Conclusions

OF THE MISSION ON THE INTERPLAY BETWEEN DATA PROTECTION AND COMPETITION

entrusted by Marie-Laure Denis, Chair of the CNIL

to Bruno Lasserre, Chair of the CADA et member of the CNIL's plenary college

with the support of

the economic analysis team of the CNIL

November 28, 2024

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Table of contents

1. General introduction

Five years after the Bundeskartellamt's first attempt to link competition and data protection, three years after the Joint statement by the two British authorities, and more than a year after the July 2023 CJEU *Meta platforms ruling*, which created a new cooperation regime between authorities, linking "data protection" and "competition" has become an obvious goal. Obvious for politicians, who wish to consider digital regulation as a whole. Obvious for the authorities, in order to deepen their cooperation in every possible way. It's also obvious to businesses, who are calling for such coherence. Fewer and fewer institutions and researchers are defending the complete independence of the two sets of regulations.

Indeed, the economic reality of digital markets and the dominant players active in them increases the interdependence between the two sets of regulations. Thus, in these situations, what happens in one of the frameworks has effects on the other, and vice versa[1]. The two legal frameworks are often described as having distinct objectives, which is true, but they also share common goals, including the protection of individual welfare, freedom of choice, fairness, transparency, which makes information more symmetrical, and the reduction of power asymmetries (Majcher, 2023).

It is necessary, for all these reasons, to clearly define what is meant by a better coordination of the two frameworks. A number of questions arise in this respect: should the link between the two areas be one-sided, or is it reciprocal, i.e. can and should data protection incorporate elements of competitive analysis? Should the question of interplay only arise in cases of conflicting norms, or should it be based on a more integrated vision or dialogue between the two regulatory frameworks, their concepts and their tools? Should coordination only concern data protection and competition, or should it extend to consumer protection, which is the area where the intersection with the other two is the most obvious, to the regulation of electronic communications and media, and even toAI?

While the question of reciprocity has now been settled by the *Meta platforms v. Bundeskartellamt* case law, the question of the nature of the interplay is the subject matter of this report. It is based on a balanced approach to the question: avoiding both the fiction of a perfect independence of regulations, and the illusion of an integration of the two frameworks (at least in the current state of positive law), the present report proposes a balanced approach based on the convergence of regulations and the dialogue of concepts and tools (cf. Figure 1).

These notions are already set out and developed in the recent Joint Statement "Competition and personal data: a common ambition" between the Autorité de la concurrence and the CNIL, published on December 12, 2023. This report aims to deepen convergence between the two regulatory frameworks, from the perspective of data protection, which is the least developed perspective at the moment. It makes 15 proposals for further convergence, dialogue, and cooperation. In doing so, it does not exclude the possibility of formulating suggestions for the Autorité de la concurrence.

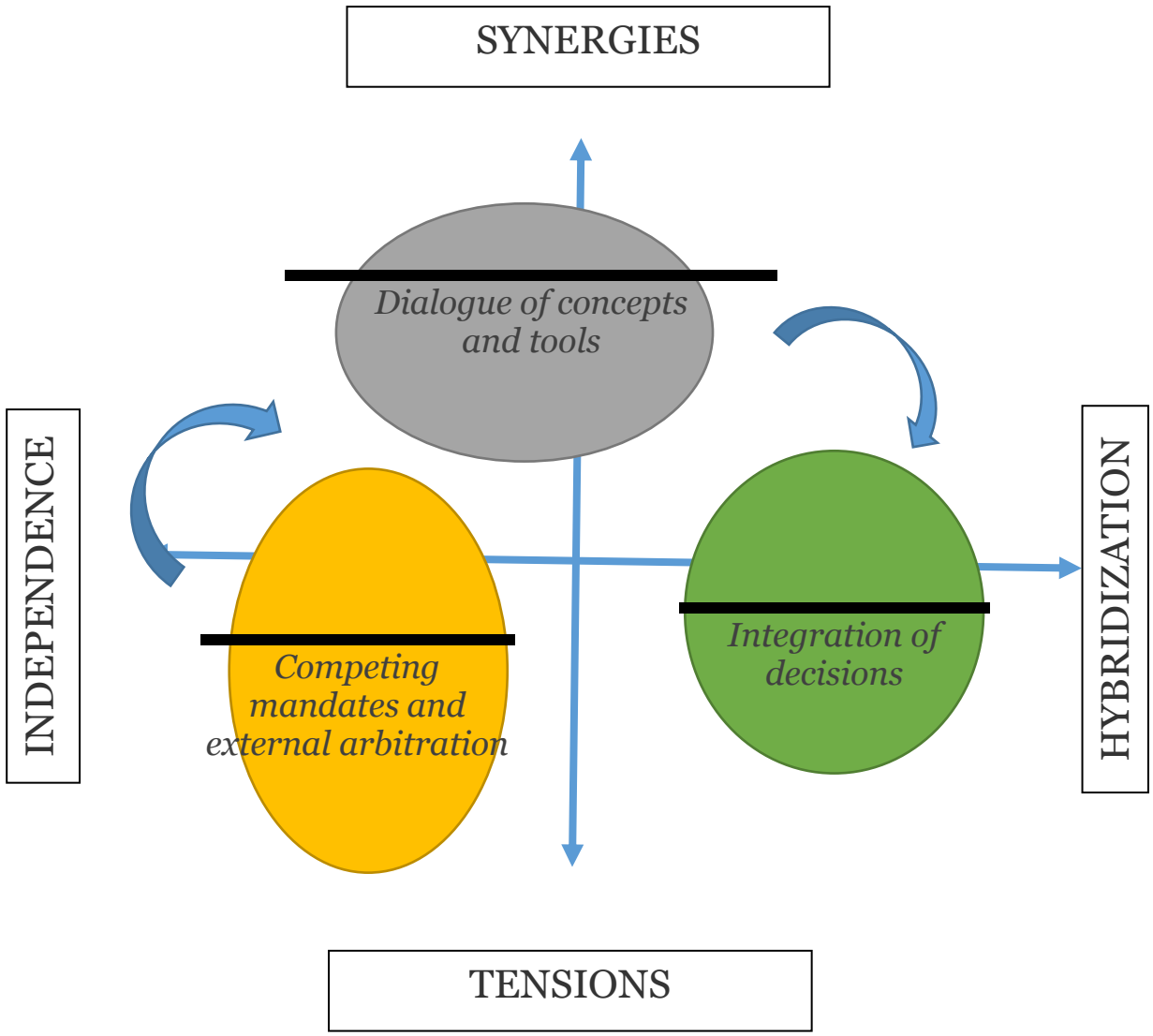
The objectives of the approach are the same as in the Joint declaration: reducing tensions ; highlighting the regulatory synergies that make regulation more effective and predictable ; illustrating the idea that there are more synergies than tensions, promoting dialogue between concepts and tools, if necessary by adapting them, enabling them to be taken into account as a source of mutual inspiration in the assessment of practices, but also in legal analysis ; making more fluid and rapid cooperation between the two authorities on concepts, doctrine and cases; reinforcing legal certainty for companies; and finally, acting for the benefit of all citizens, consumers and people concerned by the protection of their rights.

This approach is also intended to evolve towards more convergence with time : as data protection in competition and competition in data protection are taken into account in the respective practices and doctrines of the two institutions, as the dialogue of concepts and tools progresses, and as the elements of convergence made public by the two authorities develop. The hybridization of the two sets of regulations will thus be able to progress, without of course ever going so far as to merge the legal frameworks and mandates of the two authorities.

[1] Cf. the hearing of Marie-Laure Denis before the College of the Autorité de la concurrence in November 2022: https://www.cnil.fr/fr/protection-des-donnees-et-droit-de-la-concurrence-marie-laure-denis-intervient-devant-le-college-de.

Lastly, this report does not cover the interplay with consumer protection, which deserves an integrated approach with the other two areas, nor with digital regulation in general, aiming to set up cooperation between multiple authorities, which is beyond the scope of this report.

Fig.1: Different ways in which data protection and competition interplay



Legend: ***"coordinating" two legal frameworks implies considering two axes:*** *on the one hand, do we emphasize tensions (opposing objectives) or synergies (converging objectives), and on the other, do we want to promote regulation in silos (no mutual influence) or hybridization (integrating objectives, concepts and legal qualifications).*

With regard todata protection and competition, we have already moved away from a regime of complete independence emphasizing tensions (the south-west quadrant, which represents the zero degree of cooperation), but we are not in a regime where the two sets of laws integrate either (which is what would happen if we were to generalize the Meta Platforms case).

Instead, we are in a more balanced attempt to build a dialogue of concepts and tools taking advantage of synergies (mutual inspiration rather than mutual recognition) and promoting regulatory convergence.

Box 1: The CJEU Meta Platforms judgment

The possibility for a national competition authority to find a breach of the GDPR

The CJEU's Meta judgment of July 4, 2023[2] establishes**the possibility for a national competition authority to** incidentally determine a GDPR violation while assessing an abuse of dominant position **when such a finding is necessary to establish the existence of the abuse** (p. 36). According to the Court, nothing in the GDPR prohibits national competition authorities from finding, in the exercise of their functions, non-compliance with GDPR of a personal data processing carried out by an undertaking in a dominant position and liable to constitute an abuse of that position (pt 41).

The recognition of this possibility first of all supports the Court's conclusion that the protection of personal data should be taken into account in the field of competitive analysis, as recalled in the joint declaration between the Autorité de la concurrence and the CNIL[3].

Conversely, the Court opens up the possibility for national data protection authorities to consider competition law concepts in support of their own analyses. For example, the Court ruled that the dominant position of a service operator does not, as such, prevent users from validly consenting to the processing of their personal data by that operator. However, it does consider that this is an important factor in determining whether consent has been freely given. (pt. 39).

It can be deduced from this that the notions and concepts of other areas of law can usefully be mobilized in support of the analysis carried out by a data protection authority. In this context, the integration of competition analysis into the CNIL's work would appear to be essential, in order to identify situations in which the use of competition law concepts could be favored. This will also make it easier to determine the need to call on the Competition Authority, and how.

Preserving the autonomy of competent authorities

The Court nevertheless emphasized that when the national competition authority identifies a violation of the GDPR, it does not replace the supervisory authorities set up by that regulation (pt 49). Indeed, **the assessment of compliance with the GDPR must be limited to the sole purpose of finding an abuse of a dominant position and imposing measures to stop that abuse in accordance with the rules of competition law**.

Lessons can be drawn from this on the appropriate way for authorities to use the notions and concepts of other rights. Thus, **the use of notions and concepts from other areas of lawby a competent authority must be strictly limited to the sole purpose of carrying out its own missions**. The latter, as established by the texts in a state governed by the rule of law, remain unchanged.

Enhanced institutional cooperation

In this context, the Court affirms the need for enhanced institutional cooperation between national authorities, by virtue of the principle of loyal cooperation laid down by the European Treaties. The Court thus specifies that national competition authorities **must consult and cooperate loyally with the authorities ensuring compliance with the GDPR** in order to limit the risks of divergent interpretations.

The Court provides useful clarification on how this enhanced cooperation should take place. In this respect, the authorities must assist each other, **without compromising their respective objectives, and avoid divergences**. Accordingly, the Court states that the national competition authority must check whether the conduct in question has already been the subject of a decision by the competent or leading national control authority or by the CJEU, and may not depart from it. In case of doubt, the national competition authority must consult these authorities for an opinion and seek their cooperation, which in turn must respond within a reasonable timeframe (pts. 54 et seq.).

Existing **cooperation between the CNIL and the Competition Authority is set to intensify, with more frequent** consultations whenever the application of their regulations intersect. Moreover, the Court's ruling makes such cooperation **a legal obligation, rather than an option**, for member states and these authorities.

[2] CJEU, Case C-252/21, July 4, 2023, Meta Platforms Inc. and others v. Bundeskartellamt.
[3] Autorité de la concurrence and Commission nationale de l'informatique et des libertés, 2023, Competition and personal data: a common ambition, p. 7.

2. The interplay between data protection and competition

Cooperation between competition and data protection authorities has become an imperative, due to changes in the economic, regulatory and normative context. The digitization of the economy and the omnipresence of the major online actors, who make the collection and use of personal data central to their business models (2.1), explain the acuteness of this challenge. The protection of personal data as a fundamental right, and the protection of competition as an element in the proper functioning of the economy and markets, can in fact be articulated to achieve common objectives (2.2). As illustrated by the CJEU's *Meta Platforms* ruling (see Box 1), it is therefore necessary for the CNIL to take competition analysis into account in its work, in order to increase the coherence of its joint action with the other authority (2.3).

2.1 Personal data at the core of business models

2.1.1 Digitization of the economy

Driven by the rapid expansion of information technologies, a profound economic and social transformation of French society has been underway for several decades. Among these changes, the importance of digital technology has altered pre-existing economic and social logics[4].

This digital world means that companies have to reconsider their business models, integrating new dynamics of innovation. Faced with the necessity to regularly develop innovative products and services and the possibilities offered by digital technology, a logic of industrialization of innovation has taken root in the economy. Digital technology has increased the proximity that can exist between consumers and companies[5] : the business models of the late 2000s, which saw the user as a simple end-buyer, have gradually shifted towards business models that increasingly involve the consumer as the driving force behind the product or service life cycle. For example, digital platforms have integrated the user into their business models as both recipient (use of the platform) and driver (collection and use of personal data for optimization and financing purposes) of the service.

For companies, one of the consequences of these transformations has been to diversify and increase the complexity of the production methods. Indeed, while the possibilities offered by digital technology opens up a vast range of opportunities, the business model can quickly be called into question by a more recent innovation. For users, digital technologies have spread to all areas of society. As a result, it has become easier to use digital technology on a daily basis, and some uses have gotten more difficult to access or less advantageous when they are not fully digitized. Furthermore, the widespread use of digital tools has altered the consumer's relationship with the product or service offered by companies.

In reality, companies have adapted to digital transformation by integrating the user into their business models. Depending on the sector, the product, the service, and the company's needs, this integration can take various forms. Nevertheless, the central element of this transformation remains the massive collection and use of data, especially personal data. This intensive use raises questions since it can lead to behaviour that does not comply with regulations: GDPR, but also competition law and consumer law.

In fact, the changes in business models just described have increased the dependence of companies on digital tools, by strengthening the position of players who have become dominant in sectors based on digital technologies. This digitization is therefore accompanied by strong competitive challenges, underlined in France by the creation of a digital economy department by the Autorité de la concurrence in 2020, but also by the European Union with the implementation of the European digital package (DSA[6], DMA[7], Data Act[8]).

In particular, it is the collection and use of data in the broadest sense that crystallizes the essential competitive stakes of digital transformation, with many companies interested in personal data. As the joint statement by the

---

[4] P. Lemoine, 2014, « La nouvelle grammaire du succès : la transformation numérique de l'économie française », Rapport au gouvernement.
[5] Direction générale du Trésor, novembre 2020, « Numérisation des entreprises françaises », *Trésor-Eco*, n°271.
[6] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) noted here "DSA".
[7] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) noted here "DMA".
[8] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) noted here "Data Act".

CNIL and the Autorité de la Concurrence shows, joint personal data protection and competition is needed to respond appropriately to the challenges posed by the digitization of the economy.

2.1.2 The rise of massive databases and AI

The transformation of business models has changed companies' relationship with data. The collection and use of data, particularly personal data, have become central.

The increase in the amount of data used by businesses has led to the widespread creation of massive databases, also known as *Big Data*. These correspond to all the data available on a given subject (health, real estate, insurance, etc.). Data can be collected from a variety of sources, either directly or indirectly. Data is then used to obtain a better understanding of the sector, optimize production, increase sales, improve user targeting, etc. As soon as a large amount of data is collected, the likelihood of personal data being collected mechanically increases.

The growth in the training and use of massive databases has been fostered by technological advances over the last few decades. The development of faster, smarter tools with greater storage capacity has revolutionized usage and contributed to the democratization of massive data. In the process, data aggregation and extraction have become simpler, making the analysis of massive data all the more attractive to businesses. This data can be used to increase corporate knowledge and make predictions, either through the application of statistical models, or through machine learning models.

