the Covid-19 pandemic has illustrated the importance of knowledge creation in both the public and private sectors. Knowledge creation lies at the heart of digital innovation and therefore is key to unlocking significant benefits for the wider society and the economy.

The broad approach to defining personal data under GDPR, combined with a lack of clarity and harmonisation over a definition of scientific research, approach to compatibility lawful bases and exceptions create an overall effect of caution in using personal data for these purposes.

In proposing changes to address this reticence the IAF fully recognises the importance of effective safeguards and the IAF believes that more can be done to enable mature accountability approaches that create trust in the data processing.

The use of data to create knowledge in an academic setting is well understood. Less appreciated is the use of data in the commercial setting to create knowledge. Increasingly, digital agenda in both the public and private sectors are about creating safe pathways for data to be turned into information, for information to be turned into knowledge and for knowledge to facilitate actions that are societally beneficial to people and for this processing to be conducted in a manner that is lawful, fair, and just.

Knowledge creation in digital ecosystems is the generation of new insights that originates with advanced analytics (such as artificial intelligence) on data collected directly, passively, or observationally. The data is not about a specific individual, and, at this stage, it has a significantly lower impact on an individual. Knowledge creation also can be called "thinking with data." It is key for processes such as data analytics used in product or service development and improvement. It may more broadly be called "data-driven or digital innovation."

Knowledge creation, which is the pathway to the future, is conducted for three different research purposes: (1) scientific, (2) commercial, and (3) hybrid (public-private collaboration). When used as part of advanced data analytics, knowledge creation is the engine that drives the digital economy in a society. Knowledge creation differs from knowledge application. Knowledge application utilizes knowledge created on a specific or identifiable set of individuals. The process of "knowledge application" has been called "acting with data." Understanding the differences between knowledge creation and knowledge application, and the purposes for which they are being undertaken as well as the different set of risks for each, is critical to understanding how they should be regulated.

The concepts of research and knowledge creation/discovery are closely linked. Knowledge creation is a broader concept than scientific research and is focused on distillation and translation of knowledge into more outputs, bridging the gap between research and practice. Knowledge discovery is often seen as a term used to describe the broader concept of 'research' and includes activities such as data mining, with scientific research being a subset of that concept.

We refer to knowledge creation and discovery as concepts and not as intended legislative language. These terms would need to be translated into more practical language to reflect business processes such 'internal research for product improvement.' Our proposals are discussed further below.

The IAF undertook the project Making Data Driven Innovation Work (2023) to understand how organizations discover and create new knowledge. This project[2] sought to clarify the impact of regulatory and public policy uncertainty on commercial-driven knowledge creation, develop scenario driven examples of this impact, develop a public policy model that enables responsible data-driven knowledge creation through a series of compensatory controls and create a narrative and path for knowledge creation to be more formally recognized as legitimate data processing activities in next generation privacy and data protection law.

It is important that greater consideration is given to the difference between knowledge creation and knowledge application, by both policy makers and DPAs. A failure to appreciate the distinction has led to confusion and hesitancy about when advanced analytics for knowledge creation may be used and there is no distinct legal basis for processing personal data for this purpose. This challenge may require amendments to the GDPR and a new approach to interpretation and implementation.

[2] The IAF research team conducted extensive interviews with organizations from numerous fields that use data to create knowledge, even if they did not identify their processes in that way. The IAF team used the interviews to supplement the team's decade of work as researchers at the IAF and consultants working on ethical assessments and demonstrable accountability.

Many organizations use personal data as part of analytics processing (Corporate Research) to solve identified business problems, but most organizations do not use Corporate Research as a distinct processing activity more broadly because:

- Most organizations generally do not break data processing into two distinct phases: knowledge creation (I.e., the research function to identify a solution to a business problem) and knowledge application (I.e., application of the solution to the business problem), and/or
- Under GDPR, this portion of data processing (research) is complicated and/or limiting. Personal data can be processed for scientific research purposes, which is narrowly defined (see our comments below), as long as sufficient safeguards have been implemented and scientific research is run "in accordance with relevant sector-related methodological and ethical standards, in conformity with good practice" (collectively Safeguards), and/or
- Other countries and future laws limit the use of personal data for research purposes to improvement/supply of products and services or to requiring the use of de-identified personal data for research and for socially beneficial purposes.

