Deliberation SAN-2023-003 of March 16, 2023 National Commission for Computing and Liberties Nature of the deliberation: Sanction Legal status: In force Date of publication on Légifrance: Tuesday March 28, 2023 Deliberation of the restricted committee no. SAN-2023-003 of 16 March 2023 concerning the company CITYSCOOTThe National Commission for Computing and Liberties, meeting in its restricted formation composed of Mr. Alexandre LINDEN, president, Mr. Philippe-Pierre CABOURDIN, vice-president, Mrs. Christine MAUGÜÉ, Mrs. Anne DEBET, Mr. Bertrand du MARAIS and Mr Alain DRU, members; Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 relating to the protection of personal data and the free movement of such data, in particular Articles 56 and 60; Considering the law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms in particular its articles 20 and following; Considering the decree n° 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 internal regulations of the National Commission for Data Processing and liberties; Having regard to decision no. 2020-081C of 12 May 2020 of the President of the National Commission for Computing and Liberties to instruct the Secretary General to carry out or to have carried out a mission to verify any processing accessible from of the "cityscoot.eu" domain and the "CITYSCOOT" mobile application; Having regard to the decision of the President of the National Commission for Data Processing and Freedoms appointing a rapporteur before the restricted committee, dated April 12, 2021 ; Considering the report of Mrs. Valérie PEUGEOT, commissioner rapporteur, notified to the company CITYSCOOT on March 17, 2022; Having regard to the written observations submitted by the company CITYSCOOT on May 2, 2022; Having regard to the response of the rapporteur notified to the company on June 16, 2022 ; Having regard to the written observations submitted by CITYSCOOT on July 29, 2022, as well as the oral observations made during the restricted training session; Having regard to the other documents in the file; Were present, during the restricted training session of 29 September 2022:- Mrs. Valérie Peugeot, commissioner, heard in her report;As representatives of the company CITYSCOOT:[…] The company CITYSCOOT having the floor last;The restricted committee adopted the following decision:I. Facts and procedure1. CITYSCOOT (hereinafter "the company") is a simplified joint-stock company with capital of 121,002.10 euros, located at 8 rue Bayen in Paris (75017), created in 2014. The company estimates its workforce in France at 225 people. In 2019, it achieved a turnover of 21,882,031 euros for a net loss of 12,641,302 euros. In a letter dated April 21, 2021, the company estimated its turnover for the financial year ended December 31, 2020 at an amount of […].2. Since 2016, the company has offered a self-service electric scooter rental service accessible

from the "CITYSCOOT" mobile application. This is a "freefloating" shared vehicle offer, i.e. characterized by the absence of stations. The scooters are not parked in specific spaces and can be left, after use, in the rental area identified in the application. The scooters are equipped with an on-board location device that allows CITYSCOOT and users, via their mobile application, to know the position of the scooters. Renting an electric scooter from the company requires creating an account from the mobile application. This is a non-binding service that is billed by the minute.3. In France, this service is available in the Paris region and in Nice. In addition, the company has also developed its service in certain cities in Italy and Spain through two wholly-owned subsidiaries, CITYSCOOT ITALIA S.R.L. and CITYSCOOT ESPANA SL. The company currently has approximately 247,000 users in France and abroad.4. An online check was carried out on the "cityscoot.eu" website and the "CITYSCOOT" mobile application on May 13, 2020. Report no. 2020-081/1, drawn up by the delegation on the day of the check , was notified to the company on May 19, 2020. The CNIL delegation took particular care to verify the data collected and the purposes of the collection. This control was also intended to verify the supervision of subcontracting and data security.5. Three requests for additional information were then sent to the company by registered letter with acknowledgment of receipt dated June 26, 2020 and by emails dated August 27 and December 10, 2020. The company responded to these requests by letters dated July 16, September 11 and December 15, 2020.6. In accordance with Article 56 of the GDPR, the CNIL has informed all the European supervisory authorities of its competence to act as lead supervisory authority concerning the cross-border processing implemented by CITYSCOOT, namely the management user accounts and tools set up by the company, resulting from the company's main establishment being in France. After an exchange between the CNIL and the European data protection authorities within the framework of the one-stop-shop mechanism, Spain and Italy have declared themselves to be concerned by said processing.7. For the purposes of investigating these elements, the Chairperson of the Commission appointed Mrs Valérie PEUGEOT as rapporteur, on April 12, 2021, on the basis of Article 22 of the law of January 6, 1978 as amended.8. On February 17, 2022, the rapporteur sent the company an additional request relating to the anonymization of personal data carried out by hashing the data and applying a salt. The company replied by letter dated February 23, 2022.9. The rapporteur notified CITYSCOOT, on March 17, 2022, of a report detailing the breaches of the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 (hereinafter "the Regulation" or the "RGPD") and the modified law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms (hereinafter "the Data Protection Act" or "modified law of January 6, 1978") which it considered constituted in this case. This

