Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Centre for Information Policy Leadership's Response to the EU Commission Consultation on the Evaluation of the GDPR

The Centre for Information Policy Leadership (CIPL)[1] submits this response (the Paper) as input for the EU Commission's upcoming Report on the GDPR. This Paper builds and expands on CIPL's 2019 report "GDPR One Year In: Practitioners Take Stock of the Benefits and Challenges",[2] which summarised the benefits, challenges and unfulfilled promises of the GDPR for organisations.

I. Companies continue to derive benefits from the GDPR

CIPL confirms that in 2020, the GDPR continues to act as a driver of benefits for organisations by:

- Turning data protection into a mainstream business issue, beyond just legal and compliance;
- Creating momentum and focus on data protection, providing businesses with the opportunity to level-set their practices with other organisations and enabling a shift in organisational approaches to data protection through the implementation of comprehensive privacy compliance programmes;
- Aligning data protection with organisations' digital transformation, data strategy and data-driven innovation, and instilling good data hygiene and governance, thereby enabling organisations to use data responsibly;
- Forcing organisations to deliver more user-centric transparency to individuals and to reassess or build effective processes for responding to individual rights requests, resulting in improved relationships with individuals;
- Enabling more effective protection and fostering enhanced trust from individuals, business partners and investors;
- Removing burdensome notification and authorisation requirements with DPAs;
- Fostering consistency in assessing data protection risks and mitigating them;
- Impacting the business bottom line, by creating a positive return on investment from accountable practices and making data protection a strategic business driver and market differentiator;[3] and
- Making it easier to engage in international business by encouraging organisations to address data protection globally across all business lines, products, services and locations and setting a global baseline for data protection law that serves as a reference for other countries and enables economic efficiency.[4]

II. Addressing the challenges and promises of the GDPR

While the tangible benefits of the GDPR are still evident in 2020, unfortunately, so are the challenges and unfulfilled promises already highlighted by CIPL in 2019. Yet, organisations continue to invest significant resources into GDPR compliance while technology continues to evolve and to create tensions with legal norms. In addition, the COVID-19 crisis has also put into sharp focus the need for progressive GDPR interpretation while confirming the enormous potential of data in helping address this worldwide crisis. This ever-changing environment and the promises of beneficial data uses call for a shift in the approach to leverage the GDPR provisions to their fullest extent going forward.

CIPL considers that because of GDPR's principle-based, outcome-based and risk-based approach, it constitutes a solid foundation for building effective protection and trust for individuals while enabling the digital economy, including at time of crises. This Paper does not advocate for a formal review of the GDPR at this stage, as CIPL believes that the current challenges with the application of the GDPR can be resolved by the Commission, the EDPB and data protection authorities (DPAs) using the existing institutional and regulatory mechanisms and their wide interpretative powers. CIPL believes it useful to consider the current challenges of the GDPR beyond the limited points in Article 97(2) GDPR.

Consequently, we group CIPL's evaluation and recommendations in four categories:

1. **Short-term actions to make GPDR implementation more efficient, including on Article 97(2) topics;**

2. **Improvements to the EDPB and DPA collaboration and engagement;**

3. **Progressive interpretation of some of the GDPR's key substantive requirements; and**

4. **Long-term positioning of the GDPR in the broader digital landscape.**

1. Short-Term Actions to Make the Functioning of the GDPR More Efficient

1.1 International Transfer Tools (Article 97(2) topic)

Some organisations report that due to the legal uncertainty associated with data transfer tools, controller-processor relationships try to increasingly exclude cross-border data flows in order to be compliant. This, in effect means more data localisation and less free flow of data. Due to the importance of international data transfers in digital economies, CIPL reiterates the urgent need to have operational and flexible international data transfer mechanisms including:

- Updated GDPR-compliant SCCs. Importantly, CIPL disagrees with the EDPB that this should include SCCs for transfers back from EU processors to non-EU controllers;[5]

- Acknowledgement of the importance and robustness of the Privacy Shield as well as adoption of further adequacy decisions;

- More Binding Corporate Rules (BCRs) reviewed by the DPAs and approved by the EDPB[6] for controllers, processors and entities engaged in a joint economic activity; and

- EU-wide certifications and codes of conduct that can work both as accountability tools and cross-border transfer mechanisms.[7]

Considerate guidance should also be provided on how organisations should manage requests of law enforcement authorities, including in the UK, post Brexit. Organisations cannot be put in a position where they have to choose between complying with a law enforcement request or complying with the GDPR provisions.

Summary of CIPL Recommendations:

The EU Commission and the EDPB should provide a complete transfer toolkit to organisations to enable data transfers.

1.2 Cooperation, Consistency and One-Stop-Shop (Article 97(2) topic)

Smooth cooperation between DPAs and proper functioning of the consistency mechanism are essential to the harmonised implementation of the GDPR both in terms of substantive law and enforcement. It is also intended to benefit organisations that should, through the One-Stop-Shop (OSS) mechanism, work with a single-lead DPA through their main establishment for all their cross-border data processing. It appears however that this framework does not always function optimally and sometimes creates more bureaucracy than consistent and effective data protection.

First, the concept of "**main establishment**" may sometimes be ill-adapted to the realities of complex cross-border organisations that may have multiple decision-making centres located in several Member States, or in a combination of Member States and third countries. (This situation is expected to increase after Brexit). In this case, there is neither a satisfactory way to designate a main establishment nor a possibility to appoint a representative. The EDPB should consider this complexity to enable organisations to identify their lead authority more easily.

Second, CIPL considers that the OSS is more than just a way to allocate enforcement cases between DPAs. It should also enable organisations to **interact with a single regulatory interlocutor** in the EU for all cross-border EU data protection-related matters in line with Article 56(6) of the GDPR.[8] This is all the more relevant in the context of the COVID-19 crisis where organisations need to react quickly and DPAs may want to avoid being overwhelmed with requests that they may not be able to address in a timely fashion. Just like in the case of notifying the breaches in multiple Member States to the single-lead DPA, there should be an official clarification that companies can abide by the national guidance of their lead authority for all their cross-border EU matters and operations.[9] This should be the case even in situations where proximity to individuals may matter, such as for instance if a breach on a cross-border processing impacts individuals in a country different from the country where the controller's main establishment is located and where the lead DPA will be notified of the breach. Such lead DPA would then liaise with the other concerned DPAs.[10]

Finally, it appears that some DPAs may **not always respect the OSS** mechanism (deliberately or under local pressure) as they are sending orders, requests for information, starting audits or imposing fines directly on establishments present in their territory without first liaising with the competent lead DPA.[11] However, respecting the OSS enables the DPA to participate in the decision-making with the lead DPA through the cooperation procedure as a "concerned DPA". It also helps with leveraging the collective knowledge of other DPAs and addressing the lack of resources of some DPAs.[12] It avoids unnecessary administrative bottlenecks by better allocating cases. Ultimately, bypassing the OSS may have the effect of weakening the mechanism and may result in organisations established in multiple EU Member States deciding not to appoint a lead DPA.

