wissenschaftliches institut für die
digitalisierung der arbeitswelt

Strategic considerations on the future of European data protection supervision

created at the request of
European and US commercial enterprises

from
Dr. Stefan Brink
Managing Director
of the Scientific Institute for the Digitalization of the World of Work wida/Berlin
State Commissioner for Data Protection and Freedom of Information Baden-Württemberg (ret.)

June 2025

The present and future of European Data Protection Supervision and Regulation: Strategic considerations

Executive Summary

The European data protection landscape is at a critical juncture, with the General Data Protection Regulation (GDPR) facing significant challenges in its implementation. Despite its intentions to promote trust and confidence in the digital economy, the GDPR has been criticized for its inconsistent and unbalanced enforcement, lack of clarity, and inadequate coordination between national authorities and the European Commission, also with a view to the new EU data regulations (DSA/DA/AI Act/DGA). This has resulted in uncertainty and obstacles for businesses, particularly small and medium-sized enterprises (SMEs).

The current GDPR enforcement governance is characterized by politicization, a radical approach to data protection and a race to the strictest position among supervisory authorities resulting in a status that could be described as privacy absolutism, in which other interests and principles beyond data protection are no longer adequately perceived. The lack of accountability, transparency, and coherence in decision-making processes has led to a culture of caution among businesses, stifling innovation and limiting growth potential.

The causes of these negative developments can be attributed to the deficiencies of the GDPR itself, including its restrictive approach to data processing and the assignment of a central position of power to independent institutions, that unilaterally favor the interest entrusted to them. Furthermore, the flawed governance structure of the European Data Protection Board (EDPB) has exacerbated these issues.

To address these challenges, a multi-faceted approach is necessary, involving both short-term and mid-to-long-term solutions. Short-term measures include increasing transparency and predictability in decision-making processes, ensuring innovation and competitiveness are included in the mandate of supervisory authorities, and improving cooperation among regulators.

In the mid-to-long term, more substantial reforms are necessary, including the adoption of additional procedural rules for the enforcement of the GDPR (different from the current proposal of the Commission), implementing DPAs accountability, an appropriate relationship between data protection and other fundamental rights and establishing a more prominent role for a differentiated and more flexible risk-based approach. At the same time, the GDPR should be guarded against being used for petty or unsubstantiated complaints.

Ultimately, strengthening the position of the EU Commission is crucial to resolving the enforcement problem. Assigning a leading position to the Commission in the EDPB, possibly in the form of a European Digitization Authority, would provide a more effective and balanced approach to data protection regulation.

By addressing these challenges and adopting a more nuanced approach to data protection, the EU can promote a culture of innovation and growth, while protecting the rights and freedoms of individuals in an exemplary manner.

Introduction

The General Data Protection Regulation (GDPR) has been a landmark regulation in the history of data protection, aiming to protect the personal data of individuals within the European Union (EU) at a globally unique level. In the 7th year of the GDPR, the regulation has established itself far beyond the EU, but its enforcement is increasingly being perceived as problematic and hostile to data driven business and technology. We are currently witnessing a substantial debate on the role of the GDPR for innovation and competitiveness in the EU at national and European level. This analysis will examine the current state of European data protection supervision and regulation, highlighting undesirable developments, underlying key issues of the GDPR and outlining potential solutions.

Current state of European Data Protection Regulation

The European data protection landscape is at a critical juncture, with a growing chorus of voices from industry and politics calling for a rethink of the current implementation of the GDPR. As the global digital economy continues to evolve at breakneck speed, concerns are mounting that the GDPR, in its current form of application, may be hindering rather than helping Europe's competitiveness and innovation. Against this backdrop, several influential reports have highlighted the need for a more balanced approach to data protection, one that takes into account the complex interplay between consumer rights, business needs, and technological advancements.

