Deliberation 2023-036 of April 20, 2023 National Commission for Computing and Liberties Nature of the deliberation: OpinionLegal status: In force Date of publication on Légifrance: Wednesday May 17, 2023Deliberation n° 2023-036 of April 20, 2023 providing an opinion on the draft law "aimed at securing and regulating the digital space"Date of opinion: April 20, 2023N° of deliberation: 2023-036N° of request for opinion: 23005115 - 23005116Text concerned: draft law "aiming at securing and regulating the digital space"Themes: European regulations (DSA, DGA and DMA); control of the verification of the age of minors; cybersecurity filter; PeREN Basis for referral: art. 8 of the "Informatique et Libertés" law The essentials: The bill completes the provisions of European regulations on digital services and data governance; it aims to modernize the regulation of platforms and to organize the circulation of data, which the CNIL welcomes. another authority (ARCEP) the regulation of "data intermediaries" should lead to the provision of a consultation mechanism, prior and suspensive, of the CNIL in the matter. Failing this, the bill should supplement 1° of III of Article 9 in order to provide for the systematic transmission of notifications from service providers to the CNIL so that the latter is able to identify the actors wishing to process data at personal character in order, in particular, to alert them to the application of the principles relating to data protection. The CNIL considers essential a fairly broad rewrite of the provisions relating to its powers of control and sanction in this area in order to avoid a prejudicial complexification of the texts surrounding its action. EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/ EC (GDPR); Having regard to Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (RGD or DGA); Having regard to the 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 (RMN or DMA); Regulation (EU) 2022/2065 of the European Parliament and of the Council of October 19, 2022 on a single market for digital services and amending Directive 200/31/EC (RSN or DSA); Having regard to Law No. 78-17 of January 6, 1978 amended relating to data processing, files and freedoms (law "data processing and freedoms"); After having heard the reports of Mr. Bertrand DU MARAIS and Mrs. Christine MAUGUE, commissioners, and the observations of Mr. Benjamin TOUZANNE , Government Commissioner, ADOPTS THE FOLLOWING DELIBERATION:I - The referralThe government has drawn up a bill "aiming to secure and regulate the digital space", intended to ensure the proper application in national law of three European regulations relating to services (or DSA for Digital Services Act), on digital markets (or DMA for Digital Market Act) and on European data

governance (or DGA for Data Governance Act). The CNIL was seized, as a matter of urgency, by the Ministry responsible for the digital transition and telecommunications of eight articles of this bill directly related to the regulation of the digital space and, by the Ministry of Justice, of two articles relating to the control of the processing of personal data carried out by the courts in the context of their jurisdictional activities.II - The opinion of the CNILEIn introductory remarks, the CNIL welcomes the current movement tending, on the one hand, to strengthen the rights of individuals, on the other hand, to promote a controlled circulation of data. This movement is mainly reflected in the adoption of European or national texts. However, in particular due to the fragmentation of legal and regulatory regimes and therefore the resulting complexity, the proliferation of texts should not harm regulation. coherent and effective digital space. This requirement for consistency should be one of the objectives pursued by the legislator. The proliferation of texts thus results in the recognition of an increased number of regulators of the digital space. This movement is certainly inevitable: given the penetration of technologies in all aspects of life in society, there cannot be a single digital regulator. This multiplicity nevertheless imposes close cooperation between the regulators concerned, at both national and European level. The CNIL, on the strength of its experience within the European Data Protection Board (EDPS) in particular, is for its part ready and determined. CONCERNING ARTICLE 1 (ISSUE OF RECOMMENDATIONS BY THE AUTHORITY FOR THE REGULATION OF AUDIOVISUAL AND DIGITAL COMMUNICATIONS (ARCOM) FOR THE EFFECTIVE RESPECT OF THE LEGAL MAJORITY FOR ACCESS TO PORNOGRAPHIC SITES) AND ARTICLE 2 (POWERS OF SANCTION AND ADMINISTRATIVE BLOCKING OF SITES INCONVENTION OF RESPECT FOR THE LEGAL MAJORITY CONFERENCED ON ARCOM AND SWEARING OF ITS AGENTS TO REVEAL THE LACK OF CONTROL OF MINORS' ACCESS TO PORNOGRAPHIC SITES) These two articles aim to strengthen the powers of the Arcom which could: following an injunction from its president, order Internet Service Providers (ISPs) to block access to sites allowing minors to access pornographic content; impose technical requirements that systems should meet verification of age put in place for access to these sites and sanction sites that do not respect them. Age control on the Internet, if in this case it pursues a legitimate objective of protecting the youth, nevertheless raises important questions about the protection of the privacy of Internet users. Although it is not up to the CNIL, but to the Council of State, to decide on these new procedures, which will be the responsibility of ARCOM, the CNIL stresses that it considers it necessary to better articulate the two instruments, insofar as where the "recommendations" provided for in Article 1, which in this case may give rise to a sanction if the operator does not comply with them, are intended to ensure compliance with the obligation