report proposed that the restricted committee of the Commission impose an administrative fine on the company and make the decision public, but that it would no longer be possible to identify the company by name at the end of a period two years from its publication.10. On May 2, 2022, the company produced its observations in response to the sanction report.11. By letter dated June 16, 2022, the rapporteur's response was sent to the company.12. On July 29, 2022, the company submitted new observations in response to those of the rapporteur.13. By letter dated August 22, 2022, the rapporteur informed the company of the closure of the investigation.14. On August 23, 2022, the chairman of the Restricted Committee notified CITYSCOOT of a notice to attend the meeting of September 29, 2022. II. Reasons for decision15. Pursuant to Article 60, paragraph 3 of the GDPR, the draft decision adopted by the Restricted Committee was sent on February 15, 2023 to the European supervisory authorities concerned.16. As of March 15, 2023, none of the supervisory authorities concerned had raised a relevant and reasoned objection to this draft decision, so that, pursuant to Article 60(6) of the GDPR, these latter are deemed to have approved it.A. On the breach relating to the obligation to ensure the adequacy, relevance and non-excessive nature of the personal data processed pursuant to Article 5, paragraph 1, c) of the GDPR17. Article 5, paragraph 1, c) of the GDPR provides that personal data must be “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimization)”. When data is collected on the basis of legitimate interest, this collection must also not cause a disproportionate invasion of privacy, with regard to the objectives pursued by the company.18. The rapporteur notes that, as part of the investigation, the CNIL's control delegation was informed that the scooters are equipped with electronic boxes including a SIM card and a GPS geolocation system, on board the scooters. These boxes collect position data from the scooters every 30 seconds when the CITYSCOOT is active and its dashboard is on, whether it is moving or ready to roll. When the CITYSCOOT is inactive, the box collects position data every 15 minutes.19. These data are stored in "a scooter database" which contains the following data in particular: the position via the GPS and "a reservation number […] which are collected in the event that the Cityscoot is reserved, during the rental period ". They are kept for 12 months in an active database, then 12 months in intermediate archiving before being anonymized.20. The position data of the scooters, namely the location of the scooter at the point of departure and arrival of the reservation and the location during the entire journey are collected by the company for the following purposes: processing of traffic violations, processing of customer complaints, user support (in order to call for help in the event of a user falling), claims and theft management.21. To end the rental, the user must perform certain operations such as: make sure to be in an area authorized to park scooters (CITYSCOOT area), switch off the scooter, press

the "END" button located on the scooter or click on "FINISH MY RENTAL" in the mobile application and check that the green "FREE" LED is on.22. The rapporteur considers that none of the purposes put forward by the company justifies an almost permanent collection of geolocation data during the rental of a scooter.23. It is necessary to examine the relevance of the collection of this data for each of these purposes. As a preliminary point, the Restricted Committee points out that, when a vehicle is being rented, the geolocation data from this vehicle is associated with a person and constitutes personal data. On the other hand, when the scooter is not rented, the geolocation data linked to the vehicle alone are not personal data.24. The Restricted Committee notes that the company uses three separate databases:- a "scooter database" which contains the data reported by the sensors attached to the scooter (position of the scooter via a GPS, battery status, sensor of the saddle);- a "reservation database" which contains the dates and times of the start and end of each rental as well as the status of the scooter at the start and end of its rental;- a "customer database" which includes the data used to manage billing, the latter database not containing data relating to the scooter.25. The Restricted Committee notes that, if the position data of the scooters are uncorrelated from any information relating to the users in the "scooter database" and are kept in a separate database from that storing the data relating to the users, namely the "base of customer data", which constitutes a choice of IT architecture that respects privacy (privacy by design), the fact remains that this data can be cross-checked with the data present in the other databases, in particular by the through the reservation number present in each of the databases, by having extensive and simultaneous access to the databases.26. The Restricted Committee therefore considers that the geolocation data collected by CITYSCOOT when the scooter is being rented is personal data when a reconciliation is possible between the different databases, even if this reconciliation would not be only occasionally, scooter position data relating to an identified or identifiable natural person.27. In addition, the Restricted Committee notes that, although geolocation data is not sensitive data, within the meaning of Article 9 of the GDPR, it is nevertheless considered by the Article 29 working group (known as "G29") which became the European Data Protection Board (EDPB)) in its guidelines of October 4, 2017, as "highly personal data". The EDPS considers that these data are considered sensitive, in the common sense of the term, insofar as they have an impact on the exercise of a fundamental right: the collection of location data involves the freedom of movement.28 . By way of clarification, the Restricted Committee also recalls that the EDPS considered, in its guidelines 01/2020 relating to the processing of personal data in the context of connected vehicles and mobility-related applications (guidelines 01 /2020) that "when collecting personal data, vehicle and equipment manufacturers, service providers and other data controllers should bear