The Enrico Letta Report, "Much more than a market," highlights the importance of the GDPR in promoting trust and confidence in the digital economy. However, it also identifies significant challenges in its implementation, including inconsistent enforcement, lack of clarity, and inadequate coordination between national authorities and the European Commission. These issues hinder the full potential of the GDPR, creating uncertainty and obstacles for businesses of all sizes. To address these concerns, according to this report, a fix is necessary to improve enforcement, provide clearer guidance, and enhance international cooperation, ultimately ensuring that the GDPR achieves its intended goals of promoting trust, innovation, and growth in the digital economy.

The European Commission's second report on the application of the GDPR highlights significant challenges that necessitate a fix in its implementation. The report reveals that, despite being in effect since 2018, the GDPR continues to face inconsistent enforcement, insufficient resources for data protection authorities, and a lack of harmonization among Member States. The European Commission correctly identifies differing interpretations of the GDPR by national supervisory authorities as the main obstacle to the uniform application of the GDPR in the EU - this lack of harmonization affects core concepts of the GDPR like the comprehensive protection of all personal data and the broad enforceability of its provisions. And it of course limits the goals Commissioner Viviane Reding underlines when presenting the GDPR reform in 2012:

"This week, I will present my proposals for a reform of the EU's data protection rules. But already today, I can outline to you the main characteristics of the new legislation which will make the Digital Single Market more accessible for both businesses and consumers, which will make Europe more competitive and which will become an international standard-setter in terms of modern data protection rules."[1]

Additionally, the complexity and bureaucracy of the regulation create barriers for small and medium-sized enterprises, while citizen awareness about their rights under the GDPR remains low. Furthermore, the rapid evolution of technologies such as artificial intelligence raises concerns about the GDPR's effectiveness in addressing these emerging issues and urgent social and economic challenges. To address these challenges and ensure the GDPR remains effective and relevant, the EU Commission considers it necessary to improve its proper implementation and promote a more consistent and harmonized approach to data protection across the EU, enabling a free movement of personal data and consistency with the EU's digital strategy.

The Report on the competitiveness of the EU by former President of the European Central Bank Mario Draghi on behalf of the President of the EU Commission assesses the GDPR as a double-edged sword for the European economy. While the report acknowledged the merits of the GDPR in enhancing consumer privacy and trust it highlights the need for a more balanced approach to data protection, recognizing the importance of data-driven innovation for the EU economy. The report outlines the significant compliance costs the GDPR imposes, particularly on startups and small to medium enterprises (SMEs)[2]. The report deplores that these burdens hinder innovation and growth and make it more difficult for European companies to compete in the global market[3]. The report concludes that these costs can limit innovation and deter foreign investment, as businesses face challenges in navigating complex regulations[4]. Draghi warned that besides the general risk aversiveness by regulators, specifically the consequences of the GDPR **complexity and fragmented implementation,** which if not addressed, have an impact on the competitive landscape and hinder Europe's ability to lead in emerging technologies, ultimately affecting growth and economic dynamism.

In contrast to the current debate on the need to fix the data protection framework, the **legal situation currently seems to be cemented** by the GDPR, and no changes to the legal text appear to be intended by the European Commission at present given the conclusions in its recent report. The extensive political initiatives of the EU Commission, which have introduced new data protection regulations (DA/DSA/AI Act/DGA), stand in

[1] https://ec.europa.eu/commission/presscorner/api/files/document/print/en/speech_12_26/SPEECH_12_26_EN.pdf

[2] Compliance costs for European startups and small to medium enterprises (SMEs) can be prohibitive, averaging 12% of their revenues, compared to just 5% in the US.

[3] For example, the (US) hyperscalers have now moved away and cannot be caught up with, and investments of €800 billion are needed in the EU to maintain competitiveness.