Addressing these issues is key to developing proportionate and effective regulation for digital innovation in this context. It should enable the scalable and risk-based safeguards (and GDPR rights) to apply based on the risk and context of the processing. Such an approach, supported by effective accountability programmes, can enable responsible innovation. The IAF's 2019 paper Origins of Accountability: Advanced Data Analytic Processing- Update to 2013 Big Data Project explains also the importance of the knowledge creation and application, and their relationship to accountability, in more detail.

Defining Scientific Research in GDPR

There is still much uncertainty about how scientific research is defined in GDPR. While addressing this question is not the sole solution to the questions above, it is still important for certain commercial scenarios that a more balanced definition is found.

Although the GDPR adopts a "broad" definition of research in recital 159, encompassing the activities of public and private entities, this intent has not been applied in practice. There are varying member state laws defining what the term means and how the exceptions derived from Article 89 should be framed. The EDPB's legal study on the appropriate safeguards under Article 89(1) GDPR for the processing of personal data for scientific research (2021) sets out the variance of the situation clearly in its conclusions:

> *…numerous differences exist in the more detailed requirements which could impact the level of protection, such as varying or strict interpretations of the concept of scientific research, the importance attached to public interest…*

For example, the following questions can arise:

- Are clinical trials conducted by a university overseen by a medical doctor scientific research?
- Is the same research conducted by a pharmaceutical company scientific research? Is this dependent on whether a medical doctor is involved?
- What about public-private partnerships that conduct clinical research?

- Is research into neurotechnology by a national health organization scientific research, but the exact same type of research by a tech firm or medical device company not?

The Data Protection and Digital Information Bill currently progressing through the UK Parliament has taken the step of placing a clearer definition of research onto the face of statute. Clause 2 updates UK GDPR to further explain the definition:

> - *purposes of any research that can reasonably be described as scientific, whether publicly or privately funded and whether carried out as a commercial or non-commercial activity.*
> - *include processing for the purposes of technological development or demonstration, fundamental research or applied research, so far as those activities can reasonably be described as scientific.*

The IAF welcomes this amendment to UK GDPR and believes that the European Commission should also consider the benefits of such an approach. There may also be an opportunity to consider the evidence of the benefits and any risks of such an approach once the UK legislation takes effect.

The IAF therefore believes that more could be done to clarify the position of scientific research on the face of GDPR, including more explicit recognition of the activity in the commercial sector. This additional statutory language should be included alongside further references that also translate knowledge creation and discovery into practical business activities, drawing on provisions already in use in other jurisdictions, such as US State laws and Canada.

Lawful basis and exceptions for scientific research, knowledge creation and discovery

Scientific research and business activities that make up knowledge creation and discovery should also be recognised as specific lawful bases in Article 6, subject to necessity and proportionally considerations. A new condition for using special categories of data should also be created in Article 9.

A number of US State Privacy laws, for example the California Privacy Rights Act (CPRA), contain a provision exempting "personal information collected as part of a clinical trial or other research study subject to or conducted in accordance with certain clinical trial and research study regulations and guidelines" and the Colorado Privacy Act, which contains provisions that create an exemption for personal data processed for the purposes of "conducting internal research to improve, repair, or develop products, services, or technology." These provide examples of how policy makers can differentiate data processing scenarios.