Massive data represents a major source of economic opportunities for companies. Indeed, while improving company's overall performance, it can also help foster innovation. In fact, it is by exploiting massive databases that the large digital companies have developed (Zuboff, 2019)[9]. In particular, the collection and use of personal data have been key to developing competitive advantages in dynamic markets. These practices, some of which were contrary to the GDPR, have contributed to the establishment of dominant positions that raise numerous competitive issues.

Exacerbated in the digital sector, the use of massive data is now widespread throughout society and the economy. It is now commonplace to find one or more functions in a company, local authority or government department dedicated to data collection and processing.

This generalization of massive data in the economy has also enabled the construction of an attention economy "*in which companies take advantage of data to capture users' attention ever more finely, expose them to more advertising and, in a circular way, collect even more information*"[10]. For some business models, building and maintaining this attention economy is a priority. In the digital economy, the so-called « structuring platforms »[11] are particularly concerned[12]. Faced with the resurgence of intrusive practices, the question arises as to how to protect users against such market failures, i.e. situations in which the market is unable to achieve an efficient allocation of resources on its own.

In this sense, the GDPR can be "a powerful instrument for consolidating the European digital ecosystem"[13] ; however, the protection of competition appears to be inseparable in order to avoid reproducing market structures dominated by a few players and to make competition more effective.

The artificial intelligence (AI) sector is also a good example of the economic challenges associated with taking data protection and competition into account. The sector's economic development must go hand in hand with "by design" integration of personal data protection.

For the moment, artificial intelligence models require the collection and exploitation of massive amounts of data. Meaning that, alongside the race for innovation, we are seeing the development of strategies for the production and consolidation of databases adapted to artificial intelligence. In this context, the major players in the digital sector, who benefit from significant stocks of personal data, are already present across the entire

---

[9] Zuboff, S. (2019). *The age of Surveillance Capitalism*, London, England: Profile Books.
[10] Rapport d'information n°768 sur l'exposition des données, Les Notes Scientifiques de l'Office – Note n° 36 – Face à l'explosion des données, janvier 2023. [free translation, see original text]
[11] Bourreau, M. et Perrot, A. (2020). « Plateformes numériques : réguler avant qu'il ne soit trop tard ». *Notes du conseil d'analyse économique*, (6), p. 1-12.
[12] Conseil national du numérique, « Votre attention, s'il vous plaît ! Quels leviers face à l'économie de l'attention ? », juillet 2022. [free translation, see original text]
[13] Rapport Villani, Donner un sens à l'intelligence artificielle, 2018.

AI value chain[14]. This situation could lead to the construction of positions that could become dominant in this field too.

2.2 Orienting markets

2.2.1 Incentives for economic players

The free play of competition encourages companies to differentiate themselves by providing offers that stand out from those of their competitors. Protecting users' privacy and personal data can, in this respect, be part of a differentiation strategy for companies.

Nevertheless, personal data can in some cases be used to disadvantage competing companies. This situation was highlighted in the Apple/Shazam case, where "*the Commission examined whether, by acquiring control of the Shazam application and the Shazam database, Apple could have access to certain data on its competitors*"[15]. Customer information made accessible in this way was viewed by the European Commission as commercially sensitive information, considering regulatory obligations relating to personal data protection. The Microsoft/LinkedIn case also highlighted the decisive role of personal data in business strategies. In its decision, the European Commission notably concluded that the GDPR rules allowed limiting the ability of these two companies to combine and process this data.

Conversely, the numerous sanctions imposed by the CNIL show that the dynamics of competition alone is not sufficient to steer companies towards more privacy and personal data friendly behaviour. The action of institutions, as well as good cooperation between them, is essential. In this sense, the GDPR makes it possible to put in place anormative framework that incentivizes the protection of users.

Indeed, corporate choices can be guided by incentive mechanisms, which can take a variety of forms. Monetary incentives, such as financial penalties, are one way of internalizing the economic consequences of companies' privacy choices on third parties into their strategies. These are complemented by non-monetary incentives, such as formal notices or the publication of decisions, which have an effect on corporate behaviour by increasing the risk of a financial penalty or reputational damage.

The collection and use of personal data, as well as privacy protection, are therefore factors that influence companies' choices.

The GDPR can also help guide users. By promoting greater transparency, and therefore better information for individuals, personal data protection regulations make it easier for users to make informed choices, and to be guided towards offers that are more respectful of privacy and personal data. Lastly, greater consideration for privacy in users' choices in turn encourages companies to develop and improve their offerings in this area.

2.2.2 Privacy as a competitive factor

CNIL operates in a "*market economy based on the principles of freedom of consumers freedom of choice and entrepreneurial freedom* »[16]. As the joint declaration reminds us, « *free and undistorted competition helps to avoid rent-seeking behaviour that harms consumers"*[17]. However, the consumer is also an individual or a "data subject" within the meaning of the GDPR.

With the development of business models using more personal data, the protection of this data has gradually become a competition parameter to be taken into account in the decisions of competition authorities. Digital markets are characterized by the presence of players with significant market power and a tendency towards concentration. The structuring powers of these players and the difficulty of contesting their positions lead to the maintenance of concentrated market structures.

In particular, digital platforms, through the use of business models based on the accumulation and combination of data, are conducive to the development of competitive advantages centered around data accumulation. These advantages are then amplified and consolidated by the network effects specific to digital technology, which can then "*lead to dominant positions being locked-in, with the risk of damaging competition and, at the same time,*

[14] Autorité de la concurrence, Avis 24-A-05 du 28 juin 2024 relatif au fonctionnement concurrentiel du secteur de l'intelligence artificielle générative. [free translation, see original text]
[15] European Commission, april 2024, Competion *policy brief*, Issue 1, p.15.
[16] Autorité de la concurrence and Commission nationale de l'informatique et des libertés, 2023, "Competition and personal data: a common ambition", p.3.
[17] Ibid.

encouraging the misuse of personal data"[18]. A vicious circle of overexploitation and non-compliance then takes hold in both areas simultaneously.

In addition, the limited capacity of users to exercise bargaining power when facing dominant players means that, even if they wish to, they are not always able to choose an offer that is more respectful of their privacy. What's more, their behaviour can be influenced by a strong asymmetry of information between them and companies and by the implementation of strategies that bias consent ("dark-patterns", pre-selection of choices, etc.). It is also important to consider the positive and negative externalities that companies may generate as a result of collecting and processing personal data, given their effects on users.

Personal data has undeniably become an engine for growth and a commercial advantage in certain fields, notably digital and technology. For example, in the context of a merger or acquisition, personal data protection "*can be an important element of quality of a product or service offered and thus a parameter of competition between the merging parties and their rivals and an element of differentiation*"[19]. The Commission can then examine the project while taking into account the GDPR, for the purposes of assesing the limits that would apply on companies regarding the combination of data sets or the rules on the collection, processing, storage and use of data for example.

From the point of view of competition protection, the level of protection corresponds to a parameter of quality and therefore of choice for the user. A competitive market can, through innovation and sufficient competitive pressure, promote greater consideration for users' privacy and the protection of their data. This is why it is crucial for the CNIL to take into account the competitive mechanisms at work on the market, in order to encourage the creation of services and products that give users greater control over their data. Continuing to promote better conditions of choice for users, by improving the free exercise of their choices on the market, therefore requires a better understanding of the role of personal data protection as a competitive parameter.

2.2.3 Contributing to innovation

Integrating competitive analysis into work and decisions on personal data protection also makes it possible to take part in the debate concerning the GDPR's contribution to innovation. The economic literature does not permit to conclude definitively on the existence of an overall effect of the GDPR on innovation (CNIL, 2023)[20]. Nevertheless, by considering the specific competitive challenges of each market in the economic analysis made it possible to take into account the changing dynamics of innovation in sectors centered around the collection and exploitation of personal data. Competition is in fact the main driver of innovation, either to escape it or to contest existing positions.

Taking competition into account provides a better understanding of how and why companies have been forced to update their IT tools, operating methods and data management in order to innovate for GDPR compliance or to go beyond mere compliance to make privacy an element of differentiation. While these adjustments have required resources that were no longer available to invest in other research and innovation activities, nevertheless "*they can foster incremental innovation within the existing product and service portfolio*" [21]. In addition, this investment could reduce their costs related to GDPR implementation and thus improve the efficiency of the company's internal processes, which would then be an opportunity to improve the company's revenues through cost savings or incremental innovations (Blind, Niebel et Rammer, 2024).

For example, in the field of AI, innovation is based on data. Taking into account the specificities of competition enables a more comprehensive view of the sector's challenges while integrating the protection of privacy and personal data as one of the important parameters right from the design stage. In practice, "*regulators and privacy professionals in organizations, are actively working to deploy solutions to implement privacy-friendly AI and even to use AI in favor of privacy*"[22]. Data protection authorities therefore have a role in

---

[18] Ibid., p.4.
[19] European Commission, april 2024, Competion *policy brief*, Issue 1, p.5.
[20] https://doi.org/10.1080/13662716.2023.2271858. https://www.cnil.fr/fr/limpact-economique-du-rgpd-5-ans-apres.
[21] Blind, K., Niebel, C. et Rammer, C. (2024). The impact of the EU General data protection regulation on product innovation. *Industry and Innovation*, *31*(3), 311–351. https://doi.org/10.1080/13662716.2023.2271858.
[22] OECD.AI Policy Observatory (2024). A new expert group at the OECD for policy synergies in AI, data, and privacy. Available here: https://oecd.ai/en/wonk/expert-group-data-privacy.

clarifying what is a responsible and GDPR-compliant collection and use of personal data, with the aim of fostering AI innovation.

In summary, a better balance between competition and data protection will ensure an environment favorable to innovation that respects privacy and personal data.

Moreover, continuing to develop a full understanding of these economic issues, as the CNIL is doing, is necessary if we intend to make the protection of privacy and personal data a central concern for companies when they innovate. Regulation can drive innovation, of course, by encouraging « *players to carry out innovation activities in order to remain competitive on the markets* »[23]. However, innovation also depends on many other factors, such as company size, business model, economies of scale, network effects, and access to funding. Encouraging companies to innovate in terms of privacy protection requires a better understanding of the innovative and competitive dynamics of companies.

2.3 A minimal culture of competition

2.3.1 Understanding and being understood

For the CNIL, making itself understood by other authorities, in particular the Autorité de la concurrence, is a necessity. It also ensures the widest possible dissemination of the most virtuous practices and behaviours in terms of privacy and personal data. Indeed, while integrating competitive analyses into the CNIL's work improves its ability to steer market players towards better protection of individuals, it remains necessary to develop the ability to communicate with other authorities in a common language.

The development of this common language can be usefully supported by economic vocabulary. In particular, it requires an understanding of terms relating to competition, in order to better determine the points of tension and convergence. This better understanding also contributes to increase the CNIL's analytical skills on economic and competitive issues. Ultimately, it will contribute to a better understanding of joint cases and opinions in conjunction with the Autorité de la concurrence.

A better understanding of competition is also necessary in order to detect intersections between data protection and competition that could be of interest to the CNIL in certain cases. For example, some competition issues may not, at first glance, raise data protection issues. However, in some cases, the personal data protection may be an important parameter for competition. In this situation, and with a view to stepping up cooperation between the CNIL and the Autorité de la concurrence, the CNIL's expertise could be useful in complementing the Autorité's analysis. In return, the Autorité de la concurrence's expertise could help avoid inconsistencies in future decisions by the two authorities.

Building a common language through the development of respective methods and analyses would also help to strengthen the ability to identify subjects whereeach Authority could make a useful contribution.

Knowing the vocabulary of competition and taking its issues into account can also contribute to a better understanding, by professionals, of the players involved in CNIL decisions. Indeed, like all fields of law, the field of personal data protection has its own vocabulary. Developing the ability to embed the CNIL's work and decisions in a broader economic framework can make them "easy to read and understand" for a greater number of people. This can also encourage economic players to adhere to the recommendations and opinions issued. Taking competitive dynamics into account simplifies integration into companies' business models, reducing the risk that these recommendations or opinions will generate unanticipated negative economic effects for the company.

2.3.2 Better identifying economic and competitive consequences

Taking account of competition issues in the CNIL's work means identifying the main problems upstream in order to ensure that its decisions are fully efficient.

The CNIL's missions cannot be carried out without taking into account the economic and competitive consequences that could result from its decisions, opinions or recommendations. For example, the CNIL must ensure that it takes into account *« in all areas of its action, the situation of people lacking digital skills, and the specific needs of local authorities, their groupings and micro, small and medium-sized enterprises* » (art.

[23] OCDE (2023). Concurrence et innovation, Partie I : Cadre théorique - Note de référence, DAF/COMP(2023)2, p. 30. Available here: https://one.oecd.org/document/DAF/COMP(2023)2/fr/pdf. [free translation, see original text]

8.I.2.b of the French Data Protecti on Act [free translation, see original text]). Such a consideration cannot be carried out without identifying the economic and competitive issues of these players.

In addition to adapted support, better identification of economic and competitive issues enables to anticipate companies' technological and strategic developments. This strengthens the CNIL's ability to steer economic transformations towards greater protection of privacy, and to shed light on the economic and competitive issues related to personal data protection. In 2021, for example, the CNIL published a new white paper on payment data and methods, designed to "*enlighten and support professionals and anticipate future transformations*"[24].

Accelerating the identification of economic and competitive consequences also aims to increase legal certainty for companies. Moreover, the CNIL regularly draws up reference frameworks (guidelines, benchmarks, recommendations, etc.) in consultation with the players and sectors concerned. These frameworks help guide organizations in bringing their data processing into compliance[25]. Takinginto account the economic realities and business models of companies increases the relevance, scope and applicability of these reference frameworks in practice. In particular, within the context of recommendations, companies will be all the more inclined to put in place proposals that are more protective of personal data if they have been designed and proposed in line with their economic and competitive issues.

Furthermore, "information technology should be at the service of every citizen"[26] and should not operate at the detriment of users' privacy. As data protection is a fundamental right, in the event of a conflict between data protection and competition, it is possible that the judge, when confronted with this conflict, will give priority to data protection, but only after a more or less lengthy period of legal uncertainty. A better understanding of these issues will enable us to anticipate and avoid these effects, while ensuring that data protection regulations are applied in a proportionate manner.

2.3.3 Controlling the impact on competition

As recalled in the joint declaration of December 12, 2023[27], while the mission entrusted to the CNIL is to "*protect users against any harmful collection and use of their data, particularly when they are using commercial goods or services*", the aim of competition policy is to guarantee "*the conditions for free, undistorted competition between companies in the market, in the interest of consumers, by promoting innovation, diversity of supply, and attractive prices*". The two visions therefore converge in their implementation and in some of their objectives, since they are intended to serve the user, whether a company or an individual consumer.

However, in order to better control the effects of protection standards on competition, the CNIL should take them into account right from the design stage. For example, the cost of protecting personal data is proportionately "less onerous" for a large company. The economic impact on smaller companies is therefore different. These disparities, which can sometimes be very significant, call for a more asymmetrical approach to the responsibility principle, so as not to encourage the emergence of barriers to entry that are detrimental to competition and users.

In addition, the development of business models based on data collection and exploitation is reinforcing the place of personal data in the competitive dynamics of markets. The protection of privacy as a competitive parameter has direct effects not only on the choices offered to users, but also on the strategies deployed by companies. In particular, « the control of data can be a source of market power and be used for anti-competitive behaviour »[28]. Henceforth, it is advisable to better understand the impact of CNIL's decisions on competition, since they can - in certain cases and indirectly - have an effect on competition conditions.