[4] As another example of the consequences of an innovation-hostile environment in the EU Draghi highlights that of the 141 "unicorns" (founded in Europe between 2008 and 2021), 40 have moved their headquarters abroad.

stark contrast to the GDPR, which remains unchanged to this day but plays a dominant role. This disregards widely shared concerns and developments with respect to enshrined central shortcomings of the GDPR, in particular

- placing supervision in the hands of 27+ completely independent supervisory authorities (Germany alone has 17 state authorities) that are not politically accountable for decision making and pursue economic regulation from the perspective of individual protection alone, with a tendency to interpret the GDPR in a highly restrictive and isolated manner. **Entrusting independent institutions with a one-sided mandate to regulate emerging markets is an extraordinary and risky experiment.**
- the fundamental decision to classify any processing of personal data as prohibited with reservation of permission, i.e. an exception requiring justification, instead of regulating only particularly risky data processing. **This gives the right of informational self-determination a systematic prevalence over competing rights and/or interests.**

In addition to the problematic legal situation, which is difficult to change without the political will of Member States governments, the peculiarities of enforcement in the area of data protection give rise to additional problems. We see supervisory authorities, often inadequately equipped with personnel and material resources, which do neither adequately reflect in their decisions the free-movement of personal data (Art.1 (3) GDPR), nor embrace the risk-based approach (Arts. 25, 32, 35 GDPR), and insufficiently balance other rights and interests (Recital 4 GDPR). Furthermore, it becomes increasingly evident that we have a broken GDPR supervision governance with a malfunctioning One-Stop-Shop and an EDPB acting as co-regulator and quasi-legislator without the required accountability, transparency and procedural safeguards.

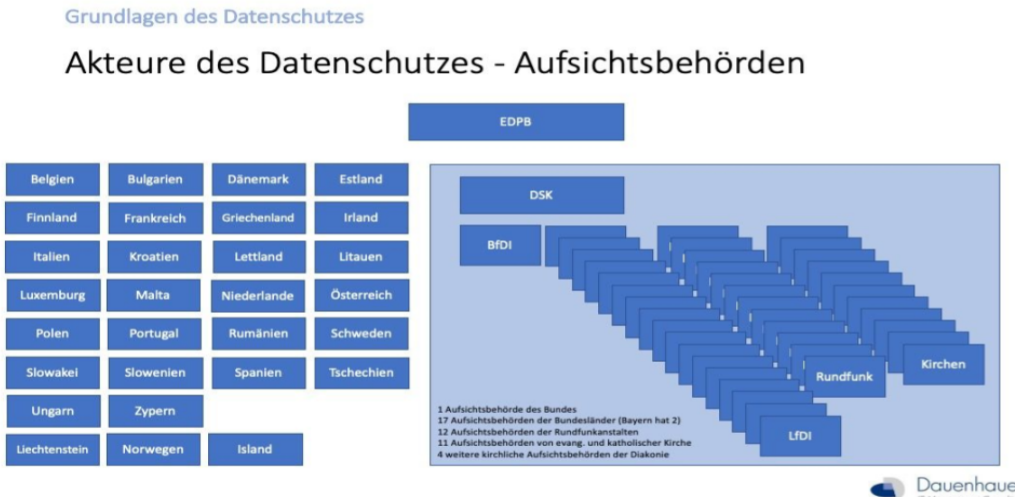
A lack of accountability for official intervention in internet-based business models is not only to be found with the national supervisory authorities, but also with their coordination and consistency body, the EDPB (see Art. 68 GDPR): Although the EDPB has its own legal personality (Art. 68 (1) GDPR) and its decisions have binding effect on the national supervisory authorities (cf. Art. 65 and 66 GDPR), these decisions cannot be directly challenged in court. Although the decisive decision-making power lies with the EDPB, it therefore bears no responsibility for its own actions. According to widespread opinion, only the implementing decisions of the national supervisory authorities are subject to judicial review. This is helped by the fact that the EDPB's decisions have been held by the EU General Court[5] to have no external effect, on the basis that they must formally be implemented by the lead supervisory authority. Therefore, if the General Court's decision

[5] https://curia.europa.eu/juris/liste.jsf?num=T-709/21

stands[6], only the lead supervisory authority is subject to judicial review,

This “lack of accountability” of the EDPB has numerous negative consequences: it makes the EDPB more “uninhibited” in its decision-making and more negligent when it comes to safeguarding procedural rights such as the right to be heard of the parties involved. As the EDPB's decision is also seen by the EDPB itself as a purely internal and preparatory act, participation rights and duties to state reasons are systematically neglected. At the same time, the Member State supervisory authorities see themselves as less responsible because they are bound by the EDPB decision, which makes them less accountable and less accountable and so much more interventionist. This distribution of roles in the GDPR also has considerable disadvantages for data subjects and data controllers: in the absence of a direct judicial review of the EDPB requirement, the first step is to go through the national courts, which means considerable costs, prolonged legal uncertainty and a possible bogging down of the legal issue in the Member State courts.

