Deliberation SAN-2021-008 of June 14, 2021 National Commission for Computing and Liberties Nature of the deliberation: Sanction Legal status: In force Date of publication on Légifrance: Thursday June 17, 2021 Deliberation of the restricted committee n°SAN-2021-008 of June 14 June 2021 concerning the company BRICO PRIVÉThe National Commission for Computing and Liberties, meeting in its restricted formation composed of Mr. Alexandre LINDEN, president, Mr. Philippe-Pierre CABOURDIN, vice-president, Mrs. Anne DEBET, Mrs. Christine MAUGÜE and Mr. Bertrand du MARAIS, members; Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 relating to the protection of personal data and the free movement of such data; Having regard to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector ues; Having regard to the postal and electronic communications code; Having regard to law no. 78-17 of January 6, 1978 relating to data processing, files and freedoms, in particular its articles 20 and following; Having regard to decree no. 2019-536 of May 29, 2019 taken for the application of law no. 78-17 of January 6, 1978 relating to data processing, files and freedoms; Having regard to deliberation no. 2013-175 of July 4, 2013 adopting the Commission's internal regulations Commission Nationale de l'Informatique et des Libertés; Having regard to decision no. verification of the processing implemented by this organization or on behalf of the company BRICO PRIVÉ; Having regard to the decision of the President of the National Commission for Computing and Liberties appointing a rapporteur to the restricted committee, dated 19 december mber 2019; Having regard to the report of Mrs Valérie PEUGEOT, reporting commissioner, notified to the company BRICO PRIVÉ on October 2, 2020; Having regard to the written observations submitted by the company BRICO PRIVÉ on November 2, 2020; Having regard to the response of the rapporteur to these notified observations on November 24, 2020 to the board of the company; Having regard to the new written observations submitted by the board of BRICO PRIVÉ, received on December 16, 2020, as well as the oral observations made during the restricted training session; Having regard to the document relating the deployment of the intermediate archiving and anonymization procedure for the data of prospects and customers of the company BRICO PRIVÉ paid by the board of the company BRICO PRIVÉ during the restricted training session; bailiff produced on February 5, 2021 as well as its appendix, sent by the board of the company to the chairman of the restricted formation and to the rapporteur on February 10, 2021; Having regard to the other The documents in the file; Were present, during the restricted committee session of January 28, 2021: Mrs. Valérie PEUGEOT, commissioner, heard in her report; As representatives of the company BRICO PRIVÉ:[…];[…]; […];[…]. BRICO PRIVÉ having the floor last;The Restricted

Committee adopted the following draft decision:I.Facts and procedure1. BRICO PRIVÉ (hereafter the company) is a simplified joint-stock company with a single partner created in 2012. Its head office is located at 55 Avenue Louis Breguet, Bâtiment Apollo in Toulouse (31400). It is chaired by BP HOLDING, a simplified joint-stock company, located at the same address.2. The company publishes the bricoprive.com website, which has been accessible in France, Spain since 2015, Italy since 2016 and Portugal since 2017. It is a private sales site dedicated to DIY, gardening and the layout of the house. Until the month of […], sales were accessible provided you had created an account on the site. Since that date, sales are visible without the precondition of creating an account. On the other hand, to make a purchase, it is always necessary to create an account on the bricoprive.com site. In 2018, the company had […] users in France, […] users in Spain, […] users in Italy and […] users in Portugal.3. In 2018, it achieved a turnover of around […] euros, for a net result of around […] euros. In 2019, it achieved a turnover of around […] euros for a net result of around […] euros. In 2020, it achieved a turnover of around […] euros, for a net result of around […] euros. BRICO PRIVÉ employed approximately 150 people in 2018.4. On November 13, 2018, pursuant to decision no. 2018-238C of September 27, 2018 of the President of the CNIL, a CNIL delegation carried out an inspection mission at the company's premises. The purpose of this mission was to verify compliance by this company with all the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter the Regulation or the GDPR) and of the law No. 78-17 of January 6, 1978 as amended relating to data processing, files and freedoms (hereinafter the amended law of January 6, 1978 or the Data Protection Act).5. The control more specifically targeted the processing of personal data of the company's customers and prospects. The checks carried out focused in particular on the retention periods of personal data, the information brought to the attention of the persons concerned with regard to the processing carried out by the company, compliance with requests to erase the personal data of persons concerned, the obligation to ensure data security and the obligation to obtain the consent of the person concerned to receive commercial prospecting by e-mail.6. At the end of the inspection, the report n°2018-238/1 was notified to the company BRICO PRIVÉ by letter dated November 19, 2018. The company sent to the Commission services, by email of the same day, the additional documents requested at the end of the inspection mission.7. By email of February 5, 2019, the company communicated on its own initiative to the delegation several additional documents, in particular a document entitled Procedure for the retention of personal data .8. The investigations having made it possible to establish the cross-border nature of the processing concerned, the CNIL informed on August 27, 2019, in accordance with Article 56 of the GDPR, all the European supervisory authorities of

