The GDPR's First Six Years

Positive Impacts, Remaining Implementation Challenges, and Recommendations for Improvement

May 2024

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Table of Contents

Table of Contents (continued)

The GDPR's First Six Years

In advance of the European Commission's (EC) pending "health check" of the General Data Protection Regulation (GDPR) under Art. 97, and four years after the EC's initial report on the GDPR, the Centre for Information Policy Leadership (CIPL)[1] has produced this Report setting out the positive impacts and the benefits of the GDPR, the continuing implementation challenges for organisations and their data protection officers (DPOs), and aspects that remain to be improved, explored or evolved further.[2] This present report draws upon a) CIPL's independent research, observations, and experiences over the past years since the GDPR came into effect, b) a survey that CIPL conducted with its Member organisations and c) discussions with industry experts, regulators and academics held at the CIPL's Executive Retreat in Madrid, Spain on 12 March, 2024.

The Report follows up on CIPL's earlier GDPR stock-take report in 2019[3], which we published as part of our GDPR implementation project at the time. As noted in our 2019 report, as well as in CIPL's Response to the EU Commission's first Consultation on the Evaluation of the GDPR in 2020[4], **the GDPR has been an important tool for protecting individuals' privacy and has substantially elevated data protection awareness globally**. Its impact can be seen in many data protection laws around the world, as well as in the global privacy compliance and data management programs of many multinational organisations that use the GDPR as their baseline standard. However, s**everal of the implementation challenges under the GDPR we identified in our 2019 report, as well as our 2020 GDPR EU Commission's consultation response, continue to persist. In some cases, they have increased, including in the form of unintended consequences resulting from particular interpretations of the GDPR provisions.**

The purpose of this follow-up report is to:

- **a.** highlight the GDPR's positive impacts,
- **b.** assess any progress that has been made on previously identified challenges,
- **c.** reflect on areas that continue to undermine the full potential of the GDPR, and
- **d.** find opportunities for potential improvements, particularly where this can be accomplished through interpretation and modified application of the existing text of the GDPR.

Ultimately, it is in everyone's interest to ensure that the GDPR remains fit for purpose and relevant in the face of changes in technology and society. **The GDPR's original ambition was to be principle-based, risk-based, technology-neutral and future-proof, to create a "coherent data protection framework" to ensure "the trust that will allow the digital economy to develop across the internal market". Data protection authorities (DPAs), courts, and privacy practitioners must keep these objectives in mind in their interpretation and application of the GDPR. This report identifies areas where this is particularly important and feasible.**

The Report also identifies areas where the GDPR's goals may be complicated by the **increasing number of other digital regulations, without sufficient articulation of the level of overlap and the relationship,** and where the respective definitions and requirements may not seem consistently aligned. In short, the present report seeks to highlight the benefits of the GDPR, as well as suggest ways to improve its effectiveness further.

I. Positive Impacts of the GDPR

1. Higher Data Privacy Awareness and Ownership in Organisations:

Improved overall organisational privacy awareness and data management, as well as greater consideration of data protection in business decisions.

For many organisations, the GDPR has made privacy and data protection considerations integral to their business decision-making, product and service development, and enterprise operations. As a result of the GDPR, within companies' there is a deeper awareness and understanding of privacy risks, not only to the organisation but also to individuals and society, and of the need for organisations to use data responsibly and in compliance with the GDPR. The GDPR has fostered a privacy-by-design mindset in many organisations and is driving their data strategy and planning. They have undergone a culture change in which privacy is factored into everyday decisions by IT, data, marketing, HR engineering and product teams. Before the GDPR, engineers and product developers might have made decisions on the processing of personal data based on cost-benefit calculations primarily as they pertain to the organisation itself as opposed to the individuals impacted by the organisation's products and services. In other words, the primary questions might previously have been: What is less costly to implement? What takes fewer man hours? Now, privacy implications for individuals play a substantial role in these assessments, including considerations of fairness and customer experience: Would this processing impact the customer negatively? Would it be fair?

2. Privacy as a Board Level Issue

Facilitated senior management focus, buy-in, and increased resources for compliance, and established effective data governance as an important business enabler and trust generator.

The GDPR has equally raised data privacy compliance "from the backroom to the boardroom", with greater focus and awareness at the C-suite and board levels across all business sectors. The primary and initial driver certainly was legal compliance and risks of non-compliance in light of the potentially immense fines created under GDPR. More importantly, the digital transformation of the economy has resulted in the "datafication" of all businesses. Hence, it transformed privacy, data protection and data governance into core business issues that require board-level attention and accountability. Data protection concerns have become among the top three enterprise risk priorities for all businesses that depend on the use and sharing of personal data.[5] Importantly, beyond risk management, top-level decision-makers increasingly recognise how data serves as an enabler of legitimate, innovative, and beneficial business purposes and why responsible use of data is a prerequisite to digital trust and confidence in increasingly volatile economic and social times. This has led to more executive focus and increased resources for data privacy teams and compliance, as privacy has become a business enabler and differentiator for many companies. The GDPR is often seen as a facilitator not just for (global) data protection compliance but also for meeting market standards, creating business solutions that meet or exceed customer expectations, and creating the foundation of trusted and sustainable business. Indeed, the GDPR's focus on privacy by design is credited for driving innovation in privacy-enhancing technologies,[6] and companies are seeing a tangible return on their investments in robust privacy management programmes.[7] In the B2B

context, having an approved or certified privacy management programme (such as BCR or ISO certification) creates trust and streamlines due diligence in selecting and negotiating third-party vendor deals, for instance.

3. Global Privacy Management Standard for Organisations

Enabled organisations to create a single privacy management program for their global operations and entities.

At a time when numerous countries in the world are passing new laws or revising their existing data privacy laws, many countries have looked to the GDPR for inspiration and adopted key GDPR principles, even if they do not always follow the GDPR word for word. This means that for many global organisations operating across different legal jurisdictions, the GDPR now provides a baseline against which to build or update their global privacy programs, while at the same time reflecting the requirements of the growing local data protection laws. Given the extraterritorial application of the GDPR and the global nature of multinational companies' processes and functions, their global affiliates and entities also adapted their processes to the new GDPR baseline and, in turn, started to set privacy standards and expectations in third countries (some of which have also introduced their own privacy regulations). Having a global privacy program set on the baseline of GDPR principles also made it easier for multinational companies to perform gap analyses and satisfy the growing data protection requirements and laws in other countries.

4. Organisational Accountability

Improved organisations' ability to build and implement accountable privacy management programs and demonstrate accountability internally to the Board and externally to regulators, customers, individuals, and shareholders.

The accountability principle and the risk-based approach incorporated in the GDPR provide an optimal framework for devising accountable privacy management programmes that deliver real and effective protection for individuals while enabling responsible use of data. The GDPR has driven organisations to be more accountable and to build and implement comprehensive and systematic data and privacy management programs with policies, procedures, controls and tools, as well as executive oversight. A 2020 paper by CIPL demonstrated that companies deliver accountable privacy programs through the following elements—leadership and oversight, risk assessments, policies and procedures, transparency, training and awareness, monitoring and verification, and escalation and internal enforcement.[8]

Importantly, the GDPR has emphasised the strategic role of the DPO as the cornerstone of organisational accountability by establishing clear functions, independence, and expectations of the DPO's role within the organisation. Since the GDPR came into force, many data privacy teams in organisations have improved their standing and authority and become an integral part of the decision-making process, facilitating the responsible use of data while protecting individuals and their data. As a result of the increased awareness of data protection issues at the board level, data privacy teams have experienced an increase in their resources, credibility and impact as trusted business advisers and their ability to provide more practical and strategic compliance advice, including translating GDPR requirements into actionable measures in line with business goals.

Additionally, the risk-based approach of the GDPR fostered a consistent practice of accountability and assessing risk within organisations—both risks to individuals and risks to the organisation. The risk-based approach has also enabled effective resource allocation that is proportionate to the actual risk (or lack thereof) of specific processing activities. An effectively implemented accountability requirement drives enhanced efficiencies at the organisational level and more effective and better protection for individuals and their data. By placing the principal burden of protecting data on organisations handling the data, both in the private and public sectors, organisational accountability also increases the overall trust in the digital economy and society.

5. Improved Data Management

Fostered good data hygiene, governance, management, and traceability, resulting in improved processes and data breach resilience.

GDPR compliance has enhanced organisational data management practices overall, resulting in a more robust approach to governance of the data lifecycle, including for non-personal data. GDPR requirements have facilitated data management and business process consolidation; better integrity and quality of data; a deeper understanding of data, its flows and uses throughout organisations and to and from third parties; and more effective risk management, including third-party vendors. Importantly, this also enabled organisations to be better positioned for big data and AI transformation, which relies on the availability of large volumes of good quality data.

Creating comprehensive privacy programs and controls has also enabled businesses to respond to regulatory changes or individual inquiries with greater speed and accuracy. Investments in automation and the increased maturity of privacy processes in response to the GDPR requirements have had a direct positive impact on individuals in terms of exercising their rights.