Added to this are the costs of a complex and inefficient EU supervisory system, which is further increased by national peculiarities such as German federalism with 17 state supervisory authorities that have to coordinate the activities on EU, the federal and state level and that have very different levels of capacity and understandings of data protection.



Overview of the fragmented supervisory structure for data protection in the EU and Germany. N.B. Supervisory authorities for the protection of privacy in electronic communications and other legal acts with an impact on data protection are excluded.

[6] It is the subject of an appeal to the CJEU

Initial Findings and Illustrative Examples

This **current state of GDPR enforcement** actually results in negative impacts and implications for legal certainty, harmonisations and the EU digital economy. The consequences are the same throughout Europe: business models based on the monetisation of personal data will neither be developed nor approved in the EU; at best, the EU will become a sales market for products that are developed and operated outside of Europe. The costs of over- and misregulation include an innovation-hostile climate and - seen over the long term - the risk of deindustrialization.

Following **three examples** shall help illustrate the inherent problems of data protection regulation and the highly problematic consequences thereof:

Example 1: EDPB Opinion on "Pay or Consent"

The European Data Protection Board's (EDPB) Opinion 08/2024 on "Pay or Consent" exemplifies the unpredictability, lack of balance, and arbitrariness that plagues GDPR supervision. This opinion highlights the challenges faced by organizations in navigating the ever-changing landscape of data protection regulations with respect to behavioral advertising, where meaningful and practical options for data processing are rejected, and even the use of personal data as a basis for business models is questioned. The opinion demonstrates the complexity and lack of certainty inherent in applicable GDPR regulation, with constantly evolving regulatory requirements, unclear boundaries, and a lack of clarity on key concepts such as "consent". Furthermore, it highlights the fragmentation and unbalanced approach to GDPR supervision, with disparate regulatory approaches, an unbalanced focus on enforcement, and a lack of harmonization across Member States.

This radical approach reflects the EDPB's explicitly anti-business positions, which disregard the provisions of the GDPR and the EU acquis, and denies that personal data can be the subject of an economic exchange at all. The EDPB steps outside the remit of the GDPR with potentially substantial consequences for businesses, consumers and the economy as well as the free and open internet widely enabled by ads sponsored business models. Ultimately, this opinion underscores the need for clearer boundaries and respective guidance, greater harmonization, and a more balanced approach to GDPR regulation taking into consideration the EU acquis.

Example 2: AI Model Training

The GDPR has created a complex landscape for companies operating in the EU, particularly when it comes to using personal data for training artificial intelligence (AI) models. The regulation's six legal bases for processing personal data have been interpreted differently by various European Data Protection Authorities (DPAs), leading to confusion and uncertainty for businesses.

For instance, some DPAs take a more restrictive stance and require consent from individuals for AI model training, denying companies the ability to rely on legitimate interests. In contrast, other DPAs have taken a more nuanced approach, allowing AI model training on the basis of legitimate

interests. It is important to note that the requirement for consent, as advocated by some DPAs, would make it difficult to train effective AI models, ultimately impacting the competitiveness of the European AI industry. At the same time, German regulatory authorities are now taking positions that no longer comply with legal principles - for example - it is claimed that unlawful training of AI models could impact the use of AI systems and thus also "infect" the application level. There are no legal arguments for this – nevertheless, this is the negotiating position of the majority of German regulators.