resulting from Article 227-24 of the penal code, for which ARCOM has, under article 2, the power to issue formal notice to take "any useful measure". privacy, Article 1 provides that the recommendations establishing the technical requirements are drawn up after consulting the CNIL. The CNIL welcomes this choice: age verification devices, which contribute to the protection of minors, can indeed present risks to the privacy of Internet users. It will therefore be a question of finding the right balance between their effectiveness and the protection of the data of the persons concerned. The CNIL has dealt with online age verification systems on several occasions, and will be able to respond quickly to requests for an opinion on Arcom's draft recommendations.CONCERNING ARTICLE 3 (CREATION OF A CRIMINAL SANCTION FOR FAILURE TO EXECUTE A REQUEST FOR THE REMOVAL OF CHILD PORN CONTENT)This draft article does not call for observations from the CNIL.CONCERNING ARTICLE 5 (CREATION OF AN ADDITIONAL PUNISHMENT OF SUSPENSION OF ACCESS TO AN ONLINE PLATFORM SERVICE)This draft article does not call for observations from the part of the CNIL, which only emphasizes that the processing that will be implemented by online platforms for the purpose of blocking the account or aimed at preventing a person from creating new ones must respect the principles and law of the protection of personal data.CONCERNING ARTICLE 6 (DEPLOYMENT OF A NATIONAL CYBERSECURITY FILTER FOR THE CONSUMER)The CNIL can only approve of the Government's desire to strengthen the protection of Internet users against the risks, which are increasingly present on the Internet , phishing attempts (sanctioned by article L163-4 of the monetary and financial code), identity theft (article 226-4-1 of the penal code), unfair or fraudulent collection of personal data (article 226-18 of the penal code) and attacks on automated data processing systems (article 323-1 of the penal code). However, it notes that this draft article leads to a new possibility for an administrative authority to impose the blocking of access to an online public communication service, which raises significant risks for the exercise of individual freedoms and in particular the freedom of expression and communication. It underlines in particular the difficulty of qualifying the offenses covered, a fortiori within the short time necessary to guarantee the effectiveness of the system, which could lead to excessive restrictions on access to information and communication services to the public in line. Such blocking therefore appears to be substantially different from that provided for child pornography sites or those glorifying terrorism and must be the subject of a procedure adapted to the issues and the difficulties of qualification. It is essential that the legitimate cybersecurity objective does not lead, in practice, to an excessive restriction of fundamental freedoms. Regarding the device itself The objective of this filter is to protect individuals, without infringing on their freedom of communication ; to this end, the bill targets, without prioritizing them, three distinct

filtering systems based on a list of suspicious email addresses provided by the administrative authority: filtering by Internet service providers (ISPs) , by providers of domain name resolution systems (DNS) and, finally, by providers of web browsers. These three methods present attacks on freedoms which are different, because they do not offer the same possibilities of control by the user, nor precision in the filtering implemented. The CNIL notes that there is a contradictory procedure allowing the publisher of the site targeted by the filtering measure to contest this registration with the administrative authority. However, for the processing necessary for the implementation of this filter to be proportionate and limited to this purpose, the CNIL considers that the filtering device should in principle remain "in the hand" of each user. Unlike devices intended to block sites provoking acts of terrorism or making apology and child pornography sites established pursuant to decree no. 2015-125 of February 5, 2015, the Internet user should always have the possibility consult, after having been warned of the risks incurred, the site concerned. This notion of control of the filter by users is not provided for by the bill but should be explicitly so, including for filtering requests addressed to ISPs or domain name resolution systems. The CNIL also warns of the risks associated with too