The risk-based approach of the GDPR, including DPIAs, privacy by design requirements, and the legitimate interest balancing test, requires—and has fostered in many organisations—a consistent internal process for accountability and risk assessment. This ensures appropriate risk-based prioritisation of mitigations and controls and more effective data management programs based on actual risk.

Finally, in a time of increased cybersecurity threats and risks, the GDPR has strengthened organisations' resilience to breaches and prepared them to respond more efficiently and effectively to incidents when they happen. Improved data management practices, combined with the requirement of state-of-the-art technical and operational measures and the clear data breach notification requirements and penalty provisions of the GDPR, provided the impetus for many organisations to invest further in preventative data and cybersecurity measures and to develop mature incident reporting and breach management procedures.

6. Enhanced Transparency and Individual Rights

Promoted user-centric transparency and individuals' rights, generating trust in organisations' data handling practices and strengthening relationships both within and outside of the organisation.

The GDPR has raised awareness among individuals about the importance of transparency and trust in the digitised world. This, in turn, has forced organisations to innovate and invest in means to deliver transparency in a meaningful manner with tools that embed privacy by design and privacy by default (e.g., layered privacy policy, audiovisual contents, links to privacy controls, child-friendly delivery, and contextual algorithmic transparency).

Transparency has not just empowered individuals but has also required organisations to carefully consider and rethink their approaches to data processing. The GDPR has created opportunities to leverage privacy programmes to enhance customer trust and build privacy-aware brands; transparency has become a competitive advantage by increasing trust and credibility in the B2C as well as the B2B context.

The enhanced individual rights under GDPR also required organisations to update their processes to ensure individuals can exercise their rights effectively. While data portability under the GDPR has not had the uptake envisioned by lawmakers, the learning from GDPR data portability can serve as guidance for the interpretation of portability clauses under the EU DMA and the DA.[9] On the other hand, data subject access rights and the right to be forgotten are frequently addressed to organisations, and organisations have made strides in streamlining and automating the process to the benefit of the individual.

7. Stronger and More Effective Data Protection Authorities

The GDPR has resulted in better-resourced, staffed and more competent DPAs.

The GDPR substantially raised the responsibilities, powers, and, in most cases, the resources of the data protection supervisory authorities (DPAs), with the result of increasing their impact and effectiveness. Statistical data show a consistent rise in the number of staff and budgets allocated to the DPAs.[10] This increase in financial and human resources is a direct result of the GDPR. However, it has not always been enough to address the expanded responsibilities of DPAs. Both the express remit of the GDPR and the realities of the digitisation of the economy and society have made DPAs the key digital regulators and de facto arbiters of effective data protection, privacy rights for individuals, and responsible data use. This, in turn, meant that DPAs had to consider their effectiveness, develop strategies, and increase their in-house technical expertise. These are all essential for DPAs to be able to provide effective oversight, engagement, enforcement, and relevant guidance with respect to emerging technologies and the information society.

In the course of the last six years, DPAs presented varied approaches in terms of using innovative regulatory tools or providing constructive guidance. Some best practice examples include:

- **Regulatory Sandboxes:** The Norwegian Data Protection Authority (Datatilsynet) has implemented a regulatory sandbox aimed at fostering privacy-enhancing innovation and digitisation. Having already completed four rounds, this sandbox facilitates guidance and meaningful, structured engagement between organisations and regulators on specific projects. The Norwegian DPA recently declared this sandbox a permanent initiative. Other regulators, such as the UK and France, have also been actively implementing regulatory sandboxes.
- **Updated AI advice and AI-related initiatives:** The French CNIL issued seven helpful "AI how-to-sheets" to support organisations who intend to deploy AI with GDPR compliance questions. In Germany, the DPA of Hamburg issued a checklist for LLM-based chatbots, and the DPA Baden-Wuertemberg published a discussion paper on the legal basis for AI under the GDPR.[11] The UK ICO is issuing a set of guidance on the implementation of key data protection principles to GenAI and seeking active input and consultation.
- **Fast lane innovation hub:** The UK's ICO created a "fast lane" innovation advice service to assist organisations in putting new products on the market quickly and efficiently in the context of remaining GDPR questions. This service exists in addition to the ICO's existing regulatory sandbox.[12]
- **Guidance on Children's Privacy:** Several DPAs have issued constructive guidance on protecting children online. For example, the Irish DPA has released four documents addressing various aspects of children's data protection rights, providing in-depth guidance for organisations navigating compliance questions related to minors. The UK's Age Appropriate Design Code has become a de facto global standard against which incoming standards will inevitably be measured. Similarly, the French CNIL's recommendations for bolstering minors' online protection and the Spanish DPA's global strategy on children's privacy, which includes specific priority measures and practical proof of concept for age assurance tools, are further positive examples.

II. Challenges and Unfulfilled Promises of the GDPR

1. Accountability and the Risk-Based Approach Not Fully Realized

DPAs and the EDPB should effectively apply and proactively encourage the accountability principle and the risk-based approach inherent in the GDPR.

Despite being cornerstones of the GDPR, the accountability principle and the risk-based approach to compliance are not always recognised by DPAs. Organisational accountability places an obligation on organisations to implement risk-based privacy management programs with policies, procedures, tools and controls and to be able to demonstrate them. It is increasingly important for organisations as they seek to demonstrate their privacy compliance, enable digital transformation and build digital trust and confidence.

CIPL's research shows that there is real interest at the board and C-suite level in demonstrating the company's commitment to data privacy and responsible use of data. Also, many companies are realising a substantial and measurable return on investment from their privacy management programs.[13] Despite the benefits for all stakeholders, promoting accountability does not appear to be a top priority of many DPAs, and there appears to be little willingness to draw upon the seminal work of the EDPB's predecessor, the Art. 29 Working Party, and its Opinion on Accountability from 2012.[14] DPAs should promote and encourage accountability further and focus on real, effective and outcomes-focused accountability in behaviours by organisations rather than on compliance box-ticking.

Finally, it is not clear how DPAs strategically apply the risk-based approach to their own strategy-setting, as well as to their oversight, guidance and enforcement decisions, so that high-risk practices are prioritised, and low- or no-risk practices (or technical breaches) are deemphasised in their enforcement programs.[15] This risks the legislative intent of the GDPR and its effectiveness and impact in practice.

2. Conservative Interpretation of GDPR and Restrictions on Data Use

DPAs and the EDPB appear restrictive in their interpretation of the GDPR, creating challenges for legitimate, safe and beneficial uses of data.

The GDPR's stated goals extend to contributing to "economic and social progress" in addition to ensuring effective data protection (Recital 2). Economic and social progress depend, to a significant extent, both on effective data protection and the responsible use of personal data across the EU. Moreover, the harmonisation goals of the GDPR are an effort to remove an "obstacle to the pursuit of economic activities" (Recital 9). Finally, the GDPR recognises that data protection is not an absolute right and must be balanced against other fundamental rights and freedoms, including the right to establish a business, freedom of expression, security, and various other rights – data protection "must be considered in relation to its function in society" (Recital 4).

Therefore, any interpretation of the GDPR should be balanced with other fundamental rights and freedoms and also take into account a broader picture. This will be even more important as GDPR interacts and overlaps with many other key digital laws and regulations in the EU, such as competition, online safety and content moderation, children's rights, cybersecurity, health data space and other data sharing.

However, DPAs appear at times to be narrowly focused on the fundamental right of data protection without due consideration of other rights and interests, including those of stakeholders beyond the controller and data subject at issue. There is a trend for an increasingly restrictive interpretation of GDPR concepts and requirements, contrary to the original legislative intent, which clearly envisioned a proportionate balancing of rights. GDPR is intended to facilitate the responsible and accountable processing of personal data to provide benefits for individuals, people, organisations, and society; the aim should not be general prevention of processing personal data, especially at times when our society and economy are becoming more dependent on use and sharing of data.

Examples where DPAs have taken a conservative and restricted approach or where there may be tensions between GDPR and other digital regulations include:

- **Limitations on the processing of special categories of data:**
  - for the purpose of fraud prevention and detection, and for compliance with financial services regulations and regulatory expectations, e.g., processing data in accordance with Art. 9 and 10 GDPR for Know Your Customer (KYC) and Anti-Money Laundering (AML) checks[16] for international organisations where "public interest" is defined under EU law and may vary in its scope by member state;
  - to detect bias in AI applications (Art. 10(5) AIA refers to high-risk AI systems);
  - for initiatives aimed at promoting gender diversity and inclusion.
- **Restrictive application of the legal grounds of legitimate interest, contractual necessity, and public interest pushes organisations to seek consent, even when it may not be appropriate at close inspection.** In particular, some of the reservations that have been expressed regarding the legitimate interest legal ground are not well-placed, as they fail to recognise that this legal ground is actually accompanied by robust accountability and risk assessment obligations, delivering real protection for individuals.[17] It also fails to recognise that the GDPR provides other, often more effective means of protecting individuals' rights, such as transparency, redress, and accountability of organisations, including risk assessments and mitigations.
- **Expansive interpretation of "personal data", which renders concepts of anonymous and pseudonymous data unobtainable.** Anonymous data has become an impossibly high aspirational goal, with even a highly theoretical potential for re-identification, leaving such data classified as "personal data".[18] This frustrates the investment and innovation in anonymisation techniques and other PETs. Where encrypted data is in the hands of a third party without the encryption keys, for instance, it should be deemed non-personal data.[19]
- **The overly restrictive interpretation of the derogations under Art. 49 limits their use** beyond what was intended by the GDPR and supported by the CJEU.[20] This makes it challenging for organisations to have the necessary legal certainty to rely on those derogations.

