Deliberation 2021-070 of May 27, 2021 National Commission for Computing and Liberties Nature of the deliberation: Recommendation Legal status: In force Date of publication on Légifrance: Tuesday June 29, 2021 Deliberation No. 2021-070 of May 27, 2021 adopting a recommendation relating to the exercise of rights through an agentThe National Commission for Data Processing and Liberties,Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 relating to the protection of persons with regard to the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC (GDPR); Having regard to Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/ 64/CE (PSD2); Considering the rule Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards on strong customer authentication and common open standards and secure communication; Having regard to law n° 78-17 of January 6, 1978 as amended relating to data processing, files and freedoms; Having regard to decree n° 2019-536 of May 29, 2019 taken for the application of the law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms; After having heard the report of Mrs Anne DEBET, commissioner, and the observations of Mr Benjamin TOUZANNE, commissioner of the Government, Formulates the following observations :This recommendation aims to propose practical methods for exercising the rights conferred by the GDPR through natural or legal persons (the agents) mandated by the persons wishing to exercise these rights (the principals) with the bodies involved. receiving this data (the data controllers). This recommendation, in particular the examples proposed therein, is neither prescriptive nor exhaustive and is intended to help agents and data controllers in their compliance process. Other methods for implementing the exercise of rights through agents may be considered if they comply with the texts in force.Article 1 - Scope of recommendation 1.1 – Legal standards and rights concernedArticle 77 of the decree implementing law no. 78-17 of January 6, 1978 relating to data processing, files and freedoms (hereinafter the Data Protection Act) provides that a request to exercise the rights (information, access, rectification, erasure, limitation of processing, portability and/or opposition) may be presented by a person specially authorized for this purpose by the applicant, if this person proves his identity and the identity of the principal, his mandate , as well as the duration and precise purpose thereof. The examples given in the recommendation relate more specifically to the exercise of the right to data portability (article 20 of the GDPR) and the right of access (article 15 GDPR). However, the Commission invites agents who choose to offer services for the exercise of

other rights conferred by the GDPR to also refer to this recommendation, for the parts that would apply to their activity. recommendation concerns all processing, as defined by Article 4 of the GDPR, which is implemented in the context of a request to exercise rights through an agent. A request to exercise rights by through an agent generally takes place in six or even seven stages: the creation of a contractual relationship between the person concerned (the principal) and the agent; the establishment of a specific mandate; the transmission by the agent the request to exercise rights to the data controller; the transmission of data by the data controller to the data subject or to the agent; the transmission of data by the agent to the data subject, or to another data controller; if necessary, the storage by the agent of the data thus obtained in a space accessible to the data subject; the possible reuse of this data by the agent. The recommendation concerns, first of all, the all of the data controllers who hold the data and who receive requests to exercise rights through agents. These controllers may be public or private entities that may be subject to specific sectoral regulations specifying certain characteristics of their processing. the interaction between the provisions of PSD2 relating to the conditions for implementing certain processing of personal data and the provisions of the GDPR, if a request is sent to an account management service provider by an account information service provider, the methods of access and transmission of this data are those provided for by the PSD2. In particular, they involve the requirement of an authorization issued by the ACPR and compliance with specific security obligations. Article L. 314-1 of the Monetary and Financial Code lists the payment services subject to this regulation, including the account information service. The latter is defined as an online service consisting in providing consolidated information concerning one or more payment accounts held by the payment service user, either with another payment service provider, or with more a payment service provider. This restitution involves processing that goes beyond the simple transmission of raw data. An organization wishing to provide such a service is therefore required to comply with the access and transmission procedures provided for by PSD2, and may not exercise the rights provided for by the GDPR for this purpose, such as the right to portability or the right to access. On the other hand, it is possible for an agent, even when the latter is also an account information service provider, to exercise the rights of access and portability provided for by the GDPR, as an agent, with an account management service provider, if PSD2 is not intended to apply to this transaction. This would be the case, for example, if the data is accessed in the context of the provision of a service not subject to PSD2, or if the data accessed does not come from a payment account within the meaning of the PSD2. In any case, the processing of personal data implemented by these organizations is subject to compliance with the GDPR, whether or not they are carried out in the context of the provision of services subject to PSD2.