coarse filtering and recommends precise determination of addresses, avoiding filtering by over-approximation (prohibiting access to legitimate addresses) or under-approximation (not filtering certain malicious addresses, however known) The possibility of control by the user and the precise determination of the incriminated addresses should allow this general public cybersecurity filter device to constitute a measure of protection of the population without constituting a measure of restriction of the freedom of communication .The CNIL therefore considers that, among the three methods opened up by the bill (ISP, DNS and browser), filtering should primarily be carried out within the browser, insofar as this device constitutes the only possibility allowing easy control. by the user. The user should be able to choose to deactivate the filter, to configure the lists of markers to be applied for filtering and to ignore the filter on a case-by-case basis (including in a browsing session). Regarding the hypothesis of a filter put in place by ISPs or providers of domain name resolution systems (DNS), similar functionalities should, ideally, be made available to users. The CNIL is nevertheless aware of the great technical difficulties in these cases, in particular to display the alert page when the flow is encrypted in HTTPS and to allow the user to easily ignore the filter. Therefore, these last two methods should only be imposed as a last resort and be subject to reinforced control. At a minimum, the filtering methods that do not allow the user to maintain control of access to the site should be subsidiary and reserved for the most serious cases. In any event, the implementation of the blocking as specified by decree no. cybersecurity.Finally, the data processed by the filter, and in particular the queries to the alert page intended to warn the Internet user of the risks, must

not be reused for other purposes, and must be deleted or anonymized as soon as possible. . With regard to control methods Independent control of filtered sites and addresses is necessary to verify that the sites subject to the filter correspond to the categories provided for by law and in particular to avoid "over-filtering" of sites unrelated to computer security. In practice, this control now rests with the judicial authority, which can already order filtering measures similar to those provided for in the draft text. As filtering is entrusted to an administrative authority, the project provides for and appoints a qualified person in charge of monitoring the system. Given the offenses likely to trigger the filtering measure, which include in particular identity theft and the illegal use of personal data, the CNIL considers that this control of the filter device should be placed within it and takes act of the Government's commitment in this direction. With regard to user information As a measure of transparency vis-à-vis users and to facilitate the exercise of their rights, the CNIL recommends that the reasons for the filtering decisions be explained to them, on the blocking page, under an understandable form. It also recommends that specific information about the cybersecurity filter should also be provided on this page. REGULATION OF DATA INTERMEDIATION SERVICES data (DGA). The purpose of this chapter is to create a new legal regime of "trusted third party" intermediaries allowing "data holders" or natural persons concerned to share their data with "data users" while retaining control of the use made of it. The legal regime thus created aims to legally secure the access of third parties to data and their circulation, while guaranteeing the rights of the persons whose data are processed or who have rights over these databases. The data covered by the DGA are both personal data and non-personal data. The CNIL would like to point out the great difficulty of distinguishing these two categories of data in practice, given the broad scope of the GDPR and the case law of the Court of Justice of the European Union (CJEU). The evolution of re-identification technologies can also lead to the boundary between the two categories of data changing over time. of the rule that mixed datasets are subject as a whole to the GDPR, data intermediation services will, to a large extent, process personal data, to varying degrees. The CNIL recalls that the competence to identify whether or not the data sets in question include personal data is conferred on it. The CNIL notes that a large part of the rules set out in article 12 of the DGA regulation (in particular the provisions of a, c, d, e, i, l, m, n and o of this article), extend, specify or repeat rules from the GDPR. It recalls that this regulation applies without prejudice to the GDPR and the powers and competences of the CNIL and that in the event of a conflict between the DGA regulation and Union law on the protection of personal data or the right adopted in accordance with this Union law, the relevant provisions on the protection of personal data prevail (3. of Article 1 of the Data Governance Regulation). Article 13 of the DGA Regulation also specifies "The powers of the competent authorities in matters