in mind that location data is particularly indicative of habits The journeys made are very characteristic in that they can make it possible to deduce the place of work, the residence as well as the centers of interest (leisures) of the driver, and can possibly reveal sensitive information such as the religion, through place of worship, or sexual orientation, through places frequented. Therefore, vehicle and equipment manufacturers, service providers and other controllers should take particular care not to collect location data, unless absolutely necessary for the purpose of the processing". These guidelines also emphasize that the collection of location data is subject to compliance with the principle that location can be activated "only when the user initiates a feature that requires knowing the location of the vehicle, and not by default and continuously when starting the car ".29. Although the company disputes the applicability of the guidelines to the present case, on the grounds that they only concern automobiles, the Restricted Committee considers that the guidelines provide relevant insight into geolocation data in general. 30. In this context, the Restricted Committee recalls that the assessment of compliance with the principle of data minimization is based on the limited nature of the data processed to what is necessary with regard to the purpose for which they are collected. Its assessment involves carrying out a necessity analysis of the personal data collected with regard to the intended purposes.31. In view of the foregoing, the Restricted Committee considers that it is appropriate to analyze only the need to collect and store position data collected every 30 seconds, since the collection of position data at the start and at the end of the tenancy is relevant with regard to the purposes pursued.32. Firstly, with regard to the management of complaints related to overbilling, the rapporteur considers that the collection of geolocation data every thirty seconds for the duration of the rental is not necessary. It specifies that the management of overbilling should be managed by contacting the user when he encounters difficulty in terminating his rental or, at the very least, by less intrusive means than quasi-geolocation. of the vehicle being rented.33. In defence, the company argues that the collection of scooter position data every 30 seconds would be necessary, as part of a service billed by the minute for situations that have generated overcharging and complaints from users when they have failed to terminate their rental correctly, in particular when: - the user loses communication with a scooter for technical or human reasons; - the user makes a complaint related to unauthorized parking areas; - the user does not stop the scooter correctly to end the rental; - the scooter has been moved by a third party.34. Collecting position data every 30 seconds would allow backtracking in 30-second increments to identify how many seconds the scooter has been stationary. She adds that users realize, very often after the fact, that the rental has not been properly terminated and do not engage with the company when ending the rental. The triggering of geolocation when the user makes contact would therefore not suffice because it

would not be possible to calculate the overcharged minutes between the time when the user wished to end the rental and did not been able to do so, and when the company was able to fix the problem and end the tenancy.35. The Restricted Committee takes note of the arguments put forward by the company to manage complaints related to overbilling. However, it points out that, for that purpose, the collection and storage of scooter geolocation data every 30 seconds is not necessary.36. Indeed, in three of the cases mentioned by the company (loss of communication with the scooter, difficulty linked to unauthorized areas, scooter moved by a third party), the Restricted Committee considers that the user can contact the company CITYSCOOT to resolve difficulties and terminate the tenancy. Geolocation could therefore be triggered on the basis of this operative event.37. With regard to cases where the user does not stop the scooter properly to end the rental, the Restricted Panel points out that the geolocation of the scooter every 30 seconds does not make it possible to determine when the user actually wanted terminate his tenancy. Indeed, the static position of the scooter, in itself, does not demonstrate the user's desire not to continue his rental.38. In addition, the Restricted Committee specifies that it would be possible to set up alternative and less intrusive mechanisms allowing the company to ensure that the user has indeed terminated the rental or, on the contrary, to notify him when this is not the case, for example by sending an SMS or confirmation, by an alert via the application, that the rental has ended.39. While the company claims to have received, for the month of June 2022, approximately 11,500 calls out of 386,766 trips relating to overbilling problems, it does not indicate the share of calls related to this specific case. The Restricted Committee considers, in the absence of precise statistics, that these cases cannot justify the almost permanent geolocation of all scooters.40. Moreover, the Restricted Committee notes that Article 7.4.6 of CITYSCOOT's general conditions of use provides that "it is the User's responsibility to check that the end of his Rental is effective. CITYSCOOT cannot be held liable for extended billing in the event of improper return of the Scooter". It is therefore up to the user to ensure that he has correctly terminated the rental.41. Secondly, with regard to the management of fines, the rapporteur considers that the geolocation data of the scooters throughout the journey are not necessary to identify the user responsible for the infringement since an overlap between the time of the offense and the person who rented the scooter during this period is sufficient to do so.42. In defence, the company claims that collecting the position of scooters every 30 seconds is necessary to obtain information about the circumstances and context of a violation. The objective is to verify whether the offense noted by the ANTAI ("National Agency for the Automated Processing of Offenses") has indeed been committed: confirm or invalidate the presence of the scooter at the location noted by the notice of offense and check whether the offense could have occurred at this location. It also