Summary of CIPL Recommendations:

The EDPB, as an EU body, should play a leading role in enabling DPAs to fully collaborate as per the provisions of the GDPR. More specifically, it should:

- **Provide a clearer definition of what a cross-border processing is as opposed to local processing, taking into account the letter and the spirit of the OSS mechanism;**
- **Clarify that as per the OSS, the lead authority is the single interlocutor for organisations;**
- **Clarify that organisations can abide by the national guidance of their lead authority for their EU cross-border operations; and**
- **Encourage DPAs to actively participate in the OSS as concerned DPAs instead of initiating their own proceedings, and highlight practices that are not compliant with the OSS.**

1.3 Harmonisation of Member States' GDPR Implementation

The overly extensive use of Members States' GDPR margin of manoeuvre has led to a lack of harmonisation of the GDPR on topics of the highest significance to many organisations, such as **children age of consent, processing of sensitive and biometric data, scientific research, processing of criminal data or processing of employee personal data**. Sometimes it is not clear why a certain national provision or exemption is not present in other Member States, such as regarding the conditions for processing sensitive biometric data, which seem to be applicable across the entire EU. This all creates compliance and operationalisation hurdles for organisations, aggravated by the lack of uniform criteria triggering the application of national laws within the EU. Some Member States themselves are calling for a more consistent approach.[13]

This also encompasses **extensive interpretation of key concepts by national governments or DPAs**, such as "public interest" or "national security" to legitimise specific national rules or government requests to organisations to share data such as in the current COVID-19 crisis. The fragmentation is increased further by national laws that go beyond what is permitted under the GDPR derogations (e.g. limitations related to individual rights; heirs exercising certain rights under the GDPR; specific national laws on digital wills, national certification criteria for the DPO role). On the opposite extreme, this may also include failing to adopt relevant national provisions to enable certain processing. For instance, as per Article 10 GDPR, processing of criminal data is possible only if authorised by EU or national law. Such processing is, however, not always explicitly authorised at the national level even though laws on anti-money laundering, prevention and detection of terrorist financing, fraud prevention and detection, and insider

risk controls impose obligations on companies that may require processing criminal data for due diligence purposes.

Summary of CIPL Recommendations:

As the gatekeeper of the internal market, the EU Commission should:

- **Map the inconsistencies and gaps in national laws; and**
- **Work with Member States to ensure a collaborative and constructive approach to making the GDPR one single law in the EU.**

1.4 Availability of Accountability Tools

The potential of GDPR certifications and codes of conduct as accountability tools and their potential for flexibility was already mentioned in CIPL's first report. One year later, no certification or code have been formally launched, and little progress has been made to expand or improve existing cross-border data transfer mechanisms (see section 1.1).

Article 42 Certifications are still not available[14] and still not envisioned as possibly covering an entire privacy management programme. The EU Commission should make use of its competences under Articles 43(8) and 43(9) of the GDPR to address this. For instance, having certified tools would be appreciated in the current COVID-19 crisis where digital tools are used increasingly in all areas of individuals' lives.[15]

In parallel, the new ISO 27701 certification[16] is likely to become a global standard that may subsume Article 42 GDPR certifications as it covers most of the requirements of the GDPR. The relationship (including interoperability) between ISO 27701 and Article 42 GDPR certifications must be clarified soon, as more and more organisations are getting certified.

In addition, organisations request that any future Article 42 GDPR certification should:

- Be achievable in a reasonable time frame and in a realistic and pragmatic manner;
- Take into consideration global and changing environments to avoid becoming obsolete;
- Be intended to relieve administrative burdens on controllers and processors (for instance by explicitly reducing the need for extensive privacy and security assessments);
- Cover an entire privacy management programme;
- Avoid duplicating existing certification from other DPAs, with the European Data Protection Seal[17] prioritised, except if the added value of having national specific certifications can be demonstrated;[18] and
- Enable certification bodies to offer certification services across the EU when a certification scheme is approved by a DPA.

BCR have not been recognised as a certification, nor as an accountability mechanism, yet most organisations that have BCR see them as such. Hence, they have not been leveraged for global interoperability purposes to enable organisations to become more efficiently certified in various global accountability schemes that have significant substantive overlap such as the APEC CBPR. The EDPB and DPAs should continue the work initiated by the Article 29 WP and APEC.[19]

Article 40 GDPR Codes of Conducts should similarly be available as soon as feasible and, importantly, the conditions for their approval streamlined, as they have significant potential to help build the data economy.[20] Unfortunately, the high threshold that certain DPAs are imposing on codes to go beyond the GDPR has a disincentivising effect on private sector initiatives, while not being founded on any GDPR provision. Codes should also be applicable to more than one single industry sector, as the GDPR itself does not provide otherwise, especially with regards to certain data processing operations or activities (e.g. blockchain, digital interface) that are similar in different sectors and where a similar approach to achieve compliance might be appropriate. A code may also be relevant when inherent technical features or other coexisting regulations require a forward-thinking or holistic approach.

Summary of CIPL Recommendations:

The EU Commission should make use of its competences under Articles 43(8) and 43(9) of the GDPR to finalise the certification regulatory framework.

The EDPB and DPAs should:

- **Complete the adoption of the regulatory framework for certifications and codes of conducts;**
- **Clarify the relationship between ISO 27701 and Article 42 GDPR certifications;**
- **Enable that certifications can cover an entire privacy management programme;**
- **Include GDPR certifications and codes of conduct in the work on BCR and CBPR interoperability; and**
- **Accept that codes are not necessarily limited to a sector and do not need to go beyond the GDPR.**

2. Improve EDPB and DPA Collaboration and Engagement

2.1 Transparency and Constructive Engagement with Stakeholders

While there has been some progress in how the EDPB ensures transparency and engages with stakeholders, CIPL believes that more constructive engagement going forward would be beneficial to all stakeholders. For instance, it is still difficult to understand how the EDPB and its subgroups function, who are the rapporteurs, what are their mandates and under what timeframe they work. Information should be more easily accessible from the website and include publication of official correspondence, and agenda and minutes of board and working group meetings. DPAs should also work towards achieving a similar level of transparency at national level.

In addition, CIPL welcomes the Article 29 WP /EDPB "Fab Lab" or multistakeholder meetings and their recent extension to industry, civil society and other stakeholders. CIPL would recommend that these meetings be organised in a more systematic manner with a focus on the quality of the contributors and not necessarily on their quantity or mandated representation. In addition, CIPL recommends EDPB's setting up a **special consultative expert group of data protection experts** to provide regular and ad hoc input, operational know-how and a deeper dive into specific topics for EDPB guidance.

CIPL also welcomes the possibility to provide **comments before the final adoption of the EDPB or DPA guidelines**, recommendations or toolkits, as well as the publication of all contributions received by the EDPB and DPAs through open consultation forms. This enables all stakeholders to consider issues in a more informed way and to understand different points of views, as well as practical considerations.

However, in order to frame the debate at a sufficiently early stage, CIPL suggests starting the dialogue even before a first draft is produced through a pre-consultation phase with input from relevant industry and stakeholders. This would enable DPOs and other experts—who are best placed to provide insights and to comment on technical and operational issues—to invest time in the process as they would feel more confident that their views might be more appropriately considered than through the current process. Indeed, early involvement would avoid the perception that once the guidance has been published in draft form, it is almost too late to provide input and too difficult to introduce new concepts and ideas, and would reduce the perception that the substantial time and effort in responding to a consultation is not likely to have an effect.[21] The DPAs and the EDPB could also ask organisations what type of guidance would be useful to them.

The guidelines issued by the EDPB and DPAs are generally seen as useful by industry in their day-to-day activities to help create GDPR-compliant products and services. They sometimes, however, appear to have the effect of imposing additional obligations to implement unnecessary processes rather than providing pragmatic controls to gauge the effectiveness of measures taken. The guidelines on the territorial scope of the GDPR for instance expand the application of the GDPR to non-EU-based processors while they may already be bound by the GDPR obligations under the Article 28 contractual requirements. The guidelines on Data Protection by Design and by Default require technology providers to disclose the cost of developing their solution to controllers, which is well beyond the remits of the GDPR and far from any current market practice.

CIPL recommends **that Guidelines produced as the result of EDPB or DPA consultation** should:

- Systematically integrate the GDPR's risk-based approach;
- Be designed to explain the "spirit" of the law, to assist organisations in assessing risks and making decisions more efficiently;
- Be outcome-based on the desired outcome of a requirement and not go into the details of internal processes and how to comply that may vary from one organisation to another;
- Contain lists of possible criteria setting forth rebuttable presumptions on whether something meets a certain definition or threshold rather than making firm and definitive statements;

- Include a discussion of the public comments received and provide an explanation of why proposed changes were rejected; and

- Be translated into English and be easily accessible, including from the EDPB website for guidelines produced by DPAs.