3. Lack of Clarity and Consistency Regarding Risk Assessments

There is a real need for a clear, consensus-based and consistent approach to assessing risk under GDPR that aligns with new risk assessment obligations under incoming digital legislation.

The risk-based approach is firmly enshrined in the GDPR and has put risk assessments into organisations' core privacy practices. However, as CIPL has noted before, the full promise of the risk-based approach in GDPR is still elusive.[21] The EDPB continues to rely on the 2017 Working Party 29 Guidelines on risk, and some national DPAs have provided templates and tools, but there is no common baseline yet.[22] There is no consensus on what constitutes actual risks and harms to individuals,

both material and immaterial, and how to determine the likelihood and severity of such risk of harm, whether to focus on the immediate harm or include future harm.

It is important to note though, that the risk-based approach is not only relevant in the context of GDPR interpretation by the DPAs. Organisations, too, have a significant role to play in effectuating the GDPR's risk-based approach by producing meaningful and robust risk assessments that address the likelihood and severity of the harms and risks to individuals and documenting legitimate interest-balancing tests. A common complaint from regulators is that there is a lack of quality data privacy impact and risk assessments by companies. These regulators perceive that the risk assessments presented to them are not done at a sufficient level of detail or not done at all.

In sum, the risk-based approach is a foundational concept of the GDPR, and the legal requirement to assess risk is explicit and implicit in many of the GDPR provisions. Yet, both the DPAs and the organisations still appear to lack a consistent understanding of the GDPR's risk-based approach, the consensus on the risk taxonomy and the measurement of the likelihood and severity, and the mature risk-assessment policies and practices to apply to their own compliance or enforcement practices respectively. In addition, so far, there has been little direct incentivisation by DPAs for organisations to focus on risk-based accountability programs, controls, and tools in accordance with assessed risk. However, CIPL experience also shows that DPAs and organisations alike understand the need and the importance of honest and transparent dialogue to progress these issues.

Finally, new legislative acts such as the DSA, AIA, and DMA impose requirements for new risk assessments that will partially overlap with those in GDPR and will have to be integrated into organisational risk assessment processes.[23] This will require legal certainty around the requirements, but also regarding how to implement these complex risk assessments in practice with overlapping interests, risks and harms. There is a real need to build more dialogue and consensus among organisations, the DPAs, and any new enforcement regulators that will have different regulatory aims on how to identify, assess and classify different risks and harms to individuals stemming from the use of data. This will require not only the mindset for sincere cooperation but also a common understanding of the GDPR's and other legislations' goals. It is also important to note that in the context of data transfers, the risk-based approach, in effect, appears to have been rejected by some DPAs, which has led to legal uncertainty and significant compliance challenges for organisations.

4. Improper Use of Individuals' Rights

Organisations observe an increase in "misuse" of certain individuals' rights under GDPR.

Providing important and effective rights to individuals has been a core achievement of the GDPR. However, organisations are experiencing some challenges related to the interpretation of these rights and the potential for abuse. Given that organisations are given a very limited scope to consider data subject access requests as unfounded or vexatious, this opens the rights to being abused and even intentionally weaponised against organisations. For example:

- Sophisticated legal actors sometimes use the GDPR for pre-litigation discovery purposes to obtain records not otherwise available or for "fishing expeditions" in contentious litigations (e.g., employment litigation).
- Access requests may be used in the service of mass litigation threats against organisations of all sizes, seeking small individual payments in exchange for not commencing legal proceedings. This expends resources that should go towards responding to legitimate data subject requests.
- Other forms of "weaponisation" of subject access requests, such as mass submission of multiple access requests or use of access requests unrelated to a privacy issue or complaint, with sole objectives to "paralyse" an organisation, test their access procedures or obtain data for some other purpose.

5. Unrealised Potential of Certifications, Codes of Conduct, and BCR

The potential of GDPR certifications and codes of conduct to demonstrate programmatic accountability has not been realised; the full potential value of BCR has not been effectuated.

While there has been progress in the last couple of years, the GDPR regime on certifications and codes of conduct has still not been fully effectuated.[24] There are less than a handful of Europe-wide sectoral codes of conduct created and approved by DPAs, such as the EU Data Protection Code of Conduct for Cloud Service Providers. Industry should renew efforts to propose reasonable codes and standards in areas of continued concern. At the same time, DPAs should approach proposed codes in the spirit of cooperation and harmonisation across the Union.

Also, the expected scope of certifications appears unnecessarily limited. For example, certifications are currently envisioned to not cover entire privacy management programs, thereby losing their potential value as comprehensive accountability mechanisms under the GDPR. Such a limited scope of certifications and codes of conduct does not appear mandated by the text of the GDPR.

While not currently the case, Binding Corporate Rules could be recognised as a certification, which would add to their value to organisations. Moreover, at present, the process of adopting BCRs remains very burdensome and adversely impacted by the lack of coordination, consistency, and resourcing of DPAs. While having BCR provided a leg up in terms of compliance when the GDPR came into force, the adoption of BCR is still not routinely recognised by DPAs and clients as a significant privacy risk mitigant, a true demonstration of accountability and an advantage when it comes to transfer risk assessments and as such it does not deliver the full potential benefits to many organisations. It is, therefore, not surprising that less than 60 sets of BCRs have been approved since 2018.

To realise the full potential of BCRs, the process of having them approved should be simplified and streamlined. Also, appropriate recognition should be given to those organisations that adopt them in terms of demonstrating their accountability for data transfers and data protection compliance more broadly. Finally, according to GDPR Articles 46 and 47, it is possible to enable data transfers between BCR-approved/certified companies and DPAs, and the Commission should work to evolve BCR further in this way. For now, BCR remains a tool that only a few companies have the resources and the time to obtain and does not provide a viable alternative for smaller or more dynamic organisations.

Finally, DPAs should proactively encourage and incentivise the use of certifications and BCRs, as both deliver more effective data privacy compliance on the ground and are true accountability mechanisms. Yet, the latest guidance of the EDPB and increased requirements on BCR seem disproportionate vis-à-vis other transfer mechanisms, such as SCC. The result makes it less appealing for organisations to embark on the BCR route.

6. Undue Complexity Regarding International Data Transfers

Issues caused by *Schrems II* and data transfer restrictions create difficulties

Cross-border data transfers under the GDPR have become increasingly complex, resource intensive, and fraught with legal uncertainty as adequacy findings can be, and have been, subject to ongoing legal challenges calling into question their reliability.

The difficulties associated with GDPR-based data transfers are not only (or necessarily) the result of the actual GDPR transfer requirements but rather their interpretation by DPAs and the EDPB following the CJEU rulings, resulting in an increasingly limited and non-risk-based paradigm for data transfers to third countries. Organisations are describing internal "data transfer fatigue" caused by the extensive bureaucratic tasks associated with international data transfers, such as the obligation to conduct individual country-specific transfer impact assessments (essentially private sector "adequacy" determinations, including concerning foreign government access to data) and other restrictive interpretations of the GDPR's transfer requirements that ignore the risk-based nature of all GDPR protections.

The transfer impact assessments, in particular, are fraught with challenges for organisations, which will neither always have the resources, nor the expertise, or sufficient regulatory guidance to assess the adequacy of foreign data protection law and enforcement practices and to make decisions in that regard that are consistent from one organisation to another. They are, essentially, being asked to do a government's job of assessing third countries' adequacy. Indeed, the paucity of adequacy determinations by the Commission since the enactment of the GDPR calls into question asking individual organisations to make such determinations reliably and repeatedly with respect to the multitude of jurisdictions to which they transfer data. [25]

Data flows are imperative to the intrinsically global nature of the data economy and technology. They are essential to the economy, organisations, governments, society, and people in all countries, including Europe. A recent paper by CIPL describes multiple real-life cases where actual disadvantages to individuals can occur from restrictions in international data transfers and data sharing, including undermining cybersecurity-related tools and fraud prevention services, cloud computing and financial services, social media services and communication tools, and human resources systems.[26]

The disproportionate compliance burdens associated with data transfer governance have a tangible negative impact on organisations' ability to focus on more pressing compliance matters with a more direct impact on the protection of individuals. The non-risk-based approach of some European DPAs has ramifications not only for the organisations subject to their specific decisions but for anyone transferring data to jurisdictions outside the EU and countries with existing adequacy findings. This could not only significantly impact European business operations involving personal data transfers outside the EEA but eventually also negatively impact the EU's own digital trade policy and (so far) successful approach of exporting data protection standards.

