CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Marie-Laure DENIS, Chair of the CNIL

The future of data protection – Effective enforcement in the digital world

Keynote speech at the EDPS conference

Friday 17 June, 2022

[Check against delivery]

Ladies and gentlemen,

Dear colleagues and friends,

Good morning everyone,

Let me first **thank Wojciech and the EDPS team** for the organisation of this conference. After two years of pandemic, we all realise how precious it is meet in person again, to stay in touch and to exchange directly among each other's.

And for sure, when it comes to effective enforcement in the digital world, we have a lot to talk about! Since yesterday, we have heard valuable and different voices, from civil society, academics and other stakeholders. Let's face it, we have also heard some criticisms; and we should certainly not turn a blind eye to them.

1. Where we are coming from and the foundations we should build upon

But to continue our discussions today, **maybe one thing I would like to start with**, before addressing critics, is where we are coming from and the initial objectives of the GDPR**.**

The GDPR was presented 10 years ago, and later on negotiated among the co-legislators, with one key objective: "to build a stronger and more coherent data protection framework in the EU, backed by strong enforcement that will allow the digital economy to develop across the internal market, put individuals in control of their own data and reinforce legal and practical certainty for economic operators and public **authorities." In other words: ensuring harmonisation through increased cooperation to ensure a uniform protection of their fundamental rights for data subjects and legal certainty for all stakeholders.**

I still believe that this objective should be our compass for the future and we should probably start by taking stock of the improvements brought by the GDPR.

For **the data subjects first**, the GDPR has brought the possibility to **file a complaint to its own data protection authority** and to have its complaint solved wherever the controller is in the European Economic Area. This is a **major improvement for thousands of complainants throughout**

Europe whose complaints are handled and solved, including through our cooperation and consistency mechanisms.

One key indicator in this regard: we have seen **that individuals have increasingly made use of their rights. Complaints received by the CNIL have almost doubled between 2016 and 2019**, going from 7,700 annual referrals to around 14,000 complaints, and we have remained at such a level since. **These are significant numbers, also considering our current resources, and it shows how the GDPR has concretely empowered individuals** in making use of their rights.

For **data controllers**, the **GDPR has provided them with a single data protection legal framework** and **a single interlocutor**. Let's recall that this is an **attractive mechanism and a powerful incentive**. We have all seen companies organizing themselves to set-up their main establishments in the EU to be able to benefit from this "one-stop-shop".

The GDPR has also been designed to provide a stable legal framework, legal certainty being key for data controllers. In this regard, an important part of our **collective effort** has therefore been to develop various guidelines on key concepts, such as the notion of legal basis, as well as on new technologies, such as on connected vehicle for instance. We have also developed practical tools for controllers, such as the guidelines to help develop Binding corporate rules or codes of conducts.

Collectively, **EU data protection authorities have adopted no less than 57 guidelines and 6 recommendations in four years**. And they produce concrete effects. Indeed, guidelines are soft law, but now it is soft law which reflects the common position of all DPAs, and in that sense, stakeholders can reasonably expect that they will be followed in practice and applied consistently by the regulators.

For data protection authorities, our cooperation and consistency mechanism - or "one-stop shop" - was in itself **a real challenge, given its novelty. Today we can say that we made it: this mechanism is now operational and working.**

- More than **2000 cross-border cases** and **almost 1000 cooperation procedures on cross-border cases have been implemented at EU level between 2018 and 2021**, following which **354 final decisions have been adopted.**
- Our enforcement efforts have also intensified, with **cumulative fines by EU DPAs amounting to €1.55 billion by the end of 2021.**

Concretely, it has become our day-to-day practice to exchange with our EU counterparts. We have set-up teams, specialised some of our staff, developed a network of colleagues within the DPAs. **Within the CNIL** we have made the choice to expand our international and European affairs department, as well as to ensuring coordination on International and EU-related matters, and our enforcement department has also developed an expertise in the field of cross-border cooperation, in particular by participating in investigations with its counterparts in the Netherlands or Luxembourg.

In our view, **to be solid and efficient this cooperation has to rely on mutual trust and common goals. We need to develop a common culture.** To achieve this, we need to develop interpersonal relations and this is what the EDPB is also about: **building efficient networks where communication is smother.**

Over the past two years, the COVID 19 pandemic affected us collectively and individually, just like anybody else. But nevertheless, we have **coordinated on major issues and adopted common positions**, including on enforcement actions. To name but a few, we led the coordination on the **so-called "101 complaints"** from NOYB concerning the use of Google Analytics tools and the transfers operated under this framework. We also issued **our first decision following the urgency procedure provided by the GDPR and a second binding decision under the dispute**

resolution procedure of article 65 GDPR concerning the processing activities of a major actor, WhatsApp.