Finally, the recommendation does not apply to services made available by actors offering tools to facilitate the exercise of rights (for example, those providing a platform on which data subjects have access to pre-drafted requests that they themselves send ), or those who play the role of connectors and transmission facilitators in the context of a portability request without exercising these rights in the name and on behalf of the persons concerned. Article 2 - Qualification of roles and responsibilities The actors must perform a preliminary analysis as to the qualification of their role, in particular in the light of the case law of the Court of Justice of the European Union and the documents published by the European Data Protection Board (EDPS) on the notion of data controller and subcontractor.Each actor, whether a data controller receiving a request to exercise rights or an agent appointed by the person data subject, is a separate data controller, unless the actors together determine the means and purposes of the processing: in this specific case, joint responsibility may be retained. Article 3 - Entry into a contractual relationship between the data subject and the representativeAs in any entry into a contractual relationship between an organization and a data subject using the latter's services, several processing operations are necessary for the performance of the contract to which the data subject is a party within the meaning of Article 6 of the GDPR. In this contractual framework, the agent plays its role of intermediary between the person concerned and the data controllers with whom the latter wishes to exercise their rights. The exercise of rights requires in particular to prove that the person is indeed the holder of the rights that he intends to exercise, that is to say that he is indeed the person known by the data controller to whom the request is made. Article 77 of the decree provides that the person concerned proves his identity by any means, and in particular by using digital identity data when this data is necessary and considered sufficient by the controller to authenticate his users. The agent can therefore only collect and transmit the relevant authentication or identification data, which does not require systematic processing of proof of sovereign identity. Article 77 of the decree also specifies that the photocopy of an identity document bearing the signature of the holder can only be requested in the event of reasonable doubts as to the identity of this person, when the situation so requires. .If the agent considers that he must ensure the identity of the person concerned before entering into a commercial relationship with him, the Commission points out that consultation of proof is generally sufficient, without this data necessarily being stored. . However, on the basis of its legitimate interest, the agent may exceptionally retain the data enabling the identity of the data subject to be justified in order to anticipate specific cases where the data controller has reasonable doubts as to the identity of the data subject. person, provided that this data is relevant to the verification carried out. In the event that the person concerned is known by the data controller under his or her sovereign identity, and that

the agent wishes to keep proof of this, the Commission recommends deploying reinforced security measures, such as: storing in an appropriate form , for example, by limiting the quality of the digitized image, by integrating a watermark with the date of collection and the identity of the data controller or by setting up mechanisms for encrypting digitized identity documents; strict management authorizations (access only to management controllers or collection services, for example); the implementation of user authentication mechanisms; the implementation of a system for logging access to identity documents, keeping for a period of six rolling months the identifier of the employee who has accessed an identity document, the internal reference of the identity document consulted, as well as as the timestamp of the consultation, associated with automatic analysis mechanisms in order to detect unauthorized access; and the use of specialized data destruction software when they are deleted. Article 4 - On the establishment of the mandate and its content In accordance with article 77 of the decree, the agent must be specially authorized by the person concerned; the precise duration and purpose of the mandate must be specified and the agent must be able to justify his mandate. Although certain aspects of a request to exercise rights through an agent may be dealt with in the framework of general conditions of use (such as, for example, the retention period, the rights that the agent proposes to exercise through it, etc.), the Commission considers that such a general clause seems insufficient to respond to the specific nature of the mandate with respect to (i) the data covered by the request; (ii) the data controller receiving the request; (iii) the identification data transmitted to the controller; (iv) the rights exercised; and (v) term of office. The Commission makes available to agents on its website an example of a standard mandate, to which agents and data controllers who hold data can refer. transmission of data without first ensuring their validity: it is their responsibility to ensure the identity of the person concerned and the veracity of the power of attorney. The Commission recommends that the agent ensure that the power of attorney contains all the elements allowing (i) to identify the holder of the right exercised and the person at the origin of the request, in the event of legal representation of the person concerned; (ii) to ensure the authenticity of the mandate; (iii) to identify the recipient to whom the data must be transmitted (i.e. the person concerned, the agent or the possible new data controller in the context of the direct transfer, permitted by the right to portability); and (iv) to identify the data controller with whom the rights must be exercised. In the event that the agent exercises the data subject's rights with several data controllers, the Commission recommends that a specific mandate contract to each data controller is concluded in order to prevent the mandate from containing unnecessary or irrelevant information such as identification information only valid with a data controller or from not being revealed to a data controller the identity of another controller holding the data subject's personal