Better control of the effects on competition also makes it possible to develop a balance between competition and the protection of user privacy. While it is important to steer players towards more privacy-protective business models, the attractiveness of these models is a prerequisite for achieving this objective. Understanding, anticipating and controlling the effects of decisions on competition allows for better adaptation and to involve stakeholders (companies and/or competition authorities) in the CNIL's reflection process. This is particularly the case when competition issues arise during the preparation of soft law documents such as recommendations

---

[24] CNIL, 2021, « When trust opays off : Today's and tomorrow's means of payment facing the challenge of data protection", Coll. White papers n°2. Available here: https://www.cnil.fr/sites/cnil/files/atoms/files/cnil-white-paper_when-trust-pays-off.pdf

[25] https://www.cnil.fr/fr/les-decisions-de-la-cnil/les-cadres-de-reference.

[26] Article 1er de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[27] Autorité de la concurrence and Commission nationale de l'informatique et des libertés, 2023, "Competition and personal data: a common ambition", p.5.

[28] Direction générale du Trésor, juillet 2022, Trésor-Eco, n°310, p.3. [free translation, see original text]

or codes of conduct. In such cases, it may be appropriate for the CNIL to consult the Autorité de la concurrence for an opinion, in order to have the best possible analysis of the market's competitive specificity.

Anticipating the future role of data for businesses also requires a full understanding of its effects on competition. Indeed, CNIL's decisions may guide the choices made by players, who could then modify their business models in response, with both a compliance and competitive strategy. Consequently, the competitive dynamics of the market can play a decisive role in terms and conditions for bringing companies to compliance.

Proposal no. 1: take competition issues into account upstream in CNIL's work. *Developing a better vision of the effects of CNIL decisions on competition helps to promote overall consistency in the application of competition and data protection. Increasing this consistency helps to foster virtuous behaviour in terms of both respect for competition and protection of privacy and personal data. It also reinforces the predictability of regulatory action and, consequently, the legal certainty for companies.*

3. The dialogue between concepts and tools

A cooperation between the CNIL and the Autorité de la concurrence, that goes beyong mitigating the tensions that may exist between two distinct regulatory frameworks and genuinely seeks convergence by developing synergies - within the limits of the legal framework defining the competencies and powers of the departments of each of these institutions - must promote a dialogue of concepts (but also of tools). Such a dialogue makes it possible to take advantage of a shared set of objectives and to foster mutual inspiration between the two regulatory frameworks. After the Meta Platforms ruling, this exercise, as exemplified by the Court itself, has become indispensable. However, in many cases, concepts and tools cannot be automatically transposed from one framework to the other, and require adaptation.

Competition law and case law have enabled the building of numerous tools and concepts which, with regard to personal data protection, can improve the consideration of competition issues in CNIL decisions (3.1). Reciprocally, the GDPR and associated case law enable competition analysis to better take account of the data practices of players in the practice of the Autorité de la concurrence (3.2). This cross consideration of personal data and competition also enables progress to be made on a risk-based approach, in order to better approach the potential effects on individuals and markets (3.3). Ultimately, this dialogue of concepts and tools between the CNIL and the Autorité de la concurrence must be reflected in existing cooperation, particularly with regard to implementation (3.4).

3.1 Considering competition in data protection

3.1.1 Dominance

Although not defined in the law, the concept of dominance has been clarified by case law as "*a position of economic strength enjoyed by an undertaking which enables it to prevent effective competition from being maintained on the relevant market by giving it the power to behave to an appreciable extent independently of its competitors, its customers and ultimately, consumers*"[29]. Moreover, the CJEU also states that "*such a position, unlike a monopoly or a quasimonopoly, does not preclude some competition but enables the undertaking profitting from it to determine, or at least to have a significant influence on the conditions under which that competition will develop, and in any case, to largely disregard competition without suffering any* detriment"[30].

A dominant position is not unlawful in itself: only its abuse is prohibited. However, with the development of business models that make massive use of personal data, privacy and corporate behaviour in terms of personal data protection have become important determinants in the analysis of a company's dominance and associated abuses.

While the role of data protection in the qualification of abuse of dominance seems destined to grow, the role of dominance (and abuse of dominance) in personal data protection, although existing, remains underdeveloped. For example, when an abuse of dominance takes the form of tied sales, an analysis of market segmentation[31] in terms of privacy can improve the competitive analysis. Conversely, this notion of abuse could be useful in

[29] CJEU, aff. 27/76, 14 févr. 1978, United Brands / Commission, Rec. p. 00207, pt 65.
[30] CJEU, aff. 85/76, 13 févr. 1979, Hoffmann-La Roche / Commission, Rec. p. 00461, pt 4.
[31] In other words, products or services with different levels of privacy protection.

identifying the contractual conditions applied when a company implements a business model offering both a free version remunerated by targeted advertising and an alternative paid service without targeted advertising.

In its decision C-252/21, relying on Recital 43 of the GDPR, which states that "*where there is a clear imbalance between the data subject and the controller*", consent cannot constitute a valid legal basis, the CJEU highlighted the important role of dominant position on the assessment of the freedom of consent[32]. It is necessary to determine whether there is a clear imbalance between the user and the service, whether consent is sought at a sufficiently granular level, and whether the data collection is strictly necessary[33]. Consequently, even though dominance increases the likelihood of such an imbalance without in itself invalidating consent, it is still up to the supplier, in this case as in others, to prove that his action does not call into question the freedom of consent [34].

Similarly, with regard to the choice of legal basis, the G29 guidelines on legitimate interest adopted in 2014 take dominance into account among the factors relevant to the balance of interests between the data subject and the controller, with the latterbeing in a better position to impose what it considers to be its legitimate interest[35].

Beyond this, a number of questions arise to better understand the role that dominance can play in data protection practice: (1) How should dominance be considered when only non-privacy-segmented alternatives are present on the market? (2) What is the role of dominance when more privacy-friendly alternatives exist? (3) What role can abuse of a dominant position have on the conditions of protection? (4) Can the absence of any alternative be explained by a dominant position?

Moreover, in the case of dominance, the risk for personal data protection is greater, as the entity could be tempted to abuse its contractual conditions [36]. Furthermore, dominance tends to reduce people's choices on the market. Consequently, taking dominance into account allows for better consideration of the existing asymmetry between the firm and individuals[37], which allows for a better assessment of whether a manifest imbalance exists.

3.1.2 Market power

In competition, market power is defined as "the *firms' ability to raise prices substantially above costs or to offer low quality products and services*"[38]. In competition law, the existence of market power is not sufficient to qualify a behaviour as anti-competitive or to prohibit a proposed merger. Moreover, the acquisition of market power may result from the free play of competition. Nevertheless, its "excessive concentration"[39] or use to restrict competition raises important issues.

For example, the Autorité de la Concurrence states that a digital platform could be defined as a company that holds structuring market power by considering "*its size, financial capacity, user community and/or the data that it* holds"[40]. This power would enable it to "*control access to or significantly affect the functioning of the market(s) in which it operates*"[41]. Thus, the company's ability to collect and use data is also a potential indicator of market power.

In personal data protection, generalizing the G29 approach, the role of market power[42] can be decisive for the assessment of the balance of interests when the processing is founded on the legal basis of legitimate interest. Holding market power enables the company to influence user choice. In some cases, this can lead to a reduction in the number of offers available on the market. As a result, the price offered becomes higher than it should be, the quality of data protection in the available offers may diminish and, ultimately, the user's ability to negotiate

---

[32] CJEU, aff. C-252/21, 4 juill. 2023, Meta Platforms Inc. e.a. contre Bundeskartellamt, pt 155.
[33] Ibid., point 144 et 149.
[34] Ibid., point 98 et 152.
[35] G29, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 9 avril 2014, pages 40 et 55.
[36] Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR), point 127.
[37] Ibid.
[38] Tirole, J. (2014). Nobel Prize Lecture, Market Failures and Public Policy.
[39] Autorité de la concurrence, 3th march 2023, Roadmap 2023-2024.
[40] Autorité de la concurrence, 19 february 2020, The Autorité de la concurrence's contribution to the debate on competition policy and digital challenges, p.7.
[41] Ibid.
[42] Graef, I. et Van Berlo, S. (2021). Towards Smarter Regulation in the Areas of Competition, Data Protection and Consumer Law: Why Greater Power Should Come with Greater Responsibility. *European Journal of Risk Regulation*, *12*(3), 674–698. https://doi.org/10.1017/err.2020.92.

or switch providers may be reduced. In this example, market power has the effect of increasing the existing asymmetry between the company and its users. It can also have the effect of skewing contractual negotiations between an actor and other partners or intermediaries when it comes to processing personal data (for example, between a data controller and its subcontractor).

Thus, through a competitive analysis of market structure and player behavior we can draw wider implications for data protection, for example to asses a possible clear imbalance or balancing interests at stake. In data protection, it is not the question of barriers to entry to the market as such that matters, but that of preserving the autonomy of the markets' users.

Box 2: "Data power", an example of a conceptual adaptation

In the digital sector, where data is at the core of the construction of competitive advantage, obtaining or reinforcing market power comes, in some cases, from controlling personal data, particularly when a digital platform is involved. From the CNIL's point of view, this phenomenon is problematic, as data protection principles require that personal data should be under the control of individuals, not data controllers, and that the latter should not be able to impose their choices on individuals in this area.

Whereas in competition law, market power refers to an actor's influence on the way supply (competitors) and demand (consumers) are organized, in data protection, we are interested in the effects of this influence on individuals through the consequences of this position on their ability to exercise their fundamental right to the personal data protection. In this respect, data power looks more like an imbalance between consumer and professional in consumer law. It may therefore be worth adapting the concepts rather than reusing them inappropriately.

From the CNIL's point of view, "data power", which can manifest itself in a number of ways in objective empirical reality, can therefore be defined as an impediment to a person's informational autonomy, due to an economic imbalance between them and the data controller, reflected in an asymmetry of information or other biases of individual rationality, and measured by a risk to the protection of that person's data or privacy.

"Data power", "a multifaceted form of power available to digital platforms, arising from their control over data flows"[43], could be particularly relevant to a better understanding of these companies' ability to act on data. Indeed, a platform's omnipresence may enable it to access, accumulate and combine large volumes of data, and while the processing may - if it complies with the GDPR - not be problematic, the power arising from the volume, variety of data, as well as the asymmetry between companies and consumers may be[44] for reasons that this concept helps expliciting.

The existence of data power could, for example, make it possible to better understand the effects of a company's behaviour on the consumer's ability to exercise choice, given existing alternative offers. In particular, taking it into account could help improve analysis of the company's ability to affect user consent. For example, the use of "dark patterns" by major platforms could in some cases be a clue to the existence of data power. In "consent or pay" models, for example, "in line with the principle of fairness, power balance should be a key consideration of the controller-data subject relationship: power imbalances should be avoided or, when impossible, they should be recognised and accounted for with suitable countermeasures. The goal is to ensure that the data subject can engage in a genuinely free choice when consenting to the processing of personal data"[45].

Initially promoted by Orla Lynskey, this concept has been taken up by Majcher (2023)[46] and some regulators such as the EDPS (Colaps et D'Cunha, 2024[47]). These authors highlight its adaptation in terms of the integrity of data subjects' informational autonomy and through the notion of "clear imbalance" in Recital 43 of the GDPR, which plays an important role in the analyses. Also, from an economic point of view, "data power" describes the

---

[43] Lynskey, O. (2019). Grappling with "Data Power": Normative Nudges from Data Protection and Privacy. *Theoretical Inquiries in Law*, *20*(1), 189-220. https://doi.org/10.1515/til-2019-0007.

[44] Karjalainen, T. (2022). The battle of power: Enforcing data protection law against companies holding data power, *Computer Law & Security Review*, 47(105742), https://doi.org/10.1016/j.clsr.2022.105742

[45] EDPB, 17 avril 2024, Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, Opinion of the Board (Art. 64).

[46] Majcher, Klaudia, 'The Big Picture', *Coherence between Data Protection and Competition Law in Digital Markets*, Oxford Data Protection & Privacy Law, Oxford, 2023, https://doi.org/10.1093/oso/9780198885610.003.0008.

[47] D'Cunha, C., Colaps, A., "A clear imbalance between the data subject and the controller : data protection and competition law", in Two decades of personal data protection, What next ? EDPS 20th Anniversary, chapitre 15, pp. 192 à 205. Luxembourg : Office des publications de l'UE, 2024.

ability of data controllers to extract value from data generated by using the service to their own benefit in the data value chain (e.g. targeted advertising), leaving the individuals concerned with negative externalities (risks, costs of data misuse, price personalization, etc.).

The scope of this concept is extensive: it can also be used to describe the asymmetrical negotiating capacity of major online platforms with other companies and intermediaries who need their data but are sometimes subject to asymmetric or even discriminatory clauses (the fairness of contractual relations is one of the subjects of the Data Act), as well as the ability of these players to keep their partners in the dark about the practices used (ex: audience measurement and the effectiveness of targeted advertising), or to modify the rules of the ecosystem to their advantage (e.g. the compliance role of mobile app stores, Google's privacy sandbox). Ultimately, this power could fuel predatory acquisitions and reduce market contestability and innovation (Majcher, 2023).

Finally, "data power" covers the lobbying capacity of these major players, their ability to influence the media and political "narrative" and thus, in the end, to make regulations evolve to their advantage, not to mention the resources they can devote to litigation to evade implementation decisions by the competent authorities, whether these relate to competition or data protection.

For Klaudia Majcher, it is possible for an authority to qualify the existence of data power according to these three dimensions: individual, economic, and political, using both a structural and behavioural analysis of the actor. This analytical grid could be usefully supplemented by an analysis of the situation of affected individuals, and in particular of the prejudices they experience, such as informational prejudices.

Proposal no. 2: experiment with the concept of "data power" as a doctrinal insight, *when more appropriate than existing competitive concepts (dominance or market power) in CNIL's data protection analyses, when assessing the relationship between a data subject and a data controller.*

3.1.3 Better defining the product or service concerned

The use of the relevant market concept by competition authorities requires technical resources and investigative powers that differ from those of the CNIL. Furthermore, it requires a product or service to be defined within a precise timeframe, in order to determine potential effects on the market. The delimitation of the relevant market is therefore, in itself, an important part of the analysis in decisions or opinions issued by the Autorité de la concurrence. It could hardly be reproduced from the point of view of a data protection authority.

Nevertheless, this approach can be a source of inspiration. Indeed, the protection of personal data invites us to take the effects of companies' practices on users as the starting point of the analysis. Therefore, there is a need for the CNIL to precisely define the product or service in question in order to best assess the degree to which companies comply with the rules of the GDPR. Thus, previous industry opinions or decisions by the Autorité de la concurrence, or even the European Commission, could enable the CNIL to confirm the choice of product or service concerned.

In addition, the methodology used to delimit the relevant market could provide indications of best practices to define the products or services concerned. One example is the notion of substitutability, i.e. the ability of one product to replace another without loss of value for the user. From a GDPR perspective, without needing an economic calculation, the notion of functional equivalence for the user could be applied. For instance, in a "pay or consent" model, this would mean that the user would benefit from a service or product with the same functionalities, regardless of the formula offered (paid or free).

Other elements from the user's point of view can usefully inspire the CNIL, such as the user's ability to make a free choice between continuing or stopping using a service. This depends on whether the user has a "genuine alternative". For example, in "pay or consent" models, where a user has no choice but to use another service that also requires consent to maintain an active service, the user could find himself in a situation of coercion, where prejudice could be accentuated.

3.1.4 Exclusivity in contractual conditions

Competition law is also concerned with exclusivity agreements. These are contracts which, under certain circumstances, have an obvious impact on competition. Their purpose may be to establish a commitment by a buyer to obtain supplies from a single manufacturer (exclusivity of supply). Commitments can also be made to ensure that the manufacturer or retailer procures exclusively from one distributor (exclusivity of procurement).

A contract may also set out terms so that, in addition to commitments on supply and/or procurement, terms and conditions of sale are laid down (concession exclusivity)[48].

Such contracts can lead to anti-competitive behaviour, such as abuse of a dominant position. Exclusivity contracts transform relations between market players, and thus alter the normal structure of competition. In particular, when a company is dominant, it may try to "foreclose its competitors by hindering them from purchasing from suppliers. The Commission considers that such input foreclosure is, in principle, liable to result in anti-competitive foreclosure if the exclusive supply obligation or the incentive ties most efficient input suppliers and if the companies competing with the dominant undertaking are unable to find alternative efficient sources of input supply"[49].