The proposed Consumer Privacy Protection Act in Canada (Bill C-27) would create an exception to consent for "Research, analysis and development":

> *21 An organization may use an individual's personal information without their knowledge or consent for the organization's internal research, analysis and development purposes, if the information is de-identified before it is used.*

The IAF notes that this approach to research and knowledge creation does not need to create unreasonable risks for data subjects. Effective safeguards should still be used and important considerations under the data protection principles, such as fairness, will remain applicable, alongside necessity and proportionality. The accountability requirements of GDPR would also continue to apply, in a risk-based manner.

The IAF also notes that the AI Act does not apply to scientific research and product orientated research, see recital 12c and in Articles 5a and 5b (current text).

Purpose limitation, anonymization and pseudonymization

Article 5(1)(b) GDPR contains an important provision that further processing for the purposes scientific research, in accordance with Article 89, is "*not be considered to be incompatible with the initial purposes".* In practice, organisations undertaking research in the EU have found that member state law and DPA guidance have made consistent application of this provision difficult. This has resulted in caution and reticence about secondary uses of data.

Peloquin et al. in the European Journal of Human Genetics explain the challenges of secondary research uses of data under GDPR, focusing on the experience of biobanking and databanking.

A key safeguard for scientific research processing is pseudonymisation, which is referenced in Article 89. There are also further provisions in member state laws that provide further detail on when pseudonymisation and anonymization should be used as a safeguards (and summarised in the EDPB legal study referenced above).

There continues to be confusion about how both terms are defined and used in practice. The default position presented by DPAs is that all key coded data at individual record level is pseudonymised data and should therefore always be treated as personal data under the GDPR, including requirements such as transparency, lawful basis and international data transfers. All of which can significantly disproportionately complicate and slow the process of research.

The 2023 case from the EU General Court (SRB v EDPS) found that pseudonymised data is not personal data if the recipient (Deloitte) doesn't have the data necessary to identify the data subject. EDPS merely examined whether it was possible to re-identify the authors of the comments from the SRB's perspective and not from Deloitte's. This case clearly highlights the inconsistencies in approach to the question of anonymised and pseudonymised data. The IAF believes that the approach of the General Court is an important position that should be clarified on the face of the GDPR, it would also be reflective of a risk-based approach to GDPR interpretation, which would also enable an approach to recognise the differences in risk between knowledge discovery and knowledge application.

Recital 26 of the GDPR and the test *"means are reasonably likely to be used to identify the natural person"* is also subject to inconsistent interpretation and there is merit in placing the language from the recital onto the face of the GDPR. The test in recital 26 on identification provides for a risk-based approach but is often not fully applied by data protection authorities in guidance they provide. The guidance often favours an approach of stating that anonymisation should aim to eliminate any possibility of re-identification.

The IAF also notes that Privacy Enhancing Technologies (PETs) such as homomorphic encryption, differential privacy, Variant Twins and K-anonymity can play an important role providing safeguards for research, including anonymisation and pseudonymisation. This can include the development of trusted research environments (TREs) and shared data spaces. PETs can also play a role as a safeguard in the international transfer of personal data. Considering the uncertainty described above there is a risk that PETs are not deployed to their full potential as organisations do not see clear incentive to justify the investment, given the current cost of PETs.

The IAF therefore proposes that the GDPR be amended so that the business activities that are part of knowledge creation and discovery should join scientific research as being recognized as a compatible purpose under Article 5.

4. Legitimate interests, accountability and responsible innovation

The GDPR contains a list of lawful basis for processing that in theory contain no hierarchy but in practice the IAF has observed that there is still often a preference towards consent, from both the European Court of Justice and the DPAs.

In the context of knowledge discovery, creation and research, and other areas of digital innovation, including AI model development, the use of consent is often unfeasible. It also challenges research principles around representation and sampling. Consent can also unfairly shift some weight onto the individual, rather than maintaining a core focus of the responsibility of the organisation.

With the emergence of AI, including foundation models, it will be important to consider lawful bases other than consent. For commercial organisations, use of the legitimate interest basis in Article 6(1)(f) is therefore of central importance for digital innovation. While some organisations have been able to use this basis under GDPR the IAF contends that further guidance is needed to provide organisations with the confidence to use legitimate interests.