of data intermediation are without prejudice to the powers of the authorities responsible for data protection (…)"; its recital 44 specifies: "In particular, for any question requiring an assessment of compliance with Regulation (EU) 2016/679, the competent authority for data intermediation services should seek, where appropriate, an opinion or a decision of the competent supervisory authority set up under the said regulation."The Government has decided not to entrust the role of competent authority in matters of intermediation services to the CNIL but to the Autorité de Régulation des Communications electronics, post and press distribution (Arcep). In order not to lead to operational complexity and legal insecurity detrimental to the actors, this choice requires perfect coordination between the two authorities. "practices of data intermediation service providers likely to raise questions related to data protection" in order to collect its possible observations before any decision. The IV also provides that Arcep collects the observations of the CNIL: for requests from intermediation service providers who are labeled pursuant to paragraph 9 of article 11 of the DGA regulations; in the context of the processing of complaints from natural or legal persons using the intermediation service. In this context, Arcep must provide it with any useful information to enable it to formulate its observations within four weeks. Although the CNIL recognizes this coordination effort by the two authorities, it nevertheless considers, primarily, that the project of law should provide, more generally, for a consultation mechanism, prior and suspensive, of the CNIL before any decision by Arcep concerning data intermediaries, so that the CNIL can examine whether or not the services in question contain , personal data and the consequences that should be drawn therefrom concerning the application of the GDPR. In the alternative, if the principle of compulsory and general consultation of the CNIL were not retained, it would be appropriate to at least to complete 1° of III of article 9 of the bill in order to provide for a systematic transmission of service provider notifications to the CNIL so that the latter can have, in particular, the "description of the data intermediation service that the data intermediation service provider intends to provide, as well as an indication of the categories listed in Article 10 to which this service falls" provided for in Article 11.6-f) of the DGA Regulation. In this way, the CNIL would be able to identify the actors processing "industrial data", which are not, or only marginally, personal data and will be almost exclusively the responsibility of ARCEP, and to distinguish them from the actors processing mainly personal data in their intermediation activity (health data, consumer study data, data useful for marketing activities, service of mandates for exercising rights on personal data, known as PIMS (Personal information management system), etc.), who must ensure that they simultaneously comply with the similar obligations provided for by certain provisions of article 12 of the DGA and certain provisions of the GDPR, under the respective controls of ARCEP and CNIL. It is appropriate, for the purposes of legal

certainty, that a dialogue between the regulators concerned, upon notification to ARCEP, allow the CNIL to inform both ARCEP and the data intermediation service on the part of its activity, which it considers to come under both regimes simultaneously. The CNIL also recommends that the law provide for mandatory consultation of the CNIL for any act of flexible law that would be adopted by Arcep for the implementation of the regulations of the provisions of the DSA which extend, repeat or supplement those of the GDPR, namely mainly a, c, d, e, i, l, m, n and o of Article 12. Finally, IV of Article 9 should provide for the possibility , for the CNIL, to notify Arcep of breaches of the requirements set out in Chapter III of the regulation that it has observed in the context of its mission to implement the protection of personal data. CONCERNING ARTICLE 10 (DATA COLLECTION POWERS OF THE DIGITAL REGULATION EXPERTISE POLE FOR RESEARCH ACTIVITIES - PEReN) Article 36 of Law No. 2021-1382 of October 25, 2021 on the regulation and protection of access to cultural works in the digital age allows PEReN to implement methods for the automated collection of publicly accessible data on online platforms as part of experiments aimed at designing or evaluating technical tools and having the strict purpose of reflection relating to the regulation of these platforms. Article 10 proposes to modify these provisions in order to: authorize the implementation of such processing for public research activities, within the meaning of Article L. 112-1 of the Code of research, which PEReN can conduct on its own initiative; to add that these public research activities can contribute to the detection, determination and understanding of systemic risks in the Union within the meaning of the regulation on digital services. The extension of PEReN's powers to research activities is justified by the legitimate objective of developing support for