FUTURE OF PRIVACY FORUM

VUB

BRUSSELS PRIVACY HUB

Brussels Privacy Symposium 2023

Understanding the EU Data Strategy Architecture: Common Threads – Points of Junction – Incongruities

Symposium Report

Authors: Bianca-Ioana Marcu and Christina Michelakaki
Copyeditor: Alexander Thompson

February 2024

The Future of Privacy Forum

In Europe, the Future of Privacy Forum (FPF) is an independent voice, maintaining neutrality in any discourse. FPF is optimistic that social and economic good can be achieved through innovation in data and technology while also respecting privacy and data protection rights. FPF has built strong partnerships across Europe through its convenings and trainings for policymakers and regulators. FPF's transatlantic engagement helps regulators, policymakers, and staff at European Union data protection authorities better understand the technologies at the forefront of data protection law. FPF explains EU data protection and privacy law and the European Court of Human Rights legal framework to make them easily understandable for stakeholders in the U.S. and around the world. FPF hopes to bridge the gap between European and U.S. privacy cultures and build a common data protection language.

A space for debate and dialogue: FPF is a non-profit organization providing a space for debate and dialogue by:

- Sharing knowledge of European privacy and data protection law with its members
- Connecting a network of key players from corporations, NGOs, academics, civil society, and regulators
- Engaging with EU regulatory bodies and policymakers
- Being a respected voice in the media
- Advising corporations and policymakers regarding technological, privacy and data protection issues
- Offering regular peer-to-peer gatherings, workshop, and training interventions in selected hotspots across Europe

Brussels Privacy Hub

At the Brussels Privacy Hub (BPH), we believe strongly in the relevance and importance of data protection and privacy law, particularly in light of the challenges posed by the rapid development of technology and globalization. We also believe that fresh and innovative thinking based on multidisciplinary research is necessary to meet these challenges. The BPH thus brings together scholars from a wide array of disciplines who collaborate with the private sector, policymakers, and NGOs to produce cutting-edge research. We believe in network-building and have built a strong network of contacts with leading privacy researchers both in and outside the EU. The BPH's main goals are to produce privacy research of the highest quality, bring together leading thinkers from around the world, and foster an interchange of ideas among privacy stakeholders in a climate of intellectual openness.

Table of Contents

1. Introduction 1

2. Opening Remarks: the GDPR as the Cornerstone of the EU Digital Regulatory Framework 2

3. Shifting the Paradigm? Dispelling the Push for Access to Data in the Data Strategy Package 3

3.1 THE FUNDAMENTAL ROLE OF THE GDPR 3

3.2 THE DATA ACT, OVERLOOKED NUANCES, AND EXPECTED IMPACTS ON COMPANIES 4

3.3 THE NEED FOR CLEAR GUIDANCE TO MEET DATA ACCESS OBLIGATIONS 4

4. A Network of Impact Assessments – from the GDPR to the DSA and the AI Act 6

4.1 IMPACT ASSESSMENTS AS TOOLS FOR REGULATING TECHNOLOGY AND PROTECTING CONSUMERS 6

4.2 DRAWING FROM THE GDPR EXPERIENCE AS WE TURN TOWARDS THE DSA AND AI ACT 7

4.3 PROVIDERS AND DEPLOYERS OF AI SYSTEMS: SHARED RESPONSIBILITIES? 8

5. What future, then, for data enforcement in Europe? 9

5.1 EXPLORING ENFORCEMENT MODELS IN EU LAWS 9

5.2 ZOOMING IN ON ENFORCEMENT AT THE MEMBER STATE LEVEL 10

5.3 FROM MEMBER STATE LEVEL SUPERVISION AND ENFORCEMENT TO THE ROLE OF THE EUROPEAN COMMISSION 10

5.4 EXPLORING THE ROLE OF DATA PROTECTION AUTHORITIES (DPAS) AND REGULATORY COOPERATION IN ENFORCING THE EU DATA STRATEGY PACKAGE 11