7. Lack of Harmonisation Across the EU

Despite its legal nature and intention, the GDPR has not fully united the privacy landscape across the EU Member States

The GDPR, as a single set of rules across the EU, has been a strong incentive for organisations to drive operational efficiencies and to offer uniform products and services across the EU Digital Single Market. Harmonisation was intended to provide legal certainty for individuals and organisations operating digitally across the EU: the GDPR's Recital 7 states that "Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced." While the GDPR does provide for a single set of rules, it has not fully delivered on the goal of harmonisation.

Factors that play a role are: a) the margin of manoeuvre afforded by GDPR and used by Member States; b) differences in the interpretation of the GDPR requirements, including the approach to risk and compliance, primarily by the supervisory authorities, but also by privacy practitioners, lawyers and academia; and c) differences in procedural and administrative law across Member States. Specific examples include:

- Member states have made use of the margin of manoeuvre provided by the GDPR (so-called "opening clauses"). This has led to the creation of differing rules in important areas, such as the age of data protection consent under Art. 8 GDPR and the processing of sensitive[27] and biometric data.
- National interpretation of GDPR norms, guidance and enforcement by DPAs show that there are diverging views, interpretations, priorities and approaches between and among DPAs and between DPAs and the EDPB (e.g., the DPA of Baden-Würtemberg's view on data transfers with respect to employees working in third countries diverges from the EDPB's final version of guidance 05/2021 from February 2023 on Chapter V GDPR; the Dutch DPA's narrow interpretation of 'legitimate interest' under Art. 6 (1) (f) GDPR to the exclusion of any commercial interests, which prompted the European Commission to react critically in a letter to the DPA; and diverging interpretations related to the roles of controller and processor in the context of clinical trials).[28] The very different responses to the COVID-19 crisis in terms of permissible data processing were a clear reminder of the necessity for a more harmonised approach to creating legal certainty for organisations and individuals alike. This should include a harmonised

interpretation of key concepts such as "public interest" to ensure legal certainty for organisations processing data in accordance with Article 6 (1) (e) GDPR. Harmonisation will continue to be a challenge where different interpretations of basic GDPR principles persist.

- Member State procedural and administrative laws differ significantly. This impacts the workings of DPAs, individuals and organisations in the actual administrative process in front of DPAs, such as complaint handling, investigations and enforcement. In some member states, DPAs may have discretion in what complaints they will take forward and respond to, while others have to address every single complaint, which ties up significant resources. Another example is data breach notifications: while GDPR does not provide a right against self-incrimination in the context of reporting data breaches, in some jurisdictions, the *nemo tenetur* principle does govern DPA's investigative powers with respect to reported breaches (e.g., Germany[29]). This divergence between Member States can have an impact on the consistency of breach reporting decisions, for instance, as the presence or absence of this principle or right can skew breach reporting in both directions. This could be addressed, at least in part, by further EDPB guidance to ensure a harmonised approach to the application of mitigating factors under Art. 83 GDPR in breach scenarios.
- CIPL research also showed that DPAs can have inconsistent approaches to using demonstrated organisational accountability as a mitigating factor in enforcement. In CIPL's 2021 white paper *"Organizational Accountability in Enforcement – How Regulators Consider Accountability in their Enforcement Decisions"*, we examined global and EU regulator practices in considering demonstrated accountability as mitigating factors in their enforcement and fine-setting decisions, including under GDPR Article 83(2), and recommended that DPAs adopt a more consistent approach.[30]

Recitals 6 and 7 of the GDPR emphasise the importance of a coherent protection framework as a driver of trust in support of the digital economy and the free flow of data within the EU. Divergent interpretations of the GDPR provisions between the EDPB, DPAs, and, in some cases, Member States stand in contrast to this goal.

8. Unfulfilled Potential of the One Stop Shop Mechanism

The One Stop Shop mechanism has not always delivered the intended efficiencies.

The One-Stop-Shop mechanism (OSS) is an essential part of the consistent implementation of the GDPR. This innovative mechanism was to introduce integrated and consistent pan-EU oversight and enforcement with respect to cross-border processing activities to enable the free flow of data and reinforce the objectives for an EU single market. It is intended to provide both businesses and individuals with legal certainty regarding the competent regulator and ensure a more streamlined, consistent process and application of the GDPR. On the whole, the aim for OSS was to deliver the envisioned benefits on the ground, where the organisation and DPA cooperate and are able to develop the trusted relationship intended by the GDPR.

However, One Stop Shop does seem impeded at times by an apparent lack of cooperation and trust among DPAs themselves. Differences among DPAs in the interpretation of the GDPR requirements and approaches to risk and compliance, as well as the overly complex process for consistency and cooperation, have resulted in frustrations among complainants and affected controller or processor organisations alike. The lack of harmonised national administrative procedures has added to further complexities and legal uncertainties for all, which is currently being addressed by the proposed regulation laying down additional procedural rules relating to the enforcement of GDPR. However, the Proposal and, in particular, the European Parliament's approach in this regard has the potential to complicate the cooperation procedure even further and, as a result, undermine the functioning of the OSS.[31]

Importantly, the intent behind the OSS and the unique position of the Lead Supervisory Authority (LSA) in the OSS process is not only to provide a single interlocutor for organisations operating across the EU but to allow the LSA to develop a body of knowledge with respect to the organisations it oversees and expertise in their operations, to facilitate more effective oversight

and enforcement. Equally, the OSS is premised on the idea of constructive engagement and dialogue between the LSA and the organisations concerned. Finally, the GDPR deliberately gave larger weight to the LSA while also enabling other DPAs to engage in the process exceptionally, as and when appropriate. Advocate General Bobek rightfully stressed the elevated role of the LSAs, noting that "vis-à-vis cross-border processing, the competence of the LSA is the rule, and the competence of other supervisory authorities is the exception".[32]

There have been attempts, however, to move away from the central decision-making of the LSA and towards concerned supervisory authorities and the EDPB.[33] In some instances, local DPAs may send orders, request information, start audits, or impose fines directly on establishments present in their territory without first involving the lead DPA appointed by the organisations. The "relevant and reasoned objection[s]" as provided by Art 6(1)(a) GDPR, which are meant to be used as an exceptional intervention for CSAs, are being raised with some frequency. This has weakened, to a degree, the very purpose of the OSS mechanism and created a sense among some observers that the GDPR cooperation and consistency mechanism is not seen as a success by the EU institutions and Member States. There appears to be a reluctance to apply the same approach to other areas of digital regulation. This is a missed opportunity for providing a useful model in other regulatory areas.

In the context of harmonisation, CIPL welcomes the European Commission's proposal to further streamline and harmonise the GDPR enforcement process (GDPR Procedural Regulation). This proposal must uphold and/or strengthen the overall functioning of the OSS system and, specifically, preserve the unique role and authority of the LSA.

CIPL also believes that there is a need to revisit the OSS mechanism, assess how its application has moved on from the spirit and the intent of the legislator and what can be done to streamline the process and achieve the purpose of the OSS. There may be a need for a wider debate on the optimal GDPR oversight and enforcement model for the EU and its Member States. This will become even more pressing as there will be a further need for DPAs to collaborate and cooperate with the digital and sectoral regulators that are charged with overseeing other digital regulations, such as the DSA, DMA and EU AI Act, for example. Both organisations and individuals in the EU need legal certainty and predictability in how these rules will apply and interact.

9. Complaints and Breach Notification Burdens DPAs and Sideline from Other Oversight Tasks

Effective oversight and constructive engagement by DPAs have been obstructed by the requirement to address all complaints and an overly strict interpretation of data breach notification rules.

As mentioned above, some member state laws oblige DPAs to handle every complaint they receive, regardless of the risk level involved or the impact on individuals. This has led to a significant burden on regulators and limits the ability to prioritise non-enforcement-related tasks. Lacking a de minimis test for enforcement issues, DPAs may spend much of their time and resources in the role of complaint-handler rather than prioritising their activities based on risks and harms to individuals, engaging in constructive engagement, providing regulatory guidance, and thought leadership.[34]

Additionally, the 72-hour notification deadline under Article 33 GDPR creates an urgency to notify without giving controllers the ability to fully assess whether a notification is required in many cases. Controllers rush to notify the DPAs out of caution in cases where additional facts might later clarify that notification was not necessary. The incentives to over-report prevent controllers from focusing on implementing effective mitigation measures aimed at reducing current and future risks. Finally, there should be a real one-stop shop rule for breach notification reporting. This should encompass reporting only to LSE or a single SA rather than having to report the same breach to multiple concerned authorities without any form of centralisation of such reporting.

10. Focus on Enforcement over Engagement

DPAs have at times seemed to privilege enforcement actions over constructive engagement.