From the point of view of personal data protection, these exclusivity agreements can lead to a restriction in the number of equivalent alternatives available to users. The doctrine of cookie walls shows that the existence of equivalent alternatives must be considered when assessing the validity of consent. This criterion is also an important element in assessing the validity of consent in the context of "consent or pay" models.

Exclusivity can also relate to questions of data access or provision. This question of asymmetrical data sharing can only be seen differently from the point of view of the two authorities: while competition authorities might see it as an anti-competitive practice, data protection authorities will assess whether the sharing was necessary to achieve the purpose of the processing, and will seek to ensure that it does not exceed that necessity. However, there is no general (*erga omnes*) obligation of open access to data held by a company, insofar as personal data does not generally qualify as an "essential infrastructure" within the meaning of competition law: as it is non-rival, it can be collected freely, subject to compliance with the applicable framework, , on the contrary, open access would increase dependence on the largest data providers[50]. On the other hand, the two authorities will agree on the need for transparency with regard to these data access partnerships (both towards the people concerned, who benefit from a legal obligation in this respect, and towards the market).

3.2 Making explicit the role of data protection as a competitive parameter

3.2.1 Lawfulness

Article 5.1 a) of the GDPR states that personal data must be "*processed lawfully, fairly and in a transparent manner in relation to the data subject*". Furthermore, processing is lawful only if it complies with one of the six legal bases of the GDPR[51].

Competitive analysis can help identify a situation in which a player would benefit from the unlawfulness of its processing. Thus, by implementing unlawful processing, the company could be able to strengthen, maintain or acquire an advantageous position on the market (concept of "unfair competition"). For a competition authority, this could also be a constitutive element of market power and/or a dominant position. In other words, the unlawfulness of a treatment could lead to adverse effects on competition. The French Court of cassation has consistently ruled that failure to comply with a regulation confers to the responsible party "*an undue competitive advantage, which may constitute unfair competition*"[52].

Moreover, considering the company's strategy may be useful to better answer various questions such as - What data are involved? How were they used? For what purposes were they processed? - that are of interest to the CNIL. The advantage derived from the unlawfulness of the processing could be corroborated by the competitive motives identified during the analysis phase.

In cases when the manifest nature of the competitive advantage thus obtained cannot be established, particularly in the absence of a decision by the Competition Authority or the European Commission, referral to the Competition Authority for an opinion is necessary. This opinion could then make it possible to characterize the unlawfulness of a processing operation under the GDPR. Consequently, integrating competitive analysis

---

[48] Reboud, L. (1968), Contrats d'exclusivité et concurrence, *L'Actualité économique*, 43(4), 617–669. https://doi.org/10.7202/1003090ar.

[49] European Commission, 24 february 2009, Communication from the Commission — Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings, 2009/C 45/02, point 32.

[50] Cf. Autorité de la concurrence et Bundeskartellamt, « Droit de la concurrence et données », étude publiée, 10 mai 2016 : https://www.autoritedelaconcurrence.fr/sites/default/files/Big%20Data%20Papier.pdf page 20.

[51] Article 6.1 of GDPR.

[52] v. p. ex. Cass. Comm. 27 septembre 2023, n°21-21.995. [free translation, see original text]

upstream of requests for advice will make it easier to identify situations requiring an advice from the Autorité de la concurrence.

Proposal no. 3: develop within CNIL's practice the consideration of competitive unlawfulness under Article 5.1 a) GDPR. *Unfair competition behaviour or anti-competitive practices, if judged or documented by competition authorities, may constitute complementary factors to breaches of data protection rules. Otherwise, the matter should be referred to the French competition authority for an opinion.*

Box 3: Compliance with the *non bis in idem* principle in the implementation of competition and data protection law

According to the *non bis in idem* principle, a general principle of law derived from criminal procedure and enshrined both in article 8 of the Declaration of the Rights of Man and of the Citizen and in article 50 of the Charter of Fundamental Rights of the European Union, no one may be prosecuted or punished twice for the same acts. This principle is not limited to "criminal" prosecutions and sanctions, but extends more generally to any sanction with a punitive character, even when it is not pronounced by a criminal court. It therefore applies to breaches of competition and data protection law, which may in particular give rise to administrative sanctions.

In this respect, in the event of successive application of competition law and data protection law in related cases, the risk of infringing this principle appears limited. Indeed, in addition to the fact that in many cases the analysis will concern distinct facts, competition law and personal data protection have very different objectives and protect dquite ifferent societal interests.

Furthermore, the case law of the French Constitutional Council[53] specifies that "*the same facts may be the subject of different prosecutions for the purposes of different types of sanctions under different sets of rules*", provided the principle of proportionality of offences and penalties is respected in the event of cumulative sanctions. Likewise, in the case of regulations with similar objectives, the case law of the CJEU indicates that this principle does not prevent a company from being sanctioned for an infringement of competition law when it has already been the subject of a final decision for non-compliance with a sector-specific regulation for the same facts[54].

3.2.2 Necessity

Whatever its legal basis, a processing must always be necessary to achieve the purpose pursued by the data controller. This purpose must be predefined.

This principle is particularly important at the time of database mergers during concentration operations between companies. The existence of a history of mergers in which personal data have been affected should induce vigilance. The data controller must be able to demonstrate that processing prior to the merger is still necessary, specifying any new conditions under which processing will be carried out.

Thus, competitive situations reducing the choices available to consumers raise the question of the number of true alternatives to a dominant solution. This is also the case for competitive structures where few players represent a genuine alternative (oligopoly, for example) recognized and established by the French Competition Authority. In such situations, it would be useful to determine both the less intrusive nature of the alternative and the user's ability to choose this alternative.

3.2.3 Free consent

Consent as a legal basis for processing must, in order to be valid within the meaning of the GDPR, be given freely by the data subject and be specific, informed, and unambiguous[55].

In order to be free, consent must be the result of a genuine and uncoerced choice on the part of the person concerned.

---

[53] For example: Cons. Const., décision n° 2021-892 QPC, 26 mars 2021, Akka technologies and others, concerning the sanction for obstruction of investigations by the competition authority. [free translation, see original text]

[54] CJEU, case C-117/20, 22 march 2022, bpost SA v Belgian Competition Authority, paragraphs 40-58.

[55] Art. 4.11 of GDPR.

However, an analysis of a data controller's position on a given market can be useful in assessing whether consent to the processing of personal data is freely given.

The *Meta Platforms* ruling provides a concrete example of how the competitive situation can be used to assess the freedom of consent of data subjects[56][57]. The dominant position of the data controller on a given market could thus, without affecting the freedom of consent as a matter of principle, be taken into account to determine whether the criterion of freedom of consent is satisfied.

Conversely, the consumer's ability to make a free choice can also be used to qualify anti-competitive behaviour. To better protect privacy, it is therefore important to consider any decisions taken by the Autorité de la concurrence or the European Commission concerning a company's competitive behaviour, particularly when privacy has been identified as one of the competitive parameters.

Moreover, the lack of freedom of user consent can also be, from a competitive point of view, the result of the abusive exercise of market power. In this situation, freedom of consent is a decisive parameter for identifying how the company has abused its market power. The absence of freedom of consent, or the manipulation of consent by dark patterns, for example, can play an important role in the Autorité de la Concurrence's characterization of abuse of market power.

In addition, when a processing operation is based on the legal basis of consent, the assessment of compliance with the principle of necessity takes into account the alternatives offered to the user (e.g. in the case of biometric data processing, with the legal basis of consent, an alternative to biometrics must exist for consent to be valid). Particularly, the data controller's ability to propose an identical processing operation that provides better privacy protection is examined. So, in this case, the presence of less privacy-intrusive alternatives on the market is an important factor in assessing whether the actor in question complies with the principle of necessity.

3.2.4 Fairness in processing

Under the terms of article 5.1 a) of the GDPR, personal data must be collected lawfully, fairly and transparently. Recital 39 of the GDPR specifies in this regard that the fact that personal data is being processed and how, should be transparent to data subjects. The information provided to data subjects on processing concerning them (identity of the controller, purposes of the processing in particular) makes it possible to ensure fair and transparent processing with regard to data subjects.

Compliance with the principle of fair processing is therefore closely linked to the transparency shown to data subjects: data processing must correspond factually to the description given to data subjects. All relevant information concerning the processing must be provided to data subjects, pursuant to Articles 13 and 14 of the GDPR, and moreover presented in a way that is easily accessible and easy to understand (recital 39 GDPR).

The principle of fairness has in this sense been described by the literature58 (and by the EDPS59 in its opinion 8/201660) as making it possible to link competition, data protection and consumer protection as it's this principle that puts the user in an informed position to decide how their data is used. Consumer law prohibits unfair commercial practices61.

For its part, competition law prohibits the imposition of "unfair trading conditions" (article 102 TFEU), considered abusive in a dominant position. In this regard, a breach of the principle of fairness in data processing could harm competition and thus increase its severity, for example with regard to transparency for data subjects.

3.2.5 Minimization

The competitive situation may also be considered when analyzing proportionality and the necessity of data collection with regard to the principle of minimization or the legal basis chosen[62].

---

[56] CJEU, case C-252/21, 4 july 2023, Meta Platforms Inc. e.a. contre Bundeskartellamt, p. 36.
[57] Article 7.4 of GDPR.
[58] I. Graef, D. Clifford et P. Valcke (2018). Fairness and enforcement; bridging competition, data protection, and consumer law, *International Data Privacy Law*, 2018, 8(3).
[59] The EDPS is the data protection authority for the institutions, bodies and agencies of the European Union.
[60] https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf
[61] Directive 2005/29 of May 11, 2005 concerning unfair business-to-consumer commercial practices in the internal market.
[62] Article 5.1.c of GDPR; art. 6 of GDPR.

The absence or low level of competition, particularly when the company is in a dominant position, could be one of the indicators of possible over-collection when consumers have no choice on the market between services involving different levels of data collection, thus violating the minimization principle.

In this context, given the biases affecting individuals' decisions and potentialincentives in place (which may, in some cases, constitute dark patterns), the data controller should demonstrate that it does not over-collect or that it allows for an effective choice between several levels of service that adjust the intensity of data collection, provided that the objectives pursued by data processing justify the collection of data at these different levels. Recent developments have tended to equate excessive data collection with abuse of a dominant position, with the supply of data being equated to a price paid[63].

Nevertheless, the type of abuse is decisive in determining if it is an indication of over-collection, and should be precisely identified.

Regarding abuse of a dominant position, practices such as self-preferencing are examples of situations where over-collection could occur. Indeed, if the accumulation of data is intended to facilitate this type of practice, compliance with the principle of data minimization could be affected.

The abuse of economic dependence can also be an indication of over-collection when it involves the exchange of personal data between companies. This abuse is characterized by excessive exploitation of the situation of dependence through abnormal, unbalanced or excessive practices that impose "*directly or indirectly unfair trading conditions*"[64]. Thus, excessive data collection could result from the dominant company's desire to over-collect.

Proposal no. 4: with a view to increasing compliance with the minimization principle, develop an analysis of the role played by anti-competitive practices in the accumulation of data and *indicators of data collection that harm individuals who cannot object to it.*

3.2.6 Qualification of actors

Market imbalances can affect the data controller's choices in terms of data protection: due to its low market power, a data controller could find its choice of business partners limited. As a result of these limited choices, it could find it more difficult to ensure that the processing operations for which it is responsible are compatible with the GDPR. For example, they could fail to require their processor to implement measures necessary for the data controller to comply with its own obligations under the GDPR, or may not find a supplier of technical solutions on the market that comply with regulations.

However, a limited choice of commercial partners and the resulting power inbalance are not intended to exempt the data controller from their own obligations with regard to data protection: for example, the data controller is always free to choose their subcontractor, even if the offer on the market is limited.

Similarly, a power inbalance between two players would have no effect on qualification under the GDPR for a given processing operation. Indeed, market power does not enter into the criteria for determining qualification under the GDPR.

Furthermore, it would be advisable for data protection authorities to consider these imbalances in their oversight practices, so as to take into account the entire processing chain and the players who have a leverage effect on the others.

In the event of a breach by the processor of its obligations to the controller under the GDPR, it is still possible for the controller to call its co-contractor into question on the grounds of the ordinary law of obligations. Providing a service as a subcontractor that does not in itself comply with the GDPR engages the subcontractor's civil liability vis-à-vis its data controller [65].

---

[63] Directive no. 2019/770 of May 20, 2019 on certain aspects of contracts for the supply of digital content and services, article 3.1 para. 2.

[64] CJEU, case T-151/01, 24 may 2007, Duales System Deutschland / Commission, Rec. p. II-1607, pt 120-122.

[65] In particular, the contract binding the controller and the processor may be rendered null and void if the failure of the co-contractor to comply with its obligations under the GDPR constitutes an error as to the essential qualities of the subject matter of the contract (see in this sense CA Grenoble, Jan. 12, 2023, no. 21/03701, in the case of website design).

3.3 A joint risk-based approach

3.3.1 Conglomerate and vertical risks

The European Commission specifies that "Vertical mergers involve companies operating at different levels of the supply chain"[66]. This is the case, for example, when a manufacturer merges with one of its distributors. On the other hand, "*Conglomerate mergers are mergers between firms that are in a relationship which is neither horizontal (as competitors in the same relevant market) nor vertical (as suppliers or customers)*"[67]. Thus, conglomerate or vertical integration creates specific competitive risks.

While vertical or conglomerate mergers are "*generally less likely to significantly impede effective competition than horizontal mergers*"[68], they may in some cases significantly hinder effective competition. Two main effects are systematically examined: coordinated and non-coordinated effects.

"*Non-coordinated effects may principally arise when non-horizontal mergers give rise to foreclosure*"[69], meaning that when "actual or potential rivals' access to supplies or markets is hampered or blocked as a result of the merger, thereby reducing these companies' ability and/or incentive to compete"[70]. This can lead to a risk of increased price for consumers or reduced service quality. With regards to data protection, such a situation could steer consumers towards alternatives that are less protective of privacy or personal data, in order to benefit from a better price. In this way, a company's strong - vertical or conglomerate integration - could limit access to better privacy protection. This risk particularly pronounced in the platform economy, which sometimes benefits from significant portfolio effects, creating incentives for vertical or conglomerate concentration.

On the other hand, "*Coordinated effects arise where the merger changes the nature of competition in such a way that firms that previously were not coordinating their behaviour, are now significantly more likely to coordinate to raise prices or otherwise harm effective competition*"[71]. This situation increases the risk to personal data protection by strengthening the incentive to combine data (coordination for access to inputs). Moreover, the DMA, although prohibiting the combination of data for access controllers, provides only a partial response as it remains limited to a cross-reference of the provisions relating to the combination of data collected by the essential platform to the legal basis of consent. Indeed, the company will be able to combine personal data if a clear choice has been presented to the end user and they have given their consent within the meaning of Articles 4 and 7 of the GDPR[72].

Other practices can also have an impact on the protection of privacy and personal data. These include tied sales and bundled sales, which consist respectively in making the purchase of one product conditional on another, and in making only a set of products available for purchase.[73]. Such practices, particularly when a company is dominant, may seek to drive competitors out of the market and steer consumer choices towards products that are less protective of personal data and privacy. In particular, such practices can artificially limit the development of privacy-friendly innovations, especially "*when the competitors excluded by the dominant undertaking are, as a result of the refusal, prevented from bringing innovative goods or services to market and/or where subsequent innovation is likely to be* stifled"[74].