its competence to act as an authority. supervisory authority and thus opened the procedure for the declaration of the authorities concerned on this case.9. On September 27, 2019, the President of the CNIL submitted a draft formal notice to the authorities concerned. Following this dissemination, three authorities formulated relevant and reasoned objections within the meaning of Article 60 of the GDPR, requesting for two of them that the draft formal notice be modified into a draft sanction, and more particularly an administrative fine for one of these two authorities. In support of this request, the authorities concerned pointed out in particular the number of infringements, the number of persons concerned and the size of the company.10. In order to complete its investigations, the CNIL, on February 6, 2020, pursuant to the aforementioned Decision No. 2018-238C, carried out an online inspection of any processing accessible from the bricoprive.com.11 domain. This control focused more specifically on the procedures for informing the persons concerned on the bricoprive.com website and on the deposit of cookies on the user's terminal when they arrive on this site.12. Following the inspection, the report no. 2018-238/2 was notified to the company BRICO PRIVÉ by letter dated February 19, 2020. The company transmitted to the Commission services, by emails of March 4 and 9 July 2020, the additional documents and information requested at the end of the inspection mission.13. On January 13, 2021, a delegation from the CNIL, pursuant to the aforementioned decision no. 2018-238C, carried out a new online control mission for any processing accessible from the bricoprive.com domain. As the company indicated that changes had been made to the procedures for depositing cookies, it was decided to carry out a new check in order to update the findings made on February 6, 2020.14. At the end of the inspection, the report n°2018-238/3 was notified to the company BRICO PRIVÉ by letter dated January 14, 2021. By email of January 26, 2021, the company sent to the Commission services the additional documents requested during the inspection.15. For the purpose of examining these elements, the President of the Commission, on December 19, 2019, appointed Mrs Valérie PEUGEOT as rapporteur on the basis of Article 22 of the law of January 6, 1978 as amended.16. At the end of her investigation, the rapporteur, on October 2, 2020, had the company BRICO PRIVÉ notified of a report detailing the breaches of the GDPR that she considered constituted in this case and indicating to the company that it had a period of one month to communicate its written observations pursuant to the provisions of Article 40 of Decree No. 2019-536 of May 29, 2019.17. This report proposed that the restricted committee of the Commission issue an injunction to bring the processing into compliance with the provisions of articles L. 34-5 of the postal and electronic communications code (hereinafter the CPCE), 82 of the law Computing and Freedoms and 5-1-e), 13, 17 and 32 of the GDPR, accompanied by a penalty payment per day of delay at the end of a period of three months following the notification

of the deliberation of the restricted formation, as well as an administrative fine. He also proposed that this decision be made public, but that it would no longer be possible to identify the company by name after the expiry of a period of two years from its publication.18. On November 2, 2020, through its counsel, the company filed observations.19. On November 5, 2020, a notice to attend the restricted training session of December 10, 2020 was sent to the company.20. On November 13, 2020, the rapporteur requested an extension to respond to the observations made by the company BRICO PRIVÉ. By email of November 16, 2020, the chairman of the Restricted Committee informed the rapporteur that she had an additional period of eight days to submit her observations. By letter dated November 24, 2020, the company was informed that it also benefited from an additional period of eight days and that, therefore, the restricted training session initially scheduled for December 10, 2020 was postponed.21. On 16 December 2020, the company produced new observations in response to those of the rapporteur.22. By letter dated January 11, 2021, the Commission services sent the company a new invitation to the restricted committee meeting of January 28, 2021.23 The company and the rapporteur presented oral observations during this meeting.24. On May 19, 2021, as part of the cooperation procedure, a draft decision was submitted to the authorities concerned on the basis of Article 60 of the GDPR concerning breaches of the GDPR.25. This project did not give rise to relevant and reasoned objections.II.Reasons for the decisionA.On the failure to define and respect a retention period for personal data proportionate to the purpose of the processing in application of article 5-1-e) of the GDPR26. Under the terms of Article 5-1 e) of the Regulation, personal data must be kept in a form allowing the identification of the persons concerned for a period not exceeding that necessary with regard to the purposes for which they are processed. ; personal data may be stored for longer periods insofar as they will be processed exclusively for archival purposes in the public interest, for scientific or historical research purposes or for statistical purposes in accordance with Article 89 , paragraph 1, provided that the appropriate technical and organizational measures required by this Regulation are implemented in order to guarantee the rights and freedoms of the data subject (restriction of storage).27. The rapporteur noted that, during the inspection of November 13, 2018, the company indicated to the delegation that no retention period for customers' personal data (customers being, according to the company, the holders of an account on the site who have already made at least one purchase) and prospects (holders of an account on the site who have never made a purchase) had not been determined and that it did not proceed to any regular deletion or archiving of such data at the end of a defined period.28. In defense, although it did not mention it during the audit, the company first argued that a retention period policy had been defined as of October 26, 2018,