At times, DPAs have seemed to prioritise enforcement actions over constructive engagement with organisations. While the significant fines introduced by the GDPR have certainly created a focus on data protection as described above, a focus on issuing fines alone may miss the opportunity for meaningful ex-ante engagement. Direct engagement with data controllers and processors can have an immediate positive impact on the benefit of the individual and prevent the need for more formal enforcement after the fact. Given rapid technological advancements and changing realities, a genuine interest in cooperation from organisations and DPAs alike is vital. Engagement could take the form of dialogue and incentives for adopting preventative measures and other accountable data governance best practices, as well as guidance on important areas of GDPR that remain open to interpretation.[35]

11. Not Tech Neutral nor Future Proof

GDPR is not fully adapted to new developments in the digital economy

The interpretation of certain concepts and requirements of the GDPR may be in tension with emerging technologies, creating conflict with the advancement of technology and the reality of our digital society. For example:

- Anonymisation can be an important tool for making digitisation compatible with the GDPR. New digital legislation, such as the DMA, Data Act, or the European Health Data Space, are all integrating the use of anonymised data.[36] However, the GDPR only partially explains when data is actually anonymised in Recital 26. Also, the very high standard supported by many DPAs (including requiring a legal basis to anonymise data) is often not practicable and may even prevent the application of some privacy-enhancing technologies (e.g., synthetic data). There is a real need for a clear and pragmatic understanding of anonymisation that takes into account the practical implications of rapidly developing technologies and the context of incoming digital regulations.[37]
- The roles of "controller", "processor", or "joint controllership" must be seen in accordance with the realities of evolving data processing environments: service providers, such as cloud providers for example, who generally have the role of a "processor" are nevertheless controllers for some limited processing activities performed for purposes of their own business, such as fraud prevention measures, or processing of service data for billing purposes, or use of meta-data for cybersecurity purposes. Assessing the role of the controller or processor must remain fact-based on who determines purpose and means, also in the context of traditional service provider-customer relationships, such as SaaS offerings. Finally, joint controllership should be an exception rather than a rule, yet there seems to be a trend to often describe parties in a relationship as joint controllers without considering how these joint controllers may be able to comply with GDPR requirements in practice.
- Data minimisation may be seen in tension with the need for AI, and especially Generative AI, to learn on vast and diverse amounts of data, some of which will be personal data;
- An overly restrictive interpretation of purpose limitation will significantly limit the ability to use data for AI training, or AI application and generally re-use data for beneficial purposes not yet knowable at the time of collection, such as in the area of medical research.[38]
- There is a legal gap in the legal basis for processing sensitive personal data for bias detection or avoidance of discrimination in the training of AI models.

- Restrictive application of the research exemption, especially denying private sector organisations the ability to apply this exemption for their own research and development activities (which have grown considerably in many technology companies), will impede companies from conducting in-house R&D and developing secure and safe products, including with PETs.
- The very broad understanding of ADM Art. 22 provisions of GDPR in the CJEU's SCHUFA decision may have a chilling effect on the use of AI in other systems or services.

12. Inconsistencies With Other EU Digital, Sectoral or National Laws

The GDPR's promise to create a single and uniform set of rules for data protection across Europe has not been realised due to inconsistencies in sectoral laws.

As part of its digital strategy package, the EU has enacted or proposed a number of new legislative pieces since 2020, such as the Digital Markets Act, the Digital Services Act, the Data Governance Act, the Data Act, the European Health Data Space, and the AI Act. While these new pieces of legislation are generally intended to apply without prejudice to the GDPR, there is inevitable overlap by virtue of direct reference to the GDPR (e.g., Art. 5 DMA regarding consent) or because personal data is in scope. The danger is that these other laws may end up derogating from GDPR, hence eroding the delicate balance of the GDPR rules intended by the legislators. The relation of the GDPR to these new acts must be clarified, and inconsistencies must be eliminated for the continued functioning of the GDPR.[39]

Equally, DPAs, in their effort to embed data protection into the wider digital framework, must also be pragmatic and look at the broader picture and the strategic aims of other digital regulators and lawmakers. Future cooperation must be a two-way street and include multiple stakeholders to ensure that data protection continues to be considered in its function in society as envisioned by Recital 4 GDPR.

We list some of the problematic overlapping areas of digital and data compliance here:

- The CJEU has opened the door for competition authorities to consider data protection rules when deciding on competition issues. Effective personal data protection, as a fundamental right, cannot be hampered by decisions made to improve competition in the market. Without more clearly structured regulatory cooperation, as in the Dutch Digital Regulation Cooperation Platform, the UK's Digital Regulator Cooperation Forum (DRCF), or the newly formed Digital Cluster Bonn in Germany, there is a real danger of divergent interpretation over time, leading to increasing legal uncertainty. Moreover, regulatory cooperation forums at the national level should eventually be extended to the EU level to ensure consistency of interpretation between different national sectoral regulators.
- One example of inconsistency between the GDPR and other Digital Strategy acts relates to consent. GDPR provides organisations with a range of legal bases for processing personal data, and organisations can choose a basis that is appropriate to their particular processing activity. As a general rule, all legal bases for processing are on equal footing with one another, meaning that there is no default legal basis and no hierarchy between them.[40] However, a number of significant legislative and regulatory developments take a different approach, such as the Digital Markets Act and its seeming preference for consent as a legal basis for data combination and cross-use, as well as court rulings, such as the CJEU Bundeskartellamt decision specifying that data processing for personalised advertising may only be based on the user's consent. These interpretations appear to create a trend towards consent as the ultimate means of protecting the individual's personal data in the digital economy.[41] This has no backing in the GDPR and will ultimately contribute to further consent fatigue, leading to reflexive box ticking instead of informed decision-making.[42]
- Overreliance on consent can also have unintended consequences. For example:
    - The right to withdraw consent may place an individual with a private health insurance contract in a position to withdraw his or her consent to data processing so that the insurer is, effectively, no longer able to fulfil

the contract, which necessitates processing health data. Thus, the data subject could, in fact, cancel the contract by withdrawing his or her consent without having to respect the regular period of notice under German contract law.

— Requiring consent in the context of activities for data security and fraud prevention, such as for data combination and cross-use in the context of the DMA, could ultimately mean expecting malicious actors to consent to the very data processing intended to detect their bad behaviours.[43]

- The overlap between the GDPR and NIS2[44] reporting obligations has raised concerns. Cyber incidence reporting under NIS2 must happen with an initial notification within 24 hours, followed up by a more detailed report within 72 hours. Where such an incident under NIS2 contains personal data, organisations in scope for NIS2 and GDPR may find themselves under obligation to determine whether or not a notification is required under two overlapping regimes within very tight and different deadlines and under threat of penalty.
- Aligning the outdated ePrivacy Directive and the GDPR is becoming increasingly difficult since the ePrivacy Regulation has still not been adopted. Efforts by the EDPB to effectively expand the scope of ePrivacy through guidance to fill this gap create a real risk that ePrivacy becomes the de facto law of all internet-based data uses, given that it regulates electronic communications.[45]
- Data portability provisions under the DMA Art 6(9) and 6(10) lack the same level of individual protection as compared to the GDPR Art. 20(4). GDPR clarifies that the right to data portability may not adversely affect the rights and freedoms of others, whereas a similar reference is missing in the DMA. This creates tension and a risk of negatively affecting individuals since the data shared under these DMA provisions will inevitably include personal data. Effective personal data protection, as a fundamental right, should not be hampered by decisions made to improve contestability or fairness in the digital single market. Conversely, the GDPR should not be interpreted in a way that unnecessarily undermines effective competition and economic growth.
- Recent developments related to children's privacy and online safety also raise concerns regarding the ability to understand how these rights interlink together without any unintended consequences. This tension is further amplified by different approaches to age assurance, DSA requirements, and the upcoming CSAM Regulation.
- New policy initiatives, such as the ENISA's EU Cloud Certification Scheme (EUCS), have the potential to create additional challenges. For example, the EUCS, which currently has the potential to impose de facto data localisation measures on cloud service providers operating in the EU, is not aligned with one of the GDPR goals to: "foster free flow of personal data and <…> the transfer to third countries and international organisations".[46]

13. Changing role of the DPO

Restrictive interpretation of the DPO functional independence affected the value of the role within the organisation

As mentioned previously, the GDPR helped to reinforce the role of the DPO within organisations. However, recent CJEU decisions and certain DPA guidance have conveyed a more narrow and inflexible interpretation of functional independence and conflict of interests. This is in addition to complex dismissal procedures, which have the potential to create internal challenges for the role of DPO.[47] Where the interpretation of "functional independence" distances the DPO too far from the rest of the organisation, it has the potential to limit the intended and important impact of the role. It may have a perverse impact if the DPO does not "have a seat at the table" and does not act as a trusted business advisor and a business enabler, as well as the protector of individuals' rights. The EDPB Report on the role of the DPO also honed in on this issue and highlighted that DPOs lack reporting to the highest level of management.

14. Increased Costs and Administrative Burden

Some of the more prescriptive requirements of the GDPR have increased administrative burdens and compliance costs for all organisations

While the GDPR is principle and risk-based, it can, in some places, still be somewhat prescriptive, resulting in high administrative burdens, especially felt by smaller organisations. Examples of such increased administrative burdens include the substantial increase in required "paperwork", such as in the context of records of processing requirements and prescriptive DPIA requirements, and greater complexity in contracting and managing large numbers of third-party vendors. A particularly significant strain on resources for organisations of all sizes has been data transfer risk assessments (see discussion below). This is not to challenge legitimate and justifiable compliance costs; instead, the issue is that in the absence of legal clarity that compliance measures must be proportional and risk-based, such measures will trend beyond what is proportional to the risks at hand and will result in inefficiencies and unnecessary costs.