These extreme and divergent approaches create significant hurdles and uncertainty for businesses operating in the EU and respective investments, making it difficult to train effective AI models or deploy them, and risking severely impacting the competitiveness of the EU AI industry. Industry and policy makers recognise and highlight the need for clarity and consistency in the application of GDPR rules, emphasizing the importance of training AI with specific and differentiated personal data. It is not to be assumed that the EDPB's expected general statement, which is also intended to have a regulatory effect beyond large online platforms, will distance itself from these positions. However, the current regulatory environment creates significant uncertainty and hurdles for businesses, underscoring the need for a more nuanced and balanced approach to GDPR regulation. Since December 17, 2024, Opinion 28/2024 of the EDPB has been in place. Rather than creating legal certainty, significant questions remain open, such as whether AI models contain personal data or in regard to the processing of Art. 9 data. And even where this Opinion opens up avenues (such as the legal basis of legitimate interest), it seems that the draft of EDPB guidelines on legitimate interest (in October) and pseudonymization (in January) close these avenues again.

Example 3: Data Transfer Saga

The history of data transfers between the EU and the USA serves as a quintessential example of the intricate complexities, lack of certainty, and fragmentation inherent in GDPR supervision. This ongoing series of events and developments highlights the challenges faced by the European Commission, supervisory authorities, and the European Court of Justice (ECJ) in establishing a reliable and consistent basis for data transfers between highly developed constitutional states.

The data transfer saga is characterized by a constantly shifting regulatory landscape, inconsistent interpretations, and a lack of clear guidelines and standards for data transfers. This has created a complex environment, making it challenging to impossible for organizations to ensure compliance with GDPR requirements. Furthermore, the disparate national approaches to GDPR supervision, inequitable distribution of power, and unbalanced enforcement have led to uncertainty and confusion among organizations and individuals involved in cross-border data transfers. This came at the cost of transatlantic business transactions and came at a considerable cost to the EU economy. Even the EU Commission was recently undone by the transfer issue: in a judgment of the European GENERAL COURT (Case T-354/22 | Bindl v Commission) of January 8, 2025, it was ordered to pay €400 in damages due to a hyperlink to the USA knowingly used by the data subject. Ultimately, this example underscores the need for a more harmonized, risk-based and balanced approach to data protection regulation, one that takes into account the diverse needs and interests of all stakeholders involved. A more coherent and effective framework for data transfers is necessary to ensure the free flow of data while protecting the rights and freedoms of individuals.

Adverse developments in European Data Protection Regulation

This precarious situation merits a deeper analysis of its causes and conditions: The current GDPR enforcement governance is characterized by a complex interplay of factors that have led to the **politicization, a radicalized approach to data protection, and a race to the strictest position** among supervisory authorities. At its core, the European data protection landscape is marked by the One-Stop-Shop principle and the European Data Protection Board (EDPB), which consists of 27 EU Member States' data protection authorities (DPAs) operating with a high degree of independence.

While the EDPB was established to ensure coherence and consistency among DPAs, its structure and mechanisms have inadvertently created an environment that fosters competition and one-upmanship among supervisory authorities. The DPAs are incentivized to demonstrate their commitment to data protection by adopting the strictest positions, which has resulted in a politicization and radicalization of some supervisory authorities. This phenomenon is further exacerbated by the lack of accountability and transparency in the decision-making processes of DPAs, allowing them to operate with relative impunity - the diffusion and lack of accountability sometimes leads to carelessness in the exercise of power.

Moreover, the coherence mechanisms established by the EDPB, such as the consistency mechanism and the dispute resolution mechanism, have been used and weaponized to impose stricter positions on controllers in other Member States. Instead of ensuring consistency and cooperation among DPAs, these mechanisms have become tools for overriding national authorities and imposing more stringent requirements on businesses. This has led to a further erosion of the One-Stop-Shop principle and created a culture of regulatory competition, where DPAs are incentivized to take extreme positions to demonstrate their commitment to data protection.

The EDPB's structure, which allows for decision-making behind closed doors and without full public consultation, has also contributed to this problem. The absence of expert input from the field and insufficient consideration of other regulations, rights, and interests, not seldom leads to harmful outcomes for legal certainty and coherence. Furthermore, the lack of transparency and accountability in the process allows DPAs to defer criticism of their decisions to a majority vote of the EDPB, rather than taking responsibility for their actions and positions.