public policies involved in the regulation of platform operators, in particular in the implementation of the DSA. This extension is no less significant in that it opens up a very important field of data collection for PEReN. These data collection methods, which would be authorized, must be specified by decree in Council of State issued after motivated public of the CNIL, in accordance with the provisions of article 36 of the law. Indeed, the current decree only targets PEReN's "experimental activities" and not permanent public research activities. The CNIL, in its opinion, will be particularly attentive to the guarantees provided to ensure that the collection methods are strictly necessary. and proportionate, taking into account the infringements they are likely to cause to fundamental rights and freedoms, including freedom of expression and freedom of opinion. ARTICLE 14 (CONTROL OF THE PROCESSING OPERATIONS OF THE COURTS)The GDPR (Article 55, paragraph 3) exempts from the control of the data protection authorities the processing operations carried out by the courts "in the exercise of their judicial function" , in particular "in order to preserve the independence of the judiciary in the performance of its judicial tasks, including when it takes

decisions" (recital 20 of the GDPR). This exclusion was recalled by the CJEU in a decision of March 22, 2022 (C□245/20); however, French law did not provide for such a control mechanism for the judicial or administrative courts. Article 13 modifies the code of administrative justice in order to entrust the control of the personal data processing operations of the administrative courts to the of the Council of State or to a member designated by it; article 14 modifies the code of judicial organization in order to entrust the control of the personal data processing operations of the judicial courts to an authority established with the Court of Cassation, composed of a president assisted by agents placed under his direction. The choice made by the Government to create a supervisory authority within each order of jurisdiction is consistent with the GDPR (recital 20). This choice could be extended to the financial courts or even to the Constitutional Council. As the bill currently stands, the Commission considers that the financial jurisdictions are not covered. For the Constitutional Council, its inclusion would come under an organic law. The CNIL considers that it retains its jurisdiction, on the one hand, for the processing implemented by the courts outside their jurisdictional functions (processing of human resources by example), on the other hand, for files used by judges in the context of a judicial activity but whose use goes beyond this framework (processing of criminal records, criminal records, etc.). While the draft law provides for the necessary powers for these supervisory authorities (ability to receive complaints, power of investigation and power to pronounce corrective measures and sanctions), the CNIL stresses the importance of giving these authorities the human and material resources necessary for their missions. Finally, the CNIL emphasizes its availability vis-à-vis these authorities to, in particular, respond to requests for advice that they may receive (article 8 I 2° e of the law " computing and Freedom"). CONCERNING ARTICLE 22 RELATING TO ADAPTATIONS TO THE "COMPUTER AND FREEDOMS" LAW Article 22 of the bill creates a Title IV bis divided into two chapters: one concerns the competences and powers of the CNIL with regard to the regulation on digital services (or DSA); the other concerning the competences and powers of the CNIL with regard to the regulation on European data governance (DGA). ON THE PROPOSED PROVISIONS IN CONNECTION WITH THE OBLIGATIONS SPECIFIC TO ONLINE PLATFORM SERVICES (DSA) Article 124-2 designates the CNIL as the competent authority to ensure compliance, by online platform providers who have their main establishment in France , or whose legal representative resides in France: of d) of 1. of article 26 of the DSA (obligation to present to each recipient of advertising information on the main parameters used to target him, as well as the way in which these parameters may be modified); of 3. of article 26 of the DSA (prohibition of presenting advertising to recipients of the service based on profiling using "sensitive" data within the meaning of the GDPR); of 2. of article 28 of the