III. Recommendations

The following recommendations are based on the above points on the unresolved implementation challenges and unfulfilled promises of the GDPR. They can largely be implemented without substantive changes to the GDPR.

1. Focus on the harmonisation goal of GDPR

a. Foster mutual trust, sincere cooperation, and capacity building amongst DPAs

The EDPB should play a more proactive role in driving further consistency in the approach to and the interpretation of data protection rules, compliance and enforcement, not just through the formal consistency procedure for cross-border processing or enforcement but also through:

- creating formal, institutional fora for discussion (among regulators and with stakeholders) and building consensus on key compliance challenges and responses to these;
- exchanging views, experiences and staff;
- horizon scanning for new issues and emerging technologies and issuing early guidance;
- creating formal training to enhance business, legal and technology acumen and skills among DPAs;
- creating cross-DPA task forces and subject matter expert groups;
- introducing formal secondments with and from law firms and corporate legal departments;
- evincing greater openness to debating differences in opinion and interpretation with multiple stakeholders;
- building an understanding of the interplay between data protection and other digital and data regulatory areas (online safety, content, children's best interest, competition, AI, data sharing, digital assets, etc.).

b. Strengthen the One-Stop-Shop (OSS)

The OSS remains a critical tool for creating consistency and a harmonised approach in the most complex enforcement cases. The EDPB, as an EU body, should play a leading role in encouraging DPAs to actively participate in the OSS in the spirit of sincere cooperation, collegiality and mutual trust. As per the OSS, the EDPB should clarify that the lead authority is the single interlocutor for organisations and highlight practices that are not compliant with the OSS. DPAs should strive towards closer cooperation with each other in complex cases and respect the role of the LSA and its decision-making process.

As the guardian of the treaties and the digital single market, the EU Commission should also work with EDPB and Member States to ensure a collaborative and constructive approach to making the GDPR one single law in the EU. The proposed Regulation to further streamline and harmonise the GDPR enforcement process is most welcome, but it must ensure that the OSS is not ultimately weakened by it.[48]

c. Harmonise GDPR Guidance

Diverging guidance on the same issues from different DPAs and the EDPB creates legal uncertainty for organisations and individuals and undermines the GDPR's harmonisation goal. To achieve the harmonisation envisioned by the GDPR, the DPAs should ensure a more centralised and harmonised approach to regulatory guidance, including in non-cross-border matters. Where it exists, organisations should be able to abide by the national guidance of their lead authority for their EU cross-border operations; national DPAs should endorse each other's existing guidance instead of adding potentially diverging new ones.

2. Provide realistic and evolving guidance and interpretation of the GDPR

a. Give effect to the GDPR's risk-based approach

To enable scalable and effective compliance, DPAs should acknowledge and apply the risk-based approach as originally intended and as set forth in the text of the GDPR. This means that accountability and all compliance measures, mitigations and controls, including in the data transfer context, must be risk-based and proportional to the actual risks at hand. Data protection is not an absolute right and must be duly balanced against other rights.

b. Recognize the co-equal status of the legal bases for processing

The GDPR does not rank or prioritise the six co-equal legal bases, and consent should not be seen as the default or most important legal basis. DPAs should clarify their understanding of this fact.

c. Resist restrictive interpretation by default and develop more pragmatic guidance

As technology has evolved and data uses have become more complex, additional guidance is needed on concrete points of concern that could be addressed without amendments to the law, such as the following:

i. The **roles and obligations of the actors involved** in the processing of personal data in complex environments, such as the payments infrastructure, cloud computing, or the AI value chain, where multiple players are acting to varying degrees on the purpose and means of the data processing carried out.

ii. Updated and clearer guidance on how organisations should approach **data subject requests** in the context of their commercialisation and inappropriate "weaponisation" for purposes of pre-trial discovery often not foreseen under national law.

iii. Updated guidance with respect to the **definition and use of anonymous and pseudonymous data**,[49] as well as the role of Privacy Enhancing and Privacy-Preserving Technologies (**PETs and PPTs**) in that context.[50] The latter would be particularly important in the context of incoming new digital legislation, such as the DMA, that requires anonymisation for data-sharing obligations.

d. Clarify guidance for lawful processing of special categories of data, including biometrics

A modernised and practical approach to the processing of special categories of data, including biometrics data, is needed to enable diversity and inclusion programs, train AI systems, and improve accuracy and fairness.

e. Clarify guidance on the role of the DPO

Guidance on the role of the DPO should be updated; a too narrow interpretation of functional independence and conflict of interests may limit the ability of the DPO to meaningfully interact with the highest level of management.

f. Transparency and Constructive Engagement with Stakeholders

CIPL has been advocating for an inclusive multistakeholder process for producing guidance. This would include dialogue between regulators and regulated organisations even before a first draft is produced through a pre-

consultation phase with input from relevant industry and other stakeholders. This would enable DPOs and other experts with practical experience to provide insights and comment on technical and operational issues. Early involvement and other opportunities for open dialogue through "fab-labs" and similar initiatives will ultimately yield more practical and relevant advice and would be more efficient than only allowing formal responses to consultations with short deadlines. Moreover, the EDPB should consider the input made during the public consultation stage of any draft guidance in a more substantial manner in order to avoid scenarios when the guidelines remain completely unchanged after multiple stakeholder inputs. A best practice would be for regulators to publish commentary on why they either adopted or declined to adopt specific recommendations.

3. Incentivize best practices and accountability

DPAs have a range of tools available to incentivise best practices and accountability, including relying on demonstrable accountability practices or the use of PETs as a mitigating factor in enforcement and when setting fines.[51] DPAs should explicitly clarify to organisations the benefits of demonstrable accountability as a way to encourage good organisational behaviours. Such ex-ante encouragement could substantially improve compliance and data protection outcomes for individuals and reduce the need for ex-post enforcement actions.

4. Create pragmatic solutions to streamline international data transfer requirements and facilitate trusted data flows

As discussed above, the importance of international data transfers cannot be overstated, and the current approach to data transfers is often becoming too complex to be manageable and detracts resources. Recommended improvements include the following:

a. Recognize and apply the GDPR's risk-based approach to data transfers

DPAs should acknowledge that the GDPR does not take a "zero risk" approach to data transfers but requires that safeguards for transferred data be proportional to the actual risk at hand.

b. Provide country "adequacy" guidance

The EDPB, together with the Commission, should engage with stakeholders to develop practical "Adequacy Light" guidance that is sector or industry-specific for different third countries, which can be used especially by SMEs and mid-sized organisations with fewer resources as part of their transfer risk assessments.

c. Work towards convergence on international data transfers and evolving transfer mechanisms

Global data flows demand multilateral transfer solutions and governance. EU DPAs, as well as policy-makers, should make every effort to further advance international data transfer interoperability, such as through efforts to align with the Global CBPRs and PRPs, promoting interoperability of standard contractual clauses, collaborating with global stakeholders on developing and/or promoting principles for government access requests for law enforcement and national security purposes, with the ultimate goal of creating a trusted multilateral framework for accountable data transfers that, among other things, is risk-based.

In addition, this work should include developing appropriate GDPR certifications and codes of conduct that can serve as transfer tools capable of becoming interoperable with Global CBPR and PRP.

In addition, the administrative process to obtain BCRs should be made easier, and the applicability and usefulness of BCRs should be broadened to allow transfers between all organisations that have BCRs and the approval process streamlined to make them attainable for SMEs. BCRs should also be recognised as valid GDPR certification, indicating the GDPR compliance of an entire privacy and data management program.

d. Interpret GDPR derogations more effectively and pragmatically

The current prevailing interpretations of the derogations in Chapter V of the GDPR are often interpreted very narrowly in ways not mandated by the GDPR. Their interpretation should be revisited. The protections for cross-border data transfers must be risk-based, meaning proportional to the likelihood and severity of the risks of a particular data transfer.[52]

e. Increase legal certainty in data transfers

The European Commission could take the following steps to increase legal certainty for data transfers:

i. Adopt a comprehensive, as well as more proactive and time-sensitive strategy for the adoption of additional adequacy determinations that also affirms the importance of the risk-based approach in the context of adequacy determinations and is also in alignment with the EU's digital trade strategy.

ii. Increase the transparency of the adequacy assessment process, including when it comes to assessing government access to personal data.

5. Enhance GDPR adaptability to the evolving digital economy and society

a. Facilitate alignment between the GDPR and new digital regulations and between relevant regulators

With the proposals and adoption of new digital laws overlapping with the GDPR, such as the AI Act, the Data Act, DSA, and DMA, there is an absolute need for:

i. additional guidance and considerations on how the overlapping or conflicting legal requirements in the digital package laws and GDPR should work and

ii. clearer alignment between DPAs and other regulators with competencies under these laws. This should involve common strategic considerations and mechanisms similar to the UK's DRCF model to ensure longer-term certainty for organisations active in the EU economy.

b. Technical expertise of DPAs

DPAs require the necessary funding to develop in-house technological expertise to ensure the DPAs' competence and effectiveness as digital regulators. Such technological expertise will enable DPAs to develop more relevant and pragmatic guidance that is grounded in a clear understanding of the technical realities of the modern data economy.

c. Support SMEs' ability to comply

Making compliance more manageable for SMEs should be an important goal. One of the longstanding criticisms of the law is that it is too bureaucratic and difficult to understand, particularly for many SMEs, and many compliance obligations are unduly burdensome for smaller organisations. Finding interpretations that reduce complexity for SMEs while maintaining core protections for individuals would help SMEs, individuals, and the EU's digital economy.[53] Also, GDPR certifications and codes of conduct designed for SMEs, particularly programmatic certifications and codes of conduct, could offer a constructive solution.