data. Finally, the agent must pay particular attention to compliance with the principle of data minimization, pursuant to Article 5 of the GDPR. The agent must therefore carry out an analysis upstream in order to ensure the relevance of the data transmitted in the mandate to the controller. In this perspective, the Commission proposes that the agents refer to the paragraphs below, as well as to the standard mandate posted on the Commission's website.4.1 – Data allowing the data controller to identify the person data subjectThe Commission recommends leaving the field open to the data subject in the mandate so that they themselves provide the data they consider relevant to enable the data controller to identify them (username, date of birth, date of last connection, for example). The agent, in his role as intermediary, can advise the data subject as to the information allowing the controller to identify him, so that only relevant and necessary information is collected and transmitted. In this respect, the mandate should recall the person concerned that his identity document should only be transmitted in support of the request if the data controller knows him under his sovereign identity (for example, in the context of a relationship with a bank). If the data controller knows the person under a pseudonym, the transmission of the identity document with the power of attorney request may not be justified. 4.2 – Data allowing the data controller to ensure the authenticity, the scope and duration of the mandate Insofar as it is the responsibility of the controller holding the data to ensure the authenticity of the mandate, it is recommended that measures allowing him to implement this obligation be taken upstream by the agents. In some cases, the use of a simple electronic signature may be considered in order to verify the identity and the will of the person concerned to establish the mandate. This signature could also make it possible to guarantee that the mandate has not undergone any modification since it was signed by the person concerned. The data controller must also be able to identify, through the mandate, the data subject to the request, the nature of the rights exercised and the duration of the mandate. The Commission recommends that the mandate expressly invite the data subject to specify his request with, for example, the categories of data subject to the exercise of the right (for example , all data relating to its interactions with customer service), the purposes of the processing (for example, all data collected to facilitate payment), the service provided by the data controller (for example, a ticketing service) or again by right that it wishes to exercise (if the agent offers it among its services). Finally, the duration of the mandate must be indicated, which implies that the date on which the mandate ends must be determined or determinable. Thus, the Commission considers that a mandate established for an indefinite period does not meet the requirement of article 77 of the decree. For example, the missions to be performed by the agent can be precisely listed, and it can be provided that the accomplishment of these will lead to the automatic termination of the mandate, in particular upon receipt of the data within

the framework of the exercise of a right to data portability. Furthermore, the Commission recalls that pursuant to Article 2004 of the Civil Code, the person concerned has the right to revoke the mandate at any time. The Commission recommends that, when the mandate is tacitly renewed, the person concerned is informed and can exercise his right of withdrawal at any time. When the person revokes their mandate, the exercise of rights through the agent must cease. The latter must therefore notify the data controllers to whom requests for the exercise of rights have been sent and which are still being processed, without prejudice to the possible notification of this revocation at the initiative of the person concerned. same.4.3 – Data allowing the data controller to identify the recipients of the dataThe mandate must expressly specify whether the agent can be made the recipient of the data, in accordance with article 77 of the decree. To ensure a smooth transmission of data, the address (postal or electronic) to which the data can be sent can also be specified, as well as any other technical means allowing the data to be received and usable as quickly as possible by the entity. recipient, such as an access key to an application programming interface ("application programming interface" or API) or even a dedicated URL, provided that the transmission by these means takes place in a secure manner and that their use by the controller does not require additional efforts. In cases where the recipient of the data is not specified in the mandate, the Commission recommends that the data be transmitted by default to the person concerned. Article 5 - On requests to exercise rights by electronic meansArticle 12 paragraph 3 of the GDPR provides that when the data subject submits his request in electronic form, the information is fo urnies electronically if possible, unless the data subject requests otherwise. If technically feasible, the Commission recommends that the authorized representative offers the data subject the possibility of choosing the channel through which he wishes to exercise his request (i.e. by post or electronically), knowing that the electronic means can be considered as the default way.5.1 - Requests to exercise rights via the use of an API Requests to exercise rights via an agent can be made via an application programming interface.APIs can significantly reduce the burden on data controllers in processing requests to exercise rights. The Commission thus encourages data controllers and agents to use this technique, in particular when they have to process a large number of requests to exercise rights. Moreover, when data controllers provide access by API, the Commission recommends that access to the API is stable, that it has a high level of availability, and that security measures adapted to the risks are implemented. The use of an API may be particularly relevant if a regular update of the data is necessary for the agent to be able to provide the service to the person concerned (for example, within the framework of an alert service on the arrival of a new telephone bill). Finally, when APIs are developed in order to comply with the requirements of Delegated Regulation