5.5 THE FUTURE OF DATA ENFORCEMENT IN EUROPE 12

6. Concluding Remarks: Aligning Enforcement with Existing Data Protection Law 13

1. Introduction

The 7th edition of the Brussels Privacy Symposium, jointly co-organized by the Future of Privacy Forum and the Brussels Privacy Hub, took place at the U-Residence of the Vrije Universiteit Brussel campus on November 14, 2023. The Symposium presented a key opportunity for a global, interdisciplinary convening to discuss one of the most important topics facing Europe's digital society today and in the years to come: **"Understanding the EU Data Strategy Architecture: Common Threads – Points of Juncture – Incongruities."**

With the program of the Symposium, the organizers aimed to transversally explore three key topics that cut through the Data Strategy legislative package of the EU and the General Data Protection Regulation (GDPR), painting an intricate picture of interplay that leaves room for tension, convergence, and the balancing of different interests and policy goals pursued by each new law. Throughout the day, participants debated the possible paradigm shift introduced by the push for access to data in the Data Strategy Package, the network of impact assessments from the GDPR to the Digital Services Act (DSA) and EU AI Act, and debated the future of enforcement of a new set of data laws in Europe.

Attendees were welcomed by Dr Gianclaudio Malgieri, Associate Professor of Law & Technology at Leiden University and co-Director of the Brussels Privacy Hub, and Jules Polonetsky, CEO at the Future of Privacy Forum. In addition to three expert panels, the Symposium opened with Keynote addresses by Commissioner Didier Reynders, European Commissioner for Justice, and Wojciech Wiewiórowski, the European Data Protection Supervisor. Commissioner Reynders specifically highlighted that **the GDPR remains the "cornerstone of the EU digital regulatory framework"** when it comes to the processing of personal data, while Supervisor Wiewiórowski cautioned that **"we need to ensure the data protection standards that we fought for, throughout many years, will not be adversely impacted by the new rules."** In the afternoon, attendees engaged in a brainstorming exercise in four different breakout sessions, and the Vice-Chair of the European Data Protection Board (EDPB), Irene Loizidou Nikolaidou, gave her closing remarks to end the conference.

The following Report outlines some of the most important outcomes from the day's conversations, highlighting the ways and places in which the EU Data Strategy Package overlaps, interacts, supports, or creates tension with key provisions of the GDPR. The Report is divided into six sections: the above general introduction; the ensuing section which provides a summary of the Opening Remarks; the next three sections which provide insights into the panel discussions; and the sixth and final section which provides a brief summary of the EDPB Vice-Chair's Closing Remarks.

2. Opening Remarks: the GDPR as the Cornerstone of the EU Digital Regulatory Framework

In the opening of the 7th Brussels Privacy Symposium, **Commissioner Didier Reynders**, European Commissioner for Justice, offered the first Keynote address. The Commissioner noted that recent legislative initiatives recognize that data is at the center of the digital transformation. While there are many benefits that the use of data can bring to the economy and society, the Commissioner argued that the individual must come first. He therefore pointed out that the GDPR remains the cornerstone of the EU digital regulatory framework. In some cases, the new initiatives complement or build on the GDPR. The Data Act (DA), for example, empowers the data user, in line with the GDPR's right to data portability. The European Health Data Space (EHDS) empowers users to control their medical data in their home country and in other Member States, while also making data available for researchers to augment their work. The EU's Artificial Intelligence (AI) Act ensures the protection of fundamental rights and safety when AI is used. Thus, the GDPR is in fact further embedded through these new Acts. The Commissioner noted that the success of all digital rules will depend on their effective enforcement, and, as such, GDPR's Procedural Reform will enhance the efficiency of cross-border enforcement of the GDPR and establish better cooperation between Data Protection Authorities (DPAs).