considers that the collection of scooter position data is necessary in order to be able to identify or prove the identity of the driver to ANTAI, the police or insurance companies.43. The Restricted Committee considers, on the one hand, that it is not necessary for the company to collect and keep the position of the scooters every 30 seconds to identify and prove the identity of a driver to the ANTAI, police or insurance companies. Indeed, the collection of the number and date of the notice of violation, the date and time of the start and end of the rental, the date and time of the offense are sufficient to meet this purpose. This data crossed with the license plate number of the scooter makes it possible to identify the person who rented the scooter. Moreover, the collection of scooter position data does not as such make it possible to establish the identity of the person responsible for the offense since it is not possible to determine whether the scooter has been moved. by the person who rented the scooter or if it has been moved by a third party to a bad parking area, since the scooter can be moved freely with or without the engine running.44. On the other hand, the Restricted Committee considers that the collection and storage of scooter position data, every 30 seconds, is excessive insofar as it concerns all the scooters rented by the company while it only responds 'for an incidental purpose in the event that a user needs these data to challenge a traffic violation.45. Thirdly, with regard to flight management, the rapporteur emphasizes that, in order to be considered proportionate, the processing of geolocation data must be rendered necessary for this purpose by a triggering event, such as a declaration of theft or suspicion of theft. The scooter geolocation data cannot therefore be considered necessary for the pursuit of the purpose linked to the risk of theft, before any triggering event.46. In defense, the company claims that collecting scooter data in the event of theft does not mean that this data is cross-referenced with the identity of users. She adds that she needs the position data of the scooters only to locate her scooters in order to find and recover them in the event of theft.47. The company specifies that it cannot rely solely on the indications of the last position provided by the user at the time of the declaration of theft, which are not necessarily reliable and that certain technical difficulties (empty battery, technical problem or even when the scooter is in a parking lot or an area where geotagging cannot be triggered) may prevent it from triggering geotagging remotely. It also specifies that the collection of scooter position data every 30 seconds makes it possible to considerably reduce the search area in the event of theft and that the geolocation system, which is integrated into the scooter, cannot be deactivated by a person searching to steal the scooter.48. The Restricted Committee recalls above all that, even if the company does not proceed to a reconciliation between the position data of the scooters and the data of the user to find a stolen vehicle, the possibility of making this reconciliation between the different databases data justifies that scooter position data is considered

personal data, subject to the requirements of the GDPR.49. Moreover, as the rapporteur points out, before any triggering event, the geolocation data of scooters cannot, in principle, be considered necessary for the pursuit of this purpose and their permanent or very close collection must be considered as excessive.50. By way of clarification, the Restricted Committee notes that the EDPS guidelines 01/2020 indicate that location data can only be fed back from the theft declaration and cannot be collected continuously the rest of the time. In this regard, the EDPS also recommends that the data controller clearly informs the data subject that there is no permanent tracking of the vehicle and that geolocation data can only be collected and transmitted from the declaration of vol.51. In addition, the Restricted Committee points out that the assessment of the limited nature to what is necessary, within the meaning of Article 5, paragraph 1, c) of the GDPR, is informed by the provisions of recital 39 of the GDPR, according to which " personal data should only be processed if the purpose of the processing cannot reasonably be achieved by other means". The existence of less intrusive means to achieve the same purposes must thus be taken into account, whether they are alternative means or data processed less frequently or in smaller numbers.52. First of all, the restricted training specifies that if the scooter is stolen outside a rental period, the scooter's position data is not linked to a reservation and therefore does not allow an individual to be identified. These are therefore not personal data and such a situation is therefore outside the scope of the present procedure.53. The restricted formation then considers that no flight scenario justifies the collection of position data every 30 seconds. On the one hand, the cases, the frequency of which the company has not established, where the scooter is stolen while in use, that is, when the user himself is on the scooter while it is running , should not justify the quasi-permanent collection of scooter position data. On the other hand, the scooter can be stolen when the user takes a break from his rental. In this case, the user may immediately contact the company CITYSCOOT as soon as the theft is observed at the end of the break, which will inform the company of the last position of the scooter.54. Asked about the number of vehicles found thanks to the last known position of the scooter, the company was unable to provide statistics demonstrating the effectiveness of geolocation every 30 seconds.55. Thus, the Restricted Committee emphasizes that, in the light of the foregoing considerations, the cases where, on the one hand, geolocation is the only means of knowing the last known position of the scooter and where, on the other hand, this last known position is actually close to the location of the scooter, appear limited. In these situations, the restricted training does not call into question the usefulness of knowing the last known position of the scooter thanks to the last geolocation data. However, this assumption is not sufficient to justify the collection of geolocation data every 30 seconds of all user journeys.56. In view of these considerations, the Restricted