Summary of CIPL Recommendations:

The EDPB and DPA should:

- **Work towards enhanced transparency;**
- **Include a pre-consultation phase before issuing draft guidance, to gather input from industry;**
- **Set up a special consultative expert group of data protection experts; and**
- **Enhance guidelines' usefulness to organisations.**

2.2 Harmonisation of DPAs' GDPR Interpretation and Implementation

In addition to the lack of harmonisation caused by the extensive use of the margin of manoeuvre left to Member States (see section 1.3), different national interpretations and a plethora of guidance by DPAs on several key GDPR topics aggravate this fragmentation. They make it more difficult to implement European-wide programmes, launch products, apply consistent data protection for individuals or work with business partners. They end up recreating barriers to the internal market as well as the bureaucracy that the GDPR was intended to reduce.

On the ground, this generates increased complexities. In B2B relationships for instance, this has led to an increase in sales and negotiation cycles that remain significantly longer than before the GDPR. Companies try to impose their governance requirements through due diligence privacy questionnaires, data processing addenda and increased supply chain transparency obligations based on their own interpretations of the GDPR. For instance, some controllers are obliging processors contractually to keep records of processing in accordance with Article 30 of the GDPR and requesting access to such records, or are trying contractually to position privacy by design and privacy by default as a data processor obligation even though it is, under Article 25 GDPR, a controller's responsibility.

Some examples of fragmented interpretation include: national lists of high-risk processing requiring a DPIA,[22] cookies, use of the consent legal basis, use of ID documentation for authentication purposes, direct marketing, data subject rights,[23] requirements to sign an Article 28 GDPR data processing agreement,[24] or use of the public interest legal basis for facial recognition processing.[25] In addition, in the early stages of the COVID-19 crisis, DPAs have published guidance in isolation, which resulted in differences in approaches, regarding the concept of anonymisation, legitimate interests, vital interests and the role of private organisations to serve public interests. This was unhelpful not only to the organisations but, most importantly, to address the crisis itself.

Also, national DPA guidance may not be consistent with each other or with the guidance issued by the EDPB. One would expect more consistency, constructive collaboration and mutual recognition of positions between DPAs. Streamlining the guidelines would also help save resources of DPAs that could be allocated

to other tasks.[26] Initiatives, such as the Polish endorsement of the French PIA tool27 should be encouraged and more systematically replicated. The review by the EDPB of the Danish standard contractual clauses for contracts between controllers and processors under Article 28 of the GDPR28 is also an opportunity for the EDPB and DPAs to agree that for consistency reasons, and because it has been approved by all DPAs, this template should be used in all countries (and translated into local languages as needed) and that no DPA should start working on a separate template.29

Finally, some national competition authorities, consumer bodies, healthcare authorities and financial regulators have started ruling on data protection topics that are within the remit of DPAs. CIPL recommends that the EDPB and DPAs play a proactive role in engaging with these regulators to resolve potentially conflicting positions and enter into memoranda of understanding to avoid conflicting and inconsistent rulings, as well as encroaching on each other's competences.

Summary of CIPL Recommendations:

The EDPB should play a leading role in reducing the number and volume of duplicative guidelines by DPAs to guardrail the way DPAs interpret and enforce the GDPR. This could mean for instance:

- **Discussing beforehand in the EDPB the plans and steps to a harmonised approach so that there are no diverging views, priorities and approaches;**
- **Requiring DPAs to leverage existing EDPB and DPA guidelines (by endorsing them and translating them into local languages) before creating new ones;**
- **Mandating that local guidelines comply with the EDPB guidelines and state why a separate national approach is necessary; and**
- **Engaging with other regulators to resolve potential conflicts of competence.**

2.3 Transparent, Harmonised and Proportionate Enforcement

Practices observed in various jurisdictions show discrepancies in enforcement that are far larger than could be explained by local administrative peculiarities or local economic factors. Some DPAs have transparently and publicly announced their enforcement and fining strategies and approach while other DPAs impose sanctions in an opaque manner without relying on any discernible calculation method. Also, DPAs don't seem to refer to the risk-based approach in their enforcement actions, nor to specific mitigating factors.

As explained in CIPL's Paper on regulatory engagement, enforcement should be used as a last resource, as deterrence and punishment have proven to have limited effectiveness in achieving the desired result of effective data protection.[30] More generally, DPAs need to balance enforcement with engagement, thought-leadership, guidance, co-regulatory approaches (such as codes and certifications) and sandboxing initiatives, and not put too much emphasis on enforcement on its own. When enforcement is necessary, transparency, consistency and proportionality in the approaches can be improved further.

1. DPAs should systematically consider the full range of GDPR's **corrective measures**[31] to decide on the most appropriate and proportionate way to remedy a particular GDPR violation, taking into account multiple factors, as well as the nature and gravity of the infringement. Fines should

remain a last-resort option for the most serious, repetitive cases or those that create real harm for individuals.

2. DPAs should develop and publish at EU level a **clear, predictable, consistent and proportionate fining model**. As of today there is no clear and consistent method for calculating fines[32] nor a clear understanding of the functioning of Article 83 of the GDPR. Contrary to widespread belief, this article does not mandate calculating fines on the basis of a percentage of the turnover of a company, but establishes the annual turnover as a criterion for establishing the upper limit of a fine that is not to be exceeded. As such, by relying on the turnover of the legal entity and applying a daily rate—regardless of the infringement at stake—the recent German fining model does not appear to set an appropriate framework to calculate proportionate fines.[33] To be **transparent** and **easily understandable**, the imposition of fines could rely on the following steps: (1) identification of infringement; (2) fine calculation on the basis of relevant and proportionate criteria; (3) application of aggravating or mitigating factors in Article 83; and (4) verification that the amount of the fine does not exceed Article 83 GDPR limits. We recognise that defining the relevant criteria for proportionate fining may be challenging in the data protection field where some data processing activities do not necessarily link to specific sales (for instance, processing of employee personal data or free services). To help resolve this, CIPL recommends that fining models and their proportionality be discussed on a broader basis among all stakeholders at the European level, to ensure EU-wide consistency and to draw lessons from other comparative areas of regulatory behaviours, such as financial, anti-corruption or competition regulators.

3. To better respond to the variety of situations, DPAs should make use of the open clause of Article 83(2)(k) GDPR[34] and define additional aggravating and **mitigating factors** not already listed in Article 83(2). The EDPB GDPR report shows that this ground is currently underused by DPAs.[35] For example, having an effective and demonstrable organisational accountability programme[36] could be one of the factors taken into account by DPAs in enforcement cases.[37] In the case of a data breach for example, if the company has put in place clear and effective policies, has trained the response team through mock exercises, made available crisis management toolkits and invested in state-of-the-art technology, this will play an important role in mitigating the potential consequences of the breach. This would also have the overall effect of incentivising and accelerating organisational accountability within organisations.[38] It is also in line with other areas of corporate compliance and regulation.

4. **Reiterative compliance and mediation** should be further promoted as an efficient way to resolve non-compliance and disputes as it often enables a swifter and more efficient resolution of cases. This may also work in the "grey areas" of data protection law and compliance, where technology challenges the legal norms and it takes a longer and a more concerted and collaborative effort to find a solution and improve compliance on the ground. Unfortunately, continuous improvement, reiterative compliance and amicable settlement models are only used by a handful of DPAs[39]; some are using other means with similar effects under local law,[40] while others would be willing to use it if national law permitted it. The EDPB should further promote amicable settlement models and the EU Commission and DPAs should work with Member States in parallel.