(EU) 2018/389, the Commission encourages players subject to PSD2 to extend their use to data not falling within the scope of PSD2, in order to to be able to respond in a secure and more fluid manner to requests to exercise the rights they may receive. 5.2 – Requests to exercise rights via the use of the data aspiration technique ("scraping") The agents can ask the data subject for his username and password in order to extract data concerning him accessible from the site of the data controller (technique known as data extraction or "scraping"). The use of authentication data with the consent of the person concerned in this regard is not prohibited in principle by the GDPR. However, given the significant risks it entails for the persons concerned, in particular with regard to preservation of the level of security provided by authentication mechanisms based on the use of passwords, the use of this technique should be strictly limited and systematically subject to obtaining valid consent from the person concerned (this is i.e. free to be given or refused, regardless of the conclusion of the mandate and subject to withdrawal at any time). Similarly, the agent would in this case become responsible for the processing of the data allowing the authentication of the data subject, and would then be required to implement the appropriate technical and organizational measures in order to guarantee a level of security adapted to the risk. case of use is one in which the data controller allows access to the data by aspiration by indicating this unequivocally in his response to the request addressed to him. In this case, the data controller and the agent are required to adapt the security measures and should, prior to the exercise of the right of access, carry out a risk analysis in order to implement the security measures. adequate so that these risks are controlled. For example, these measures may consist of the establishment of authentication dedicated to the agent allowing its identification and traceability of access, the provision of a degraded version of the site containing only the information to which the agent may have access, or the use of a temporary password dedicated to the agent on the user account. The second corresponds to the case where a data controller does not respond to a request made several times, beyond the deadlines provided for by the GDPR. In this case, the Commission recommends that the agent implement the following measures: (i) the data subject has been fully informed of the risks incurred in obtaining consent; (ii) the data controller has been notified in advance that an aspiration will be implemented with the information allowing him to identify access by the agent (such as the latter's IP address, the date, the time and duration of its connection, etc.); (iii) the agent is able to provide a valid mandate to the data controller if the latter so requests, even if the data has already been collected; (iv) the agent does not collect data of which he does not have to know with regard to the mandate, in particular by allowing the principal to verify, rectify or delete all or part of the data collected by this means; and (v) the password ordinarily used by the user is not transmitted to the agent. To this end, agents

should set up a system allowing the extraction to be carried out via the data subject's browser (for example, via a specific extension in the browser). Failing this, the Commission recommends that the authorized representative inform the person concerned of the need to change his password to create a temporary one allowing access to his account, then to modify it again once this access has been achieved by the authorized representative. . The Commission recommends in any event that, in the exceptional case where the authorized representative uses a password, dedicated or temporary, this should not be accessible to any member of his staff and should be deleted immediately after access to the data. . If suction is used on a recurring basis, the agent must regularly inform the person of the existence of this access and ask him to confirm his wish to continue the collection. The Commission also points out that the agents considering using this technique data collection cannot require the deactivation of legitimate security measures put in place by data controllers, such as systems for blocking access to content by robots such as the use of captchas or suspension systems access to certain IP addresses representing a proven security risk.Article 6 - On the response provided by the data controller to the request to exercise rights The Commission encourages players to collaborate as much as possible in order to facilitate the exercise of rights persons and reminds them that they cannot create additional conditions, devoid of legal basis, which would prevent the abou ment of a request to exercise rights.6.1 – On the extension of the response time when a request is complexIn accordance with Article 12 paragraph 3 of the GDPR, the controller must inform the person of the measures taken to respond at his request, as soon as possible and in any case within one month of receipt of the request. If necessary, this period may be extended by two months taking into account the complexity and the number of requests. The controller must be able to demonstrate the complexity of the request; the mere fact that a request is made through an agent is not sufficient to automatically extend the response time. The agent should fully play its role as intermediary between the controller and the data subject. For example, if the data controller acknowledges receipt of the request, confirms that it has been taken into account (in particular in the case of a request for rectification or deletion) or if he responds by informing that a two-month extension is necessary , the authorized representative should transmit this information to the data subject. In this respect, the Commission recommends that the data subject be able to follow the progress of the agent's mission, at any time during its performance (without prejudice to the obligations of transparency and the exercise of rights relating to the processing of his data at personal character by the said agent). that is, in a format that systems must be able to process automatically. Although this article only relates to data subject to a portability request, the Commission encourages data controllers and agents to use global or sector-wide standard formats, and