such that no breach could not be criticized for the definition of retention periods.29. In its observations of December 16, 2020, the company then indicated that the data of customers and prospects used for commercial prospecting purposes or relating to the management of their account were now kept on an active basis until the account was deleted or, in case of inactivity, for three years from their last connection to the account. At the end of these periods, the company specified that only the data necessary for pre-litigation or litigation purposes are archived until the date corresponding to the legal requirement justifying their retention, then that they would be deleted.30. Finally, during the restricted training session and while the investigation procedure was closed, the company produced a document aimed at providing proof of the deployment of an intermediate archiving procedure and an anonymization process Datas. By email of February 10, 2021, the company sent, through its counsel, a report drawn up on February 5, 2021, as well as its appendix, relating to the procedure for anonymizing the data of prospects and customers of the company BRICO PRIVÉ.31. According to the Restricted Committee, with regard to the definition of retention periods applicable to the data of customers and prospects of the company BRICO PRIVÉ, it should first be noted that the document entitled Procedure for the retention of personal data is dated October 26, 2018, i.e. before the audit. However, it was not communicated to the delegation until two months after the inspection was carried out, on February 5, 2019, and on the day of the inspection, November 13, 2018, the company indicated to the delegation that no retention period is implemented in .32 database. The Restricted Committee then notes that during the inspection of November 13, 2018, the delegation noted the presence, in the active database, of personal data of 16,653 people who had not placed an order for more than five years, without the company either able to provide an explanation or to provide justification as to the duration of this storage or to provide proof of more recent contact with said customers (exchange with customer service, click on a promotional link appearing in email, etc.). In addition, the Restricted Committee notes that in response to a request for additional services from the CNIL, the company provided, on March 4, 2020, an Excel table from which it appears that it kept the personal data of more than 130,000 people who had not logged into their customer account for more than five years.33. Therefore, if the Restricted Committee takes note that the company BRICO PRIVÉ now implements retention periods, compliance with which makes it possible to comply with the provisions of Article 5-1-e) of the GDPR - by guaranteeing that the data does not are not kept for periods exceeding that necessary for the purposes for which they are processed - it considers, in any event, that on the day of the inspection, the retention period policy was not respected and that the data were retained for excessive periods of time. The CNIL's delegation of control has in fact noted that personal data was kept for periods much

longer than those defined in the aforementioned document and which did not appear to be appropriate with regard to the purposes for which the data are processed. 34. In addition, the Restricted Committee considers that the company had not provided, on the date of the closing of the investigation, any elements to certify compliance on this point. It considers in any case that, in accordance with article 40 of the decree of May 29, 2019 taken for the application of the Data Protection Act, the elements submitted during the session of January 28, 2021 are not, in l state, sufficient to decide at this stage on its possible compliance with article 5-1-e) of the GDPR.35. In view of all of these elements, the Restricted Committee considers that the breach of Article 5-1-e) of the GDPR is clear and that the company has not fully complied on the closing date of the instruction.B.On the breach of the obligation to inform individuals pursuant to Article 13 of the GDPR36. Article 13 of the GDPR requires the data controller to provide, at the time the data is collected, information relating to his identity and contact details, those of the data protection officer, the purposes of the processing and its basis. legal status, the recipients or categories of recipients of personal data, their transfer, where applicable, their retention period, the rights enjoyed by individuals and the right to lodge a complaint with a supervisory authority.37 . The rapporteur notes that, as shown by the findings made during the on-site inspection of November 13, 2018, then the online inspection of February 6, 2020, the information made available to users of the site was not complete within the meaning of section 13 of the Regulations. Indeed, certain mandatory information provided for by this article – namely the contact details of the data protection officer, the retention periods, the legal bases of the processing and certain rights from which individuals benefit under the GDPR – were not provided. to the knowledge of the persons concerned on the bricoprive.com site, whether through the general conditions of sale, the legal notices and personal data or the personal data retention policy.38. In defence, the company indicates that it has made corrections, as part of the procedure, in order to provide information that complies with the requirements of the GDPR.39. Firstly, with regard to the contact details of the data protection officer, the Restricted Committee notes that the company acknowledged that these were not present on the bricoprive.com site until the notification of the sanction report , but specified that it was nevertheless possible to send him a request via an "unsubscribe and unsubscribe" section within a contact form.40. On this point, the Restricted Committee first recalls that, although it may be a useful method, allowing customers and prospects to be put in touch with the data protection officer via a contact form dedicated to unsubscribing and unsubscribing is not a measure likely to allow compliance with the provisions of Article 13 of the GDPR, which requires providing the contact details of the data protection officer. In addition, the Restricted Committee notes that on the date of the on-site inspection of November 13, 2018,

this form was accessible from a section entitled Customer Service – contact us, which it is specified that it allowed questions to be asked about an order or information about [the] products [of the company]. Under these conditions, data subjects could not spontaneously expect to be put in touch with the data protection officer to exercise their rights under the GDPR. In any event, individuals may wish to use the contact details of the data protection officer to make requests to exercise rights which do not relate solely to unsubscribe and unsubscribe requests, for example a request for the right to access.41. Under these conditions, the Restricted Committee considers that the company has not complied with the provisions of Article 13 of the GDPR.42. The Restricted Committee nevertheless notes that the company has adopted measures within the framework of the sanction procedure and has justified having brought its data protection policy into conformity, which now contains the contact details of the data protection officer.43. Secondly, with regard to retention periods, the company indicated that it informed the CNIL services by email of February 5, 2019 that its data retention policy had been made available to the persons concerned on its bricoprive.com website. following the on-site inspection of 13 November 2018.44. In this regard, the Restricted Committee notes first of all that the findings made during the inspection of November 13, 2018 attest to the absence of information on retention periods in the legal notices and personal data, the general conditions of sale or any other document available on the company's website. The Restricted Committee then notes that, while during the online check of February 6, 2020, the delegation did indeed note the presence of a link to a personal data retention policy, the latter also noted that this link was inactive. Therefore, said policy was inaccessible to users, as it was not available elsewhere on the site.45. Under these conditions, the Restricted Committee considers that the breach of Article 13 of the GDPR is well established on this point since the personal data is collected from the person concerned and that the information on the retention periods appears among those to be communicated in this case, insofar as it makes it possible to guarantee fair and transparent processing of the personal data concerned. Thus, for example, information on storage periods allows data subjects to know for how long the data is kept by the data controller and, consequently, for how long they can exercise their right of access.46 . The Restricted Committee nevertheless notes that, in the context of the sanction procedure, the company has justified having brought its data protection policy into conformity, which now contains the information relating to the retention periods for the data processed.47. Thirdly, with regard to the information relating to the legal bases, the company has not disputed that until October 30, 2020, no information relating to the legal bases was made available to the persons concerned in the document titled legal notice and personal data . However, it argued that it cannot be blamed for a total lack of information relating to the legal bases insofar as