Committee considers that, in a large part of the cases of use, the collection and storage of geolocation data every 30 seconds during the rental of the scooter is not necessary for the management of flights. The fact of systematically carrying out this collection, for the cases of use where it could be effectively useful on the basis of the legitimate interest of the company, appears to cause a disproportionate invasion of privacy. Indeed, as pointed out above, the company's collection and storage of all the journeys of scooter users leads it to handle highly personal data (see CNIL, FR, July 7, 2022, Sanction, No. SAN-2022-015, published).57. Fourthly, with regard to accident management, the rapporteur maintains that the collection of geolocation data for this purpose can only take place after a causal event, in particular the technical notification when the scooter is too inclined or a request for assistance by the customer, making this collection necessary.58. In defense, the company claims that it is necessary to collect position data from scooters every 30 seconds and cross-reference it with user data in order to be able to contact the user when the detector has sent a technical notification revealing an accident and assist this user within the framework of the declaration and the formalities of finding. She adds that accidents do not necessarily trigger a technical notification, especially when the scooter does not tilt enough. It also states that it is regularly asked by insurance companies, a posteriori, to obtain information on accidents of which it had no knowledge, such as the precise location of the scooter at the time of the accident.59. The Restricted Committee first stresses that it is legitimate for the company to want to provide assistance to users who are victims of a traffic accident while renting a scooter. However, to provide such assistance to users, the company must be aware of the occurrence of an accident.60. The Restricted Committee considers that, when the company becomes aware of the occurrence of an accident involving a rented scooter, it can geolocate this vehicle in order, if necessary, to provide assistance to the user.61. The Restricted Committee considers that, in the vast majority of cases, a causal event allows the company to be aware of the accident, whether it is the technical notification of the scooter being too inclined or the call from the user.62. The Restricted Committee considers that geolocation every 30 seconds of all scooters throughout the rental period, prior to any information relating to an accident, is not necessary to provide assistance to a user. The collection and storage of quasi-permanent geolocation data is therefore neither adequate nor relevant with regard to this purpose.63. It follows from all of the foregoing that the Restricted Committee considers that none of the purposes put forward by the company justifies the collection of geolocation data every 30 seconds during the rental of a scooter and the storage of these data. Such a practice is indeed very intrusive in the privacy of users insofar as it is likely to reveal their movements, their places of frequentation, all the stops made during a journey, which amounts to calling into

question their freedom to move anonymously. The Restricted Committee notes in this respect that it emerges from the developments above that the company could offer an identical service without collecting geolocation data on an almost permanent basis.64. The Restricted Committee therefore considers that these facts constitute a breach of Article 5, paragraph 1, c) of the GDPR.B. On the breach of the obligation to define and respect a retention period for personal data proportionate to the purpose of the processing pursuant to Article 5, paragraph 1, e) of the GDPR65. According to Article 5, paragraph 1, e) of the Regulation, personal data must be "kept in a form allowing the identification of data subjects for a period not exceeding that necessary for 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(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 (limitation of storage)".66. The rapporteur noted in her report that it emerged from exchanges with the company that the position data of the scooters are stored indefinitely in the scooter database, while the company also specifies that this data is anonymised after twenty-four months. The rapporteur considered that keeping a user's geolocation data indefinitely or for twenty-four months on an active basis exceeds the time necessary for the purposes for which the data is processed, relating to the management of customer complaints and the management of fines, claims and theft.67. In defence, the company explained that, contrary to what was indicated in the report, it does not keep personal data "without time limit" and in no case for twenty-four months on an active basis. It specified that the position data of the scooters are kept for twelve months in an active database and that, at the end of these twelve months, the position data of the scooters are no longer kept in the active database but are archived in an intermediate database. . After this conservation of twelve months in intermediate archiving, the data is subject to anonymization.68. During the meeting, taking into account the elements communicated by the company within the framework of the investigation, the rapporteur considered that the durations and methods of data retention, with regard to the purposes mentioned, comply with the requirements of the GDPR. It therefore proposed to the Restricted Committee not to uphold the breach in question.69. The Restricted Committee considers that the breach of Article 5, paragraph 1, e) of the GDPR is not established.C. On the breach of the obligation to regulate by a formalized legal act the processing carried out by a subcontractor in application of Article 28, paragraph 3 of the GDPR70. According to Article 28, paragraph 3 of the GDPR, the processing carried out by a processor for a controller must be governed by a contract which defines the object and the duration