While the outcome of the balancing test largely determines whether Article 6(1)(f) may be relied upon as a legal ground for processing, it also should be seen as a tool for accountability and should help organisations build compliance at the outset and demonstrate compliance when called upon.

The IAF therefore believes that reliance on legitimate interests can be an effective mechanism to protect people and enable responsible innovation. The focus on necessity and proportionality in the provision ensure that the provision is not a "workaround" or "shortcut" for commercial organisations to undertake unfair processing. When relying on legitimate interests, the data protection principles still apply, including fairness.

The IAF's 2017 report on Legitimate Interests and Integrated Risk and Benefits Assessment also highlights the value of a joined up approach between legitimate interests and the data protection impact assessment requirements in GDPR. An approach to multi-dimensional proportionality, as set out by the IAF can also enable the private sector to implement an approach to risk and rights balancing that reflects the context of their business. This approach recognises the range of rights in the EU Charter, not just data protection and privacy. Taking such an approach is also scalable to risks and the different context of knowledge creation, discovery and research.

As part of an accountability programme, use of the legitimate interest provision can enable trust and confidence in how data is used and provide an audit trail for organisations to demonstrate to DPAs how they have addressed risk to individuals.

The IAF therefore proposes that the DPAs and the EDPB invest more resources into guidance and tools to support effective use of legitimate interests. They should do this in the context of wider guidance on accountability and data protection assessments. It is also important that EDPB guidance is issued on the question of how legitimate interests intersect with commercial interests once the Court of Justice has ruled in the case of Koninklijke Nederlandse Lawn Tennisbond. The IAF respectfully submits that such a narrow interpretation proposed by the Dutch DPA is contrary to other rights contained in the Charter.

5. AI and GDPR

The IAF has previously submitted comments on the Commission's proposed AI Act. The IAF noted the value in the two-step approach used by the legislation, between AI developers and AI users. Such an approach fits with the two-step risk-based approach for GDPR advocated by the IAF: data (knowledge creation) and acting with data (knowledge application). In our submission for this review, we have reiterated some of the points raised in our original comments on the Act.

The IAF also welcomes the AI Act's carve-out for scientific research and product orientated research in recitals 12c and in Articles 5a and 5b (current text).

The IAF highlights the importance of joined up guidance between EDPB and the new EU AI Office, to provide early clarity about the interplay between the GDPR and AI Act.

GDPR and using personal data in AI training

AI models, particularly foundation models, require large volumes of data and often from a significant range of sources, which may include personal data, anonymised data and data unrelated to people. While AI model requirements may change in future, the current position is that scale and scope are often needed to maintain the utility of the model. Diversity of training data will also be important for addressing bias and discrimination. This then creates a tension with GDPR principles such as data minimisation and compatibility.

The fact that the AI Act recognises a legal basis for using personal data to safeguard against bias and discrimination is welcome but uncertainty on these issues could remain without amendments to the GDPR to mirror the position. Or EDPB should clarify the position in guidance.

In many cases, training data is not about the interests of a single individual but rather the interests of a broader group or society as a whole impacted by the insights that come from the AI processing. While the legitimate intertest balancing concept could be interpreted more broadly in the AI context, at this point there is no authority for doing so. There is a need for further clarification on application of legitimate intertest to AI data training.

In the UK the Information Commissioner has issued a consultation on generative AI, which will cover this issue. The open consultation is a welcome approach that we would encourage the European Data Protection Board to take on this issue.

GDPR, AI and risk assessment

Considering the two-step concept outlined above the IAF proposes that there is merit in amending Article 35 of the GDPR. It should be amended to apply to the application of insights stage (use of data) more clearly, where there is a much greater risk to individuals, and not at the knowledge creation and discovery stage.