some of them were available through different media, for example in the general conditions of sale, and that a build job was in progress at the time of the .48 checks. The Restricted Committee notes that until October 30, 2020, the persons concerned were not informed of all the legal bases of the processing carried out. In any event, while certain information was available in other documents, the Restricted Committee notes that they were not exhaustive, and furthermore that the accessibility and provision of information at the time of collection of the data of the data subject is a requirement pursuant to Recital 61 and Articles 12 and 13 of the GDPR.49. In view of the foregoing, the Restricted Committee considers that the company did not comply with the provisions of Article 13 of the GDPR.50. The Restricted Committee nevertheless notes that, during the sanction procedure, the company demonstrated that it had brought its data protection policy into conformity, which now contains full information on the legal bases.51. Fourthly, with regard to the information relating to the rights of the persons concerned, the company maintained that the absence of mention of certain IT rights and freedoms on the bricoprive.com site results from a simple oversight and does not constitute in no case a desire on the part of Brico Privé to prevent the exercise of certain rights by the persons concerned .52. The Restricted Committee nevertheless notes that, during the checks carried out on November 13, 2018 and February 6, 2020, the delegation of control found that the company did not inform the persons concerned of their rights to limitation of processing, portability data as well as that of lodging a complaint with a supervisory authority.53. Under these conditions, the Restricted Committee considers that the breach of Article 13 of the GDPR is established on this point when the personal data is collected from the data subject and the information missing in this case is among those to be communicated in this case. Indeed, informing people of all their rights helps to guarantee fair and transparent processing, in that it facilitates their exercise and thus helps to ensure that the people concerned have control over the processing of their data.54 . The Restricted Committee nevertheless notes that the company has justified having brought its data protection policy into compliance, which now contains complete information on the rights of the persons concerned. In addition, the company indicates that it has posted a page intended for the description of the rights from which individuals benefit under the GDPR, accessible via a link at the bottom of each page of its site.55. Therefore, the Restricted Committee considers that the aforementioned facts constitute a breach of Article 13 of the GDPR, but that the company complied on the closing date of the investigation on all the points raised.C .On the failure to comply with the request to erase personal data pursuant to Article 17 of the GDPR56. Pursuant to Article 17 of the GDPR, the data subject has the right to obtain from the data controller the erasure, as soon as possible, of personal data concerning him and the data controller has the obligation to

erase such personal data without undue delay where one of the following grounds applies: a) the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed; b ) the data subject withdraws the consent on which the processing is based in accordance with Article 6(1)(a) (…) and there is no other legal basis for the processing; c) the data subject s objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2) (… ) .57. During the control of November 13, 2018, the control delegation was informed that when a person requests the deletion of their account, the company does not delete the personal data but only deactivates the account in question, preventing the person to connect to it and blocking the sending of commercial prospecting. The delegation thus noted the presence in the database of the personal data of a customer of the company (surname, first name and e-mail address) who had previously made a request for erasure by e-mail. Access to his account had simply been disabled.58. The Restricted Committee holds that it is thus established that the company did not fully comply with the requests for erasure.59. The Restricted Committee considers that if, after a request for erasure, certain personal data of customers may be kept in intermediate archiving, in particular under legal obligations or for probative purposes or when the company has a compelling legitimate reason , those not necessary in the context of compliance with these other obligations or purposes must be deleted after the exercise of this right when the conditions set out in Article 17 of the GDPR are met. It notes in this respect that this was at least the case for the processing of the electronic address used for commercial prospecting purposes, since this processing is based on consent and the right to erasure is open in case of withdrawal of consent, and that it does not appear from the elements of the procedure that the retention of the data in question was legitimate on another basis.60. In view of the foregoing, the Restricted Committee considers that the breach of Article 17 of the GDPR has been established.61. It nevertheless notes that, in the context of the sanction procedure, the company justified having taken measures to comply with Article 17 of the GDPR.62. The company first justified having erased the data of the customer who had exercised his right to erasure. It then specified that it had taken various measures to improve the processing of requests to exercise rights, by centralizing the receipt of requests, by putting online a form for exercising rights - downloadable online via a direct link inserted on the information dedicated to the rights of individuals - and by creating the email address dpo@bricoprive.com, dedicated to questions relating to personal data and managed by the company's data protection officer. In addition, the company indicated that it has put in place a document containing model letters of response to requests to exercise rights, including a letter of response to requests to exercise the right to erasure. Finally, the company has