In the Symposium's second Keynote address, **Wojciech Wiewiórowski**, the European Data Protection Supervisor, highlighted the importance of discussing data protection in the context of the EU's "data strategy architecture" and related legislative initiatives. The Supervisor argued that **we should avoid a simplistic categorization of the new "data laws" and stressed the need to recognize their distinct characteristics.** He also mentioned that one of the biggest challenges is going to be the enforcement of all the new laws and, in particular, the challenge to ensure regulatory consistency. The Supervisor also delved into the specifics of the Digital Services Act (DSA) and Digital Markets Act (DMA), emphasizing the interplay between these instruments and the GDPR. He finally noted that the EDPS "will remain vigilant" to ensure that data protection standards will not be adversely impacted by the new rules. He concluded on a positive note, assuring that we will be able to find ways for individuals to both reap the benefits of an increasingly digital economy and enjoy optimal protection of their fundamental rights.

3. Shifting the Paradigm? Dispelling the Push for Access to Data in the Data Strategy Package

The first panel of the Symposium, "Shifting the Paradigm? Dispelling the Push for Access to Data in the Data Strategy Package," delved into the concept of data access. Most Acts in the Data Strategy Package mandate a relevant data access obligation. Under the DMA, gatekeepers have an obligation to share data created by users with both end users and business users through continuous and real-time data portability. Article 40 of the DSA mandates that very large online platforms (VLOPs) and very large online search engines (VLOSEs) have an obligation to share data with competent authorities upon reasoned requests. Both the Data Governance Act (DGA) and the DA concern non-personal data, but deciding which categories of data fall under their scope becomes a rather complex task. The panel analyzed how the GDPR's strong requirements and obligations can remain in full force alongside such new obligations. The panel featured Anna Buchta, Head of Unit "Policy and Consultation" at the EDPS, John Miller, Senior Vice President for Policy and General Counsel at the Information Technology Industry Council (ITI), Amal Taleb, Director of EU Government Affairs at SAP, and was moderated by Christina Michelakaki, Policy Fellow for Global Privacy at FPF.

3.1. THE FUNDAMENTAL ROLE OF THE GDPR

Anna Buchta explained that the EDPS has been actively involved in exploring the interplay between data protection principles and regulations, competition rules, and consumer protection laws for over a decade. The EDPS emphasizes the importance of clearly defining the objectives of each regulation to ensure consistent and coherent interpretation of the law. Buchta noted that under EU law, all regulations are equal, *but some regulations are more equal than others,* referring to the prevalence of the GDPR. Regarding the relationship between the GDPR and the other regulations in the Data Strategy Package, she explained that the EDPS highlights that the GDPR's legal basis indicates its precedence over the other instruments. This is further supported by Article 23 of the GDPR, which mandates compliance with its requirements for compatibility with data protection principles as stipulated by the EU Charter of Fundamental Rights (EU Charter), and Article 8 of the Charter in particular.

Buchta noted that to achieve consistent interpretation, the EDPS advocates for structured cooperation between DPAs and other relevant bodies. Initiatives towards this direction are the DMA's High-Level Group and the DGA's European Data Innovation Board. Even though these bodies will not enforce the law or work on specific cases, they will provide a forum for exchange to hopefully arrive at consistent and coherent interpretations of the law. She also pointed to the duty of loyal cooperation, including consultation of the DPA when considering aspects that are also pertinent to data protection and to the application of the GDPR. This follows directly from the jurisprudence of the Court of Justice of the European Union (CJEU). The EDPS also foresees the development of EDPB guidelines, such as guidance on the interplay between the GDPR and the DMA, and has already established a task force dedicated to the interplay between data protection, competition, and consumer protection rules.

Buchta expressed skepticism on whether we can refer to the current regulatory landscape as a paradigm shift, insofar as data governance and data protection are concerned. She argued that even if our "datafied" society calls for more processing activities, the GDPR is still in force and should be taken into consideration to ensure that processing personal data is done in line with the law and the EU Charter. Therefore, despite the intricate nature of the new regulations, Buchta underscored the importance of aligning all processes with GDPR's requirements, especially emphasizing a case-by-case evaluation to determine the correct legal basis for data processing.