5. DPAs regulatory oversight and enforcement strategies should be reviewed and **adapted to changing circumstances**. For instance, in the context of the COVID-19 crisis, the ICO issued a

regulatory forbearance statement to indicate that it would reassess its priorities and resources, to focus on areas that are likely to cause the greatest public harm and that it would take into account companies' efforts to fight COVID-19 when enforcing the GDPR.[41] Similarly, CIPL suggested a similar pragmatic approach by DPAs and the EDPB when addressing and enforcing GDPR data flows requirements in a case of a hard Brexit.

Summary of CIPL Recommendations:

The EDPB and the DPAs should:

- **Publish their regulatory strategy and priorities;**
- **Agree on the EU level and publish a clear, predictable, consistent and proportionate fining model and work with stakeholders to tailor it to the data protection field;**
- **Recognise organisational accountability as a mitigating factor under Article 83 GDPR; and**
- **Promote reiterative compliance and amicable settlement practices between organisations and DPAs.**

3. Open Questions Regarding the Interpretation of GDPR's Key Substantive Requirements

3.1 Legal Bases for Processing

There is a perception that, based on the questionable belief that consent inherently empowers individuals, DPAs view and favour consent as the most protective legal basis for processing while construing other legal bases in an increasingly narrow manner. While it was clear before, the COVID-19 crisis has further illustrated the limits of some of the current interpretations of the GDPR legal bases. DPAs and the EDPB should not by default dismiss certain types of processing *ex-ante* under a particular legal basis but should be open to novel interpretations and to leveraging the GDPR's leeway on this issue to its fullest extent.

CIPL has long been advocating moving away from the consent paradigm because:

(1) In many contexts, consent is **ineffective** in protecting the individual, generates consent fatigue and negatively impacts user experience.[42]

(2) Consent may not be the appropriate legal basis due to its **intrinsic invalidity** in certain areas, such as in the employment context or in other cases as decided on a case-by-case basis.[43]

(3) Consent does not work in **B2B relationships** as in most cases individuals whose data is processed are the controller's employees who cannot validly consent.

(4) Because it needs to be specific, obtaining valid consent is not adapted to **data sharing scenarios with numerous and frequent communications** between multiple actors, such as in vehicle-to-vehicle communications[44] or in case of sophisticated security schemes in the financial sector that rely on biometric data.[45]

(5) Consent is challenging **healthcare research scenarios** because patient data is also often key-coded so that patients' identities are not revealed to the receiving organisations—making consent even more difficult to manage.

(6) In some specific sectors, reliance on consent may **weaken security** as it may give ammunition to fraudsters to bypass or game a fraud prevention system.[46]

(7) More generally, the possibility for the individual to **withdraw consent** makes this legal basis too unstable for quite a number of processing activities, especially those that have a broader public benefit for society, people and organisations.

The **legitimate interest** legal basis may be more appropriate to the reality of the processing operation while enabling effective protection of individuals.[47] It allows for data processing which, while not strictly required for the actual fulfilment of the contract, is nonetheless necessary to provide the expected quality of service, e.g. better customer service, guarantee of IT security, fraud prevention, optimisation of procedures, customer contact improvement, advertising, market research, assertion of legal claims and defence in legal disputes.[48] The recent guidance of the Dutch DPA excludes reliance on the legitimate interest basis for serving commercial interests such as profit maximisation and profiling.[49] The interpretation also contradicts the GDPR, as direct marketing, for instance, can be considered as a legitimate interest.[50]

Similarly, because of lack of clarity on the definition of direct marketing, and the interaction with the ePrivacy Directive, some organisations have refrained from reaching out to their customers (even in business-to-business context) in the aftermath of COVID-19 to understand how they can serve or assist them by fear of falling under the qualification of "direct marketing".

This narrow interpretation of the Dutch DPA appears unrealistic in our data-driven society, where the EU Commission and national governments are also trying to develop a competitive digital and data strategy for Europe to enable data to be used responsibly for beneficial and societal purposes and drive European-based data innovation. As recognised by the Cremer report mandated by the EU Commission on "Competition Policy for the Digital Era", the legitimate interest legal basis may also be a more suitable legal basis for enabling innovative uses of data.[51] Although the legitimate interest legal basis should not be seen as a catch-all and its appropriate application should be vigorously enforced, it is important that companies have some flexibility to identify permissible processing activities based on legitimate interests, provided of course that the balancing test allows for it.

Similarly, the **contractual necessity** legal basis has been too narrowly interpreted. As highlighted in its response to the contractual necessity guidelines,[52] CIPL considers that it is ultimately up to the organisations to decide what service they provide and to assess what processing is necessary for the execution, performance and control of the contract.[53] CIPL also regrets the missed opportunity of the EDPB guidelines to leverage the Article 6(4) GDPR "compatibility test" to enable broader reliance on the contractual necessity legal basis (as was requested by stakeholders during the consultation phase).

Also, reliance on the **legal obligation** basis for processing has been too narrowly interpreted. At a minimum, this legal basis covers compliance with the obligations of the GDPR itself. It should also be applicable to national, EU and foreign laws imposing legal obligations on companies.[54]

Finally, the current COVID-19 crisis and the need for organisations to quickly address unforeseen challenges have also highlighted the necessity to further consider the interpretation of legal bases under the GDPR, such as legitimate interest and legal obligation, as well as **public interest** and **vital interest**. Where organisations are increasingly asked to perform a public interest duty and act in the public interest—to protect health and safety of employees and customers—the public interest legal bases can be extended also to cover processing performed by private companies (and not just public entities). This is relevant for instance for processing of employee health data, including temperature measurement to avoid the further spread of the virus and maintain a safe working environment (where consent is inherently deemed invalid).

Summary of CIPL Recommendations:

The EDPB and the DPAs should:

- **Reject the common belief that consent is the *sine qua non* of effective data protection and clarify that the GDPR does not favour consent over other legal bases;**
- **Adopt a more flexible interpretation of the legitimate interest, contractual necessity and legal obligation legal bases; and**
- **Explore when and how organisations may rely on the public interest and vital interest legal bases.**

3.2. Anonymised Data

The discussions surrounding the use of contact tracing apps to help fight the COVID-19 crisis have brought the topic of anonymisation to the forefront. CIPL considers that technical measures such as anonymisation can be helpful when organisations have to react quickly in a crisis situation without sacrificing privacy protections or undermining trust.[55] Yet positions among the DPAs differ when it comes to defining and trusting anonymisation techniques, with the Dutch DPA even considering that absolute anonymisation is impossible.[56] This lack of agreement is unfortunate, as it contributes to undermining trust in a situation where time is of the essence.

The potential for anonymisation is also enormous when it comes to enabling the use of data for training of AI and helping reduce compliance risk for organisations.[57] As a consequence, a flexible interpretation of the notion of anonymous data is essential. An appropriate standard for anonymisation has been put forward by the US Federal Trade Commission in a 2012 privacy report: reasonable de-identification coupled with contractual and legal safeguards against inappropriate re-identification.[58]

Organisations should also be allowed to process pseudonymous data under a regime not containing the full-fledged requirements of the GDPR, provided they implement relevant technical or organisational risk mitigation and safeguards. Even if the GDPR qualifies pseudonymous data as personal data, the application of the GDPR obligations must be adapted to take into account the fact that the data can no longer be attributed to a specific data subject without the use of additional information. This could be particularly relevant in the context of crises such as COVID-19 where use of pseudonymous data can help fight the crisis with more efficiency than anonymised data and, more generally, in the context of business-

to-government data sharing when organisations are being asked by public bodies to provide their data sets in order to inform public policymaking.[59]

Summary of CIPL Recommendations:

The EDPB and DPAs should:

- **Adopt a consistent interpretation of the notion of anonymous data; and**
- **Clarify the legal regime applicable to pseudonymous data.**

3.3. Risk Based Approach and Risk Assessment

The GDPR embeds the risk-based approach to allow organisations to consider risks and harms to individuals and to build their accountable privacy management programme and calibrate compliance accordingly. As a consequence, organisations have latitude in using personal data in no- or low-risk contexts while enabling more targeted and effective protection where actual risks are identified, in particular through the performance of DPIAs.