In addition, the merger of companies may lead to one of the merging parties retrieving data held by the other company. While this consequence may not raise any risk from a competition point of view, the purpose of the merger could be seen, in some cases, as an attempton the part of the data controller to circumvent GDPR rules

---

[66] European Commission, 18 october 2018, Guidelines on the assessment of non-horizontal mergers under the Council Regulation on the control of concentrations between undertakings, 2008/C 265/07, point 4.
[67] Ibid., point 5.
[68] Ibid., point 11.
[69] Ibid., point 18.
[70] Ibid.
[71] Ibid., point 19.
[72] Article 5.2 of Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).
[73] European Commission, 24 February 2009, Communication from the Commission — Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings, 2009/C 45/02.
[74] Ibid., point 87.

on the reuse of personal data. The rise of data-driven mergers increases the risk of such situations arising, whether the integration is vertical, conglomerate or horizontal.

Understanding these situations and practices, as well as incorporating their implications for privacy protection, is important for improving the analysis and decisions that can be made.

3.3.2 Structural and behavioral risks

To better understand the impact of corporate practices and behaviour on personal data protection and privacy. We need to distinguish between structural and behavioural risks. These two categories do not have the same effects on the market, and can therefore have different consequences in terms of personal data protection. While structural risks correspond to market structure issues between players, behavioural risks concern the practices and behaviours put in place by the company.

Indeed, certain anti-competitive practices or mergers can have the effect of modifying market structure by creating or strengthening one or more market players. These situations give rise to a heightened risk of reinforcing a company's market power, in the form of power over data. This reinforcement can lead to behaviour that is harmful from a data protection point of view. For example, increasing a company's data power can facilitate the implementation of over-collection practices that could be contrary to the principle of minimization. Such situations are more frequently identified in merger projects analyzed by the Autorité de la concurrence.

Behavioural risks, on the other hand, stem from practices designed to alter the way the market operates. These situations can lead to a reduction in the overall level of competition on the market, and strengthen the position of one or more players.

It must therefore be possible for the two authorities to carry out a joint analysis of these risks: both from the point of view of mergers and market practices. Ideally, the two authorities should establish a joint work program to explore risks, with the periodic identification of subjects of common interest for which informal exchanges of expertise, voluntary joint hearings, and joint studies would be envisaged.

In addition, as the law stands at the moment, the CNIL staff can be called on as external rapporteurs by the l'Autorité de la concurrence in case investigations, contributing to the exchange of expertise. Likewise, Autorité de la concurrence staff can be invited when necessary to CNIL's sector-specific "compliance clubs", when competition issues are likely to be raised.

Proposal no. 5: Jointly explore risks and markets *through exchanges of expertise, voluntary joint hearings, or joint studies between the CNIL and the Autorité de la concurrence.*

3.3.3 Data Protection Impact Assessments (DPIAs)

When the market structure is not sufficiently competitive, the dominant company or companies may have more incentive to carry out large-scale processing of data, sometimes sensitive data. Similarly, the acquisition of power over data (e.g. privileged or less costly access, combination possibilities, economies of scale) creates additional risks for individuals (see Box 2). In such cases, it may be necessary to carry out a data protection impact assessment (DPIA) for such processing operations. Indeed, a DPIA must be carried out when the processing is "*likely to result in a high risk to the rights and freedoms of affected individuals*" (art. 35-1 of the GDPR). In this respect, the collection of personal data on a large scale, combined with another risk factor, is a decisive criterion for the mandatory nature of a DPIA[75].

Thus, the notion of "data power", as an element of the risk to be analyzed, could reinforce the need to set up a DPIA. In particular, the study of potential impacts could be improved by taking greater account of the risky nature of the company's processing operations, given its position on the market and its influence over the data.

In particular, the assessment of the controller's legitimate interest when describing the processing operations envisaged[76], the balance of interests between the individual and the controller and the purposes of the processing should be supplemented by a consideration of the company's power over the data. In addition,

[75] G29, Guidelines on data protection impact assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation (EU) 2016/679, 4 Apr. 2017.
[76] Article 35.7.a GDPR.

situations of dominance could, in certain cases, have the effect of modifying the assessment of the necessity and proportionality of processing operations[77].

3.4 A better structured cooperation, including for implementation

3.4.1 Varied organizational approach accross countries

In the digital economy, cooperation between data protection and competition authorities in regulatory enforcement, i.e. on specific cases where breaches are identified, is particularly useful. There are many examples of cooperation between data protection and competition authorities in Europe and worldwide. Most involve pooling resources to analyze specific sectors. However, few countries have a formal structure for cooperation between the two authorities, which is the only way to exchange information on cases. For example, countries such as Argentina, Brazil, Japan and Canada are developing numerous collaborations between their national regulators without formal structures.

This is also the case in Germany, although German merger legislation has been modernized, and in Italy and Mexico. Nevertheless, in some countries, cooperation is organized either by provisions in the law, which allow for lifting professional secrecy obligations, or through joint declarations. Cooperation between the CNIL and the Autorité de la concurrence falls into the latter category.

Finally, more structured forms of cooperation also exist, such as the *Australian Digital Platform Regulators Forum* (DP-REG), the *Netherlands' Digital Regulation Cooperation Platform* (SDT), the *Irish Digital Regulators Group* (DRG) and the *Digital Regulation Cooperation Forum* (DRCF) in the UK. These are similar to exchange forums between authorities, but are not restricted to data protection and competition authorities. These forums can be considered the most advanced forms of cooperation. In France, the SREN Act created a national coordination network for the regulation of digital services, which brings together independent administrative authorities (AAIs) and government departments, but does not encroach on the missions of AAIs as defined by the Act[78].

In particular, the DRCF[79] provides the United Kingdom a successful model of cooperation between the data protection, competition, financial markets and communications authorities.

The DRCF regularly conducts studies, organizes seminars and conferences, and participates in developping common positions for its members. The forum is staffed by a team of permanent employees, supplemented by staff from member authorities. However, the DRCF is not intended to become a structure with powers of its own, nor to cooperate on cases. Its purpose is to reinforce coherence, increase collaboration and develop the capacities of member authorities.

3.4.2 Structuring work with the Autorité de la concurrence

The referral mechanism between the CNIL and the Autorité de la concurrence enables each authority to refer to the other when situations are identified. This mechanism gives the authorities full control over the frequency and subjects of referrals. Moreover, the various opinions issued by the two authorities demonstrate the diversity of possible contributions. In addition, closer cooperation on concrete cases enables each authority to better understand the other's analyses.

In fact, both Article R. 463-9 of the French Commercial Code and Article 15 of Law no. 2017-55 of January 20, 2017 on the general status of independent administrative authorities and independent public authorities allow the two authorities to exchange information on cases without being bound by professional secrecy towards each other.

De facto, the Autorité de la concurrence has regularly mobilized this mechanism in its litigation procedures, and the CNIL referred the matter to the Competition Authority for an opinion for the first time in 2023 as part of its draft recommendation on mobile applications[80]. Both authorities have systematically paid close attention to the

---

[77] Article 35.7.b of GDPR.
[78] New article 7-4 of the French law on confidence in the digital economy, amended by article 51 of law no. 2024-449 of May 21, 2024 aimed at securing and regulating the digital space.
[79] The DRCF is a non-statutory, voluntary body set up by the UK government. Four British regulators - the CMA, the ICO, Ofcom and the FCA - contribute to it. Its aim is to promote cooperation and exchanges between these regulators. To this end, it publishes studies, organizes workshops and conferences, and participates in the development of common positions.
[80] https://www.cnil.fr/fr/applications-mobiles-la-cnil-publie-ses-recommandations-pour-mieux-proteger-la-vie-privee

opinions issued, in order to fully account for the comments and recommendations made. Increased cooperation with the Autorité de la concurrence also shows that the current organization allows for joint work, and that this cooperation can be further intensified while maintaining the initial organization.

Moreover, the current structure is straightforward, ensuring that the actions of the two authorities are easy to understand for economic players. It ensures consistency in the desire to maintain clarity in each authority's competencies, while taking account of the other's challenges. In addition, with increasing experience in informal referrals and exchanges, both authorities are improving the implementation of their cooperative framework.

3.4.3 Deepening cooperation through a contact point

Without modifying the existing framework, improvements could be envisaged to strengthen the link between personal data protection and competition. This cooperation must take place on three levels: concepts, doctrine, and cases of implementation[81].

The joint declaration already mentions *« joint work (...) lead to identification of new regulatory issues requiring convergence* »[82], which covers the dialogue of concepts and tools. The joint declaration calls on the two authorities to « *improve dialogue between their respective legal frameworks* »[83]. The definition of an annual work program in this area could be envisaged to encourage exchanges on these subjects. It would then be necessary to define what would make it possible to animate the debate. Similarly, seminars, workshops, joint studies, or inter-departmental exchange meetings could be organized to encourage reflection on more sectoral or thematic issues. These prospective discussions would then contribute to the ongoing cooperation on cases submitted to or taken up by the authorities. Lastly, regular public communication on the state of cooperation between the CNIL and the Autorité de la concurrence could make it possible to assess progress, and to present and explain the main results of cooperation to the public and to businesses.

To be effective, the regular organization of joint meetings and work requires centralized coordination of needs and resources. For this reason, a contact point could be set up within each authority to steer cooperation (identification of topics, internal cooperation to facilitate processing, reporting, etc.).

Finally, neither the legislative framework nor that of the joint declaration outlines procedures for resolving disagreements. Currently, there are no obligations for the two authorities to reach full agreement on all points, provided they can demonstrate that they have "considered", even partially, the other authority's opinion on key issues, ensuring an overall convergence.

Proposal no. 6**: to deepen cooperation between the two authorities* ***across concepts, doctrine, and cases, establish a contact point within each authority, in charge of steering cooperation.

4 Operational consequences for the CNIL

For the CNIL, protecting privacy and personal data requires better consideration of economic and competitive realities. Although the GDPR is not an economic regulation, but rather a matter of fundamental freedoms, economic and competitive perspective contributes significantly to its effectiveness and impact.

Through proactive action, the CNIL can contribute to build an economy more favorable to privacy and personal data protection, which will yield positive outcomes for users who are also consumers (4.1). To achieve this, it is essential to develop the CNIL's ability to better understand and determine how to integrate competition issues into its work (4.2). Lastly, taking into account competitive analysis tools could help improve the calculation of the amount of sanctions for which the company's practices reinforce its economic power (4.3).

[81] Autorité de la concurrence and Commission nationale de l'informatique et des libertés, 2023, "Competition and personal data: a common ambition", p. 13.
[82] Ibid.
[83] Ibid., p. 1.

4.1 Steering the economy towards greater privacy consideration

4.1.1 Level the playing field

The CNIL's soft law instruments (guidelines, recommendations, codes of conduct, etc.) are designed to inform market players about the various regulatory provisions in their respective fields, and their interpretation. They can play a decisive role in the way companies build their data collection and usage strategies. In any case, they help steer companies in the same sector towards more privacy-friendly practices. They therefore encourage the implementation of standards that improve personal data protection.

Codes of conduct and recommendations also help direct corporate behaviour towards a better integration of privacy into their business models. This implementation can be an important differentiating factor for a company in the market. Thus, while providing the means to build ambitious business models, these codes of conduct and recommendations establish a fairer competitive framework, even when there are asymmetrical capabilities between businesses. They also contribute to legal certainty for companies.

For example, the recommendation on mobile applications published in September 2024 reminded the various players in these ecosystems of their regulatory obligations. Although this market is characterized by the presence of structuring players, the recommendation encourages all companies to adopt more virtuous behaviour in terms of privacy and personal data protection. In addition, it proposes a number of best practices requiring companies to rethink their business modelsby incorporating stronger data protection measures.

So, through the protection of privacy, the CNIL promotes fair conditions for data collection and usage. These conditions enable both the small and the large players to benefit from similar regulatory application conditions. In addition, the CNIL's support approach, availablefor all players, ensures that companies have equal access to the regulator.

4.1.2 Innovation

The role of innovation in competition is fundamental. Innovation can stimulate competition by encouraging players to create new products or services that appeal to consumers. Consequently, competition authorities assess both existing and potential competition in their competitive assessments. Innovation can be a decisive parameter in potential competition by limitting or countering market power or the dominance of a company on a given market.

In addition, innovation can also be used "as a countervailing factor for market power, a defence mechanism against anti-competitive conduct, or as a source of productivity gains"[84]. This role only appears in specific situations and conditions. Indeed, some markets are characterized by significant innovation dynamics, which can enable them to compete with dominant companies with significant market power. The history of digital markets has shown that these positions can be rapidly challenged when disruptive innovations are proposed.

The introduction of the GDPR represented both a regulatory and technical revolution. As a result, while during the first few years of the regulation's implementation, companies focused on bringing themselves, for the most part, into compliance, new opportunities have since arisen. Thus, the GDPR has accelerated research and investment in GDPR compliance and privacy protection. *De facto*, companies have grasped the importance of personal data protection in their business models, since transitioning to more virtuous models requires offering innovative solutions. As such, compliance investments contribute significantly to innovation.

Thus, in addition to being a competitive parameter, the protection of privacy and personal data has also become a driver of innovation in many fields, such as cybersecurity, cloud computing and artificial intelligence. So, promoting personal data protection also contributes to encourage players to pursue their innovations. Greater promotion of privacy as a parameter for innovation will enhance market contestability. The example of the advertising market shows that when privacy protection is promoted, innovative solutions can rapidly emerge from companies of all sizes, de facto fostering more intense competition on the market. However, competition and data protection authorities must cooperate closely to prevent either data protection or competition from being abused to the detriment of one or the other.

This means, that in addition to taking data protection competition issues into account upstream (see above), the Autorité de la concurrence must recognize privacy protection as a legitimate objective in business models. At the same time, the CNIL must also be attentive to help detect "privacy washing" behaviour.

---

[84] OCDE, 2023, The Role of Innovation in Competition Enforcement, OECD Competition Policy Roundtable Background Note, DAF/COMP(2023)12, p. 6.

4.1.3 Empowering individuals : portability

As stipulated in Article 20.1 of the GDPR, users "*have the right to receive personal data concerning them, which they have provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided*"[85]. The right to portability is therefore a right for individuals that can be exercised under certain conditions.

As the OECD points out, "*data portability and interoperability measures can promote competition, both within and between digital platforms. These measures can address consumer lock-in, promote unbundling, and enable multi-homing*"[86].

Therefore, promoting portability can benefit users by enabling them to exercise their rights, and by promoting competition in the marketplace. A more ambitious approach would not only make the right to portability more effective, but would also stimulate competition, reducing the "lock-in" effects of major digital services and innovation in the economy.

In particular, the right to portability can be used by competition authorities as a means of reinforcing market contestability in the application of Article 102 TFEU and merger control.

Moreover, in the digital sector, the ability of national competition authorities to open investigations under the DMA strengthens the link between the promotion of greater contestability contestabilitywith personal data protection. Article 6.9 of the DMA stipulates that the "*gatekeeper shall provide end users and third parties authorised by an end user, at their request and free of charge, with effective portability of data provided by the end user or generated through the activity of the end user in the context of the use of the relevant core platform service.This includes by providing, free of charge, tools to facilitate the effective exercise of such data portability, particularly by ensuring the provision of continuous and real-time access to such data*".

The user has a right to portability under both the DMA and the GDPR. As the scope of the DMA's right to portability is broader than that of the GDPR, it could make it possible to protect the user by taking into account both personal data and the company's competitive behaviour.

Proposal no. 7: initiate a specific joint reflection on the right to portability of personal data, and its consequences in terms of personal data protection and competition. *This reflection could, where appropriate, involve other players or authorities with expertise in personal data portability or interoperability, such as Arcep, and be coordinated with the various existing or upcomimg forums (e.g. DMA High Level Group, French national coordination network for the regulation of digital services).*

4.2 Better integrating competition protection upstream

4.2.1 Developing regular awareness of competitive questions

Enhancing the consideration of competition issues in the CNIL's work requires raising awareness of competition issues within the organization. To this end, internal training courses could be organized on general economic topics and competition analysis to provide a better understanding of how the work of a competition authority is structured and what it can contribute to the CNIL. Cross-training sessions between the CNIL and the Autorité de la concurrence staff could also be considered. This would make it possible to propose specific examples and share the experience of investigations, for example.