3.2. THE DATA ACT, OVERLOOKED NUANCES, AND EXPECTED IMPACTS ON COMPANIES

Michelakaki turned to **John Miller** for a deep-dive into the provisions of the DA and DGA. Miller delved into the complexities of the DGA, noting that the Act aims to increase access to public sector data while fostering innovation and offering a less complicated framework than the one proposed by the DA. He noted that as data is central to the business models of ITI's member companies, there are concerns about legal uncertainties introduced by the Act, particularly in determining the scope of products and data covered by the legislation. He also revealed that companies are currently asking questions about whether they actually have to collect data that they would not normally collect in order to comply with the Act's provisions. Miller touched on potential conflicts with data portability rights under the GDPR and stressed the importance of regulatory guidance and collaboration among the different regulators to navigate the complexities introduced by the DA, underscoring the need for clarity.

Miller emphasized potential impacts on international data transfers, highlighting that the DA complicates the legal landscape and poses challenges for companies looking to transfer data across borders, particularly non-personal data. The distinction between personal and non-personal data, and the potential sweeping impact of the DA on various data sets, create a complex landscape. He noted that many companies will struggle to segregate personal data from non-personal data. Furthermore, Miller argued that, despite the GDPR being the instrument with fundamental rights at stake, it establishes a less restrictive regime compared to the DA, particularly in the context of transferring non-personal data. He explained that the DA does not include an adequacy regime for transferring non-personal data, meaning that it creates a cumbersome necessity for a relevant impact assessment.

3.3. THE NEED FOR CLEAR GUIDANCE TO MEET DATA ACCESS OBLIGATIONS

On the topic of expected impacts on businesses working with data, Michelakaki turned to **Amal Taleb** to reflect on additional challenges. Touching on the DMA and the DSA, Taleb underscored the overlooked nuances within the Acts, especially those affecting smaller companies. Taleb delved into the complexities of the DA, arguing that it should have been split into multiple sections to address distinct topics such as IoT data sharing, business-to-government data access, and cloud switching. She discussed that the scope of the DA is unclear, for instance with regard to the definition of users in IoT scenarios, where distinguishing between personal and non-personal data becomes challenging. Taleb noted that the absence of a hierarchy between regulations, except for the fundamental role of the GDPR, is noteworthy and calls for comprehensive guidelines to navigate and harmonize the evolving legislative landscape.

With regard to the DA, Taleb noted, in a similar vein as Miller, that businesses will now need to "rearticulate" everything. This is not only because the GDPR is going to be more complicated to apply, but also because businesses are now required to look at each dataset in turn and figure out which process or obligation applies to its component parts. Companies have to dive deep into the detail and the structure of each dataset, a very novel task for most of them. Taleb noted that this is why, for instance, it has been very difficult for companies to move from on-premise systems to cloud systems as such a transition requires a clear understanding of how data is structured, requiring a huge investment of human resources and finance. The panelists concluded that there is a need for clear guidance and regulatory coherence to address the complexities introduced by new data access and sharing requirements, as well as further collaborative efforts between regulators, DPAs, and businesses to ensure effective and practical implementation of the new regulations.

4. A Network of Impact Assessments – from the GDPR to the DSA and the AI Act

The second panel of the day, "A Network of Impact Assessments – From the GDPR to the DSA and the AI Act," analyzed both the rationale and practical elements of impact assessments required by the various laws within the EU Data Strategy architecture. It also explored the role of impact assessments in assessing and mitigating risks to individuals' fundamental rights and focused on drawing from the experiences gained from Data Protection Impact Assessments (DPIAs) under the GDPR. The panel featured Alessandro Mantelero, Associate Professor of Private Law and Law and Technology at the Polytechnic University of Turin; Frederico Oliviera da Silva, Senior Legal Officer at BEUC, The European Consumer Organisation; Karolina Mojzesowicz, Deputy Head of Unit for Data Protection at the European Commission; Jocelyn Aqua, Data, Privacy and Ethics Leader at PwC; and was moderated by Giancluadio Malgieri, Associate Professor of Law and Technology at Leiden University.