undertaken to set up a tracking system for requests to exercise rights in a specific tool. D. On the breach relating to the obligation to ensure the security of personal data in application of article 32 of the GDPR63. Pursuant to Article 32 of the GDPR 1. Taking into account the state of knowledge, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risks, the degree of which probability and severity varies, for the rights and freedoms of natural persons, the controller and the processor implement the appropriate technical and organizational measures to guarantee a level of security appropriate to the risk, including, among other things, as required:a) pseudonymization and encryption of personal data;b) means to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;c) means to to restore the availability of personal data and access to them within appropriate timeframes in the event of a physical or technical incident; d) a procedure for testing, analyzing and evaluating regularly the effectiveness of the technical and organizational measures to ensure the security of the processing […].64. Firstly, the rapporteur notes first of all that at the time of the check on November 13, 2018, authentication when creating an account on the bricoprive.com site was based on a password consisting of only six characters digital, type 123456 . The rapporteur then notes that, with regard to the company's employees, the password to access the customer relationship management software […] was made up of eight characters, containing at least one number and one letter. Finally, the rapporteur notes that the authentication of employees to the databases was insufficiently secure due to the storage of the passwords allowing access to them, in clear text, in a text file contained on a company computer.65. In defence, the company does not dispute these facts, but argues that the security obligation resulting from article 32 of the GDPR was an obligation of means and not of result, so that the security obligation of the data controller consists to implement measures to reduce the risks to an acceptable level, without it being mandatory, or even possible, to obtain a level of safety making them zero. The company also pointed out that it has never suffered a personal data breach.66. The Restricted Committee considers that the absence of a personal data breach is not sufficient to demonstrate the absence of a breach, any more than a data breach is in itself sufficient to characterize a breach of Article 32 of the GDPR. It is up to the restricted training to verify that the data controller or, where applicable, the subcontractor, has implemented, in application of this article, appropriate technical and organizational measures to prevent the risks of violations and misuse. of this data. The appropriateness of the measures is assessed by verifying that the defendant has proportioned these measures, in the state of the information available to him through reasonable diligence, to the seriousness and probability of the foreseeable risks, according to the nature and context of the data processing, as well as the cost and

complexity of possible measures.67. The Restricted Committee then considers that the length and complexity of a password remain basic criteria for assessing its strength. It notes in this regard that the need for a strong password is also emphasized by the National Information Systems Security Agency.68. By way of clarification, the Restricted Committee recalls that to ensure a sufficient level of security and meet the robustness requirements of passwords, when authentication is based solely on an identifier and a password, the CNIL recommends, in its deliberation no. 2017-012 of January 19, 2017, that the password has at least twelve characters - containing at least one uppercase letter, one lowercase letter, one number and one special character - or has at least eight characters - containing three of these four categories of characteristics - if it is accompanied by an additional measure such as, for example, the delay of access to the account after several failures (temporary suspension of access, the duration of which increases as attempts are made), the implementation of a mechanism to guard against automated and intensive submissions of attempts (such as a captcha) and/or blocking of the account after several authentication attempts unsuccessful cation.69. In this case, the Restricted Committee considers that with regard to the undemanding rules governing their composition, the robustness of the passwords accepted by the company was too weak, leading to a risk of compromise of the associated accounts and personal data. they contain.70. Finally, the Restricted Committee points out that storing passwords for accessing databases in plain text in a text file contained on a company computer is not a secure password management solution. In fact, authentication based on the use of a short or simple password can lead to attacks by unauthorized third parties, such as brute force attacks which consist in successively and systematically testing numerous passwords password and thus allow the associated accounts and the data they contain to be compromised.71. Under these conditions, the Restricted Committee considers that the password management policy of the company in question was not sufficiently robust and restrictive to guarantee data security, within the meaning of Article 32 of the GDPR.72. It nevertheless notes that, in the context of the sanction procedure, the company indicated, with regard to customer accounts, that it now requires a strong password comprising a minimum of twelve characters, including one uppercase letter, one lowercase letter, one numeric character and a special character, which was corroborated by a screen print. For employees, the company has implemented a strong password to access the customer relationship management software […]. Regarding the storage of database access passwords in a clear file, it justified having stopped this practice and set up a secure password management solution, by subscribing to the solution [… ] which guarantees encrypted storage of passwords.73. Secondly, the rapporteur notes that the hash function used to store the passwords of employee users of the