of the processing, the nature and the purpose of the processing. , the type of personal data, the categories of data subjects and the obligations and rights of the controller. This contract must also provide for the conditions under which the subcontractor undertakes to carry out the processing operations on behalf of the controller.71. The rapporteur was able to observe that the company CITYSCOOT uses fifteen subcontractors having access to or hosting personal data. Of these fifteen contracts, it considers that the contracts with the companies […] do not contain all the information provided for by the GDPR. The contract with the company […] only generally provides for the security obligations incumbent on the subcontractor and it does not mention the obligation of the subcontractor to provide the data controller with all the information to demonstrate compliance with the obligations provided for, allow audits to be carried out and contribute to these audits. The contract with the company […] does not provide for a procedure for deleting or returning the personal data of the subcontractor to the data controller at the end of the contract. The contract with the company […], very incomplete, does not specify in particular the purpose of the processing, nor its duration. Finally, the contract with the company […] does not cover the category of persons concerned by the processing.72. In defence, the company claims that the contracts with the companies […] have been modified, following checks by the CNIL services, in order to comply with the GDPR. With regard to the contract with the company […], the company considers that the subcontractor undertakes to implement the measures which are those required by article 32 of the GDPR and that the contract provides for the conditions under which the subcontractor provides CITYSCOOT with the necessary information. Regarding the contract with the company […], the company affirms that the data is processed in accordance with the subcontractor's data retention policy according to which any data is deleted or erased after the end of the retention period. conservation, period which is 14 months before anonymisation.73. The Restricted Committee recalls, as a preliminary point, that in its guidelines 07/2020 of 7 July 2021 concerning the notions of controller and processor in the GDPR, the EDPS affirms that "while the elements referred to in Article 28 of the Regulation constitute the essential content of the contract, the latter should allow the controller and the processor to further clarify how these essential elements will be implemented by resorting to detailed instructions. processing should not merely reproduce the provisions of the GDPR; it should include more specific and concrete information on how the conditions will be fulfilled and on the level of security required for the processing of personal data which makes the object of the said agreement" (§ 112). Therefore, the particulars referred to in Article 28(3) must not only appear in the subcontract, but they must also be sufficiently precise and detailed to enable the proper processing of personal data to be ensured. 74. With regard to the contract with the company […], the

"accountability" clause effectively provides that the subcontractor must answer the data controller's questions and provide him, on request, with any document requested. However, it is not expressly stated that the subcontractor must have all the information available to it to enable audits to be carried out and contribute to these audits.75. The Restricted Committee also considers that the "security" clause, which provides that the subcontractor implements technical and organizational measures to ensure a level of security appropriate to the risk, should be more precise. Indeed, by way of illustration, in its Guidelines 07/2020, the EDPS affirms that "the agreement should avoid merely repeating these assistance obligations and should contain details on how the processor is invited to help the data controller to fulfill the listed obligations. For example, standard procedures and forms can be annexed to the agreement to allow the processor to provide the data controller with all the necessary information [… ] the processor is first obliged to help the controller to comply with the obligation to adopt appropriate technical and organizational measures in order to guarantee the security of the processing.Although this may, to a certain extent, impinge on the requirement that the processor itself adopt appropriate security measures, when the processing operations of the processor fall within the scope of the GDPR, these two obligations remain separate, one referring to the measures specific to the processor and the other to those of the controller". Here, only the security objectives to be achieved are described, without specifying the means of achieving them, such as a description of the processes or mechanisms developed in annexes to the contract. In the absence of details on the means to fulfill the obligation to put in place technical and organizational measures to ensure a level of security adapted to the risk, the Restricted Committee considers that the contract does not meet the requirements of the GDPR.76. With regard to the contract with the company […], the Restricted Committee considers that if the contract provides for a retention period policy for personal data, there is no mention of the fate of the data in the event of termination of the contract. between the two companies. Indeed, the data retention period policy and the fate of the data at the end of the contract are the subject of two different mentions by article 28, paragraph 3 of the GDPR. Article 28, paragraph 3, (g) provides that the contract must indicate that the processor "according to the choice of the data controller, deletes all personal data or returns them to the data controller at the end of the service services relating to processing, and destroys existing copies". Accordingly, this reference must therefore be referred to specifically and separately in the contract.77. With regard to contracts with companies […], the Restricted Committee takes note of the fact that the company has made sure to bring the contracts into compliance with the requirements of the GDPR. However, at the date of the inspections, the said contracts did not meet these requirements. Indeed, the contract with the company […], very

incomplete, did not cover in particular the purpose of the processing, the duration of the processing, the type of personal data processed. The contract concluded with the company […], for its part, did not specify the category of persons targeted by the processing.78. Therefore, in view of all of these elements, the Restricted Committee considers that the breach of Article 28 paragraph 3 of the GDPR is clear.D. On the breach of the obligation to inform the user and obtain his consent before registering and reading information on his electronic communication terminal equipment in application of article 82 of the law of January 6, 197879. Article 82 of law n° 78-17 of January 6, 1978 relating to data processing, files and modified freedoms provides that "any subscriber or user of an electronic communications service must be informed in a clear and complete manner , unless it has been done beforehand, by the controller or his representative: 1° The purpose of any action aimed at accessing, by electronic transmission, information already stored in his terminal communications equipment electronically, or to register information in this equipment; 2° The means at his disposal to oppose it. Such access or registrations can only take place on condition that the subscriber or the user has expressed, after having received this information, his consent which may result from appropriate parameters of his connection device or any other device placed under his control. These provisions are not applicable if access to information stored in the user's terminal equipment or the recording of information in the user's terminal equipment: 1° Either, has the exclusive purpose of allowing or facilitate electronic communication; 2° Either, is strictly necessary for the provision of an online communication service at the express request of the user ".80. The rapporteur considers that the company CITYSCOOT, insofar as it publishes the website "cityscoot. eu" and the CITYSCOOT mobile application, has a share of responsibility in respecting the obligations of article 82 of the "Informatique et Libertés" law for the operations of reading and / or writing information carried out in the terminal users via the reCaptcha mechanism provided by Google, when creating an account on the mobile application as well as during connection and the forgotten password procedure on the website. CITYSCOOT does not provide any information, in particular through a consent window, about the collection of information stored on the user's equipment, nor the means to refuse this collection. stored on his equipment or on the recording of information on his equipment is not collected at any time.81. In defense, the company claims to use the reCaptcha mechanism for the sole purpose of ensuring the security of the user authentication mechanism. It specifies that the implementation of such a mechanism complies with CNIL deliberation no. 2017-012 of January 19, 2017, which does not specify that it is mandatory to obtain the consent of users. It adds that the use of reCaptcha must benefit from the second exemption provided for in article 82 of the law "Informatique et Libertés" in that the service is requested by the user - namely