The importance of a joined-up approach to rights balancing and risk assessment under GDPR was noted above in relation to legitimate interest and data protection. There is a need for guidance from the EDPB and the AI office on how to join up and integrate assessments required under GDPR with assessments required under the AI Act, including assessments for fundamental rights. Such a joined-up approach will enable efficiency and clearer sight of the key risks and mitigations, plus integration into an overall approach to data governance within an organisation.

For a risk-based approach to data protection implementation and oversight for AI to be effective, a definition for the negative consequences to be avoided is needed. It is necessary for such a

definition to be broad enough to include the full range of potential negative outcomes to be managed and to be flexible enough to enable practical prioritization of risk. The IAF would encourage an approach that set outs a broad concept of "Adverse Processing Impact", which provide more effective and proportionate assessment rather than just focusing on the broader concepts of harms or risks. The IAF's paper on Adverse Processing Impact and Defining Risk sets out how this could be approached and it aligns with the NIST privacy framework: a tool for improving privacy through enterprise risk management, version 1.0.

GDPR, AI, automated decision making

The recent Court of Justice judgment in Schufa, covering article 22 of GDPR and automated decision making, has implications beyond credit scoring. The ruling by the court "to fill a legal gap" implies that the risk scores produced by businesses like fraud detection and identity verification are automated decisions. It suggests controllers will need to obtain consent before calculating creditworthiness or other types of algorithm-based scoring that are used in a wide variety of business processes. GDPR Article 22 only concerns acting with data. The CJEU overlooks the distinction between thinking and acting with data to reach a broad interpretation of the term "decision" in GDPR Article 22(1). In the IAF's view the judgment is inconsistent with modern data analytics and well-established credit scoring practices and may be at odds with the evolving role analytic driven decision-making plays in many aspects of life. The IAF has set out further analysis in a policy paper.

The IAF proposes that Article 22 should be revised to describe more clearly profiling and automated decision making. Profiling is central to the knowledge discovery process. As such, it should be subject to a DPIA to ascertain that processing is conducted in a legal and fair manner. Automated decision-making is a separate process. It too should be subject to assessments, and the risks from a particular automated decision-making process should be understood and documented. Currently, the GDPR confuses the connections between the two.

Need for joined up regulation on AI

AI will lead to winners and losers in a modern global economy. For example, autonomous trucks may make for safer highways, but they also will lead to a need for fewer drivers. Data protection authorities do not decide on the balance between safer highways and truck driver employment. The IAF believes that the data protection authorities should have the power to oversee required processes by organizations to identify the risk of unfair outcomes, and other regulators should make appropriate decisions on whether knowledge application creates prohibited outcomes as determined by laws and societal norms.

The European Commission should take steps to enable joined up regulation between the data protection authorities, the AI office and other EU regulators. We encourage the EU to look at the approaches to joined up digital regulation in the UK, Australia and Canada. The UK Digital Regulation Co-operation Forum is the most advanced of these efforts, for example the work undertaken by the UK ICO and CMA to join up their approach to assess the data protection and competition issues in relation to the Google Sandbox proposal for digital advertising.

GDPR, AI and deletion

Outcome-based interpretations of GDPR will be needed to address how it will apply to AI. One such example is the issue of deletion – in relation to the 'storage limitation principle' under Article 5 and the right to erasure under Article 17.

The relationship between AI training data, AI models and usage is complex. The tokenised data structure of generative AI foundation models makes the question of deletion challenging. While it may be possible to delete training data, the question of removing personal data from models is complex, as the structure is different from relational databases or other data systems organisations have traditionally used. Deletion from models could require a process of retraining, which could be highly disruptive to the operation of the AI system, introduce inaccuracies or sample-size overweight or underweight, and in many cases may not be feasible. To give effect to the deletion concept will require innovation; it is possible that techniques such as "unlearning" and mechanisms that filter information at the levels of system prompts can be used. Such mechanisms can provide protections from adverse impacts even if they do not meet the traditional technical definition of deletion. The IAF would encourage the development of guidance that reflects the intention of provisions and recognises the value of privacy enhancing solutions that can give effect to the GDPR provisions in terms of preventing adverse impacts.