bricoprive.com site was obsolete (MD5).74. In defence, the company does not dispute these facts, but takes up the same argument on the obligation of means.75. The Restricted Committee recalls that the use of the MD5 hash function by the company is no longer considered to be state-of-the-art since 2004 and its use in cryptography or security is prohibited. Thus, the use of this algorithm would allow a person having knowledge of the hashed password to decipher it without difficulty in a very short time (for example, by means of freely accessible Internet sites which make it possible to find the value corresponding to the password hash).76. Under these conditions, given the risks incurred by the persons mentioned above, the Restricted Committee considers that the hashing system used did not make it possible to guarantee the security of the data, within the meaning of Article 32 of the GDPR.77. It nevertheless notes that, in the context of the penalty proceedings, the company demonstrated that it had implemented a satisfactory system for hashing, in SHA256, all of the users' passwords.78. Thirdly, the rapporteur notes that the employees of the company had access to a copy of the BRICO PRIVÉ production database through an account shared by four employees.79. In defence, the company does not dispute these facts, but takes up the same argument on the obligation of means.80. The Restricted Committee recalls that the allocation of a unique identifier per user and the prohibition of shared accounts are among the essential precautions in order to guarantee effective traceability of access to a database. In this case, the sharing of the account allowing access to the copy of the production database by four employees does not make it possible to guarantee correct authentication of users and, consequently, effective management of authorizations and correct traceability. accesses. Such a lack of traceability of access thus does not make it possible to identify fraudulent access or the author of any deterioration or deletion of personal data.81. Under these conditions, the Restricted Committee considers that the use of a generic account does not guarantee data security, within the meaning of Article 32 of the GDPR.82. It nevertheless notes that, within the framework of the sanction procedure, the company justified having taken measures by setting up an authentication system by accredited user.E.On the breach of obligations relating to information (cookies) stored on the electronic communications terminal equipment of users pursuant to article 82 of the Data Protection Act 83. Article 82 of the Data Protection Act requires that users be informed and that their consent be obtained before any data processing operation. registration or access to information already stored in their equipment. Any deposit of cookies or other tracers must therefore be preceded by the information and consent of the persons. This requirement does not apply to cookies whose exclusive purpose is to allow or facilitate communication by electronic means or being strictly necessary for the provision of an online communication service at the express request of the user .84. The

rapporteur considers that the company did not comply with these provisions since it appears from the online checks of February 6, 2020 and January 13, 2021 that when arriving on the bricoprive.com website several cookies do not fall within the scope of the two exceptions mentioned above were placed on the user's terminal as soon as he arrived on the site's home page, and before any action on his part.85. The company does not contest these facts.86. The Restricted Committee notes that it appears from the findings made during the online check of February 6, 2020 that the deposit of thirty-two cookies was automatic upon arrival on the home page of the site, and before any action of the user. In response to a request for additional services from the CNIL, the company indicated on March 4, 2020 that the purposes of the cookies deposited consist of having a better knowledge of customers, better advertising targeting and personalizing the offer and promotional operations. .87. The Restricted Committee also notes that, even though the company had stated, in its observations in response of December 16, 2020, to have ceased, since November 10, 2020, to deposit cookies subject to consent automatically upon the arrival of users on its site, the delegation noted, during the online check of January 13, 2021, the deposit of thirteen cookies as soon as it arrived on the site. By email of January 26, 2021, the company sent the additional documents requested during the check and confirmed in particular that, among the said cookies deposited, some had an advertising purpose.88. Therefore, the cookies deposited not having the exclusive purpose of allowing or facilitating communication by electronic means and not being strictly necessary for the provision of the service, their deposit required the company to obtain the consent of the users beforehand. 89. The Restricted Committee therefore considers that a breach of Article 82 of the Data Protection Act has been constituted.90. The Restricted Committee nevertheless points out that the company made significant changes to its website during the sanction procedure and that the cookies for which the consent of the users is required are no longer automatically deposited in the user's terminal at arrival on the home page of the site since January 26, 2021. F. On the breach relating to the obligation to obtain the consent of the person concerned by a direct prospecting operation by means of an e-mail in application of the article L. 34-5 of the CPCE91. Under the terms of Article L. 34-5 of the CPCE: Direct prospecting by means of an automated electronic communications system within the meaning of 6° of Article L. 32, a fax machine or electronic mail using the contact details of a natural person, subscriber or user, who has not previously expressed his consent to receive direct prospecting by this means. For the purposes of this article, consent means any expression of free, specific and informed will by which a person accepts that personal data concerning him be used for the purpose of direct marketing. […] However, direct prospecting by e-mail is authorized if the recipient's contact details have been collected from him, in compliance with the

provisions of law n ° 78-17 of January 6, 1978 relating to data processing, files and freedoms. , on the occasion of a sale or the provision of services, if the direct prospecting concerns similar products or services provided by the same natural or legal person, and if the recipient is offered, expressly and without ambiguity, the possibility of opposing, free of charge, except those linked to the transmission of the refusal, and in a simple manner, the use of his contact details at the time they are collected and each time a prospecting e-mail is sent to him in case he has not refused such use from the outset .92. The rapporteur notes that during the checks carried out on 13 November 2018 and 6 February 2020, the delegation noted that, when creating an account without a purchase act on the company's website, no process aimed at obtaining consent to the collection and processing of personal data for the purposes of commercial prospecting by e-mail was not implemented.93. In defence, the company maintains that because of the information notices present on the site, the people who created an account could not be unaware that the company would regularly send them commercial communications by e-mail. It also reminds that to validate a registration when creating an account on the company's website, the person must accept the general conditions of sale of the company which provide that their personal data will be used by the company in order to inform him by e-mail of upcoming sales and special offers.94. The Restricted Committee considers that the creation of an account does not prejudge the possible ordering of products from the company BRICO PRIVÉ. The Restricted Committee considers that in the absence of a purchase, the company cannot usefully invoke the benefit of the exception created by article L. 34-5 of the CPCE allowing prospecting without prior consent when the contact details of the recipient have been collected from him on the occasion of a sale or the provision of services if the direct marketing concerns similar products or services provided by the same natural or legal person.95. Therefore, the Restricted Committee considers that it was up to the company to obtain the prior, free, specific and informed consent of persons creating an account on the company's website without having made a purchase, to receive prospecting messages directly by e-mail, in accordance with paragraph 1 of article L. 34-5 of the CPCE.96. Under these conditions, the Restricted Committee considers that the breach of Article L. 34-5 of the CPCE is constituted. As part of the procedure, the company has justified having inserted on the online account creation form a box to tick allowing specific and unambiguous consent to be taken into account for people wishing to create an account in the future.97. For people who already had an account on the bricoprive.com site, the company indicates that it plans to send prospecting emails only to people who have already made a purchase on its site. She also indicates that she sent emails to obtain the agreement of […] prospects who had not yet given their consent to receive prospecting electronically or made a purchase following the creation