registration or connection to the service. of CITYSCOOT - and that the actions of reading and writing information present on the terminals are necessary to ensure the security of the service. It specifies that if it is not required to collect the consent of its users for the use that it makes of the reCaptcha itself, it cannot be required to collect it on behalf of the company Google. She claims that the Google reCaptcha mechanism, directly integrated into the site, provides a link to Google's privacy policy, implying that Google considers itself responsible for processing and informs users itself. Furthermore, CITYSCOOT cannot itself modify the presentation or configuration of the mechanism and therefore does not have the option of integrating a checkbox or another information link. The company affirms that deliberation n° 2020-092 of September 17, 2020 is subsequent to the control procedure and cannot be applied for the analysis of the collection of user consent, the analysis having to be carried out on the regime prior to the said deliberation. However, it concludes that it will no longer have recourse to this mechanism from October 2022.82. The Restricted Committee notes, firstly, that the Council of State has ruled (CE, June 6, 2018, Editions Croque Futur, No. 412589, Rec.), that under the obligations incumbent on the publisher of a site that deposits "third-party cookies", include that of ensuring with its partners, on the one hand, that they do not issue, through its site, tracers that do not comply with the regulations applicable in France, and on the other hand, that of taking any useful steps with them to put an end to breaches. The Council of State has in particular ruled that "site editors who authorize the deposit and use of such "cookies" by third parties when visiting their site must also be considered as data controllers, even though they are not subject to all the obligations imposed on the third party who issued the "cookie", in particular when the latter alone retains control of compliance with its purpose or its retention period. As part of the obligations incumbent on the site editor in such a case, include that of ensuring with its partners that they do not issue, through its site, "cookies" which do not respect the regulations applicable in France and that of taking any useful steps with them to put an end to breaches" (see also CNIL, FR, September 27, 2021, Sanction, No. SAN-2021-013, published).83 . The Restricted Committee also notes that while the recommendations issued by the Commission on cookies have recently changed to take into account the changes brought about by the GDPR in terms of consent in particular, these changes have no impact in the case of species and it has continuously been considered, as indicated by deliberation no. 2013-378 of December 5, 2013 adopting a recommendation relating to cookies and other tracers covered by article 32-II of the law of January 6, 1978 since repealed, that "when several actors are involved in the deposit and reading of cookies (for example when publishers facilitate the deposit of cookies which are then read by advertising agencies), each of them must be considered as jointly responsible for the obligations arising from the provisions of

the aforementioned article 32-II [current article 82 of the law of January 6, 1978]". This deliberation specifies that this is the case for "publishers of websites (or publishers of mobile applications for example) and their partners (advertising agencies, social networks, publishers of audience measurement solutions, etc.). Indeed, insofar as site editors are often the only point of contact for Internet users and the deposit of third-party Cookies is dependent on navigation on their site, it is their responsibility to proceed, alone or jointly with their partners , to the prior information and to obtaining the consent explained in Article 2 of this recommendation". The Restricted Committee also specifies that it has already enshrined the liability of website publishers in several decisions (see in this sense, Deliberation SAN-2021-013 of July 27, 2021).84. The Restricted Committee notes that a reCaptcha mechanism, provided by Google, is used when creating an account on the mobile application as well as during connection and the forgotten password procedure on the website. The Restricted Committee considers that it is indeed the publisher of the site - in this case CITYSCOOT - who chose to use the reCaptcha mechanism and therefore allowed the actions of reading and writing the information present on the users' terminals .85. In view of the foregoing, the Restricted Committee considers that the company is unfounded in maintaining that it has no obligation or liability with respect to the operations carried out by Google via reCaptcha aimed at accessing information already stored in the electronic communications terminal equipment of users, or to enter information in this equipment, without their consent, when they visit its site. It therefore considers that the company is also responsible for compliance with the provisions of Article 82 of the "Informatique et Libertés" law when using Google's reCaptcha mechanism.86. Secondly, the Restricted Committee considers that if a data controller can claim an exemption from providing information and obtaining consent when the read/write operations carried out in a user's terminal are for the sole purpose of securing an authentication mechanism for the benefit of users (see in this sense, CNIL, FR, September 27, 2021, Sanction, No. SAN-2021-013, published), it is different when these operations also continue to other purposes which are not strictly necessary for the provision of a service. However, the Google reCaptcha mechanism is not only intended to secure the authentication mechanism for the benefit of users, but also allows analysis operations on the part of Google, which Google itself specifies in its general conditions of use.87. The Restricted Committee notes that GOOGLE informs companies using reCaptcha technology, in the general conditions of use available online, that the operation of the reCAPTCHA API is based on the collection of hardware and software information (such as device and application data) and that this data is transmitted to Google for analysis. The GOOGLE company also specifies that it is the responsibility of these companies to inform users and request their authorization for the collection and sharing of data