6. International data transfers

Aside from the interface with AI, one of the most impactful GDPR developments since 2020 has been implementation of the Schrems II judgment. The IAF contends that, overall, the impacts of the judgment have been negative, as the resources diverted into compliance with data transfer requirements in GDPR have been out of proportion to the risks involved. Companies have had to divert resource away from areas of compliance such as accountability programmes and wider data governance related to the use of new technologies. This may have slowed innovation at a time when GDPR has crucial role to play in ensuring responsible use of new technologies.

The disproportionate outcomes from the case are evident from enforcement decisions against controllers using web tools such as Google Analytics, when there is no reasonable evidence to suggest such personal data could be accessed by US government authorities or what adverse impacts were likely. These decisions were also made despite various privacy enhancing measures such as homomorphic encryption being put into place to also reduce the risk of identifiability.

The position under GDPR lacks a risk-based approach or limits to accountability, given the issues related to government access to data that companies are unable to control. The approach of using Transfer Impact Assessments (TIAs) to assess government access to data in third countries may be unsustainable and a more proportionate solution is needed for the long term – one that considers transfers to third countries beyond the EU – U.S. dynamic. While the EU-U.S. Data Privacy Framework provides a strong mechanism for some multinational organizations, it is an incomplete solution to the broader global data economy.

The IAF advocates for a system based around accountability and risk, including the role of Global Cross Border Privacy Rules (CBPR). As noted earlier in our comments, the IAF highlights the importance of an approach that considers the full range of rights in the EU Charter, creating a fairer approach of rights-balancing.

Risk based approach to international data transfers

The EDPB have rejected the notion that a risk-based approach from GDPR applies to data transfers. There have been several papers that counter this standpoint from a legal perspective. See articles by Lokke Moerel, Paul Breitbarth and Clifford Chance/DLA Piper.

The IAF supports the view that the accountability requirement of article 24 includes the risk-based approach. It follows that article 24 has horizontal application and where international data transfer requirements are obligations of the controller, the risk-based approach of Article 24 should apply.

The IAF also notes the approach taken by the UK ICO in its transfer risk assessment guidance, which is more reflective of the risk based intention of GDPR.

The Information Accountability Foundation (IAF) argued in its March 2021 paper, Addressing Human Resource Data Flows in Light of European Data Protection Board Recommendations, that by prohibiting consideration of subjective factors, and thereby making it impossible for companies to access HR data either remotely or stored in the cloud, the right to protection of personal data is prioritized over other individual rights set forth in the Charter of Fundamental Rights of the EU (Charter). In particular, EU individuals' fundamental rights to engage in work and freedoms to choose an occupation and to conduct a business are undermined and the right to protection of personal data is favored.

The IAF therefore proposes that Chapter V of the GDPR is amended to make clear how the risk-based approach applies.

Accountability and data transfers

Under the current implementation of GDPR the incentives to invest in accountability mechanisms are currently low. Most organisations favor using standard contractual clauses (SCCs) and the approach of marrying them of transfer impact assessments has become a standard approach for organisations. Many do not see enough value from investment in binding corporate rules (BCRs) due to the application time and resource overheads, added to the burden of TIAs that will still be required for BCRs. The market for certification and codes of conduct has also been slow to develop as the EDPB guidance on using them for transfers is recent.

The IAF would urge a rethinking of the Chapter V provisions with a much greater focus on accountability and risk, so that data transfers are not seen as a separate compliance activity under GDPR. International transfers should be integrated into the wider accountability and data governance programmes within organisations. This integration would also create a stronger business case for accountability programmes and the long term benefits they can bring in protecting personal data and enabling its use.