DSA (prohibition of advertising based on the profiling of minors). Firstly, the CNIL considers that this new allocation of powers is logical insofar as these provisions only reinforce, for online platform providers, certain specific obligations resulting from the GDPR. The correct application of the provisions of Articles 26 ("advertising on online platforms"), 27 ("transparency of the recommendation system") and 28 ("protection of minors online") of the DSA, which refer more or less directly to issues related to data protection, will require coordination between the designated competent authorities (Arcom or Directorate General for Competition, Consumer Affairs and Fraud Prevention DGCCRF) and the CNIL. The CNIL stresses that coordination will also be necessary between it and the other competent authorities for the implementation of the DSA, whose other obligations often have a link or an impact on the protection of personal data. Finally, it recalls that it will retain its own competence on issues related to data protection by the GDPR, the regulation on digital services being understood "without prejudice (…) to Union law on data protection of a personal nature" (art. 2 4 g) of the DSA), which is also recalled by the draft article 124-1 of the law "computing and freedoms. Secondly, the bill aims to allow the CNIL, as the competent authority, to monitor the correct application of the provisions of the regulation entrusted to it and thus complete its powers of control and sanction.Articles 51 and 52 of the DSA allow Member States to determine the system of checks and sanctions applicable to infringements. Mainly, the CNIL emphasizes the need to ensure that the various systems that it will be responsible for applying in terms of checks and sanctions are harmonized as much as possible to ensure compliance with the different European regulations. Indeed, the coexistence of different regimes, responding to distinct procedural rules, would in practice prove to be particularly complex to apply, even though the regulations are ultimately intended to apply to the same players, and to penalize breaches that may be observed during the same control procedures. The CNIL therefore considers, for the purposes of clarity and legal certainty, it is preferable to integrate the new rules resulting from the DSA as much as possible into the existing procedural provisions, which are contained not only in the "computing and freedoms" law (articles 19 to 22-1) but also in its implementing decree. The new provisions introduced into the law could thus be limited mainly to: listing the competences of the CNIL for the application of certain provisions of the DSA; referring to the powers of control provided for in article 19 of the law "computing and freedoms", which could be supplemented to contain all the powers provided for by article 51 of the DSA (power of seizure in particular); refer to the applicable corrective measures which are provided for by article 20 of the law, by specifying the specificities resulting from the DSASi this option was not retained, the CNIL wishes to share the following observations on the proposed provisions.Concerning the "powers of investigation" of the CNIL:Article 124-2 refers to article 19 of the law "computer and

freedoms" which uses the word "control". This reference alone may not appear sufficient given the current drafting of Article 19 of the "Informatique et Libertés" law, the DSA providing for broader powers than those currently available to the CNIL. The authorities are notably vested with a power of seizure (Article 51.1.b)) and a power to record the responses of staff members or representatives of online platform providers with their consent using any means. technique (Article 51.1 c)). The CNIL considers the modification of article 19 necessary in order to enable it to extend to all the procedures it conducts these two means of investigation – seizure and hearing of personnel. Moreover, the second sentence of the last paragraph of article 124-2 of the bill seems to contain an error insofar as reference is made to the last paragraph of 1 of article 51; it seems that the last paragraph of 2 of article 51 should be read. In any event, it also seems necessary to clarify what is meant by "warning". This name could lead to confusion with the warning defined in I of article 20 of the law "Informatique et Libertés". Concerning the powers of formal notice and sanction of the CNIL: The proposed article 124-3 aims to adapt the powers of formal notice and sanction of the CNIL to the regulation of platforms as provided for by the DSA. Modifications editorial appear necessary to clarify the concept of "commitments" made by online platform providers to ensure the compliance of their services. The power of the competent authorities to accept such undertakings is provided for in point a) of 2 of Article 51 of the DSA, as well as in Article 71 of the same regulation in the case of very large online platforms, but without any precision. The CNIL also questions the relevance of a commitment for an indefinite period. A decree could usefully specify the procedure according to which these commitments are proposed to the president of the CNIL and then accepted by them. This appears all the more necessary since the 2nd paragraph of this article makes a reference to the "conditions provided for in I" for submitting these commitments, whereas no condition is provided for in this first paragraph. of article 124-3 relating to the calculation of penalty payments and fines, the CNIL wonders why it is specified that the amount of turnover to be taken into account to determine the applicable ceilings is the amount " excluding taxes", although this is not provided for by the DSA; this precision would introduce a specificity for these calculations compared to the methods applicable under the law "Informatique et Libertés" (article 20 III) and the GDPR (article 83). The CNIL also wonders about the practical implications of this clarification. For the sake of readability of the applicable provisions, the specific powers of the chairman of the restricted training provided for in III of Article 124-3 should be the subject of an IV, and not be incorporated into the powers of the Restricted Committee. With regard to the provisional injunctions that may be adopted when the breach observed appears likely to create serious damage, if the CNIL welcomes this possibility, these provisions should be supplemented to specify in particular the scope of these injunctions. As