Generally, organisations welcome the GDPR DPIA as an efficient risk assessment tool that creates a standard for everyone to follow within an organisation and that helps build the record of processing (even if most processing operations do not reach the high-risk threshold for a full-blown DPIA). In practice, this has been a great incentive for organisations to do systematic risk assessments and to be mindful of privacy by design, so that privacy risk mitigation measures are taken very early on, to avoid hitting the high-risk threshold. However, the line between a simple privacy risk analysis (e.g. a new product which does not trigger DPIA requirements) and a DPIA (e.g. where sensitive data is processed or processing occurs on a large scale) may be somewhat arbitrary and subjective and the **methodology** to assess, document and mitigate risks in the context of such analyses may vary significantly.[60] Moreover, there are often discrepancies from country to country in local DPAs' expectations in terms of what a DPIA should look like and what it should achieve. While any new activity involving the processing of personal data requires carrying out a privacy risk analysis, it is important that this is not turned into a systematic obligation for organisations to prove that no DPIA is required with respect to each and every one of their processing activities.

Further, organisations would welcome that any clarification on a methodology **for privacy risk analyses be more holistic** and take into account not only the GDPR, but also align with industry practices and other standards, such as ISO standards or NIST (National Institute of Standards and Technology).

Finally, risks to individuals cannot be seen in isolation from other fundamental rights and societal interests. **Potential benefits** for other human rights, as well as reticence risks (i.e. what would be the consequence to individuals and society of not going forward with a specific project due to potential risks?) should be part of risk assessments and DPIAs. Article 35(1) GDPR uses the notion of "impact", which can include both negative and positive factors and does not prevent the inclusion of more factors than those listed in the GDPR[61] to ensure that all relevant variables are considered to inform the final decision. Discussions about the AI and machine learning technology, as well as the COVID-19 crisis, have exemplified the need for a broader impact assessment, that also includes benefits and risk reticence considerations. It is important that the EDPB and DPAs recognise the complexity of risk assessments and the diverse

nature of variables especially in the AI context[62] and take a nuanced and agile approach beyond just a simplistic assessment of whether something is low or high risk.

Summary of CIPL Recommendations:

The EDPB and the EU Commission should:

- **Enable more dialogue to build consensus between stakeholders and DPAs on how to identify and assess risks and harms to individuals;**
- **Clarify that privacy risk analysis should not be turned into a systematic obligation to justify and prove that a processing does not require a DPIA; and**
- **Recognise that not only risks but also benefits and reticence risks must be taken into account in assessing the impact of processing.**

3.4. Data Security and Data Breaches

Security is a key building block of data protection and of the GDPR. Lack of proper security can endanger compliance with many if not all GDPR provisions. It generally poses risk to a whole processing operation that may be affecting multiple individuals as opposed to concerning a single individual only. Unfortunately, the bar is getting higher as hackers and cyberattacks become more sophisticated. Even the most mature companies with large teams and significant resources are facing security breach issues.

For instance, strict **employee data protection** rules may have the counterproductive effect of making it extremely difficult (if not sometimes outright impossible) for employers to comply with their security and breach notification requirements under the GDPR. Indeed, some of the technical and organisational measures that are indispensable to comply with these requirements do unavoidably involve a certain level of employee monitoring. However, some of these measures cannot always be implemented, as they may violate some national data protection laws or its strict interpretation. Moreover, deployment of such measures may require lengthy consultations with employee representative bodies that may have a different objective and can use data protection compliance as a negotiation chip. Consequently, in an environment in which the controller needs to achieve security against a fast-evolving cybersecurity threat landscape and risks its reputation when suffering and notifying a data breach, these localised exemptions delay or even prevent employers from doing what is required to protect the personal data of their employees. To date, the EDPB and DPAs have refrained from providing any practical and helpful guidance on how to resolve this inherent contradiction.

In addition, the **data breach notification process** should be further smoothed, especially in case of cross-border incidents and in particular for organisations that do not have a main establishment in the EU. Organisations complain of having to submit various national notification forms to different regulators, some of which are generally difficult to fill out and sometimes have to be filled out online, making it difficult for multiple and geographically spread teams to fill out the relevant sections. In practice, a single security incident could trigger the obligation to notify under multiple EU and national laws (NIS Directive, ePrivacy Directive, financial regulation), to multiple authorities, in different countries, within different timelines, and require different types of information in different formats. For these reasons, the breach

notification process to the DPAs should be unified and simplified with a centralised, single reporting form in English[63] applicable across all EU countries (and translated into local languages, as the case may be).

There is also uncertainty around the **reporting time frame** when a weekend or bank holiday falls into the notice period of 72 hours.[64] Furthermore, it is unclear in which cases DPAs would accept a **delayed notification**, where such notification cannot be made within 72 hours. With cyberattacks being increasingly unexpected and sophisticated, it is harder for companies to avoid them. In some of the most extreme cases, companies may not even be able to communicate and employees may be prevented from using their professional email addresses. Such situations should justify special and ad hoc attention by the DPAs. There should be further engagement between the EDPB, DPAs and industry to define use cases and scenarios or thresholds where such delayed notification would be expected.

With regards to the **breach reporting threshold**, while the GDPR states that no notification is required where the breach is unlikely to result in a risk to the rights and freedoms of individuals, in practice it is unclear in which cases such risk is unlikely. This lack of consensus on how to identify and measure risks to individuals and serious consequences of getting the notification wrong leads to organisations' over reporting data breaches and "swamping" DPAs with thousands of unnecessary or trivial notifications. CIPL believes that the breach reporting threshold is too low[65] and should be raised to apply to cases where risks are more than minimal or purely theoretical—likelihood and severity of risk must be considered. The EDPB should work together with organisations to build consensus and updated guidance with examples of non-reportable breaches.

The GDPR notification requirement is just one of the many actions that organisations must perform as a result of the breach, the priority being to **understand the breach and take all measures necessary to mitigate its consequences**. Other key tasks, such as supporting the business and the incident response teams throughout the breach mitigation and resolution process, addressing complaints from consumers, communicating publicly, handling relations with customers or vendors, handling queries from other regulators, also have to be performed. In addition, organisations may have to handle a flow of data access requests arising as a result of notifying individuals of the breach, which the organisations may not be able to address within the one-month delay. This may trigger complaints to the DPA. Although DPAs have an obligation to handle any complaint, it is expected that such complaints would arise in the event they are related to a previous breach notification of the controller. The EDPB should clarify that in the case of breach, the delay to respond to individual requests should be extended to two months in accordance with Article 12(3) GDPR requiring to take into account "the complexity and number of the requests." DPAs should also be prepared to assist the company depending on the circumstances.

Finally, CIPL highlights that **access to the ICANN[66] WHOIS database** (recently re-named to "Lookup"[67]) that includes domain names' owner information, such as email, phone and physical address, is becoming too overly restricted. Criminals frequently reuse the same registration data and cybersecurity services use this information to help determine the legitimacy of websites, with machine automation correlating domains registered with the same contact information, enabling filters to quickly block all related domains. The GDPR's restrictive interpretation[68] could have a negative effect on cybersecurity as security professionals can no longer quickly access the data in the Lookup database, such as the domain owners' names, emails and phone numbers. It makes it difficult to identify attack sources, leads to an increase in malicious emails and extends attack timelines. The European Commission should raise awareness to foster

cybersecurity within the EU and support negotiations between ICANN and the EDPB to find a workable solution.

Summary of CIPL Recommendations:

The EDPB and the DPAs should:

- **Work towards defining a consistent risk assessment methodology;**
- **Create a single breach reporting form in English applicable across all EU countries;**
- **Raise the threshold to notify DPAs and individuals of a breach; and**
- **Consider a lighter touch response to individual complaints related to notified data breaches.**

The European Commission should raise awareness to foster cybersecurity within the EU and support negotiations between ICANN and the EDPB.