The CNIL could also strengthen its monitoring and alert mechanisms by regularly inviting the Autorité de la concurrence to present the decisions and work most relevant to the CNIL. Such monitoring and alerts could be supplemented by a regular presentation on past, current and upcoming work from both institutions.

Competition related topics that intersect with personal data protection could also be more regularly communicated in CNIL plenary sessions. The summary of an opinion or decision by the Autorité de la concurrence or the European Commission, when they concern data, regularly involve issues or even consequences for privacy or personal data protection. The College could therefore benefit from such insights.

In addition, it is crucial for the CNIL to continue to examine the economic consequences of its decisions from both an ex-post and an ex-ante perspective. Indeed, integrating competitive and economic issues into the CNIL's

[85] Article 20.1 of the GDPR.
[86] OECD, 7 may 2021, Data portability, interoperability and digital platforms competition – Background Note, DAF/COMP (2021)5, p. 2.

work would enable better consideration of the potential effects of its decisions or recommendations. Among the factors to be verified in these impact studies is the competitive impact of a decision or the direction of the chosen doctrine, so that the decision-making process is fully informed on these aspects.

Proposal no. 8: Regularly organize cross-training sessions *on competition and data protection issues for both authorities.*

4.2.2 Deepen the integration of economics into CNIL's work

One of the primary benefits of incorporating competition issues into the CNIL's work is to better understand the economic and market context in which affected companies operate. To fully benefit from competitive analyses, the CNIL must have prior knowledge of the main economic stakes for a company, and of the market(s) in which it operates. For this reason, it is essential to continue internal business models analyses. Indeed, the CNIL should be able to form an initial opinion before integrating other analyses (from industry or an economic regulator) into its work. The integration of business model analyses, and more generally of the company's economic context, should therefore be reinforced in the CNIL's work.

Economic analysis should also help identify priority areas for CNIL to explore. For example, the emergence of new business models, sectoral changes, or the introduction of more profitable technology, can alter personal data practices. In some situations, these changes can generate new risks for the protection of personal data. It is the CNIL's responsibility to be able to detect and even anticipate these risks, in order to implement necessary recommendations and maintain heightened vigilance on these subjects.

Last but not least, internal economic expertise on markets and business models, both qualitative and quantitative, is essential to fully understand the impact of an upcoming decision (on a player and its market) or of a direction of doctrine (resulting from an act of soft law or a response to a request for advice).

4.3 Clarifying our proportional approach to sanctions

4.3.1 Similar but different tools

Incorporating market position in the CNIL's sanction mechanism must be approached with caution. Indeed, the power to apply penalties entrusted to the Autorité de la concurrence is designed to "*prevent and repress anticompetitive practices, which can have a considerable impact on the economy*"[87]. It also covers all merger-related litigation, including breaches in the procedural phases. On the other hand, the CNIL can initiate sanctions proceedings in cases of GDPR or Data Protection Act violations. Its focus is on the impact of the violations on the public order of data protection and the safeguarding of fundamental rights. These mechanisms therefore pursue different objectives.

Nevertheless, both authorities have the ability to adjust the amount of their fines on a case-by-case basis, and have a variety of measures at their disposal (public disclosure of sanctions, formal notices, injunctions, etc.). On the other hand, when it comes to calculating the amount of penalties, the criteria differ but sometimes overlap such as when it comes to taking a company's financial capacity into account. However, the calculation of the penalty cannot be based on the same rules, since in competition law, the starting point is the value of the damage caused "to the market"[88]. However, many CNIL sanctions do lend themselves to market harm assesment as their purpose is not to strengthen a company's market power. Instead, the economic reasoning will focus on the benefits derived from the violation or the harm suffered by individuals.

On the other hand, the respondent's market position, when it translates into data power, can aggravate any or all of the components of harm resulting from a GDPR violation: benefits derived from the breach, harm to individuals, harm to society. It might therefore be appropriate to identify objective structural or behavioural factors that can be empirically assesed to provide a better understanding of a company's exisiting prejudice to a large number of users, or its potential capacity to cause it.

Thus, as in competition, the calculation of fines in data protection enforcementcan be based on a set of objective economic factors.

---

[87] https://www.autoritedelaconcurrence.fr/en/litigation-activity.

[88] https://www.autoritedelaconcurrence.fr/en/communiques-de-presse/autorite-de-la-concurrence-revises-its-procedural-notice-fines.

4.3.2 Identifying and incorportating aggravating competitive factors

Even if concepts such as dominant position or market power are rooted in the assessment context of a competition authority, they can be adapted as part of the analysis of factors to be taken into account when calculating a data protection fine. Moreover, Article 83.2 k) of the GDPR specifies that "*any other aggravating or mitigating factor applicable to the circumstances of the case*"[89] must be considered when determining a fine amount. Thus, when a company has the ability to collect and exploit vast sets of data, for example, i.e. data power [90], this could constitute an aggravating circumstance. Indeed, in the context of a breach of the GDPR rules, this ability could enable the company to cause greater damage thus increasing the severity of the violation. In particular, this data power could come from a dominant position on the market and therefore privileged access to a vast set of personal data, from network effects discouraging consumers from switching providers, or from portfolio effects enabling easy combination of datasets.

Other elements that could characterise aggravating circumstances could be used by the CNIL, such as decisions by the Autorité de la concurrence to fine a company for anti-competitive practices. Although it does not fall within the same framework, behaviour that does not comply with competition law could signal to the CNIL risks in the company's handling of data. If a company is capable of putting in place mechanisms that could have an effect on its competitors, it could also be in a position to implement a strategy aimed at users that would have harmful consequences for their privacy. The company's market power, which enables it to influence the conditions under which business is conducted on a given market, and which in data protection terms translates into data power, could therefore be decisive in assessing the company's ability to act positively or negatively for the protection of privacy and personal data on the same market, and evaluate whether the company's role in privacy protection is positive, negative or neutral.

The existence of agreements between companies, whether or not they comply with competition law, could also give an indication of heightened risks for the protection of personal data. Indeed, in some situations, agreements may lead to the combination of personal data. The DMA confirms this approach, even if its scope is restricted to access controllers. Thus, agreements between companies may be aimed at exchanging or combining personal data, thereby increasing the risks for individuals. In addition, this type of agreement could serve as an indicator of a "*processing operations which are subject to the requirement for a data protection impact assessment (Art. 35.4 of the GDPR)*"[91].

4.3.3 Better proportioning sanctions to company behavior

Considering othe proportionality principle when determining a CNIL fine may, in particular circumstances, reduce the final amount. To do so, the authority must take into account risks related to the company's viability and ability to pay, considering the social and economic context in which it operates[92]. The CNIL could usefully draw on existing competitive analyses to identify whether there is objective evidence of deterioration or improvement in the economic sector in which the company operates. The sectoral investigations carried out by the Autorité de la concurrence, as well as the analyses carried out with its decisions[93]constitute elements that can be rapidly mobilized by the CNIL within the framework defined by the aforementioned Meta Platforms ruling.

In addition, the CNIL could further incorporate the notion of undertaking under competition law in its sanctioning procedures. This would enable sanctions to be more proportionate to a company's financial capabilities. In competition cases, the CJEU defines an undertaking as "*any entity engaged in an economic activity, irrespective of the legal status of that entity and the way in which it is financed*"[94]. In its ruling C-807/21, the Court specified that an entity means "*an economic unit, even if in law that economic unit consists of several persons, natural or legal. This economic unit consists of a unitary organisation of personal, tangible*

---

[89] Article 83.2 point k of the GDPR.
[90] Klaudia Majcher, "Coherence between data protection and competition law in digital markets", Oxford data protection and privacy law series, Oxford UP, 2023.
[91] CNIL, Délibération n° 2018-327 du 11 octobre 2018 portant adoption de la liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise.
[92] EDPB, 24 May 2023, Guidelines 04/2022 on the calculation of administrative fines under the GDPR, pp. 45-46.
[93] By way of example, the CNIL had taken into account, in its penalty decision of December 7, 2020 concerning Google (paragraphs 124 to 127), point 313 of the Autorité de la concurrence's decision no. 19-D-26 of December 19, 2019 concerning Google Search.
[94] CJEU, case C-807/21, 5 december 2023, Deutsche Wohnen SE against Staatsanwaltschaft Berlin, pt 56.

and intangible elements which pursues a specific economic aim on a long-term basis"[95]. The Court therefore considers that « *where the recipient of the administrative fine is, or is part of of an undertaking, within the meaning of Articles 101 and 102 TFEU, the maximum fine amount is calculated based on a percentage of the total worldwide annual turnover of the undertaking concerned for the preceding financial year*» [96]. This ruling enables the liability a European subsidiary acting as a data controller while placing the economic assessment of the fine amount on the parent company (inclusion of profits in balance sheets, applicable sales ceiling, capital support in the event of difficulties, etc).

Moreover, the method used by the Autorité de la concurrence to determine financial penalties, updated in 2011 and modified in 2021, could serve as an inspiration for the means that the CNIL could mobilize[97], even if not directly transposable. It allows us to benefit from the competition authorities' experience in determining financial penalties, by providing useful information on the factors used to assess the severity of the violation, such as the nature of the infringement, the activities of persons likely to be affected, or the intentional nature of the violation.

Lastly, a competitive analysis could help asess the need to use reputational effects as a deterrent. Article 22 of the French Data Protection Act stipulates that « *the restricted committee may publish the measures it takes. It may also order their publication in the journals, newspapers and media it designates, at the expense of the sanctioned parties* » [98]. Thus, for example, when the competitive analysis shows that the practices and/or decisions of the concerned company may have an effect on competitors' choices, publishing the sanction could reinforce its dissuasive effect.

Proposal No. 9: Better proportion sanctions to the company's behaviour by making it, where applicable, an aggravating factor *of the sanction under Article 83.2 k) GDPR: increase the penalty based on benefits derived from the breach, the severity of harm to individuals, and the possible negative ecosystemic effects.*

5 Consequences for cooperation with the Autorité de la concurrence

As illustrated by the example of the *Bundeskartellamt* (German competition authority), closer cooperation between the two authorities could provide the opportunity for the Autorité de la concurrence to enrich its methods of competitive analysis, in light of the latest doctrinal advances, particularly when personal data is involved. The CNIL's assistance could make it easier to identify and understand players' practices in this field. This requires strengthening the CNIL's ability to cooperate and make recommendations to the Autorité de la concurrence (5.1). The joint declaration signed by the CNIL and the Autorité de la concurrence in December 2023 already provides a framework for enhanced cooperation, which needs to be clarified in practice (5.2). In particular, a contribution from the CNIL in the analysis of appropriate behavioural and structural commitments or a joint reflection on companies' compliance programs could help the Autorité de la concurrence better integrate personal data protection (5.3).

5.1 Assisting the Autorité de la concurrence in its investigations and decisions affecting data protection

5.1.1 Defining of the relevant market

The relevant market corresponds to the market(s) in question for the application of competition law. It enables the European Commission "*identify and define the boundaries of competition between undertakings. The main*

[95] Ibid.
[96] Ibid., point 57.
[97] Autorité de la concurrence, 30 juillet 2021, Communiqué de l'Autorité de la concurrence relatif à la méthode de détermination des sanctions pécuniaires.
[98] Article 22 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. [free translation, see original text]

purpose of market definition is to identify in a systematic way the effective and immediate competitive constraints faced by the undertakings involved (8) when they offer specific products (9) in a given territory"[99]. It thus leads "*to the identification of the relevant competitors of the undertaking(s) involved when they offer those products, as well as the relevant customers. Only products that exert effective and immediate competitive constraints within the relevant timeframe are part of the same relevant market as those of the undertaking(s) involved, while other less effective, or merely potential, constraints are considered as part of the competitive assessment*"[100] .

Thus, the Commission defines "*the concerned markets when there is a need to assess the relative competitive strength of* undertakings"[101]. The definition of relevant markets is therefore a crucial step in competition cases, whether for assesing anti-competitive practices or merger control.

The methodology, main criteria, and evidence used to define concerned markets were updated in 2024 to reflect developments over the past twenty years, such as "the *digitalization of the economy and new ways of offering goods and services, as well as the increasingly interconnected and globalized nature of commercial exchanges*"[102]. The aim of this update is to ensure that competition policy contributes to both the ecological and digital transitions, as well as the resilience of the single market by maintaining the smooth operation of markets and remedying market failures.

In this context, the updated guidelines on the notice on relevant markets include the consideration of qualitative competition parameters. Specifically, when defining the relevant market, "*the Commission takes into account the various parameters of competition that customers consider relevant in the area and period assessed. Those parameters may include the product's price, but also its level of innovation, and its quality in various aspects*"[103], such as the level of privacy protection offered. Indeed, the rise of business models centered on the collection and use of data highlights the need to consider privacy protection from the outset when defining the relevant market.

So, taking this into account will improve the definition of product and geographic markets, highlighting, for example, the different segmentations of the concerned markets.

In particular, these considerations are particularly relevant "*in cases involving digital, technological, or communication products and services, where consumer data is part of the product itself*"[104]. Indeed, *in Microsoft/LinkedIn, the Commission considered privacy requirements and the data protection regulatory framework when defining the geographic market. The Commission's investigation highlighted differences in regulatory and privacy requirements across EEA countries, which stakeholders viewed as examples of differences when it comes to the provision of social network services across the EEA*"[105]. Indeed, in this case, some stakeholders saw privacy as a determinant element in understanding local customer requirements, since privacy rules vary from country to country.

Where applicable, if the markets in which the companies concerned operate have not been the subject of a published doctrine by the CNIL, current best practices lead the Autorité de la concurrence to contact the CNIL. For instance, during the review of the TF1/M6 merger project, initial informal exchanges between the two authorities made it possible to identify existing personal data processing operations. If necessary, a request for an opinion can also be made, in order to benefit from a complete analysis of the concerned companies' data processing activities.

5.1.2 Merger control

In the European Union, merger control is defined as any lasting change of control of the undertakings involved in a transaction resulting in "*the merger of two or more previously independent undertakings or parts of undertakings, or the acquisition, by one or more persons already controlling at least one undertaking, or by one or more undertakings, of direct or indirect control of the whole or parts of one or more other undertakings*

---

[99] European Commission, 22 February 2024, Communication from the Commission – Commission Notice on the definition of the relevant market for the purposes of Union competition law, C/2024/1645, point 6.
[100] Ibid.
[101] Ibid, point 8.
[102] Ibid, point 3.
[103] Ibid., point 15.
[104] European Commission, Non-Price Competition: EU Merger Control Framework and Case Practice, Competition *Policy brief*, p. 7.
[105] Ibid.

whether through equity participation, or asset purchase, contractual agreements, or other means,"[106]. The aim of the control is to establish whether these operations arecompatibile with maintaining sufficient competition in the affected markets.

In particular, "*a concentration which would significantly impede effective competition, in the common market or a substantial part of it, particularly through the creation or strengthening of a dominant position, shall be declared incompatible with the common market*"[107].

In addition, the European Commission considers personal data protection and privacy to be a competitive parameter that can be "*particularly relevant parameters of competition in mergers in the digital and technology industries, where companies use the data collected from customers/users for commercial profit. As such, the data that a company controls have in some industries become a key driver of competition and a source of competitive advantage*" [108]. The development of business models based on the exploitation and collection of personal data reinforces the need to consider privacy as an increasingly important competitive parameter.

Furthermore, "*privacy can be an important element of the quality of a product or service offered and thus a parameter of competition between the merging parties and their rivals and an element of differentiation*"[109]. Thus, even if the personal data protection- and privacy - falls within the scope of its eponymous regulation, merger control can find valuable assesment elements in them.

The number of data-driven merger projects increased, leading the Commission to assess the extent to which "*the parties compete with respect to privacy and whether the transaction could have a negative impact on privacy-related* competition"[110]. The Apple/Shazam case illustrates the role that privacy can play as an important element in competition between music streaming service providers. The Microsoft/LinkedIn case also shows that privacy is an « *important parameter of competition and a driver of customer choice in the market for professional social networking services*"[111]. In particular, privacy was used to assess the impact of potential foreclosure practices following the transaction.