4.1. IMPACT ASSESSMENTS AS TOOLS FOR REGULATING TECHNOLOGY AND PROTECTING CONSUMERS

To start the conversation, Malgieri asked **Alessandro Mantelero** to contextualize the development of impact assessments as a tool for regulating technology. Mantelero noted that while impact assessments are not new, the way in which they are framed by EU laws regulating data has developed over time. In this sense, impact assessments are not only a product safety and security requirement by traditional product liability laws; they are now also used as a tool for assessing risks posed to fundamental rights. The DSA, for example, provides limited, linear requirements for what is to be considered when assessing fundamental rights impacts. On the other hand, the broad scope of application of AI systems requires a similarly broad analysis of fundamental rights impacts under the proposed AI Act.

According to Mantelero, we can look at impact assessments through the logic of acceptability, which has its roots in industrial technology regulation. Through this logic, there is an acceptance that there are risks posed by a certain technology, and that providers can try as much as possible to mitigate those risks. However, the logic of acceptability in the context of AI, for example, shows a shift to a different kind of paradigm: one which, Mantelero argued, acknowledges that if society wants to benefit from AI applications, individuals sometimes have to pay in terms of rights.

Malgieri turned to **Frederico Oliviera da Silva** to provide a consumer protection perspective on the best approach for conducting a meaningful impact assessment. Da Silva considered that there is tension between the product safety model adopted by the AI Act and the need to consider impacts on fundamental rights. He noted that the Fundamental Rights Impact Assessment (FRIA) was a missing element from the AI Act proposals and offered BEUC's support for the ex-ante impact assessment proposed by the European Parliament during negotiations.

Da Silva explained that the requirement to conduct impact assessments comes back to the precautionary principle, which is an elementary principle of consumer law. The precautionary principle states that impact assessments must be conducted before releasing a system or technology

to the market in order to ensure that consumers and their rights are protected. However, according to da Silva, a robust enforcement model is needed for the governance of impact assessments. He noted that authorities have a responsibility to follow up on the implementation of impact assessments in practice, and must have the human, technical, and financial resources to be able to do so effectively. In this sense, the transparency of such enforcement is a key requirement in which consumers, consumer organizations, and NGOs should have access to documentation and information to be able to check whether impact assessments were carried out in accordance with the law.

4.2. DRAWING FROM THE GDPR EXPERIENCE AS WE TURN TOWARDS THE DSA AND AI ACT

With this in mind, Malgieri turned to **Karolina Mojzesowicz** to address the complexity of impact assessments from a data protection perspective, whether they are contradictory, parallel, and sufficient to address possible risks to fundamental rights. Mojzesowicz explained the European Commission's position that all aspects of personal data processing are already embedded and covered by the tools provided by the GDPR. Examples of such tools include having to establish a legal basis for personal data processing, implementing measures for fulfilling data subject rights, and implementing technical and organizational measures.

Going beyond the GDPR, Mojzesowicz noted that, in the view of the European Commission, Article 9 of the proposed AI Act on risk assessment in the context of high-risk AI includes the need to assess impacts on fundamental rights. While the draft AI Act, as of November 2023, focuses on the obligations of providers of high-risk AI, there is also a push for deployers to similarly conduct impact assessments. However, Mojzesowics wondered whether deployers of AI would be equipped with sufficient knowledge of the system to conduct such an assessment, particularly when they are a small company. Importantly, Mojzesowicz noted that while personal data is always an aspect, the DSA and AI Act do not only focus on regulating personal data processing. Indeed, all impact assessments focus on addressing fundamental rights that are impacted by both personal and non-personal data processing. In this sense, the European Commission sees the network of impact assessments as complementary and, in some cases, as parallel.

Continuing to draw on experiences from data protection law and the tools already provided by the GDPR, Malgieri turned to **Jocelyn Aqua** to share insights on the practical and business perspectives on impact assessments. Aqua noted that impact assessments present both a burden and an opportunity for organizations. She highlighted that the ability of private companies to carry out DPIAs has significantly grown as they are able to conceptualize their processing activities from a risk mitigation perspective. However, Aqua explained that there is also a sentiment of fatigue insofar as impact assessments are concerned, noting that companies are increasingly looking to find synergies between compliance requirements that are global in nature. As organizations conduct this exercise, Aqua noted that it is important to have further guidance that clearly maps out what the requirements and expectations are within the network of laws.