4. Longer-Term Recommendations on the GDPR's Position in the Broader Digital Landscape

4.1 GDPR and Other EU Laws

There are a growing number of inconsistencies between the GDPR and sectoral EU laws. For example, the Payment Services Directive 2 and the Clinical Trial Regulation place consent as the main legal ground for processing whereas Article 6 GDPR puts all legal bases, including consent, on an equal footing. The Audiovisual Services Directive provides for specific age verification systems for displaying content to minors, but does not indicate how they relate to Articles 8 and 12 of the GDPR. The E-Commerce Directive provides for a specific liability regime of intermediaries that does not square well with the liability framework of controllers and processors of the GDPR when content is also deemed personal data.

Therefore, it is important that when new requirements relating to data use are introduced in other laws, the interaction with the GDPR is fully considered to ensure alignment and avoid inconsistencies. This is particularly relevant for the draft ePrivacy regulation, which in its current state may generate further confusion regarding the role of consent vis-à-vis other legal bases. Similarly, the future EU AI framework must take full consideration that the GDPR already regulates use of personal data in AI.[69] The EU Commission must conduct a gap analysis to avoid creating duplicative or conflicting obligations for controllers and processors and creating legal uncertainty.

Summary of CIPL Recommendations:

The EU Commission should ensure that before new EU legislation impacting personal data is proposed, a gap analysis is conducted to avoid creating duplicative or conflicting obligations and legal uncertainty.

4.2 GDPR and New Technologies

As already highlighted by CIPL,[70] AI technology creates tensions with core data protection principles.[71] The EDPB and DPAs should work with industry to help resolve these tensions through creative, forward-

thinking and progressive interpretation of some GDPR requirements, so that individuals and society can enjoy the full benefits of AI and Europe can stay competitive and promote European-based data-driven business and innovation. CIPL suggests interpretative clarifications on the following points:

- **Definition of personal data**: AI technologies usually need vast amounts of data to function optimally in the algorithm-training phase, where the risks to individuals are smaller or non-existent. In cases where personal data is "incidentally" collected in low volumes as part of vast training datasets that are intended to be focused on non-personal data,[72] this would trigger the application of the GDPR to the whole data set, which may hamper its further use. A progressive approach would be to exempt the data set from GDPR requirements in this situation.

- **Purpose limitation**: Algorithmic training per se or repurposing of data for AI purposes should be considered a specific purpose under Article 5(1)(b) GDPR or a compatible purpose under Article 6(4) GDPR. One other option would be to interpret more broadly the notion of purpose. A narrow definition of the purpose can lead very quickly to the necessity of a change of purpose and thus the impossibility of a lawful further use of the data.[73]

- **Transparency**: GDPR transparency requirements should be relaxed where organisations do not have a relationship with individuals (e.g. use of data made publicly available for research). In such case, the "disproportionate" exemption in Article 14(5)(b) GDPR should be applicable.

- **Legal bases for processing**: Consent may not be a workable legal base for data processing for the purpose of algorithmic training. Rather, this processing could be based on the legitimate interest of the controller under Article 6(1)(f) GDPR provided that the balancing test allows for it.

- **Sensitive personal data**: As the COVID-19 crisis has demonstrated, there should be more expansive grounds for processing of sensitive personal data in the context of AI (subject to the implementation of appropriate safeguards). In addition, AI has the potential to detect bias more easily and in a more reliable manner than humans, but to do this, it requires access to sensitive data to effectively audit the model.[74] Sensitive data processing and retention are therefore required to ensure algorithmic data processing is fair—not biased and not discriminatory, and complies with GDPR.

- **Individual rights**: The application of rights of individuals should be clarified where their exercise could render algorithmic training impossible. Further, an individual's withdrawal of consent should not require that the model be retrained without their data. The change should be forward-looking, not retrospective.

- **Automated decision-making (ADM)**: Article 22(1) GDPR should not be construed as a prohibition, but as a right that may be invoked by individuals in addition to all other relevant safeguards of the GDPR such as the right to explanation, correction, contesting a decision and redress.[75]

Finally, in order to further resolve tensions between new technologies and data protection, the EDPB should promote and DPAs should embrace **regulatory sandboxes** to allow for the supervised testing of innovative products, while helping DPAs better understand the technologies they are regulating.[76] The current COVID-19 crisis and the need to reconcile the use of data to save lives with data protection

principles could constitute an interesting use case study for a sandbox. Also, the experiences of the UK ICO, which has launched regulatory sandboxes in a pilot phase with 10 organisations, should be illustrative for other DPAs and encourage them to embark on these innovative regulatory methods. The EU Commission should clarify the DPAs' competence to deploy regulatory sandboxes as per the GDPR.

Summary of CIPL Recommendations:

The EDPB and DPAs should:

- **Work with industry to resolve tensions between AI and core data protection concepts; and**
- **Clarify the DPAs' competence to deploy regulatory sandboxes.**

4.3 GDPR and the Data Economy

The EU Commission's recently published strategy to create a European Data Space[77] should also call attention to the fact that data sharing practices between all types of organisations will significantly increase. The COVID-19 crisis has highlighted the huge value of responsible data sharing between private and public actors to address the crisis.

However, seamless and effective **free movement of data across organisations** in the EU requires resolving the implementation and interpretation challenges of the GDPR that currently have the effect of erecting barriers.[78] In addition, some longstanding core principles of data protection (such as confidentiality, purpose limitation, prohibition of unauthorised disclosure) and the lack of clear allocation of responsibilities in a controller-to-controller context should not have a crippling effect on data sharing practices between accountable organisations. To anticipate this, the EDPB and the DPAs should work with organisations to develop an adapted framework for accountable data sharing. This framework should avoid an overly "user centric" approach making data sharing systematically dependent on choices made by individuals, as this may actually defeat the data sharing purpose. Instead, DPAs and the EU commission should incentivise organisations adopting accountable best practices and safeguards to ensure responsible data sharing. In particular, it is important to raise awareness that sharing data with third parties need not be risky if undertaken within appropriate accountability frameworks.

Summary of CIPL Recommendations:

The EDPB and DPAs should set up working groups with industry to develop a data sharing framework.

CIPL is grateful for the opportunity to provide comments in the context of GDPR evaluation, with a special focus on consistency and cooperation mechanisms and international data transfers. The May 2020 GDPR evaluation represents an important step for public debate on some of the unfulfilled promises of the GDPR as well as its opportunities going forward. It is a moment for clarifying the objectives, resetting priorities, reducing divergences and driving consistency to have one law for one continent in our connected and increasingly complex world. The GDPR offers considerable scope for building compliance solutions in a cooperative and constructive manner to enable responsible innovation that protects individuals and ensures that data protection challenges are properly addressed.

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

If you would like to discuss any of these recommendations or require additional information, please contact Bojana Bellamy, Markus Heyder, mheyder@huntonAK.com, Nathalie Laneret, nlaneret@huntonAK.com, Sam Grogan, sgrogan@huntonAK.com, Matthew Starr, mstarr@huntonAK.com or Giovanna Carloni, gcarloni@huntonAK.com.

---

[1] 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/. 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] 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.

[3] See CISCO report linking accountability and privacy return on investment https://www.cisco.com/c/dam/en/us/products/collateral/security/2020-data-privacy-cybersecurity-series-jan-2020.pdf.

[4] This efficiency of scale is also relevant for SMEs that can purchase online solutions to comply with local laws and simultaneously comply with the laws across the world, thereby lowering barriers to entry into foreign markets.

[5] See CIPL's recommendations on the need for updated SCCs to reflect GDPR terms, adapt to the GDPR's expanded territorial scope, offer a modular approach and cover processor-to-subprocessor relationships. Updates to the SCC should not lead to imposing unmanageable security obligations or requirements for companies to assess a country's data protection legislation before data can be transferred outside the EU. In addition, it is necessary that organisations have a transition period for the implementation of updated SCCs to forthcoming contracts and that current SCCs related to ongoing contracts can remain in place.