In addition, greater consideration of the damage to privacy created by both structural and behavioral factors (notably, but not exclusively, when the business models to be merged are heterogeneous in their added value to privacy, when the merger increases the scale of data processing or the possibilities for combining data, or when the merger appears motivated by the desire to acquire control over datasets) enable better apprehension of potential economic damage. Similarly, a relative assessment of the GDPR compliance levels of the entities involved would enable recommendations to be made to avoid the risks of lowering the overall level of compliance of the new entity.

Furthermore, privacy could also be studied as a likely efficiency gain resulting from focus. For example, GDPR compliance or improved privacy awareness for users can improve product quality. These effects could also, in some cases, be taken into account in the analysis of elements counterbalancing the negative effects of the merger.

Additionally, merger control can help protect pioneering companies in the field of privacy protection. These smaller companies with less ressources are able to compete based on the quality of their offerings, particularly in terms of privacy protection[112]. The acquisition of a company in this category could enable a major corporation to prioritize its own products, while limitting or even eliminating the dissemination of the pioneering company's innovations. In this situation, merger control has the capacity to protect both competition and consumer privacy. Any vigilance strategy regarding predatory acquisitions should therefore include a component for measuring the risk to privacy and personal data.

Thus, in many cases, privacy is a decisive factor in the assessment of merger projects. The methodology for taking this into account is still under construction, and will also depend on potential litigation. But it already seems essential to build a coherent methodology for assessing privacy as a competitive parameter. The CNIL's assistance in this area could enable the Autorité de la concurrence to better identify non-compliant or

---

[106] Article 3.a and 3.b of Council Regulation (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings (the "EC Merger Regulation"), *Official Journal*, L 024, p. 0001 - 0022.
[107] Article 2.3 of the EC Merger Regulation.
[108] European Commission, Non-Price Competition: EU Merger Control Framework and Case Practice, Competition *Policy brief*, p. 5.
[109] Ibid.
[110] Ibid, p. 11.
[111] Ibid.
[112] OCDE, 16 june 2023, Theories of harm for digital mergers – Background Note, DAF/COMP(2023)6, p. 1-51.

problematic behavior from the point of view of personal data protection, making them easier to consider in assessments.

Finally, some proposed mergers may require a deeper analysis of the importance of personal data for the merging parties. This could involve, for example, the combination of personal data, access to sensitive data, etc. An opinion from the CNIL would contribute to a better understanding of the effects of the potential merger on the market. The CNIL's opinion could therefore be sought out during the analysis phase of merger projects. Such exchanges could be encouraged in the context of the Competition Authority's investigation of certain in-depth examination procedures ("phase 2"), which are likely to present more complex issues in terms of competitive dynamics analysis. The legally stipulated processing times for these procedures (an additional 65 working days over and above the 25 working days for the "phase 1" rapid examination phase) offer greater scope for constructive discussions between the CNIL and the Autorité de la concurrence if necessary, including informal exchanges specifically on remedies if the case lends itself to this.

Proposal no. 10: Encourage formal or informal referral to the CNIL when privacy and personal data are at stake in a merger case, particularly in cases of in-depth examination procedures (phase 2).

5.1.3 Anti-competitive practices (antitrust)

The Treaty on the Functioning of the European Union also prohibits anti-competitive (antitrust) practices, whether in the form of agreements and commercial practices (Article 101) [113] or abuse of a dominant position[114].

Article 101 prohibits agreements or collusions through which companies restrict or distort competition. "*Agreements may be horizontal (between competitors at the same level of the supply chain fixing prices or limiting production) or vertical (such as between a manufacturer and a distributor). However, Article 101(3) allows restrictive agreements if they generate more positive than negative effects (e.g., if they improve production or product distribution)*"[115].

In addition, Article 102 "*prohibits a firm from abusing its dominant position (i.e. a substantial market share) by charging excessively low prices to prevent others competitors from entering the market or discriminating among business* partners"[116].

Under these two articles, the Commission and national competition authorities can impose fines on companies engaging in such practices.

The integration of privacy protection into the analysis of anti-competitive practices is particularly relevant in cases of abuse of a dominant position. Particularly in the digital sector, the possibilities offered by the exploitation of massive databases may, in some cases, encourage the combination of different databases containing personal data. The competitive advantages conferred by the possession of such databases also influence companies' behaviour regarding data collection and exploitation.

Consequently, such practices could constitute an abuse if their objective, even if secondary, is to limit effective competition in the market. In particular, personal data can make a database sufficiently unique to potentially constitute a barrier to entry or reduce market contestability. Compliance with the GDPR may then be decisive in identifying whether the company has, in addition to having committed a potential abuse of a dominant position, benefited from an undue advantage conferred by GDPR non-compliant data collection and/or exploitation, and whether these two violations overlap. Thus, in such cases, informal discussions specifically on remedies would also be useful if the case warrants it.

Furthermore, although it may, under certain conditions, comply with the GDPR, the pooling of personal data could enable companies to exchange critical information about their respective customers, even though CNIL's work encourages players to also comply with competition law. This type of practice could alert the Autorité de la concurrence, particularly if it observes forms of alignment in practices, such as commercial or pricing practices, or avoidance strategies[117].

[113] Article 101 of the TFEU.
[114] Article 102 of the TFEU.
[115] Office des publications de l'Union européenne, 24 mars 2017, Synthèses de la législation de l'UE – Antitrust.
[116] Ibid.
[117] Eymas F. et Bensebaa F. (2021), Petits distributeurs indépendants : de l'évitement à l'indifférence concurrentielle ?, Finance Contrôle Stratégie, 24(3), https://doi.org/10.4000/fcs.8258.

Moreover, agreements between companies on data collection or sharing conditions that aim to organize GDPR non-compliance or leading to a decline in privacy protection on a given market, if not prosecuted by the Autorité de la concurrence under antitrust laws, could constitute an aggravating factor in a CNIL sanctioning procedure.

***Proposal no. 11**: encourage **a formal or informal referral to the CNIL when the pooling or combination of databases is at stake in an antitrust case**, in order to examine whether any GDPR non-compliance in such cases, even if motivated by efficiency, would not constitute an abuse of dominant position.*

5.2 Putting the joint declaration into practice

5.2.1 Frequency of informal exchanges

For many CNIL projects, such as internal notes, communications, recommendations, etc., a competitive perspective helps better understand the sector and ecosystem in which the concerned players operate. Nevertheless, formal request for an opinion should not be a systematic solution for all of CNIL's work. This is the case when the work involves internal notes or communications to the CNIL's college. Indeed, the referral process is more rigid than informal exchanges. In particular, the latter allows for the rapid acquisition of extensive information.

For example, during the initial phases of analysis, informal exchanges with the Autorité de la concurrence's departments could help improve sectoral knowledge. The CNIL and the Autorité de la concurrence could consider creating a framework to identify situations where exchanges should probably be considered. When these exchanges highlight significant issues and problems requiring cross opinions, they should facilitate requesting for a referral.

Increasing these informal exchanges could increase the number of requests from different departments. Therefore, it seems important to facilitate collaboration between the CNIL and the Autorité de la concurrence, to ensure full use of these exchanges. To this end, the two institutions could create a single-entry point to facilitate contact with the relevant departments and the distribution of cases. This point of contact would have a steering and programming function for exchanges between concerned departments, identifying at an early stage which exchanges would be necessary and on which themes. This point of entry would also have the capacity to respond to general inquiries - ongoing studies, work schedule, etc. - quickly and better understand informations needed by the requesting departments (see proposal no. 6).

5.2.2 Frequency of referrals for opinion

The Competition Authority has referred several cases to the CNIL for an opinion. The first referral from the CNIL to the Competition Authority was in 2023, concerning the recommendation on mobile applications. Therefore, an increase in the frequency of opinions could be considered, though it should not become systematic given the workload involved in producing an opinion. However, such an increase would require joint consideration of how to optimize response times to referrals, in order to best align with the regulatory rhythms of the two authorities.

In particular, increasing the frequency of these notices will help to develop a shared culture of referral, which will facilitate their use. Similar to the integration of the Autorité de la concurrence's comments in the recommendation on mobile applications, the Autorité de la concurrence could facilitate the development of this shared culture by writing with the CNIL, a public document explaining how the CNIL's opinion has been taken into account in its own opinions.

Increasing the frequency of referrals also requires better identification of suitable topics. Their detection could be facilitated by the construction of a framework enabling to detect when a referral would be potentially useful. This document could be co-developed by the Autorité de la concurrence and the CNIL. It could also incorporate the framework on informal exchanges proposed earlier (see point 5.2.1).

5.2.3 Building a shared reflection

Developing cross-analyses taking into account both competition and personal data protection also requires to bring together the work and reflections of the CNIL and the Autorité de la concurrence. While workshops have already been held on an ad hoc basis, the two authorities could set up regular workshops on topical issues. These would bring together staff from the CNIL and the Autorité de la concurrence to discuss predefined topics. These workshops would alternate between being hosted by the CNIL and the Autorité de la concurrence, with two moderators from each authority. They would help to increase knowledge and mutual understanding of the other

authority's analyses of a subject of common interest. Eah session would produce an operational summary of conclusions that would enrich the doctrine of both authorities on the selected issues.

In addition to these regular workshops, a "competition and personal data" seminar could be organized in the medium term. It would provide an opportunity to communicate and exchange information on the development of decisions, documents and work on this issue. It would provide an opportunity to bring together staff from the authorities, as well as leading figures from the worlds of academia, business and civil society. Like the internal workshops, this event would be co-organized by the CNIL and the Autorité de la concurrence. A partnership with a university could be envisaged, as well as a rotating location of the event venue.

Proposal no. 12: capitalize on cooperation in the area of doctrine *by drafting operational summaries of conclusions from internal workshops, systematically publishing reports on how cross opinions have been integrated, and regularly organizing academic events on subjects related to "competition and data protection".*

In addition, when subjects of common interest are identified by the two authorities, the CNIL and the Autorité de la concurrence could carry out joint thematic studies. These thematic studies could be supplemented by voluntary joint hearings that do not require the mobilization of the Autorité's investigative powers (see proposal 5 above). Specifically, when GDPR-related elements are identified, the contribution of CNIL's services should help facilitate the work of the Autorité de la concurrence, including in determining whether the CNIL should be referred to for an opinion.

5.3 Reflection on alternatives to sanctions

5.3.1 Behavioral commitments

Article L. 464-2 of the French Commercial Code and Article 9 of Regulation 1/2003 stipulate that by companies can commit to ending existing anti-competitive practices. In such cases, competition authorities can then make these commitments binding for the company. This procedure enables companies to propose solutions adapted to their business model while enabling the authorities to reduce negotiation costs and duration of proceedings[118].

Several types of commitments can be made. However, they depend on the nature of the infringement and, considering the principle of proportionality, their ability to resolve the initial competition problem. Indeed, the principle of proportionality in competition law requires "*identification of the remedy best adapted to the competition issue encountered. This quest for proportionality also informs the determination of the duration of commitments*"[119].

Among these, behavioral commitments are the most widely used in response to potentially anti-competitive practices. They involve regulating a company's behaviour through the use of commercial or strategic constraints[120]. These commitments may, for example, involve modifying or deleting contractual clauses (Aut. Conc., dec. Nos. 06-D-24, 11-D-08), guaranteeing access to essential infrastructure or to a closed group (Aut. Conc., dec.no. 12-D-06), communicating information to competitors (Aut. Conc., dec.no. 14-D-09), prohibiting two companies from the same group from bidding simultaneously for public contracts (Aut. Conc., dec.no. 08-D-29) or imposing the implementation of compliance programs (Aut. Conc., dec.nos. 14-D-19, 15-D-19)[121].

Thus, the Autorité de la concurrence has considerable flexibility in the precise determination of behavioural commitments. This flexibility could enable it, when privacy is identified as an important parameter of the analyzed practices, to impose measures that take privacy into account.

When identifying potentially anti-competitive practices involving data processing that may not comply with the GDPR, the Autorité de la concurrence could make it mandatory for a company, as a commitment, to approach the CNIL to achieve compliance. Thus, whenever such practices involve personal data, the Autorité de la concurrence could make it compulsory, after discussion with the CNIL to assess the appropriateness, that companies establish contact with it.

More generally, it might be beneficial for the Autorité de la concurrence **to informally consult the CNIL, where appropriate, for the drafting of commitments in terms of privacy, personal data**

[118] Marie Cartapanis, Engagements (pratiques anticoncurrentielles), Dictionnaire de droit de la concurrence, Concurrences, Art. N° 12301.
[119] Autorité de la concurrence, Behavioural remedies, Les essentiels, La documentation Française, Direction de l'information légale et administrative, Paris, 2019, p. 275.
[120] Ibid.
[121] Ibid, p. 335.

protection, and GDPR compliance, with the CNIL, for its part, able to provide a response very quickly to the Autorité's college.

Proposal No. 13: *When competition concerns related to potentially GDPR non-compliant data processing operations have been identified,* ***consider the possibility for the Autorité de la concurrence to*** require companies to commit to *contacting the CNIL to remedy these instances of non-compliances.*

5.3.2 Structural commitments

Except for behavioral commitments, companies can also propose structural commitments. These measures correspond to "*directly modifying, by themselves, the structure of the markets (the number, quality, or scope of operators active on a market)*"[122]. These commitments may take the form of definitive transfers, renunciation of contractual or property rights. For example, the measures may be designed to impose a transfer of assets on a company in order to restore or maintain competition on a market. Notably, structural commitments are intended to be more limited and short-lived than behavioral commitments, which may be more far-reaching and require monitoring by the Autorité de la concurrence.

However, although it is possible to impose structural commitments as part of proceedings concerning potential anti-competitive practices, in practice they are not used by the Autorité de la concurrence in this context. Indeed, anti-competitive practices relate to the most market-damaging behaviour of companies and behavioural commitments are better suited to target these practices.

On the other hand, so-called "quasi-structural" remedies can be imposed. These are commitments with rapid effects that require simple, inexpensive monitoring. Due to their flexibility, they can also involve substantial changes to the organization and operating rules of companies. Examples include licensing agreements (Aut. conc., dec. no. 05-D-25), the introduction or development of cost accounting (decision no. 17-D-09), or the separation of activities inside and outside the market by a monopolist (Aut. conc., dec. no. 12-D-04)[123].

The CNIL could contribute to implementing commitments related to personal data. Particularly, when licensing agreements include access to personal data, the Authority could require the company to contact the CNIL to ensure that the proposals are compatible with the GDPR (see proposal no. 13).

5.3.3 Promoting "joint compliance"

The aforementioned joint declaration highlights the importance of "*economic stakeholders considering privacy and personal data, as well as compliance with the competitive framework, by design of a product or* service"[124]. This approach should help to improve and guide consumers' choices towards the most virtuous companies in terms of privacy. Encouraging companies to think about the features of their products or services from the point of view of both competition law and GDPR compliance is, therefore, a crucial stake. As a consequence,it is also particularly relevant to take DPIAs into account, for example in merger cases.

Moreover, the Autorité de la concurrence encourages companies to set up a competition compliance program. The Autorité's framework document indicates that this program can be designed as a stand-alone initiative, or as part of a general compliance policy, covering other aspects of compliance, such as personal data protection[125].

A more demanding stance on these compliance programs would clarify expectations for companies. Indeed, every company should give priority to the implementation of a comprehensive compliance policy that effectively articulate all existing regulations. To this end, the CNIL and the Autorité de la concurrence could work on a joint framework document on compliance programs, particularly regarding impact studies. Companies would benefit from greater legal certainty and improved transparency. Both institutions would also benefit from fostering joint compliance, whether a company's case is first approached from a GDPR or competition law perspective.