6. Adopt an "outcome-based" and risk-based approach to oversight, regulation and enforcement

DPAs may consider developing or strengthening an "outcome-based approach" to oversight, regulation, and enforcement. This would emphasise greater understanding of outcomes that need to be achieved behind a legal requirement, the means of achieving these outcomes in the most effective way and emphasising guidance, constructive engagement and co-regulating together with regulated entities to reach these outcomes and reduce the need for enforcement.[54] Ultimately, non-compliance and enforcement are not a sign of effective regulation and good outcomes.

This approach would also enable regulators to be more risk-based in all their activities – from setting the strategy to executing that strategy, from guidance, supervision and enforcement. In the times when regulators' resources are increasingly being disproportionate to the regulatory challenges and needs of the market, regulators need to "be selective to be effective" – they must focus their resources and strategies on key areas that represent high risks for data protection and rights of individuals and those areas that have maximum impact and implicate most of the public interest.

Enforcement should be used as a last resort, when appropriate, for gross or intentional misconduct, non-compliance and repeated offences. In modern regulation and regulatory behaviours, theory and practice, deterrence and punishment have proven to have limited effectiveness in achieving the desired result of effective data protection.[55] DPAs should balance enforcement with meaningful stakeholder engagement, thought leadership, guidance, co-regulatory approaches (such as codes and certifications) and sandbox initiatives. These non-enforcement-related regulator tasks and responsibilities can be substantially more impactful in achieving the desired outcomes of the GDPR.

Endnotes

1 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 90+ member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/ Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

2 CIPL received 24 individual responses from leading companies with a presence in the European Union.

3 CIPL GDPR Stocktaking Report - GDPR One Year In - Practitioners Take Stock of the Benefits and Challenges, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_report_on_gdpr_one_year_in_-_practitioners_take_stock_of_the_benefits_and_challenges.pdf.

4 CIPL Response to the EU Commission's Public Consultation on the Evaluation of the GDPR, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_eu_commission_consultation_on_gdpr_evaluation__28_april_2020_.pdf.

5 Cisco-CIPL Report on Business Benefits of Investing in Data Privacy Management Programs, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cisco-cipl_report_on_business_benefits_of_investing_in_data_privacy_management_programs__10_jan_2023_.pdf

6 See also CIPL White Paper "Understanding the Role of PETs and PPTs in the Digital Age", https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-understanding-pets-and-ppts-dec2023.pdf.

7 See CIPL report with Cisco Center for Excellence, Business benefits in Data Privacy Management Programs, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cisco-cipl_report_on_business_benefits_of_investing_in_data_privacy_management_programs__10_jan_2023_.pdf

8 What Good and Effective Data Privacy Accountability Looks Like: Mapping Organisations' Practices to the CIPL Accountability Framework, May 2020. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_mapping_report__27_may_2020__v2.0.pdf.

9 CIPL Discussion Paper "Data Sharing Obligations Under the DMA: Challenges and Opportunities", available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/data_sharing_obligations_under_the_dma_-_challenges_and_opportunities_-_may24.pdf.

10 European Data Protection Board, Contribution of the EDPB to the report on the application of the GDPR under Article 97, 2023, available at https://edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-report-application-gdpr-under-article-97-2023_en, p 28-29.

11 The Hamburg Commissioner for Data Protection and Freedom of Information, "Checklist for the use of LLM-based chatbots", available at https://datenschutzhamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/20231113_Checklist_LLM_Chatbots_EN.pdf; Baden-Wurttemberg SA Discussion Paper, "Legal bases in data protection for the use of artificial intelligence", available at https://www.baden-wuerttemberg.datenschutz.de/legal-bases-in-data-protection-for-ai/.

12 Efforts by the UK ICO and Norway's Datatilsynet are included due to their proximity to GDPR and similarities in data protection systems.

13 CIPL/CISCO Report "Business Benefits of Investing in Data Privacy Management Programs, January 2023", available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cisco-cipl_report_on_business_benefits_of_investing_in_data_privacy_management_programs__10_jan_2023_.pdf

14 For example, the Working Party 29, Opinion 3/2010 on the principle of accountability states that: "In summary, the above shows the critical need for data controllers to apply real and effective data protection measures aimed at good data protection governance while minimising the legal, economic and reputational risks that are likely to derive from poor data protection practice. As further developed below, accountability-based mechanisms aim at delivering these goals".

15 CIPL Paper "Regulating for Results Paper - Regulating for Results: Strategies and Priorities for Leadership and Engagement"

16 Which in turn aids the fight against organised crime which is in large parts financed by money laundering.

17 See CIPL White Paper "How the "Legitimate Interests" Ground for Processing Enables Responsible Data Use and Innovation", 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; and CIPL Legitimate Interest Paper - CIPL Examples of Legitimate Interest Grounds for Processing of Personal Data, 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.

18 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

19 Important to consider the recent CJEU judgement in Single Resolution Board v. European Data Protection Supervisor (Case T-557/20), where the Court ruled that in order to determine whether an individual is identifiable, account should be taken of all means reasonably likely to be used, and that this test must be performed from the perspective of the recipient/holder of the data. In other words, the determination of whether data is personal or not, and anonymised or not, must be made from the point of view of the organisation that has (and is using) the data—a processor or a third-party service provider, or another business receiving the data set. This ruling has been interpreted by some to mean that if the decryption key is inaccessible, then the data could be deemed anonymous.

20 In case C-316/18, the CJEU states: "As to whether it is appropriate to maintain the effects of that decision for the purposes of avoiding the creation of a legal vacuum, the Court notes that, in any event, in view of Article 49 of the GDPR, the annulment of an adequacy decision such as the Privacy Shield Decision is not liable to create such a legal vacuum. That article details the conditions under which transfers of personal data to third countries may take place in the absence of an adequacy decision under Article 45(3) of the GDPR or appropriate safeguards under Article 46 of the GDPR.". In addition, we highlight the statements made by Prof. Dr Von Danwitz, the judge-rapporteur in the CJEU *Schrems I and II* cases, explaining that GDPR Articles 46 and 49 cover the absence of an adequacy decision and that the derogations under Article 49 GDPR are not so narrow that they restrict any kind of transfer, recording available here: https://www.youtube.com/watch?v=2hyETsfhErg&t=8590s; The EDPB noted that "Article 49 GDPR has an exceptional nature. The derogations it contains must be interpreted restrictively and mainly relate to processing activities that are occasional and non-repetitive".

21 See Centre for Information Policy Leadership Risk Paper - Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf.

22 Some notable examples include: CNIL Privacy Impact Assessment software, methodology, templates and knowledge bases, available at https://www.cnil.fr/en/privacy-impact-assessment-pia; AEPD Template for DPIA report for private sector, available at https://www.aepd.es/es/documento/modelo-informe-EIPD-sector-privado-en.rtf; AEPD GDPR Risk Assessment Tool, available at https://evalua-riesgo.aepd.es/index_en.html.

23 Article 34 of the Digital Services Act requires providers of very large online platforms and of very large online search engines to diligently identify, analyze and assess any systemic risks in the Union stemming from the design or functioning of their service and its related systems, including algorithmic systems, or from the use made of their services. In addition, Article 9 of the AI Act (unofficial final text) imposes an obligation to establish, implement, document and maintain a risk management system in relation to high-risk AI systems. This requires the analysis of the known and the reasonably foreseeable risks that the high-risk AI system can pose to the health, safety or fundamental rights when the high-risk AI system is used in accordance with its intended purpose. Finally, Article 11 of the Digital Markets Act requires designated gatekeepers to provide the Commission with a report (within 6 months after their designations) describing in a detailed and transparent manner the measures they have implemented to ensure compliance with the obligations prescribed under the regulation.

24 Council of the European Union (2023) Council position and findings on the application of the GDPR (Doc. No. 13775/23).

25 In addition Art. 36 of the Data Act will impose similar assessments for non-personal data.

26 Centre for Information Policy Leadership and TLS Discussion Paper I: The Real Life Harms of Data Localization Policies, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-tls_discussion_paper_paper_i_-_the_real_life_harms_of_data_localization_policies.pdf.

27 For instance in Germany a number of individual laws determine data protection in the health care context.

28 A copy of the letter can be found here: https://static.nrc.nl/2022/pdf/letter-dutch-dpa-legitimate-interest.pdf

29 Section. 43 (4) BDGS " A notification pursuant to Article 33 of Regulation (EU) 2016/679 or a communication pursuant to Article 34 (1) of Regulation (EU) 2016/679 may be used in proceedings pursuant to the Administrative Offences Act against the person required to provide a notification or a communication or relatives as referred to in Section 52 (1) of the Code of Criminal Procedure only with the consent of the person required to provide a notification or a communication."