4.3. PROVIDERS AND DEPLOYERS OF AI SYSTEMS: SHARED RESPONSIBILITIES?

Responding to the business perspective provided by Aqua, Mantelero added that in his perspective the FRIA is a tool that all companies need to perform to achieve a better balance between the provider of an AI system and the first user of that system. In this sense, not all of the burden can be on the provider of the AI system because they cannot realistically imagine what all of its applications might be. At the same time, the deployers of AI can benefit from the assessment conducted by the provider and can then add on to that assessment as they deploy the technology in real-world scenarios. With this in mind, Mantelero noted that businesses may still face issues because the AI Act proposes three different types of assessments: the technological assessment in Annex 3, the Conformity Assessment, and the FRIA. In his view, and in response to Aqua's point on global requirements for AI regulation, Mantelero suggested that European lawmakers look to Article 1 of the Brazilian AI Bill, which already sets out the criteria for considering impacts on individuals' rights.

Bringing together the consumer and business perspectives, da Silva highlighted that there needs to be guidance and support accompanying the AI Act, especially for SMEs. However, in his perspective, there should be no exemptions from the exercise of impact assessments in the AI Act, particularly considering that potential harms of AI can be quite significant, irrespective of the size of the company deploying such technologies. Da Silva noted that there should also be increased clarity with regard to the recurrence of FRIAs in the AI Act so these assessments can be carried out on a regular basis.

Addressing the size of the deployer of AI, Mojzesowicz added that the context of the deployment of AI matters more than the size of its deployer. In her view, one of the central elements that needs to be considered by the AI Act is how to ensure that the FRIA is framed as a meaningful exercise, rather than a box-ticking effort. Mojzesowicz added that, in her opinion, data protection is only a small part of the FRIA and the AI Act, and questioned whether data protection professionals are best equipped to facilitate the implementation of this assessment. With this in mind, Mojzesowicz highlighted the importance of training the next generation of human rights and technology experts.

Responding to this, Aqua noted that no single individual is equipped to conduct impact assessments on their own. Drawing on the experience gained from DPIAs, data protection professionals had to work across organizations and teams including with engineering, product, marketing, and finance teams in order to conduct a meaningful DPIA. Aqua added that, as a result, data protection professionals are already used to ongoing and iterative communication across their organization to ensure compliance.

5. What Future, then, for Data Enforcement in Europe?

The third and last panel of the Symposium, "What Future, then, for Data Enforcement in Europe?" explored the move towards centralized enforcement of the EU data strategy package. It provided an overview of how the EU enforces its laws, how we should understand the models of centralized and decentralized enforcement, and addressed the need for continuous and improved regulatory dialogue to address the complex network of laws regulating the digital environment. The panel featured Merijn Chamon, Professor of EU Law at Vrije Universiteit Brussel; Annemarie Sipkes, Director of the Telecommunications, Transport and Postal Services Department at the Netherlands Authority for Consumers and Markets (ACM); Romain Robert, Member of the Litigation Chamber at the Belgian Data Protection Authority and Privacy and Digital Law Consultant; Claire Gayrel, Legal Officer for Digital Markets at DG CNCT in the European Commission; and Gabriela Zanfir-Fortuna, VP for Global Privacy at FPF, as moderator.

5.1. EXPLORING ENFORCEMENT MODELS IN EU LAW

Zanfir-Fortuna introduced the topic of the panel by noting that the EU data strategy package introduces a shift from the decentralized model of enforcement towards a more centralized model. We now see a push for centralization, particularly with the DMA, but also with the DSA for the VLOPs and VLOSEs, where the European Commission is exclusively competent to enforce the rules. We also see a proliferation in national supervisory authorities that will be competent to enforce parts of the data strategy package, meaning that the entire enforcement ecosystem will become more complex. To help understand the background of enforcement in EU law, Zanfir-Fortuna turned to **Merijn Chamon** for a brief overview of the EU legal system.