This development also has significant consequences in the member states. In Germany, for instance, the supervisory authorities are under increasing pressure due to the perception that data protection practices are hostile to innovation and the economy. As a result, new supervisory tasks for example in the area of AI surveillance are being assigned to other institutions. These political and institutional reactions to perceived enforcement problems do not, however, lead to a self-reflection by the data protection authorities, but rather to a further radicalization of the positions of the

supervisory authorities. This radicalization is not only limited to the content of their positions but also extends to their politicization, ultimately affecting the legal obligations of these state bodies as public authorities subject to the law.

Back to the European level: The way the EDPB is set up allows for one-sided decision-making and does not provide sufficient accountability for its decisions. This has led to a situation where supervisory authorities are getting rougher with each other, and the concentration of responsibility of the one-stop-shop is being respected less and less. The EU Commission and other institutions, such as competition authorities, are also engaged in a race for an even tougher data protection position, further exacerbating the problem.

The consequences of this misalignment

The current GDPR enforcement governance has led to a concerning trend of privacy absolutism over other legitimate interests and rights, lack of balance in resolving conflicts of interest, and a zero-risk approach among Data Protection Authorities (DPAs). This phenomenon is not a result of overregulation, but rather misregulation, where DPAs have deviated from the original intent of the GDPR.

The GDPR was designed to be a forward-thinking, in principle risk-based, and technologically neutral framework that empowers DPAs to intervene in cases where personal data pose significant risks to EU users' privacy. However, in practice, DPAs have moved away from this risk-based approach and failed to strike a necessary balance between different fundamental rights.[7] Specifically, they struggle to evaluate and factor in the economic and societal benefits of technological advancements against potential risks, balance the right to data protection with other fundamental rights and freedoms, including the freedom to conduct a business, and adopt an evidence-based position regarding perceived areas of risk.

As a result, DPAs tend to resort to highly restrictive policies, such as restricting data transfers, personalized ads, and AI training, which may be easier to enforce but ultimately foster legal uncertainty and stifle commerce, innovation, and progress. This approach is problematic for several reasons. Firstly, it fails to consider the broader societal and economic implications of technological advancements, leading to a narrow focus on data protection at the expense of other important interests. Secondly, it creates a culture of fear and caution, where businesses are reluctant to invest in new technologies or innovate due to the uncertainty and risk of regulatory action.

Furthermore, this approach undermines the GDPR's original goal of contributing to the single market of data. By adopting overly restrictive policies, DPAs are creating a

[7] https://fpf.org/blog/what-happened-to-the-risk-based-approach-to-data-transfers/

fragmented regulatory landscape that hinders the free flow of data across borders. The lack of capacity and predictability among national supervisory authorities has resulted in inconsistent enforcement, creating uncertainty and confusion among businesses. This, in turn, can lead to a loss of competitiveness for European businesses, as they struggle to keep pace with their global counterparts.

Moreover, the zero-risk approach adopted by DPAs is unrealistic and unachievable - and not legally required. It is impossible to eliminate all risks associated with the use of personal data, and attempting to do so can lead to unintended consequences, such as over-regulation and stifling innovation. A more balanced approach would recognize that some level of risk is inherent in any activity involving personal data and seek to mitigate those risks through proportionate and effective measures.

In conclusion, it becomes evident that the current GDPR enforcement governance has created an environment that encourages **politicization, radicalization, and a race to the strictest position among supervisory authorities**. The lack of accountability, transparency, and coherence in the decision-making processes of DPAs, combined with the inappropriate use of coherence mechanisms and the EDPB's structure, have all contributed to this phenomenon. At the same time, the current GDPR enforcement governance has resulted in a concerning **trend of privacy absolutism, lack of balance, and a zero-risk approach among DPAs**. This approach is misguided and can have serious consequences for commerce, innovation, and progress.

Underlying Causes for Adverse Developments

The causes of the negative developments in the European data protection landscape can be attributed to two primary factors: the deficiencies of the GDPR itself and the flawed Data Protection Enforcement governance structure and practices.