6 Consequences for cooperation at the European level

While better interplay between data protection and competition at national level is necessary, it must be aligned with the existing European environment. Indeed, it is at the European level that the interplay of the two

[122] Ibid., p. 262.
[123] Ibid., p. 335.
[124] Autorité de la concurrence and Commission nationale de l'informatique et des libertés, 2023, Competition and personal data : a common ambition, p. 10.
[125] Autorité de la concurrence, Framework document of 23 May 2022 on competition compliance programmes, p. 1.

frameworks and the dialogue of concepts and tools would have the greatest impact, particularly with regard to the major digital players.

It is essential for both the CNIL and the Autorité de la concurrence, to understand and ntegrate European normative developments to maintain the effectiveness of national cooperation (6.1). The CNIL and the Autorité de la concurrence also share a common interest in disseminating and promoting the main principles of their cooperation project national advances at the European level (6.2). Beyond decisions and analyses, considering competition issues could even lead to initiating reflection on the current European governance of data protection (6.3).

6.1 Integrating European normative developments

6.1.1 Taking other European texts into account

Cooperation between authorities such as the CNIL and the Autorité de la concurrence has also been strengthened at the European level, thanks to the creation of new exchange forums. For example, a High-Level Group has been set up to reflect on the interaction between the Digital Market Act ("DMA") and other existing regulations. It brings together various networks of regulators, including the European Data Protection Board ("EDPB") and the European Competition Network ("ECN"). Indeed, the DMA includes several references to personal data and the GDPR. This text, which has significant effects on competition, requires close cooperation between competition and data protection authorities.

The Data Act also reinforces the need for cooperation at both the national and the European levels, since it concerns both competition and personal data protection. Moreover, the EDPB has stated that they "*also acknowledge the importance of providing a more effective right to data portability and welcomes this objective, aiming to facilitate innovation and promoting competition*"[126]. However, various risks exist, such as collection, sharing, and use without the individual's knowledge, generated by companies' rights to access, use, and share company data with other entities, including other businesses, etc[127]. A European cooperation framework is therefore essential to ensure a proper interplay between competition and personal data protection challenges. Similarly, interoperability issues require closer cooperation with competition authorities to understand the full range of competitive issues across the different sectors studied.

6.1.2 Continuous monitoring and impact on similar European initiatives

Participation in European seminars can maintain continuous monitoring of European cooperation initiatives. Regular informal exchanges between the CNIL and the Autorité de la concurrence could be organized to pool information on these initiatives. In this respect, exchanges between contact points should be planned to ensure the efficient information sharing.

Although the work carried out by the Global Privacy Assembly ("GPA") does exist, the OECD could play a leading role in organizing discussions on inter-regulation. It could take a greater interest in European specificities and contribute to opening up the debate at the international level by increasing the number of workshops and working groups dedicated to the interplay between personal data protection and competition. The CNIL and the Autorité de la concurence could also stay informed of recent OECD developments on this subject. These various exchange formats would be an opportunity to deepen reflection and help maintaining a dynamic environment for discussion on this issue.

6.2 Projecting progress at EU level

6.2.1 Promoting the joint declaration at the European level

Among European Union countries, the joint declaration between the CNIL and the Autorité de la concurrence offers one of the most advanced frameworks for cooperation between data protection and competition. In order to maintain a high level of legal certainty for all players, but also to avoid any risk of forum-shopping, which would consist of a company strategically choosing the data protection authority most favorable to its interests, the definition of a harmonized approach at European level in this respect is highly relevant. It would also enable each national data protection authorities to take up this subject in the same way as their more advanced

[126] EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), point 11, p. 7.
[127] Ibid., point 13 et 14, p. 8.

counterparts: while the EDPB already enables coordination mechanisms to be set up between data protection authorities, establishing a coordination mechanism at European level with the competition authorities could further facilitate cooperation at national level.

The CNIL could thus position the joint declaration as an example of cooperation that could inspire the practices of European data protection authorities. To this end, the CNIL should emphasize the use of the joint declaration as a reference in European work. This promotion of cooperation could have its counterpart in the Autorité de la concurrence. The integration of the joint declaration as a reference should therefore be encouraged by the Autorité de la concurrence. In particular, when the CNIL and the Autorité de la concurrence work on similar or even joint subjects at the European level, their positions could be coordinated beforehand through informal exchanges at national level.

The introduction of greater cooperation between data protection and competition authorities requires a broader consideration to integrate competition in European work. To this end, a coherent and regular discourse on the benefits of cooperation must be ensured at the various levels of EDPB discussion. Particularly, participation in drafting teams enables us to have a direct impact on the drafting of positions that best articulate competition and data protection. CNIL's presence in sub-groups and working groups can also help promote its work on the same subject. In addition, our voice in the plenary session could help emphasize the need to strengthen cooperation on this subject at EU level.

6.2.2 Publicly promoting EDPB work on interplay

In addition, numerous seminars with a European dimension take place. These exchanges provide an opportunity to publicize the joint declaration and identify similar or equivalent initiatives. The CNIL and the Autorité de la concurrence may jointly take part in seminars and workshops on the relationship between competition and personal data. For example, the OECD recently organized an event on the subject, demonstrating the ability of the two authorities to cooperate[128]. The CNIL should therefore continue its work to identify useful forums for the promotion of the joint declaration by involving the Autorité de la concurrence in the process.

Moreover, at European Commission level, a conference bringing together institutional, academic, private and civil society players could be organized to discuss the interplay between competition and personal data. It would highlight the various cooperation frameworks existing in Europe, with the joint declaration between the CNIL and the Autorité de la concurrence as an example of advanced cooperation. This conference would also be an opportunity to highlight new academic and private sector developments on these issues, with a view to identifying subjects requiring further cooperation between authorities.

6.2.3 The key role of the C&C Task Force

Promoting this work at European level falls within the scope of the Consumer and Competition (C&C) task force, created within the EDPB in March 2023 and responsible for work on the interplay between personal data protection, competition and consumer protection. The CNIL could continue to contribute to this work to promote a stronger framework for cooperation. In particular, this task force already works in coherencecooperation with the European Competition Network and the European Commission. As a result, it is able to identify and mobilize the relevant players to develop ideas on the interplay between competition and personal data.

As the mandate of the C&C Task Force is set for two years and ends at the beginning of 2025, it could be proposed to extend this framework by making it a focal point, within the EDPB, for the interplay between these different legal frameworks, including on concrete cases. After an initial stage of doctrine definition, reflected by the publication of a position paper inspired by the joint declaration, the task force could usefully play a role in the concrete integration of competition concerns into EDPB practice. As such, it should be systematically consulted by the various sub-groups when a case raises issues of interplay between these different legal frameworks. In addition, the task force could develop a "*peer review*" role to encourage the various national authorities to develop their profile in terms of cooperation with their counterparts.

In this way, the EDPB could draw on the work of the task force to promote harmonization of practices at European level and encourage cooperation. In addition, the CNIL's presence in this working group as coordinator helps to maintain a dynamic that favors cooperation between authorities. The development of guidance drafted jointly with the European Competition Network should also be encouraged.

---

[128] OCDE, 13 june 2024, The intersection between competition and data privacy – Background Note, DAF/COMP(2024)4.

Eventually, as the work on "consent or pay" has shown, the task force should be able to play a pivotal role in organizing a dialogue between the EDPB and the European Competition Network on a regular basis.

Proposal no. 14: extend the C&C Task Force and develop its work program *to make it play a pivotal role in the interplay between competition, consumer protection and personal data at European level, moving forward the EDPB contribution in this regard.*

6.3 Regarding the European data governance

6.3.1 Different cooperation networks

Articles 56, 60, 61 and 62 GDPR organize law enforcement cooperation between data protection authorities by creating a system of one-stop-shop, mutual assistance and joint operations. The authorities therefore have the possibility of setting up coordinated actions in order to investigate a case. In addition, they shall take appropriate measures to respond to requests when the mutual assistance mechanism is triggered. The assistance mechanism may concern "*information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations*"[129]. Furthermore, in accordance with the "one-stop-shop" system, in the case of a complaint concerning cross-border processing involving several establishments within the European Union, the data protection authority of the Member State where the main establishment is located is competent. It is then referred to as the lead authority.

Similarly, the creation of the European Competition Network by Regulation (EC) No. 1/2003 has established a formal cooperation mechanism between competition authorities. The main objective is the effective and uniform application of Articles 101 and 102 of the Treaty on the Functioning of the European Union. One of the key differences between this network and its data protection counterpart is the cooperation mechanism for case allocation and assistance. Indeed, the competition authority receiving the complaint or initiating proceedings generally remains in charge of cases, although reassignment may be envisaged at the start of proceedings "*where either that authority considered that it was not well placed to act or where other authorities also considered themselves well placed to act*"[130]. In such cases, "*for an effective protection of competition and of the Community interest*"[131], network members may reassign the case to a better-placed authority, provided that ongoing investigations are not interrupted.

This adaptation of the country of origin principle in competition matters not only reduces the risk of forum shopping, by giving priority to markets where the competitive risks are highest, but also encourages healthy emulation between national authorities, by providing a stimulus in terms of expertise and team mobilization. This could set an interesting precedent in the case of data protection, which is entirely based on the principle of the country of the main establishment of the data controller, which is sometimes a challenge[132], and the role of national authorities in that regard

6.3.2 The merits of alternative case allocation rules

A comparative analysis could therefore be carried out to examine whether GDPR attribution rules and the EDPB's role could not evolve over time by introducing a principle inspired by the ECN's principle of authorities well placed to deal with the case. Such an adaptation of the country of origin principle would be quite natural in data protection, a field aiming at protecting the fundamental rights of data subjects in the countries where the goods and services concerned are marketed to individuals.

As a starting point for reflection, in competition matters, the European Commission defines three main criteria for identifying whether an authority is well placed: (1) the substantial nature of the effects of the company's practices or agreements on its territory, (2) the ability of the authority to effectively bring the infringement to an end, and (3) the ability to gather evidence in support of the action, including with the assistance of other authorities[133]. If this approach were adopted, it would ultimately require an amendment to Article 56 GDPR by

[129] Article 61.1 GDPR.
[130] Commission notice on cooperation within the Network of Competition Authorities, 2004/C 101/03, Official Journal n° C 101 du 27/04/2004, p. 0043 – 005, point 6.
[131] Ibid., point 7.
[132] See the interview with I. Falque-Pierrotin in EDPS, 2024, for example.
[133] Commission notice on cooperation within the Network of Competition Authorities, 2004/C 101/03, Official Journal n° C 101 du 27/04/2004, p. 0043 – 005, point 8.

opening up the possibility of attribution to authorities that are not the lead supervisory authority nor even an authority concerned within the meaning of Article 60 of the GDPR.

This "*well-placed authority*" could, for example, be one with greater expertise and experience in economic and competition matters. In its coordinating role, the EDPB Secretariat could facilitate this allocation process under conditions of strong neutrality, in the same way as the European Commission does within the framework of the European Competition Network.

Data protection authorities could also draw inspiration from the natipnal competition authorities' use of the European Competition Network. This could result in increased use of Articles 61 and 62 of the GDPR for cross-border processing. Although these provisions are already used, national situations could benefit from assistance from other data protection authorities. In particular, Article 62 may make it possible to strengthen investigation capacities through the European level, along the lines of what competition authorities are able to do, via joint investigations, for example.

6.3.3 Towards prospective thinking

While there is a cooperation mechanism between data protection authorities, as well as a one-stop-shop for harmonizing national oversight decisions at European level, it is not equivalent to the system of parallel competences of the European competition network. Indeed, in competition matters, in certain situations, the European Commission may be well placed to deal with a case, thus ensuring better consideration of cases with EU-wide effects. This is not the case with data protection, as the EDPB has no supervisory powers over private data controllers established in different Member states. This is why the answer to the question is not univocal: a forward-looking reflection could be initiated in this regard - following the example of what had been done done prior to the establishment of the European Competition Network - on the means of an efficient division of labor and an effective and homogeneous application of the GDPR, which would focus on (i) examining the merits of the arrangements adopted in the area of competition (ii) verifying the legitimacy of of applying the country of origin principle in the area of fundamental rights and (iii) guaranteeing the non-fragmentation of the internal market via appropriate cooperation processes.

Another difference between the two frameworks stems from the requirement, laid down by the GDPR, for data protection authorities to be independent from the government. As a result, the federal architecture based on the exclusive competence of the European Commission cannot be retained. The rules governing the division of labor should therefore not entrust tasks to the Commission, but rather be decided by common agreement within the EDPB. At a time when certain authorities may be reluctant to embark on this path, such considerations could provide some safeguards for a managed evolution of European data protection governance.

Proposal no. 15: carry out a comparative and forward-looking analysis of the different ways to allocate competences between regulatory authorities across the European Union*, focusing in particular on the systems in place for protecting competition, protecting personal data, and regulating the financial, media and energy markets.*

***

7 Appendix : List of proposals

Proposal no. 1: take competition issues into account upstream in CNIL's work. Developing a better vision of the effects of CNIL decisions on competition helps to promote overall consistency in the application of competition and data protection. Increasing this consistency helps to foster virtuous behaviour in terms of both respect for competition and protection of privacy and personal data. It also reinforces the predictability of regulatory action and, consequently, the legal certainty for companies.

Proposal no. 2: experiment with the concept of "data power" as a doctrinal insight, when more appropriate than existing competitive concepts (dominance or market power) in CNIL's data protection analyses, when assessing the relationship between a data subject and a data controller.

Proposal no. 3: develop within CNIL's practice the consideration of competitive unlawfulness under Article 5.1 a) GDPR. Unfair competition behaviour or anti-competitive practices, if judged or documented by competition authorities, may constitute complementary factors to breaches of data protection rules. Otherwise, the matter should be referred to the French competition authority for an opinion.

Proposal no. 4: with a view to increasing compliance with the minimization principle, develop an analysis of the role played by anti-competitive practices in the accumulation of data and indicators of data collection that harm individuals who cannot object to it.

Proposal no. 5: Jointly explore risks and markets through exchanges of expertise, voluntary joint hearings, or joint studies between the CNIL and the Autorité de la concurrence**.**

Proposal no. 6: to deepen cooperation between the two authorities across concepts**, doctrine, and cases, establish a contact point within each authority, in charge of steering cooperation**

Proposal no. 7: initiate a specific joint reflection on the right to portability of personal data, and its consequences in terms of personal data protection and competition. This reflection could, where appropriate, involve other players or authorities with expertise in personal data portability or interoperability, such as Arcep, and be coordinated with the various existing or upcomimg forums (e.g. DMA High Level Group, French national coordination network for the regulation of digital services).

Proposal no. 8: Regularly organize cross-training sessions on competition and data protection issues for both authorities.

Proposal no. 9: Better proportion sanctions to the company's behaviour by making it, where applicable, an aggravating factor of the sanction under Article 83.2 k) GDPR: increase the penalty based on benefits derived from the breach, the severity of harm to individuals, and the possible negative ecosystemic effects.

Proposal no. 10: Encourage formal or informal referral to the CNIL when privacy and personal data are at stake in a merger case, particularly in cases of in-depth examination procedures (phase 2).

Proposal no. 11: encourage **a formal or informal referral to the CNIL when the pooling or combination of databases is at stake in an antitrust case**, in order to examine whether any GDPR non-compliance in such cases, even if motivated by efficiency, would not constitute an abuse of dominant position.

Proposal no. 12: capitalize on cooperation in the area of doctrine by drafting operational summaries of conclusions from internal workshops, systematically publishing reports on how cross opinions have been integrated, and regularly organizing academic events on subjects related to "competition and data protection".

Proposal no. 13: When competition concerns related to potentially GDPR non-compliant data processing operations have been identified, **consider the possibility for the Autorité de la concurrence to** require companies to commit to contacting the CNIL to remedy these instances of non-compliances.

Proposal no. 14: extend the C&C Task Force and develop its work program to make it play a pivotal role in the interplay between competition, consumer protection and personal data at European level, moving forward the EDPB contribution in this regard.

Proposal no. 15: carry out a comparative and forward-looking analysis of the different ways to allocate competences between regulatory authorities across the European Union, focusing in particular on the systems in place for protecting competition, protecting personal data, and regulating the financial, media and energy markets.