Chamon observed that the EU is currently in a phase of experimentation when it comes to the enforcement of EU law. This might be surprising for some, considering the fact that the EU already settled on a model for the enforcement of its laws in the 1950s. This model was based on the principle of negative integration, whereby Member States were brought together and allowed to integrate on the basis of policies prohibiting them from taking certain actions. These obligations were the core tenets of EU law on integration for a long time.

Chamon added that with the development of the EU internal market in the 1980s, negative obligations became integrated with positive obligations through active policies for EU Member States. At the time, positive integration rules were not so ambitious. Today, however, we see that the EU proposes very ambitious legislative packages not just in data but in many other fields. Chamon noted that with this development, the challenge of properly and uniformly enforcing these ambitious legislative packages has become a research field in its own right.

With this in mind, Chamon particularly recalled the important principle of Article 291(1) of the Treaty on the Functioning of the European Union (TFEU), which enshrines the basic principle that EU law, as a rule, is implemented and enforced by EU Member States. This also introduces the principle of subsidiarity, whereby Member States have the primary responsibility for implementation and enforcement. If States cannot do so as intended, the EU has the mandate to step in. As Zanfir-Fortuna summarized, as a matter of general principle and EU constitutional law, the preference is to leave enforcement to the Member State level, taking into account the principle of subsidiarity.

5.2. ZOOMING IN ON ENFORCEMENT AT THE MEMBER STATE LEVEL

With the background of EU law in mind, Zanfir-Fortuna turned to **Annemarie Sipkes** to share her experience of enforcement at the national level in The Netherlands. Sipkes noted that the primary mission of the Dutch Authority for Consumers and Markets (ACM) is to ensure a well-functioning market for all people and businesses, now and in the future. She added that an economic regulator wants to make sure that the market works well both from a consumer and an economic perspective. For this purpose, we have *ex-post* and *ex-ante* instruments to help regulators assess whether laws and markets are working well.

Sipkes highlighted that, already six years ago, the ACM looked at all of the new digital companies in the market from a consumer protection and competition perspective to ensure The Netherlands had a thriving digital economy. With the new challenges posed by digital players, the ACM also focused on online harms, determining the scope of harmful online content and products that could pose harm to consumers. To do so, Sipkes noted that regulatory coordination both within The Netherlands and within the broader European community was vital, for instance in the shape of continuous dialogue between national and EU regulators, as well as other key stakeholders.

5.3. FROM MEMBER STATE LEVEL SUPERVISION AND ENFORCEMENT TO THE ROLE OF THE EUROPEAN COMMISSION

Having heard the regulatory-level perspective of the ACM in The Netherlands, Zanfir-Fortuna turned to **Claire Gayrel** to share her insights on enforcement at the European Commission level, particularly with regard to the DMA. Gayrel provided that the European Commission's primary enforcement objective for the DMA, so far, has been to leverage all necessary expertise to address gatekeepers. Much of the first phase of DMA enforcement focused on the designation of gatekeepers, in cooperation with national authorities, with the goal of ensuring contestability.

Gayrel added that the DMA in particular builds on knowledge acquired in consumer protection cases and data protection non-compliance and, as such, is inherently interdisciplinary. The DMA builds upon and provides specific obligations for structural issues that have been identified and diagnosed in the past ten years by national competent authorities. As a result, the European Commission is now able to take this forward, while retaining the interdisciplinary expertise of the community of national authorities.

Assessing the enforcement model under the DMA, **Romain Robert** noted that the primary function of this Act is to protect the market, rather than individual fundamental rights. According to Robert, this can be seen in the fact that the DMA's complaints mechanism is limited in that you can only *notify* the European Commission of a potential issue. As such, there is no specific right for a complainant to complain against provisions within the DMA.

Comparing the enforcement of the DMA with the DSA, Robert noted that the objectives of the DSA are more varied in nature, in that its scope is to protect the market, but also businesses, users, individuals, consumers, and data subjects. The private enforcement model introduced by the DSA

provides the right to lodge a complaint with the DSA coordinator. In this respect, Robert noted that it is a positive development that NGOs can complain on behalf of individuals under the DSA. However, Robert asserted that the DSA could go further in this regard by, for example, including an explicit right not only to submit a complaint, but also to have a *decision* to a complaint. Robert also noted that while the European Commission is exclusively tasked with enforcing the DSA, the law itself does not specify exactly what the Commission can and cannot do in this regard. Robert added that besides the landscape of different regulators and regulatory models, the Collective Redress Directive, which is not often talked about as part of enforcement, could provide much-needed answers to the future of resolving digital rights complaints.