preferably open and documented (e.g. XML, JSON, CSV, with useful metadata at the best possible level of granularity, while maintaining a high level of abstraction) to respond to requests to exercise rights. the transmission channel, Article 12 of the GDPR states that where the data subject submits his or her request in electronic form, the information shall be provided electronically, where possible, unless the data subject requests that it be provided. either otherwise. The Commission thus notes that the GDPR lays down a principle of parallelism of forms. Also, if the agent has implemented measures allowing the data subject to exercise his request by post, similar measures should be taken to allow the data to be received by this same channel. The direct transmission of data to the agent by the data controller may be required under the right to portability, when technically possible and provided for in the mandate. As part of a right of access, the Commission encourages data controllers to send the data to the agent when the latter is designated as recipient by the person concerned in the mandate.Article 7 - On the refusal to grant a request to exercise rights through an agent7.1 - When the request is manifestly unfounded or excessiveArticle 12 paragraph 5 b) of the GDPR states that when the requests of a data subject are "manifestly" unfounded or excessive, in particular because of their repetitive nature, the data controller may refuse to respond to these requests. The Commission considers that the manifestly unfounded or excessive nature of a request should be assessed on a case-by-case basis by the controller holding the data, and that the term manifestly implies that the unfounded nature is undeniable and obvious. .The Commission considers that the fact that a request is made through an agent does not mean that it is manifestly unfounded. In addition, the Commission recalls that the data controllers holding the data are not responsible for the subsequent uses that the agents would make once the data have been transmitted: the manifestly unfounded nature cannot be characterized by possible reuses, which are entirely within the the responsibility of the agent. The Commission recalls that the quantity of data which is the subject of the request does not constitute sufficient justification for considering that a request is excessive. Finally, the EDPS considered in his guidelines on the right to data portability that the cases in which the data controller can refuse to provide the requested information should be very rare, even when it comes to multiple requests. In this spirit, the Commission considers that the repetitive nature of requests to exercise rights is not in itself sufficient to consider them excessive. However, the Commission considers that the renewal of a request to exercise rights could be considered as excessive if a strictly similar request has already been sent to the data controller, whereas (i) this request relates to the same set of data and the same rights; (ii) that no response has yet been delivered; and that (iii) the response period (one month which can be extended by two months) available to the data controller has not yet expired. Conversely, the renewal of a

request relating to the same set of data and on the same rights should not be considered excessive if the response time has elapsed and the data controller has not complied with his obligations by not responding to the request, or has responded in an unsatisfactory manner (if, for example, he has not correctly rectified the data or has not transferred all the portable data). If a first request has already been fully satisfied by the controller, the conditions under which a request relating to the same set of data and for the same rights can be renewed are generally linked to one-off events, such as : the wish of the data subject to add a new recipient to his request for data portability; or when the data subject can reasonably consider that new data has appeared or that the processing methods have changed, as indicated in recital 63 of the GDPR. With regard to the addition of a new recipient in the context of a request for portability, the Commission encourages the agent to put in place a mechanism enabling the data subject to add a new recipient directly on his platform, if the data has been kept by the agent, in order to avoid renewing the request for portability. portability with the data controller. In all cases, the Commission recommends that the data subject be free to determine the scope of his request and be able to choose to renew the same mandate. As a good practice, the trustee can advise her to target her renewal request or to specify the reasons why she considers that a renewal is necessary. In general, the Commission recommends not to provide for renewal by default or periodicity of a mandate, unless: the nature of the processing makes it possible to anticipate that modifications will be regularly made to the data concerned and that the agent offers a service for periodic updating of the data; or if the data transmission takes place via an API. Indeed, the use of an API makes it possible to considerably reduce the burden relating to the processing of repetitive requests for the exercise of rights and reduces the probability that requests may be considered as imposing an excessive burden. Finally, the data controller cannot keep silence when receiving a request to exercise rights. If he refuses to do so, he must, pursuant to Article 12 paragraph 6 of the GDPR, justify the reasons for his refusal. This justification may be made to the agent, who must inform the person concerned. Failing this, the data controller exposes himself to the filing of a complaint with the Commission or to legal action if the person concerned wishes to contest the implicit or explicit refusal to take his request into account. 7.2 - When the controller processing has reasonable doubts about the identity of the data subject to the identity of the person. Thus, if the information previously provided in the mandate is sufficient, it is in principle not necessary to collect additional information. On the other hand, these reasonable doubts can for example be characterized in the event of homonymy. In cases where the controller has reasonable doubts about the identity of the person, in particular when the person uses a pseudonym which with the information held by himself, he can collect additional information to confirm the identity, knowing