Firstly, the GDPR's prohibition with reservation of permission approach has led to a change of direction towards a slowed innovation and data economy. Article 6 of the GDPR, which outlines the principles for lawful processing of personal data, has been interpreted as a restrictive framework that prioritizes individual informational self-determination over other rights and economic interests. By classifying all personal data processing as prohibited with reservation of permission, the framework creates a culture of caution where companies prioritize business continuation over innovation, making them vulnerable to disruptors. The assumption of illegality and draconian punishments lead to maladaptive behavior, stifling innovation and limiting growth, ultimately threatening European companies' competitiveness in the global economy. A more nuanced approach is needed and also required by the principle of proportionality, focusing on particularly risky data processing activities and providing clear guidelines for compliance, to strike a balance between data protection and innovation. This approach poses a significant economic risk to companies innovating

in the digital space and has resulted in a culture of caution among businesses, who are hesitant to invest in new technologies or innovate due to the uncertainty and risk of regulatory action.

Furthermore, the assignment of a central position of power to independent institutions with no checks and balances to hold them accountable, such as the data protection supervisory authorities, has created an imbalance in the regulatory framework. These authorities were established to safeguard and strengthen individual informational self-determination, but they have failed to take a balanced position that includes and promotes the common good and considers other rights and interests. The case law of the European Court of Justice (ECJ) on the GDPR has reinforced this one-sided understanding, stating that "the high level of data protection" should be the guiding principle. As a result, supervisory authorities have unilaterally taken the side of data subjects, neglecting their responsibility to balanced regulation.

The GDPR provisions concerning the cooperation of the supervisory authorities and the consistency mechanism (which make up almost half of the GDPR) also prove to be a systematic obstacle. The competent supervisory authorities (one stop shop) are thus restricted in their role; ultimately, they only make preliminary decisions until the EDPB has spoken. This leads to hesitant positioning on the part of the lead supervisory authority – and to offensive and exaggerated positions on the part of the concerned supervisory authorities. This lack of legitimacy (and accountability) leads to an overly active EDPB, which slows down the capacity of the leading Supervisory Authority to take decisions. This in turn means that controllers have even less legal certainty as they are in the end dealing with the EDPB Members rather than one LSA for product launches etc.

Moreover, the supervisory authorities' perception of themselves as antagonists of the data processing industry has led to a confrontational approach, where they strive to limit the data economy rather than balancing interests. This adversarial mindset has created a toxic environment, where businesses are viewed as adversaries rather than responsible stakeholders in ensuring the sensible use of personal data.

Fixing the GDPR Enforcement System: Opportunities and Solution Options

To address the politicization, radicalization, and a race to the strictest position among supervisory authorities, as well as the issue of privacy absolutism over other legitimate interests and rights, lack of balance, and a zero-risk approach among DPAs, it is essential to adopt a multi-faceted approach that involves both short-term and mid-to-long-term solutions.

Short-term solutions

In the short term, several measures can be taken to address the current issues. Firstly, **increasing transparency and predictability** in decision-making processes at the EU level is crucial. This can be achieved by introducing greater openness in procedures, such as **systematic and broader participation of stakeholders** in the run-up to EDPB decisions. The early involvement of stakeholders from industry, science and consumer organizations should be understood as a legal obligation, rather than being left to the discretion of the EDPB.

Secondly, **ensuring innovation and competitiveness** should be **included in the mandate of supervisory authorities**, as exemplified by the French CNIL's objective of promoting innovation (*draft law*). An adapted authority mandate that explicitly includes the free movement of data, the digital single market or internal data market, competitiveness, and innovation would help to strike a better balance between data protection and other fundamental rights and interests.

Thirdly, supervisory authorities must ensure **structured dialogue and regular exchange with business, politics, and civil society**, as laid down in Article 70(4) of the GDPR.

Improved cooperation among federal regulators in the Member States can lead to greater professionalism and predictability, which can be achieved through procedural changes such as moving away from the (German) unanimity principle and making majority decisions binding for all regulatory authorities.