of their account. .98. During the restricted training session, the company also specified that in order to comply with the provisions of article L. 34-5 of the CPCE, it intended to send to each prospect who had not yet given their consent five emails aimed at obtaining their agreement to receive prospecting electronically. These five emails would be sent within a period of 100 days from the prospect's last activity date. The company has indicated that after 100 days of inactivity on the part of the prospect and without the latter's consent to receive commercial prospecting following the five emails it will have sent to him, it will stop prospecting him. 99. The Restricted Committee considers that soliciting the persons in question to ask them if they wish to receive prospecting emails constitutes in itself processing which can only be based, in this case, on a possible legitimate interest of the company. It appears from the documents in the file that the prospects, by choosing to create an account on the company's site to have access to its offers, have shown a certain interest in the services offered by the latter and that, therefore, they can reasonably expect the company to contact them. However, it considers that sending prospects five emails, a fortiori during a period of 100 days, exceeds the number of emails that they could reasonably expect.100. Under these conditions, the Restricted Committee considers that the company did not fully comply on the closing date of the investigation.III. On corrective measures and their publicity101. Under the terms of III of article 20 of the law of January 6, 1978 as amended: When the data controller or its subcontractor does not comply with the obligations resulting from regulation (EU) 2016/679 of April 27, 2016 or from this law, the President of the National Commission for Computing and Liberties may also, if necessary after having sent him the warning provided for in I of this article or, if necessary in addition to a formal notice provided for in II , seize the restricted formation of the commission with a view to the pronouncement, after adversarial procedure, of one or more of the following measures: […] 2° An injunction to bring the processing into conformity with the obligations resulting from the regulation (EU) 2016/679 of April 27, 2016 or of this law or to satisfy the requests presented by the person concerned in order to exercise their rights, which may be accompanied, except in cases where the processing is implemented by the State , of a penalty whose mon both cannot exceed €100,000 per day of delay from the date set by the restricted committee; […] 7° With the exception of cases where the processing is implemented by the State, an administrative fine not exceeding 10 million euros or, in the case of a company, 2% of the turnover total worldwide annual business for the previous fiscal year, whichever is greater. In the cases mentioned in 5 and 6 of Article 83 of Regulation (EU) 2016/679 of April 27, 2016, these ceilings are increased, respectively, to 20 million euros and 4% of said turnover. The restricted committee takes into account, in determining the amount of the fine, the criteria specified in the same article 83. Article 83 of the GDPR

provides that each supervisory authority shall ensure that the administrative fines imposed under this article for breaches of this Regulation referred to in paragraphs 4, 5 and 6 are in each case effective, proportionate and dissuasive, before specifying the elements to be taken into account in deciding whether to impose an administrative fine and to decide on the amount of this fine.102. First, on the principle of imposing a fine, the company argues that such a measure is not justified. It emphasizes in particular that it has never been condemned by the Restricted Committee, that the aforementioned breaches do not in any way constitute a deliberate violation of the GDPR, that the persons concerned have not suffered any damage, that no particular data referred to in Articles 9 and 10 of the GDPR is concerned, that it has cooperated in good faith with the CNIL throughout the procedure and that it has taken compliance measures.103. The Restricted Committee recalls that it must take into account, for the pronouncement of an administrative fine, the criteria specified in Article 83 of the GDPR, such as the nature, gravity and duration of the violation, the measures taken by the controller to mitigate the damage suffered by data subjects, the degree of cooperation with the supervisory authority and the categories of personal data affected by the breach.104. The Restricted Committee firstly considers that the company has shown gross negligence with regard to the fundamental principles of the GDPR since six breaches have been established, relating in particular to the principle of limiting the duration of data retention, the obligation to inform data subjects of the processing of their personal data and that of respecting their rights.105. The Restricted Committee then notes that several breaches noted concerned a large number of people, namely […] users in France, […] in Spain, […] in Italy and […] in Portugal.106. Finally, the Restricted Committee notes that the compliance measures put in place following the notification of the sanction report do not concern all the breaches and do not exonerate the company from its responsibility for the past, in particular in view of the shortcomings noted.,107. Consequently, the Restricted Committee considers that an administrative fine should be imposed with regard to the breaches of Articles 5-1-e), 13, 17 and 32 of the GDPR, 82 of the Data Protection Act and L. 34 -5 of CPCE.108. Secondly, with regard to the amount of the fine for breaches of the GDPR, the Restricted Committee recalls that paragraph 3 of Article 83 of the Rules provides that in the event of multiple breaches, as is the case in In this case, the total amount of the fine cannot exceed the amount set for the most serious violation. Insofar as the company is accused of breaching Articles 5-1-e), 13, 17 and 32 of the Regulations, the maximum amount of the fine that may be withheld is 20 million euros or 4 % of worldwide annual turnover, whichever is higher.109. With regard to the amount of the fine relating to the breach of Article 82 of the Data Protection Act and Article L.34-5 of the CPCE, the Restricted Committee recalls that with regard to the breaches of provisions originating in texts other