that specific attention must be paid to the principle of data relevance. For example, if the data controller does not know the person under his sovereign identity, collecting the identity document to carry out additional checks is in principle not relevant. In this respect, the Commission encourages the adoption of authentication protocols shared between the agent and the data controller, so that the latter can ensure that the data subject is indeed who he claims to be, and to facilitate the direct transmission of data. For the collection of additional information, the data controller can turn to both the agent and the data subject. In the latter case, the Commission invites data controllers to monitor and keep the agent informed of this process. For example, he can set up authentication mechanisms allowing the person concerned to connect to the online service with his identifiers and ask him to confirm that the request really came from him. The data controller may also contact it directly in order to check the consistency with information it already has (purchase history, loyalty card number, etc.). 7.3 - On the possibility of refusing a request due to 'a technical impossibility When the answer is provided in an electronic form, the transmission of the data can be done by means of a direct transmission or automated tools allowing the extraction of the relevant data (such as APIs for example). The Commission encourages data controllers and agents to develop standardized systems in order to reduce the technical obstacles which hinder the direct transmission of data. The adoption of standardized technologies can take place at several levels: at the level of data transfer, particularly in the context of data portability when establishing the communication protocol between data controllers (widely used protocols are recommended , such as REST HTTP/S, SOAP, etc.); at the level of the data format, so that the content thereof can be easily interpreted by another data controller; at the level of the semantics of the data, it is i.e. their meaning in a particular context. In order to facilitate understanding of the data model, documentation, semantic or modeling languages (such as UML) may be used. The Commission considers that the simple fact that the agent and the controller have not developed similar transmission mechanisms (direct or by automated tool) is not sufficient to conclude that the exercise of rights is technically impossible. It will therefore be necessary for the agent and the data controller to make reasonable efforts to find technical solutions allowing the proper transmission of the data. 8.1 - On the restructuring/reorganization of the data With regard to the possibility for the agent to restructure the data before transmitting them to the data subject, the Commission invites the agents to clearly inform the persons, specifying in the contract whether this restructuring is an integral part of the service offered or if the data subject retains the possibility of receiving the raw data. The data processing carried out in this context may be based on the performance of the contract to which the data subject is a party, provided that the restructuring carried out is an integral part of the service requested and expected by the data subject.