these provisions are drafted, this power seems broad and not limited to requests for compliance, but can also include measures allowing the provisional suspension of the disputed facts. Similarly, the applicable procedure would also need to be clarified, in particular with regard to the methods envisaged to ensure adversarial proceedings or with regard to the period during which these measures could apply (and whether they would be effective, where applicable, until the adoption of a final decision by the restricted committee). The CNIL questions the advisability of providing for the possibility of resorting to a simplified sanction procedure, such as that provided for in article 22-1 of the law "Informatique et Libertés", for non-compliance with the applicable obligations. to online platform providers who come under the jurisdiction of the CNIL. digital services alongside the coordinator for digital services "where provided for by national law". The CNIL therefore recommends including a provision to this effect in the "Informatique et Libertés" law. Finally, the CNIL considers that it would be appropriate to make the following editorial changes: in addition to the reference to the "rules mentioned in this chapter" (II of article 214-3), the proposed provisions could make explicit reference to the applicable regulation in order to guarantee the full application of the rules resulting from this regulation and to increase the readability of the legal framework in force; in II of article 124-3, reference could be made to "the online platform provider" and not to the "service ", to directly target the actor to whom the defined obligations fall; with regard to the following passage of III of Article 124-3 - "It may be accompanied by a penalty payment, the daily amount of which may not exceed 5% of income or the average daily worldwide pre-tax turnover of the online platform service provider concerned for the previous financial year (…)" - the underlined terms do not appear necessary. These last two editorial changes would allow the same terminology to be used in all the proposed articles, and thus avoid any confusion with regard to the actors concerned. ON THE PROPOSED PROVISIONS IN CONNECTION WITH ALTRUISM IN TERMS OF DATA and Freedoms" aims to recognize the CNIL as the competent authority in matters of data altruism within the meaning of the European Data Governance Regulation (DGA) in order in particular to ensure the recording and control of compliance with the provisions of Chapter IV of this regulation. The CNIL welcomes this choice, logical in that altruism in terms of data relates in particular to personal data. The CNIL considers that it meets the conditions set out in Article 26 ("requirements relating to the competent authorities") of the regulation. of data altruism by chapter IV of the DGA regulation. II of article 124-5 provides that "In the event of a breach of these requirements, the National Commission for Computing and Liberties shall take the corrective measures set out in l 'article 24 of the same regulation'; however, the text does not indicate precisely which corrective measures are referred to (in particular whether these are only the measures provided for in 3 and 4

of Article 24 of the DGA Regulation), by whom they could be adopted (for example the president of the CNIL or the services of the Commission) and according to which procedure. more specifically, on the fact of making referral to the Restricted Committee - competent to pronounce a measure falling under 5 of Article 24 of Regulation (EU) 2022/868 of 30 May 2022 - conditional on prior recourse to other corrective measures . This condition results from the following wording "If, despite the corrective measures, the altruistic organization does not comply, the president of the National Commission for Computing and Liberties may refer the matter to the restricted formation of the commission with a view to pronouncing , after adversarial proceedings, one or more of the following measures (…)". However, on reading Article 24 of Regulation (EU) 2022/868 of May 30, 2022, such a precondition does not seem to be set by the regulation, which rather envisages the possibility of combining different successive measures. The CNIL therefore calls to review these provisions to better specify the measures in question and the competent authorities for each of them. It also underlines the need to integrate them into the existing procedural provisions, which are notably provided for by the implementing decree of the law "Informatique et Libertés".President

Marie-Laure DENIS