5.4. EXPLORING THE ROLE OF DATA PROTECTION AUTHORITIES (DPAS) AND REGULATORY COOPERATION IN Enforcing the EU Data Strategy Package

With the context of DMA and DSA enforcement in mind, Zanfir-Fortuna asked the panelists to share their views on how they envisage collaboration with DPAs in enforcing the data strategy package, noting that personal data processing underpins most of the activities of the players that are regulated by the new architecture of laws. In this regard, Sipkes noted that there are already multiple regulations where the ACM works together with DPAs. For example, once the ACM identifies a privacy-related issue in its enforcement of various laws, the team immediately involves the Dutch DPA on the basis of a Memorandum of Understanding (MoU) between the two parties.

Gayrel added that for the European Commission, a High-Level Group has been established under the DMA to foster collaboration between different regulators. The European Data Protection Supervisor and the European Data Protection Board are central contributors to the High-Level Group, as it relates to, for example, obligations under the DMA with a strong interplay with the GDPR. Going further, Gayrel noted that the information reported under Article 15 of the DMA, under which gatekeepers have an obligation to provide an independently audited description of any techniques used to profile consumers, will also be relevant for GDPR enforcement, as well as for DSA enforcement. The obligation to conduct an independent audit and submit its results to the Commission introduces a new kind of transparency report under the DMA, built and developed with GDPR enforcement in mind.

Responding to the transparency reporting requirements under the DMA and DSA, Robert noted that it would be difficult for consumer protection and privacy enforcement organizations to enforce something they cannot access. This is because these reports are not made public, similar to how the DPIA is not made public to the data subject under the GDPR. As such, Robert encouraged the audience to consider how trust, transparency, and effective enforcement can be expected when key stakeholders, including civil society, do not have access to such important documents.

5.5. THE FUTURE OF DATA ENFORCEMENT IN EUROPE

Considering the future of data enforcement in Europe, and reflecting on the contributions of the panelists, Zanfir-Fortuna recalled the voice of Giovanni Buttarelli. In his role as European Data Protection Supervisor, Buttarelli had envisioned that the future of the enforcement of digital rights and the digital economy could be overseen by a meta-regulator, such as a European Digital Regulator that would oversee the entire architecture.

Reflecting on the future of data enforcement in Europe, Gayrel added that it is up to European regulators to decide whether we end up with an EU-wide agency for digital platforms. So far, the DMA and DSA enforcement for VLOPs at the Commission level is somehow a first step towards a central place where we can discuss a vision for the digital market which includes privacy, competition, and innovation in the digital world. Sipkes noted that having central cooperation avenues is a crucial step to enforcement: this sets down norms that are valid throughout the Union and can ensure consistency and predictability to help beneficially develop the digital world.

6. Concluding Remarks: Aligning Enforcement with Existing Data Protection Law

In her concluding remarks for the day, Vice-Chair of the European Data Protection Board (EDPB), Irene Loizidou Nikolaidou, highlighted the Board's ongoing work to align EU Data Strategy enforcement with data protection law. The Vice-Chair stressed that the EDPB has established a task force to guide DPAs in navigating the practical challenges arising from the DMA and emphasized the EDPB's involvement in the DMA High Level Group and its role in providing advice to the European Commission. With regard to the DSA, she stressed that the EDPB pledges to offer expertise to the European Commission to ensure that DSA enforcement aligns with data protection laws, noting that the EDPB is committed to supporting the Act's implementation. She concluded that **"the DSA, like the DMA, should not be read on its own. It applies in addition to the GDPR."**

1350 Eye Street NW, Suite 350, Washington, DC 20005
Avenue Marnix 13-17, 1000 Brussels, Belgium

fpf.org