Let me stress also that one of **the strengths of the GDPR** is that it provides for the **possibility to complement and adjust the practice on several aspects**. It allows us to remain agile by entrusting the EDPB with different ways of complementing and clarifying the rules, including in terms of procedures.

When the GDPR was discussed, the EDPB has precisely been set up to allow our cooperation to be effective by providing for the possibility to issue various types of documents and positions, from soft law to binding decisions. The **GDPR has also been shaped with margins of flexibility to allow the EDPB and its members to complement and adjust the application of this text to the practice**. Let's then recall that the GDPR comprises intrinsically the flexibility necessary to also complement the **channels of cooperation**.

2. Where we are now and the challenges to be addressed

We are all gathered today to discuss the future of data protection and how to ensure an effective enforcement in the digital world and, in this regard, we should also **be realistic about the remaining challenges to be addressed.**

Let's be clear, **we do not consider status quo as an option and we are fully aware of the margins for progress and the obstacles** that we still have to overcome, including to ensure optimal cooperation. W**e also hear the criticisms or expectations that are sometimes becoming more pressing,** especially regarding decisions on major digital players.

Within the EDPB, **we are collectively aware of these expectations and challenges**. **And we want to respond to them quickly and effectively**. This is one of the priorities for the CNIL. The CNIL remains fully committed to keep contributing to the work and efforts of the EDPB. We even contribute in triggering the dispute resolution mechanism. In this regard, we have two Article 65 procedures in progress, one to clarify jurisdictional issues, the other one on proportionality of sanctions.

And this gives me the occasion to stress on one message when it comes to cooperation: **the use of these emergency or dispute resolution procedures should not be seen as a failure of cooperation but as a way to move forward and create jurisprudence.**

As I did for the improvement brought by the GDPR, I would like now to move to **what we can do and how we can improve things in the near future.**

From the data subjects' perspective, I want to mention a recent **study carried out by the CNIL digital innovation laboratory**. **We looked, from a sociological point of view, at who the people filing complaints to the CNIL are**. Some of the study results revealed a specific profile of individuals addressing the CNIL. **This survey shows that men, senior executives and people with a master's degree or higher are overrepresented.**

This has to change. We need to increase our effort in awareness-raising, but also more generally in digital education.

Regarding data controllers, we should certainly **keep on developing further guidance to ensure legal certainty and practical tools.**

And now, from the DPAs perspective, how can we improve cooperation on enforcement?

As it was already recalled, including by Aleid a few minutes ago, **all Heads of EU DPAs have gathered in Vienna** a few weeks ago to work on a common strategy to improve our cooperation at the European level and to **ensure concrete progresses are made in the months and years to come. Once again, this is a priority and a necessity for the entire European collective.**

At EU level, we want to **prioritise cases of strategic importance, and this will most probably – but not only – concern big tech companies.**

We need to concentrate our collective efforts on cases which fulfil a number of quantitative and qualitative criteria such as cases affecting a large number of data subjects in the EU, cases dealing with a structural or recurring problem in several member states or cases related to the intersection of data protection with other legal fields.

We have already started implementing the actions listed in our statement: **strategic cases are being selected,** and hopefully by this summer we will launch **pilot procedures to test how to accompany and ease the formal cooperation** process through increased and closer work of DPAs on these prioritised cases.

Once these strategic cases are identified, under the direction of the Lead Supervisory Authority, **an action plan will be established at EDPB level to ensure that the work will be conducted in the most efficient manner and within a fixed timeline.** This is one of the commitments we have made in order to ensure swifter enforcement, including towards big tech companies. The CNIL will take its part in the collective effort in this respect.

Enforcement towards big tech companies is indeed one of the main critics we hear frequently. **To be clear: these companies are on our radar and several procedures are currently ongoing** also **at national level** – which of course I cannot comment in details now.

On top of the elements already mentioned, **two other things seem to me important in order to make the GDPR more effective:**

- First we need to further **intensify our cooperation among EU DPAs** and I would say to use a famous term in EU law "sincere cooperation", and to **ensure an optimal exchange of information among ourselves to be able to act swiftly and effectively.**
- Second, we have also committed to **identify a list of procedural aspects that could be further harmonised in EU law to maximise the positive impact of GDPR cooperation**. Harmonised horizontal provisions in administrative procedural law could bridge differences in the DPAs' conduct of (cross-border) proceedings to increase efficiency.