8.2. - On the retention of data by the agentThe data transmitted to the agent by the data controller must in principle be deleted, once the purpose of the processing resulting from the mandate has been achieved, which corresponds in principle to the transmission of the data to the data subject or to another data controller. However, the agent may offer a feature allowing the person concerned to keep the data on a dedicated storage space that he makes available to him so that he can access it at any time. . In such a case, the person concerned must be able to define the duration of data retention and to decide at any time on their deletion. The Commission recommends that the following measures be taken for the methods of data retention: put in place a data access control management policy, which must be guaranteed only to authorized persons, in order to protect against destruction, theft and modification by malicious persons; set up the logging of access and modifications made; if the data is of a sensitive nature, guarantee its confidentiality through encryption measures with key management under the sole control of the user; if the data is important, guarantee its availability and set up replication mechanisms in order to be able to restore them in case of loss; set up a deletion policy once the planned retention period has been reached.A Article 9 - On the reuse of data transmitted to the agent Data controllers responding to requests to exercise rights are not responsible for the processing carried out by the agent. Only agents are responsible for this processing and must, as such, ensure their lawfulness, both with regard to the GDPR and other regulations. The purpose of the mandate referred to in the last paragraph of Article 77 of the decree application of the Data Protection Act is exclusively to exercise the rights of the person concerned in his name and on his behalf. It therefore does not authorize as such the reuse of personal data collected in this context by the agent for his own account. Such reuse must be considered separately, as an autonomous processing of personal data fully subject to compliance with all the provisions of the GDPR. This processing must in particular meet one or more specific, explicit and legitimate purposes and be implemented under the control of the data subject. For example, the agent may offer the data subject an additional service based on the reuse of its data, to which it can freely subscribe. In this case, only the data necessary for the provision of the service explicitly requested by the person may be used and the latter must be able to reconsider their choice at any time and request the deletion of the data concerning them. In general, if the data collected through the mandate were to be subject to processing that goes beyond their transmission, by the agent or any other third party to whom the data subject has entrusted them, this processing should fully comply with all the provisions of the GDPR and should in particular have a valid legal basis under its article 6. In this respect, the collection of the specific, free and informed consent of the persons concerned must be privileged, and will often be compulsory, prior to any reuse of their data for

purposes unrelated to the mandate to exercise rights, since such reuse cannot be based on the execution of the mandate contract con understood with the person concerned and does not appear, in general, to fall within his reasonable expectations. a compatibility analysis of purposes pursuant to Article 6(4) of the GDPR and have a valid legal basis. Thus, the Commission considers that in the vast majority of cases, a form of consent from the person will be necessary before proceeding with any reuse of the data transmitted in the context of the exercise of rights, unless this reuse has a strong link with this exercise, and that the other compatibility criteria listed in Article 6(4) are fulfilled. The Commission encourages trustees to offer, where appropriate, a granular choice by type of data and use. Thus, the data subject should have the choice to decide on a case-by-case basis which re-uses it allows. The agent must also provide the data subject with all relevant and useful information on the new processing operations that he plans to implement. , in a clear, concise and transparent manner, pursuant to Article 13 of the GDPR. Thus, the person must be able to understand precisely what will be done with the data concerning him. It is also up to the agents to ensure that they comply with the other regulations that may apply, in particular competition law, the right of database producers or the civil theory of abuse of rights. Finally, the right to obtain a copy of the data must not infringe the rights and freedoms of others (article 15 paragraph 4 of the GDPR) . If the right to portability does not infringe the rights and freedoms of third parties (Article 20 paragraph 4 of the GDPR) when the data concerning third parties also relate to the data subject at the origin of the request, the processing of third-party data by a new data controller must be subject to particular vigilance. In this respect, the EDPS considers that the new data controller may have a legitimate interest in processing the data of these third parties in order to provide a service to the data subject allowing him to process this data for his personal use, and only for this use. . Conversely, the rights and freedoms of third parties do not seem to be respected if the agent uses their data for its own purposes. Thus, the Commission considers that agents should refrain from reusing data relating to third parties for their own purposes.Article 10 - On the security of data transmission With regard to the security of data transmitted directly to end users, the Commission recommends that the following measures be implemented by the sending entity (controller or agent): ensure the confidentiality of the data exchanged during their transmission, for example by encrypting the communications with algorithms and keys at the state of the art; ensure that only the person concerned can access their data. This can result in the possibility of accessing data from a user account accessible only after authentication, or by sharing a secret through a communication channel different from that by which the data is transmitted, allowing the data to be decrypted when it is accessed from an unauthenticated environment; implement a traceability

mechanism illustrating the path of the data. With regard to security measures, when the data is transmitted to the agent or to a third-party data controller, the Commission recommends that the following measures be implemented: ensure the confidentiality of data exchanged during transmission by encrypting communications with state-of-the-art algorithms and keys; set up mutual authentication mechanisms for the entities concerned; use strong authentication mechanisms for the authentication of personnel authorized to access data; set up mechanisms for traceability of access to data, associated with the keeping of traceability logs and mechanisms for the automatic analysis of this data in accordance to the recommendation on logging adopted by the Commission on 14 October 2021The President eMarie-Laure DENIS