- CIPL White Paper on Key Issues Relating to Standard Contractual Clauses for International Transfers and the Way Forward for New Standard Contractual Clauses under the GDPR https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_scc_final_paper.pdf.

[6] Only three companies had BCR approved in two years. See https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_fr. DPAs should also be sufficiently equipped to ensure that BCRs projects are reviewed and approved swiftly.

[7] Certifications provide a higher degree of compliance certainty than an audit can deliver and, if coupled with an ISO standard, are more globally scalable. Therefore, they represent an attractive option to enable cross-border data transfers.

[8] "The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor".

[9] See Guidelines on Personal data breach notification under Regulation 2016/679 (wp250rev.01). https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49827 page 17. "It should be clear that in the event of a breach involving cross-border processing, notification must be made to the lead supervisory authority, which is not necessarily where the affected data subjects are located, or indeed where the breach has taken place".

[10] See for instance a real case scenario to illustrate the difficulties faced by organisations when DPAs do not respect the OSS: (1) The organisation notifies the lead DPA of the cross-border breach; (2) The notified lead DPA does not have actual jurisdiction in the territories where the risk created by the breach is concentrated, and has to liaise with its counterparts through the consistency mechanism, which is cumbersome, time consuming and impractical; (3) The individuals who are actually at risk turn to their local DPA for guidance and find that their DPA is neither informed nor competent concerning the breach; (4) As a result, the uninformed DPA tends to blame the controller for not notifying the breach in the first place (even though doing so would have been contrary to the OSS mechanism); (5) Consequently, caught in the rivalry between the various DPAs, controllers notify breaches either multiple times in multiple places, or

away from their main establishment, in either case frustrating their lead DPA while also renouncing to the OSS mechanism.

[11] Some organisations report that some DPAs sometimes designate the local establishment as the main establishment´s representative to artificially create an appearance of legitimacy.

[12] See https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf.

[13] See comments from Germany, Ireland and the Netherlands. https://data.consilium.europa.eu/doc/document/ST-12756-2019-REV-1/en/pdf.

[14] The French and Spanish DPO certifications are based on national laws and not on Article 42 GDPR.

[15] See letter that some MEPs sent to the EU Commission asking to speed up on certifications for digital product or service offered in Europe, particularly in the context of the COVID-19 crisis. https://medium.com/@RenewEurope/meps-demand-eu-privacy-certificate-for-digital-products-73392b8b13fa.

[16] https://www.iso.org/standard/71670.html. ISO 277001 is an extension of the information security certification ISO27001:2013, which focuses on Information Security. See CNIL's position: "In short, ISO 27701 is a global standard: it is not GDPR specific, nor does it constitute, as such, a GDPR certification instrument as described in Article 42 of the regulation". https://www.cnil.fr/en/iso-27701-international-standard-addressing-personal-data-protection.

[17] Article 42(1) GDPR provides that Member States, the DPAs, the EDPB and the Commission shall encourage the establishment of data protection certification mechanisms, in particular at Union level.

[18] See Dutch comments https://data.consilium.europa.eu/doc/document/ST-12756-2019-REV-1/en/pdf at page 49.

[19] Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp212_en.pdf.

[20] See EU Commission 19 February 2020 Communication on a European strategy for data that recommends the development of Codes of Conduct on processing personal data in the health sector. Codes of conduct could help research in general—as a guidance document for legal clarity, and it can help guide through national laws in terms of where to take them into account.

[21] Some DPOs are even proactively choosing not to engage at all on the ostensible grounds of lacking the time and resources.

[22] The 27 different lists of high-risk processing requiring a DPIA renders the obligation to conduct a DPIA very cumbersome, it not impossible for cross-border data processing. As a result some organisations tend to avoid having to run DPIAs, sometimes even by abandoning complex cross-border business projects rather than taking on a burdensome and lengthy process with unpredictable costs and uncertain outcomes. The EDPB should produce a single list that would supersede the national lists and update it regularly.

[23] For example, the abusive use of individual access requests in employment relationships or the weaponising of data subject rights has been a worrying trend, and the different approaches of DPAs have not helped limiting the abuses and enabling organisations to provide a balanced response.

[24] E.g. in Italy and Spain, Article 28 GDPR is interpreted as being applicable to professional services, even if they are provided in the premises of the controller, while other EU countries do not require Article 28 contracts.

[25] DPAs apply different thresholds on the use of biometric data on the basis of Article 9(2)(g): For example, the Swedish DPA fined a school for performing a facial-recognition trial because it was not necessary in the "substantial public interest". On the contrary, in Denmark the roll-out of AI-powered face-tracking at a football stadium was authorised by the DPA on the basis of substantial public interest.

[26] 21 DPAs have expressed that their human, financial and technical resources are not sufficient. See EDPB report, page 30. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf.

[27] Polish DPA recommending the use of the CNIL PIA tool for conducting a DPIA: https://uodo.gov.pl/en/558/940.

[28] https://edpb.europa.eu/news/news/2019/first-standard-contractual-clauses-contracts-between-controllers-and-processors-art_fr.

[29] It seems that the Baden-Wuerttemberg DPA has also worked on Article 28 clauses.

[30] As explained in CIPL's Paper on regulatory engagement, more generally, DPAs should prioritise open and constructive relationships with the organisations and incentivise good behaviours, as deterrence and punishment have proven to have limited effectiveness in achieving the desired result of effective data protection. See CIPL 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.

[31] Article 58(2) GDPR.

[32] Several fining guidelines have been published: EDPB, Guidelines on the application and setting of administrative fines WP 253 http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889, the Netherlands https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-14586_0.pdf and Germany https://www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf.
[33] As a comparison, EU competition law—that was intended to be an inspiration to the GDPR fining model—does not rely on the turnover of the entity to define the amount of the fine. The fine is generally calculated on the basis of the sales of the products or services concerned by the infringement during the last full year of the infringement. As a result, the fine is more proportionate, especially if the infringement covers products or services whose sales amount to a small share of the turnover of the legal entity. See https://ec.europa.eu/competition/cartels/overview/factsheet_fines_en.pdf.
[34] Article 83(2) GDPR provides: "When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following: […] any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement".
[35] Examples provided by the DPAs include for instance: one-time misconduct, subsequent elimination or restoration of the lawful conditions, measures taken to avoid infringement in the future, collaboration in the proceedings, confession, negligence by omission, non-systematic nature of the processing, economic situation of the company, controller reported the offense, no material damage, infringement resulting from incorrect interpretation of the law, voluntary compensation of loss, processing concerned a small number of individuals.
[36] This requires organisations to implement comprehensive privacy programmes governing all aspects of the collection and use of personal information and be able to demonstrate the existence and effectiveness of such programmes upon request. See CIPL Accountability Discussion Paper 1 - The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society; July 2018; https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf.
[37] The mitigating factors should also include building policies and processes, investing in privacy by design, mapping data processing, developing a privacy programme training employees and business partners, providing transparency through privacy statements or in-product just-in-time notices, setting up a privacy hub, facilitating the exercise of individuals' rights through an automated privacy dashboard and a privacy-specific help desk, conducting risk analyses and DPIAs, performing audits, ensuring all documentation is maintained in good shape, appointing a DPO when not legally required, putting in place an assurance framework and effective risk management.
[38] CIPL Accountability Discussion Paper 2 - Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability - July 2018. 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.
[39] Austria, Belgium, Bulgaria, Spain, Ireland, Italy, Latvia, Malta.
[40] Cyprus, Czech, Germany, Finland, France, Greece, Luxembourg, Netherlands, Slovenia,
[41] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/04/how-we-will-regulate-during-coronavirus/.
[42] See for instance the Human Rights, Big Data and Technology Project of the University of Essex's Human Rights Centre, which has identified a number of trends in relation to the use of consent as a legal ground, including consensual exhaustion, challenges consumers face in assessing short-term benefit against potential long-term harm and the difficulty of scaling privacy self-management given the number of parties that collect personal data from users today. https://www.essex.ac.uk/research-projects/human-rights-big-data-and-technology.
[43] See parental consent deemed invalid for the use of facial recognition in high school due to the public school authority position that does not enable free and informed consent of parents for the processing of their children's personal data. https://www.legalis.net/jurisprudences/tribunal-administratif-de-marseille-9eme-ch-jugement-du-27-fevrier-2020/.
[44] Vehicles make decisions on the basis of location data in real time in the driver or passenger's best interests. See EDPB Guidelines on connected vehicles providing that in most cases consent would apply. Pages 5 and 6. https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf.
[45] In the context of the PSD2 Directive for instance, Strong Customer Authentication (SCA) may involve multiparty processing of personal data where different actors are involved (e.g. the card issuing bank, the entity assisting the bank with authentication, the merchant, the merchant payment processor, the acquirer), which makes it extremely complex to collect consents and maintain a proper proof thereof.