30 CIPL White Paper - Organizational Accountability in Data Protection Enforcement - How Regulators Consider Accountability in their Enforcement Decisions, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_organizational_accountability_in_data_protection_enforcement_-_how_regulators_consider_accountability_in_their_enforcement_decisions__6_oct_2021__3_.pdf.

31 See the European Commission Proposal on laying down additional procedural rules relating to the enforcement of the GDPR, available here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023PC0348; and CIPL and Hunton Andrews Kurth Opinion Piece analysing the proposed Regulation and European Parliament's Report, available here: https://www.huntonprivacyblog.com/2024/02/13/the-european-commission-draft-gdpr-procedural-regulation-and-european-parliament-draft-libe-report-on-the-road-to-harmony/.

32 Opinion of the Advocate General Bobek in Case C-645/19, para 47: "Therefore, it seems rather clear to me from the text of the GDPR that, vis-à-vis cross-border processing, the competence of the LSA is the rule, and the competence of other supervisory authorities is the exception".

33 See discussion in CIPL and Hunton Andrews Kurth Opinion Piece analysing the proposed Regulation and European Parliament's Report, available here: https://www.huntonprivacyblog.com/2024/02/13/the-european-commission-draft-gdpr-procedural-regulation-and-european-parliament-draft-libe-report-on-the-road-to-harmony/.

34 CIPL Paper "Regulating for Results Paper - Regulating for Results: Strategies and Priorities for Leadership and Engagement", available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_final_draft_-_regulating_for_results_-_strategies_and_priorities_for_leadership_and_engagement_2_.pdf.

35 Prof. Christopher Hodges suggests an Outcome-Based Cooperation Regulation (OBCR) model, in which regulators to "co-create" with industry and other stakeholders by agreeing on common purposes and desired outcomes. According to Hodges, scientific research has shown that this model is superior to the traditional "rule-breach-enforcement" model that banks on deterrence. Reserving "hard enforcement" only "as a last resort," OBCR encourages ex-ante constructive engagement between regulators and regulated entities, as well as guidance on best practices and other supportive measures; it seeks to account for the goals of business (commercial success and profit) and the goals of governments, regulators, and societies (economic growth and protection from harm) with acceptable risk. OBCR is based on trust, requiring all stakeholders (including regulators) to show that they are trustworthy. OBCR aims to create a framework that supports cooperation rather than conflict in regulation. See Christopher Hodges, Supporting Cooperative Behavior, July 20, 2022, available at https://www.indr.org.uk/_files/ugd/6b9149_c7e339a0f5dd4999a220d609573d6352.pdf; Christopher Hodges, An Introduction to Outcome Based Cooperative Regulation (OBCR), available at https://55c366d1-05de-46e1-a383-a8f804514d8a.filesusr.com/ugd/6b9149_9424aee004ff4051bd67025c867f1f79.docx?dn=2202%20An%20Introduction%20to%20OBCR.docx; Christopher Hodges, Outcome-Based Cooperation - In Communities, Business, Regulation, and Dispute Resolution, 2022, Bloomsbury Publishing, available at https://www.bloomsbury.com/us/outcomebased-cooperation-9781509962495/; Christopher Hodges, Ethical Business Regulation; Growing Empirical Evidence, 2016, available at https://assets.publishing.service.gov.uk/media/5a800de040f0b62305b88e56/16-113-ethical-business-regulation.pdf.

36 Article 6(11) DMA states the following: "The gatekeeper shall provide to any third-party undertaking providing online search engines, at its request, with access on fair, reasonable and non-discriminatory terms to ranking, query, click and view in relation to free and paid search generated by end users on its online search engines. Any such query, click and view data that constitutes personal data shall be anonymised".

37 The CJEU appears to take a more subjective view of anonymisation. The upcoming EDPB Guidelines on anonymization should take this into account. See Single Resolution Board v. European Data Protection Supervisor (Case T-557/20), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62020TJ0557.

38 The proposed EHDS Regulation would impose purpose limitations for the secondary use of data with a list of authorised and unauthorised data processing. However, it raises concerns that this will fulfil the high GDPR bar in this regard.

39 See also CIPL DMA discussion paper https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_dma_limiting_legal_basis_may2023.pdf.

40 Article 8 (2) of the Charter of Fundamental Rights, in whose light the GDPR must be read, also stipulates to "with the consent of the person concerned or some other legals basis laid down by law" with regards to when personal data may be processed.

41 See an excellent and extensive analysis by Martin Nettesheim, Data Protection in Contractual Relationships Art. 6(1) (b) GDPR, April 2023, p. 26 following.

42 CIPL Infographic "A Day in the Life – Data Consent", available at https://www.informationpolicycentre.com/cipl-blog/a-day-in-the-life-data-consent.

43 CIPL White Paper - 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.

44 Art. 31(3) NIS2 (Directive 2022/2555 on measures for a high common level of cybersecurity across the Union) stipulates that competent authorities should cooperate with DPAs in the case of incidents resulting in personal data breaches, but that does not necessarily alleviate the concerns of organisations in scope.

45 Please see the recent EDPB draft Guidance on the interpretation of ePrivacy Directive Art. 5(3) https://edpb.europa.eu/our-work-tools/documents/public-consultations/2023/guidelines-22023-technical-scope-art-53-eprivacy_en and CIPL response to the public consultation on the draft Guidelines https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_public_consultation_on_edpb_guidelines_2_2023.pdf.

46 GDPR Recital 6.

47 Cases C-534/20 – Leistritz and C-453/21 – X-FAB; European Data Protection Board Report - Coordinated Enforcement Action, Designation and Position of Data Protection Officers, available at https://www.edpb.europa.eu/our-work-tools/our-documents/other/coordinated-enforcement-action-designation-and-position-data_en.

48 See also https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_ec_proposal_on_gdpr_procedural_regulation_3_september_2023.pdf.

49 Council of the European Union (2023) Council position and findings on the application of the GDPR (Doc. No. 13775/23).

50 In this context, CIPL proposes to take into account the US FTC model for anonymization. The FTC model requires reasonable technical anonymisation, coupled with a legal prohibition against re-identification (with exceptions for when re-identification is necessary) and contractual and administrative safeguards against re-identification. CIPL believes that this combination of safeguards provides an effective and practical standard, given that technical measures alone are not sufficient to ensure true anonymisation. Basing an approach to anonymisation on theoretical rather than practical standards creates a "no-go" zone for anonymous data. This standard could provide a safe harbour for organisations looking to use previously identifiable data for research and other socially beneficial purposes. Also see, United States Federal Trade Commission Report "Protecting Consumer Privacy in an Era of Rapid Change -- Recommendations for Business and Policymakers", March 2012, at p. 20-21, available at https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers.

51 CIPL Paper - Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability, available at: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_2_-_incentivising_accountability_-_how_data_protection_authorities_and_law_makers_can_encourage_accountability.pdf; CIPL White Paper - Organizational Accountability in Data Protection Enforcement - How Regulators Consider Accountability in their Enforcement Decision, available at: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_organizational_accountability_in_data_protection_enforcement_-_how_regulators_consider_accountability_in_their_enforcement_decisions__6_oct_2021__3_.pdf.

52 Please see Prof. Christakis Paper The "Zero Risk" Fallacy: International Data Transfers, Foreign Governments' Access to Data and the Need for a Risk-Based Approach, which reviews the current approach to data transfers critically and provides insight into the risk based approach of Chapter V GDPR, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/the_zero_risk_fallacy_-_t.christakis_feb24.pdf.

53 Council of the European Union (2023) Council position and findings on the application of the GDPR (Doc. No. 13775/23).

54 CIPL Paper "Regulating for Results Paper - Regulating for Results: Strategies and Priorities for Leadership and Engagement", available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_final_draft_-_regulating_for_results_-_strategies_and_priorities_for_leadership_and_engagement_2_.pdf.

55 See Christopher Hodges, Supporting Cooperative Behavior, July 20, 2022, available at https://www.indr.org.uk/_files/ugd/6b9149_c7e339a0f5dd4999a220d609573d6352.pdf; Christopher Hodges, An Introduction to Outcome Based Cooperative Regulation (OBCR), available at https://55c366d1-05de-46e1-a383-a8f804514d8a.filesusr.com/ugd/6b9149_9424aee004ff4051bd67025c867f1f79.docx?dn=2202%20An%20Introduction%20to%20OBCR.docx; Christopher Hodges, Outcome-Based Cooperation - In Communities, Business, Regulation, and Dispute Resolution, 2022, Bloomsbury Publishing, available at https://www.bloomsbury.com/us/outcomebased-cooperation-9781509962495/; Christopher Hodges, Ethical Business Regulation; Growing Empirical Evidence, 2016, available at https://assets.publishing.service.gov.uk/media/5a800de040f0b62305b88e56/16-113-ethical-business-regulation.pdf.

About the Centre for Information Policy Leadership

CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 90 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at

http://www.informationpolicycentre.com/.

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

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

Brussels Office
Avenue des Arts 47-49
1000 Brussels
+32 2 643 58 00

24260.0524