I am pleased to hear that the European Commission has also identified this issue and is willing to address it, as declared by Vera Jourova yesterday. We are supportive of such an initiative and are willing to contribute to this process.

W**e have also decided collectively to undertake several other priority actions:**

- DPAs will place particular emphasis on **early and sustained sharing of all relevant information**.
- The EDPB will facilitate the **use of all instruments provided for in the GDPR**, including Article 62 joint investigations.
- We also need to **streamline and make full use of Article 65 dispute resolution mechanism and Article 66 urgency procedures by DPAs**.

We have also heard **calls for more centralized enforcement mechanism** and I would like to say a few words about it today. **First, it has to be said that the one-stop-shop mechanism is already**

partly centralised, it is certainly unique and it could be described as an integrated decentralisation. All national authorities have competence on their territory but decide collectively on cross-border cases, with **a single EU bodies for dispute resolution and, ultimately, a single decision at EU level, through the EDPB.**

An important element to keep in mind on our discussions is that, contrary to other regulatory fields, **we are not regulating market conditions but protecting a fundamental right, enshrined in our primary law**. Our model is unique also because it has to **meet two essential criteria**:

- **Allow each individual to file a complaint to its national authority** regardless of the company concerned in Europe (or beyond).
- **Ensure, in compliance the Charter and the Treaties, that enforcement of data protection rules is the responsibility of independents authorities**. A competence which cannot be devolved to the executive branch at national or EU level.

Let's also recall that the competition enforcement model, often taken as an example, has significantly evolved over the years. It started in the late 60s with a fully centralised enforcement mechanism by the European Commission which did not proved fully efficient and national competition authorities have progressively been integrated in the mechanisms over the years. The adoption of the Digital Market Act illustrates a trend for a new centralisation phase, but national competition authorities remain involved in the process.

Furthermore, we should remind that it took several, if not many, years before big competition decision were adopted; there's always a learning curve when you set up new enforcement models. But it's true that **when it comes to the digital ecosystem and its rapid evolutions, we cannot afford waiting several years and we need to act now**. **And that's why we have collectively decided to act**, building upon our current model, to deliver more swiftly, address our current challenges and meet our common objectives.

Finally, and this is not completely in our hands as DPAs: let's recall that the GDPR places **an obligation on Member States to provide their national authorities with sufficient resources to carry out their duties.**

It's not only a question of numbers, of staff and budget, it is about **meeting our ambitions for the regulation of the digital ecosystems.** Effective enforcement in the digital world means independent authorities are provided with effective means to achieve this goal.

For several years now the CNIL has seen its resources increasing, we are on the right trend, but it needs to be amplified given the many challenges ahead. And this is certainly true for all EU DPAs; we also count on the European Commission to **ensure all Member States comply with their obligations in this regard.**

Conclusion

To conclude, if you allow me, I would like to highlight **four lessons I believe can be drawn more generally from these first 4 years of GDPR** to inform the next few years ahead of us:

Without minimizing our current challenges, **the first lesson may be that the we should not be shy in our attempts to regulate the digital ecosystem.** Some critics said at the time of the adoption of the GDPR that it would never work, and that personal data processing would no longer be possible in the EU. They were wrong and instead, the GDPR has become a global standard for personal data protection.

The second lesson is that we should be probably more proactive in explaining and promoting the GDPR towards companies, including SMEs, as a competitive tool which can

become a competition distinctive advantage. Data protection and privacy are becoming a growing consumer demands, even at international level, and we need to make further use of this leverage.

The third lesson is that our digital environment is evolving rapidly and that we need to react more swiftly in order to be able to address effectively certain practices and data processing, before they become a *de facto* reality. This is what we aim to achieve with our renewed commitment and priority actions among EU DPAs.

The fourth lesson is that data protection regulation alone will not address all challenges currently facing our digital economy and societies. We need a comprehensive approach and that's what the EU has been promoting with new regulatory frameworks such as the DGA, DSA, DMA, Data Act and the AI regulation. But we need to keep in mind that our regulatory framework needs to remain coherent, and understandable, for individuals and for companies. It is therefore essential to ensure coherence and that we work further on governance, for an optimal regulatory cooperation across different regulatory fields, as already mentioned yesterday by Margrethe Vestager.

I believe that we should seize the unique opportunity of this conference to exchange views while keeping in mind these elements, and always aiming at our initial objectives. **The future of data protection has always been to make it a concrete reality for individuals, as a fundamental right**. And maybe today more than ever, we have a **duty to succeed collectively, not only as a regulatory or policy objective, but also for the promotion and preservation of our common values.**