than the GDPR, as is the case with article L.34-5 of the CPCE which transposes the ePrivacy directive into domestic law, article 20 paragraph III of the Data Protection Act and Libertés gives it jurisdiction to pronounce various sanctions, in particular an administrative fine, the maximum amount of which may be equivalent to 2% of the total worldwide annual turnover of the previous financial year carried out by the data controller. In addition, the determination of the amount of this fine is also assessed with regard to the criteria specified by Article 83 of the GDPR.110. The Restricted Committee also recalls that administrative fines must be dissuasive but proportionate. It considers in particular that the activity of the company and its financial situation must be taken into account for the determination of the sanction and in particular, in the event of an administrative fine, of its amount. It notes in this respect that the company reports a turnover from 2018 to 2020 of around […] euros, then around […] euros and finally around […] euros for a net result respectively. EUR […], then EUR […] and finally EUR […]. She deduces from this that the amount of the fine proposed by the rapporteur is far from reaching the maximum amount of the financial penalty provided for by the GDPR since it represents a maximum of […]% of the company's turnover. In view of these elements, the Restricted Committee considers that the imposition of a fine of 500,000 euros appears justified, i.e. 300,000 euros for breaches of Articles 5-1-e), 13, 17 and 32 of the GDPR and 200,000 euros for breaches of article 82 of the Data Protection Act and article L. 34-5 of the CPCE.111. Thirdly, an injunction to bring the processing into compliance with the provisions of Articles 5-1-e) of the GDPR and L. 34-5 of the CPCE was proposed by the rapporteur when notifying the report.112. The company maintains that the actions it has taken with regard to all of the shortcomings identified should lead to the non-compliance with the rapporteur's proposal for injunctions.113. With regard to the breach of the obligation to define and comply with a retention period for personal data proportionate to the purpose of the processing pursuant to Article 5-1-e) of the GDPR, the company indicates that it has implemented set up an internal procedure to archive and then anonymize the data.114. The Restricted Committee considers, however, that the company had not provided, on the date of the closing of the investigation, elements allowing it to certify compliance on this point. In any case, it considers that the elements produced during the meeting are not sufficient to rule at this stage on its possible compliance with Article 5-1-e) of the GDPR.115. With regard to the breach relating to the obligation to obtain the consent of the person concerned by a direct marketing operation by means of an automated electronic communications system pursuant to Article L. 34-5 of the CPCE, the training Restricted considers that the company has taken satisfactory measures to now obtain people's consent when creating an account on the bricoprive.com website. The Restricted Committee also notes that the company has undertaken, as part of the procedure, to

no longer send direct prospecting messages by e-mail to prospects without their prior consent. However, it considers that it has not demonstrated its complete compliance with Article L. 34-5 of the CPCE insofar as it intends to seek the agreement of persons who have created an account in the past up to five times. Consequently, the Restricted Committee considers that an injunction should be issued on this point.116. Fourthly, the restricted committee considers that the publicity of the sanction is justified with regard to the plurality of breaches noted, their persistence, their seriousness and the number of people concerned.FOR THESE REASONSThe restricted committee of the CNIL, after having deliberated, decides to: pronounce against BRICO PRIVÉ an administrative fine in the amount of 500,000 (five hundred thousand) euros, which breaks down as follows: 300,000 (three hundred thousand) euros for the breaches to Articles 5-1-e), 13, 17 and 32 of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 (hereinafter the GDPR); 200,000 (two hundred thousand) euros for breaches of article 82 of law no. 78-17 of January 6, 1978 relating to data processing, files and freedoms as amended and of article L. 34-5 of the postal and electronic communications code (hereafter after the CPCE); pronounce against the company BRICO PRIVÉ an injunction to put in formed the processing with the obligations resulting from articles and 5-1-e) of the GDPR and L. 34-5 of the CPCE, and in particular: with regard to the breach of the principle of limitation of the retention period of personal data , implement a policy for the retention of personal data that does not exceed the duration necessary for the purposes for which they are collected and processed, and in particular: stop retaining the personal data of former customers of the website of the company at the end of the fixed period of inactivity, proceed with the purging of such data kept by the company until the date of the deliberation of the restricted formation and justify the deletion of this personal data at the - beyond a defined period of inactivity, which it will be up to the company to justify; justify an intermediate archiving procedure for customers' personal data, put in place after having sorted the relevant data to be archived and deleted irrelevant data, as well as the starting point of this archiving (for example, with regard to invoices archived for accounting purposes); with regard to the breach of the obligation to obtain the consent of the person concerned by a direct prospecting operation by means of an automated electronic communications system: stop prospecting non-customers who have not expressed their consent, except to obtain their consent; a penalty payment of 500 (five hundred) euros per day of delay at the end of a period of three months following the notification of this deliberation, the supporting documents of compliance must be sent to the restricted training in this period; make public, on the CNIL website and on the Légifrance website, its deliberation, which will no longer identify the company by name at the end of a period of two years from its p Publication.The PresidentAlexandre

LINDEN