Mid-to-long-term solutions

In the mid-to-long term, more substantial reforms are necessary to address the underlying causes of the current issues. Firstly, the proposal for a Regulation of the European Parliament and of the Council laying down **additional procedural rules for the enforcement of the GDPR** should be reassessed to provide a more robust framework for ensuring consistency and cooperation among supervisory authorities, accountability for their decisions and certainty as well as effective procedural rights for controllers. **This would require that current Trilogue texts are reassessed and**

reconsidered.

Since, from a political perspective, the responsibility for its decisions lies with the EDPB, it should be possible to challenge them directly before the General Court/CJEU - also for reasons of time and because of the legal uncertainty that will exist until then. The European Court of Justice's ability to challenge decisions of the EU Commission under antitrust law could serve as a model for this. In the meantime, the CJEU will have the opportunity to establish direct challengeability of EDPB decisions by companies / other third parties in the EU courts.[8]

Secondly, an **appropriate relationship between data protection and other fundamental rights**, such as entrepreneurial freedom, must be implemented. This requires a more nuanced approach that takes into account the complex interplay between different fundamental rights and interests.

Thirdly, a **more prominent role for the risk-based approach** should be established, particularly for personal references/anonymization, data transfers, and sensitive data. This would enable a more balanced approach to data protection that takes into account the specific risks and benefits associated with different types of data processing.

Strengthening the EU Commission's position

Ultimately, the enforcement problem can only be convincingly resolved by **strengthening the position of the EU Commission, as far as GDPR interpretation and cross-border enforcement affecting the single market are concerned**. The Commission is best placed to develop and maintain a uniform, consistent position that is not one-sidedly fixated on data protection (and benefits from a competent legal service whose expertise is not limited to data protection, is better resourced and equipped to conduct the balance that is needed and to abide by the rule of law). To achieve this, the Commission could be assigned a leading position in the EDPB, possibly in the form of a European Digitization Authority, with **national supervisory authorities playing an advisory role**. This would correct the historical misalignment and lack of accountability that has led to the current issues and provide a more effective and balanced approach to data protection regulation. A single EU enforcer for cross border controllers would have legitimacy at the right level and prevent a diffusion of responsibility.

[8] See further Mlex Article on the *C-97/23 P — WhatsApp Ireland v EDPB* hearing: “WhatsApp argues for direct challenge of EU privacy watchdogs’ decision. (2024, November 26). Retrieved from *https://www.mlex.com/mlex/articles/2265801?scroll=1&related=1*

Conclusion

In conclusion, the European data protection landscape is at a critical juncture, with the GDPR facing significant challenges in its implementation. The current GDPR enforcement governance is characterized by politicization, radicalization, and a race to the strictest position among supervisory authorities, resulting in privacy absolutism over other legitimate interests and rights and a lack of balance. This has led to uncertainty and obstacles for businesses, particularly small and medium-sized enterprises (SMEs), and has hindered innovation and growth.

To address these challenges, a multi-faceted approach is necessary, involving both short-term and mid-to-long-term solutions. Short-term measures include increasing transparency and predictability in decision-making processes, ensuring innovation and competitiveness are included in the mandate of supervisory authorities, and improving cooperation among federal regulators.

In the mid-to-long term, more substantial reforms are necessary, including the adoption of appropriate procedural rules for the enforcement of the GDPR reassessing the current proposal discussed in the trilogues, implementing an appropriate relationship between data protection and other fundamental rights, and establishing a more prominent role for the risk-based approach.

Ultimately, strengthening the position of the EU Commission is crucial to resolving the enforcement problem. Assigning a leading position to the Commission in the EDPB, possibly in the form of a European Digitization Authority, would provide a more effective and balanced approach to data protection regulation.

By adopting a more nuanced approach to data protection, the EU can promote a culture of innovation and growth, while protecting the rights and freedoms of individuals in an exemplary manner. It is essential that policymakers and stakeholders work together to address the challenges facing the GDPR and ensure that it remains a relevant and effective framework for regulating data protection in the digital age.

Managing Director
of the Scientific Institute for the Digitalization of the World of Work wida/Berlin
State Commissioner for Data Protection and Freedom of Information Baden-Württemberg (ret.)