[46] CIPL welcomes that some Member States' laws have introduced an exception from the requirement to obtain consent for security-related purposes (e.g. the Netherlands), but regrets the lack of alignment amongst the Member States (see Section 1 of the Paper).
[47] CIPL considers that the legitimate legal base is more protective for the individual than consent as the burden to protect the data relies on the organisation that must conduct a document a proper balancing of interest test and ensure appropriate risk-based and accountable data processing measures. See 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 https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf.
[48] For more examples of possible legitimate interest cases, please refer to the CIPL paper in note 47.
[49] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/normuitleg_gerechtvaardigd_belang.pdf.
[50] See last sentence of recital 47 of the GDPR.
[51] https://op.europa.eu/en/publication-detail/-/publication/21dc175c-7b76-11e9-9f05-01aa75ed71a1/language-en – See at page 80: *"[i]n some settings, obtaining valid consent for uses that do not immediately benefit the data subject granting consent may be burdensome. Where the risk to the individual data subject is small but the potential usefulness of data access is high, interest balancing may then provide an alternative basis for data processing. Depending on legal standards, Article 6(1)(f) GDPR may thus well facilitate access to data for innovative, while non-privacy-intrusive purposes*".
[52] See CIPL's comments on the EDPB's Draft Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_final_comments_on_the_edpbs_guidelines_on_the_processing_of_personal_data_under_article_6_1__b__gdpr_in_the_context_of_the_provision_of_online_services_to_data_subjects.pdf.
[53] This is also part of the organisation's fundamental freedom to run a business under Article 16 of the European Charter of Human Rights. In addition, the GDPR should not be interpreted to govern the legality of the content of a contract, the scope of a contractual duty, what is necessary to a contract or whether general terms and conditions have been validly incorporated into a contract.
[54] It is still not clear how companies are supposed to resolve tensions between the GDPR and other national or foreign laws with extraterritorial effects that require the processing of sensitive data and criminal records for which processing is restricted by the GDPR, but which are essential to support compliance with anti-bribery and corruption laws, know your client laws or counterterrorism financing laws. Even for those organisations located outside the EU, the need to conduct due diligence on potential partners in the EU may trigger the GDPR under its extraterritorial criteria of "monitoring [EU data subjects'] behaviour" set forth in Article 3(2)(b) GDPR.
[55] See "Covid-19 Meets Privacy: A Case Study for Accountability" https://www.informationpolicycentre.com/cipl-blog.
[56] See Dutch DPA press release on use of telecom data in the fight against COVID-19, of 1 April 2020. https://autoriteitpersoonsgegevens.nl/nl/nieuws/gebruik-telecomdata-tegen-corona-alleen-met-wet.
[57] See CIPL Second Report on AI: Hard Issues and Practical Solutions at page 16. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_second_report_-_artificial_intelligence_and_data_protection_-_hard_issues_and_practical_solutions__27_february_2020_.pdf.
[58] See FTC 2012 Report "Protecting Consumer Privacy in an Era of Change – Recommendations for Businesses and Policymakers", at 21, available at https://www.ftc.gov/news-events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy.
[59] See report of the High-Level Expert Group on Business-to-Government Data Sharing https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64954.
[60] This is also worsened by the different DPA lists in defining high risks and the multitude of different guidance materials, templates, recommendations, methodologies and approaches that DPAs, professional organisations, specialised consultancies and other experts have produced.
[61] Article 35(7) GDPR provides that "[t]he assessment shall contain at least […]".
[62] See ICO blog on how trade-offs between data protection principles need to be performed and documented in the context of AI. "Organisations using AI need to identify and assess such trade-offs, and strike an appropriate balance between competing requirements. The right balance in any particular trade-off will depend on the specific sectoral and

social context an organisation operates in, and the impact on data subjects." https://ico.org.uk/about-the-ico/news-and-events/ai-blog-trade-offs/.

[63] See Dutch Comments on page 51 https://data.consilium.europa.eu/doc/document/ST-12756-2019-REV-1/en/pdf.

[64] Regulation (EEC, EURATOM) 1182/71 of the Council of 3 June 1971 determining the rules applicable to periods, dates and time limits includes language relating to periods of "two days or more", stating that "[a]ny period of two days or more shall include at least two working days". It is not clear, however, whether this provision also applies to periods expressed in hours.

[65] This has been clearly flagged by the German DPAs in their December 2019 "Report on the Experience Gained in the Implementation of the GDPR" (See https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/12/Evaluation-Report-German-DPAs-Clean.pdf. The very broad scope of paragraph 1 ("unlikely to result in a risk") thus leads to very many trivial and minor cases' being notified, placing a heavy burden on the supervisory authorities and, ultimately, resulting in their failing to spot the truly relevant cases.) The German DPAs suggest that the GDPR reporting breach threshold should be amended to limit the obligation to report only those incidents "which are likely to result in more than merely a minimal risk for the rights and freedoms of natural persons". This has also been raised in the EU Council Draft Report on the evaluation of the GDPR (https://data.consilium.europa.eu/doc/document/ST-12756-2019-REV-1/en/pdf).

[66] Internet Corporation for Assigned Names and Numbers.

[67] https://lookup.icann.org/.

[68] https://edpb.europa.eu/sites/edpb/files/files/file1/icann_letter_en.pdf.

[69] See CIPL/Hunton Legal Note: How the GDPR regulates AI. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-hunton_andrews_kurth_legal_note_-_how_gdpr_regulates_ai__12_march_2020_.pdf.

[70] See CIPL paper: "Artificial Intelligence and Data Protection in Tension," 10 October 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_ai_first_report_-_artificial_intelligence_and_data_protection_in_te....pdf.

[71] See also tension created with the blockchain technology highlighted in the EU Parliament Report "Blockchain and the GDPR. Can distributed ledgers be squared with European data protection law?" https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf.

[72] The collection of data in industrial processes may for instance include personal data of employees and their responsibilities and activities as it relates to such processes. This is also the case in machine-to-machine communication in the connected vehicle sphere that is considered by the EDPB as personal data. See note 26.

[73] See note 57 at page 16.

[74] See note 57 at page 6.

[75] See CIPL comments to WP29 Guidelines on ADM and profiling, 1 December 2017 https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_to_wp29_guidelines_on_automated_individual_decision-making_and_profiling.pdf.

[76] See CIPL white paper "Regulatory Sandboxes in Data Protection: Constructive Engagement and Innovative Regulation in Practice" https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_regulatory_sandboxes_in_data_protection_-_constructive_engagement_and_innovative_regulation_in_practice__8_march_2019_.pdf.

[77] See EU Commission Communication, "A European Strategy for Data" https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf. See EU data strategy. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy.

[78] According to Article 1(3) GDPR, "The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data".