Approaching transfers through the lens of accountability would also refocus the relationship between organisations (e.g. controller and processor) into "chains of accountability" rather than contractual documents that are often agreed, filed and never referred to.

Government access to data and the interaction with international data transfers

There is a need for better information resources to assist organisations in the task of assessing destination third countries. A free to use portal of resources (produced by EDPB or the Commission) and categories of information about each area of assessment would be of real assistance. While categorising countries under stark categories of risk (red, green etc) would be counterproductive, the portal should enable swifter assessment and understanding what risk the third country posed and how their surveillance mechanisms and safeguards compare to the standards set out in the EDPB guidance. This is a short term to medium solution and a longer-term solution should be found.

The OECD Declaration on Government Access to Personal Data Held by Private Sector Entities (2022) was an important milestone – it delivered a common set of principles for government access, amongst democratic countries under the rule of law. While the Declaration was non-binding it was the first time such an international consensus had been reached across such a broad range of countries, at government level, and beyond the EU and Council of Europe. The IAF recognises the potential of this initiative, as it can refocus accountability for government access. The GDPR recital 105 could be amended to recognise the OECD Declaration as a relevant factor in assessing adequacy, alongside Council of Europe Convention 108.

The recent article by Chris Docksey and Kenneth Propp, An International Path Forward on National Security Access to Personal Data, makes an important case for a *"counterpart accountability mechanism for government access to personal data".* The IAF supports the exploration of this concept and that the US and EU could play leading a leading role in developing a voluntary but binding international code of conduct, with some form of external, independent means of checking adherence. Such as approach could build on what the OECD Declaration has set the foundation for.

7. The approach of Data Protection Authorities (DPAs) to GDPR implementation

Lastly, the IAF wishes to comment on how the approach of EU DPAs should evolve to address the emerging challenges of AI regulation and ensure a better balance between data protection and other fundamental rights in the EU charter.

The IAF recognises the importance of independence for all DPAs but there is evidence that the notion of complete independence in Article 52 of GDPR has become counterproductive. Such a notion can develop a situation where data protection authorities downplay the importance of accountability to stakeholders and give lower priority to the wider economic and societal impacts of their activities.

DPAs communicate their role as focused on upholding individual rights. While this will always be an essential role there is a need to for the DPAs to understand their role as regulators. A regulatory mindset will enable a greater focus on creating a balanced system of end-to-end regulation, with strategic outcomes in mind. As GDPR impacts business models it is now much closer to an economic system of regulation, and this should be reflected in the strategic approach.

As noted above there is a need to improve the consistency of the guidance issued by the data protection authorities, on legitimate interests in particular. There is also a need for further guidance to be issued on accountability and how to apply a risk-based approach in practice. There is also a need for interpretation of GDPR focused on practical outcomes and not just technical application.

The IAF would highlight the importance of consultation and engagement with stakeholders – this should be transparent and planned consultation where the range of stakeholders engaged reflect the full range of impacts from the activities of the DPA. The stakeholders should also be able to how understand how the authority responds to their inputs.

The IAF also calls for all EU DPAs to consult on, and publish, a formal regulatory strategy – setting their objectives and priorities, and how they will allocate resource dependent on risk. This would also present an opportunity for the DPAs to set out a proactive approach to regulation, that balanced ex-ante and ex-post measures to achieve the outcomes of the GDPR. Such an approach

would also equip the DPAs in their task regulating personal data and AI systems, given the pace of change and the need for agile and outcome-based regulation. The IAF would also encourage DPAs to explore coregulatory mechanism such as sandboxes, to support a proactive approach to regulatory advice.

The IAF would therefore propose that Article 59 of the GDPR is amended to require DPAs to produce strategies that cover a three-year period, alongside a more detailed annual workplan to deliver the strategies. The strategies should also contain key performance indicators that are then covered in the annual report. The GDPR should also be amended to provide a clear legal basis for DPAs to use sandboxes, as in the AI Act.