with GOOGLE.88. In the present case, it is apparent from these elements that CITYSCOOT should have informed the users and obtained their consent, which is not the case here.89. Indeed, if the company CITYSCOOT informed, on the date of the control, the users, within the framework of its confidentiality policy, that "during your visit to our Site or Application, navigation and location data, resulting from cookies or similar technologies, will be collected", the precise purposes of the cookies used, the possibility of opposing them or the fact that the continuation of the visit constituted a form of consent were not included in the information provided by the company. In addition, the information, accessible via the privacy policy on the site, was only provided after the deposit of cookies and other tracers and in a non-specific way, while the recommendation resulting from deliberation n ° 2020-092 of 17 September 2020 clearly provides that the information must be specific and pre-filing. Therefore, it cannot be considered that the users were informed and that the consent was validly obtained in the light of the recommendations of deliberation no. 2020-092 of September 17, 2020.90. Finally, with regard to the opposability of deliberation no. 2020-092 of September 17, 2020 for the purposes of analyzing the collection of users' consent, the Restricted Committee recalls that deliberation no. 2020-092 adopting a recommendation proposing practical methods of compliance in the event of the use of "cookies and other tracers" aims to interpret the applicable legislative provisions and to inform the actors on the implementation of concrete measures to guarantee compliance with these provisions , so that they implement these measures or measures having equivalent effect. In this sense, it is specified in the recommendations that the main purpose of these "is to recall and explain the law applicable to the operations of reading and/or writing information (hereinafter the "tracers") in the electronic communications terminal equipment of the subscriber or user (hereinafter "users")".91. The Commission recalled, in the context of its recommendation of September 17, 2020, that "when none of the exceptions provided for in Article 82 of the "Informatique et Libertés" law is applicable, users must, on the one hand , to receive information in accordance with this article, supplemented, where appropriate, by the requirements of the GDPR, and, on the other hand, to be informed of the consequences of their choice ".92. The Restricted Committee notes that the CNIL did not create in its recommendation any new obligations for the players, but limited itself to illustrating in concrete terms how Article 82 of the law should be applied.93. In this respect, the fact that the recommendation of September 17, 2020 would not be enforceable against the company given the methods of obtaining consent applicable on the date of the inspection, is irrelevant since article 82 of the Data Protection Act freedoms provides that "any user of an electronic communications service must be informed in a clear and complete manner, unless he has been informed beforehand, by the controller or his representative: 1. Of the

purpose of any action tending to access, by means of electronic transmission, information already stored in his terminal electronic communications equipment, or to register information in this equipment; 2. The means at his disposal to oppose it ".94. In any event, the Restricted Committee notes that the company did not inform the user, even with regard to the provisions of the former recommendation resulting from deliberation no. 2013-378 of December 5, 2013, prior to those of deliberation no. 2020-092, of the precise purpose of cookies, of the possibility of opposing them and of the fact that continuing to browse constitutes agreement to the deposit of cookies on your terminal.95. Finally, the Restricted Committee notes that the company CITYSCOOT intends to no longer use this mechanism as of October 2022. However, on the date of the inspections, the said mechanism was indeed used.96. Therefore, in view of the foregoing, the Restricted Committee considers that the company has failed to comply with its obligations under Article 82 of the "Informatique et Libertés" law by allowing the deposit of cookies on the user's terminal via the mechanism of reCaptcha provided by the Google company without informing the users and without obtaining their consent.III. On corrective measures and publicity97. Under the terms of III of article 20 of the modified law of January 6, 1978: "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 the 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: […] 7° With the exception of cases where the processing is implemented by the State, an administrative fine not to exceed 10 million euros or, in the case of a company, 2% of the total worldwide annual turnover of the previous financial year, whichever is higher. 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 ".98. Article 83 of the GDPR provides that "Each supervisory authority shall ensure that the administrative fines imposed in 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.99 Firstly, with regard to the principle of the imposition of a fine, the Restricted Committee recalls that it must take into account, for the imposition of a fine administrative, the criteria specified in Article 83 of the GDPR, such as the nature, gravity and duration of the breach, the measures taken by the controller to mitigate the damage suffered by

the data subjects, the degree of cooperation with the supervisory authority and the categories of personal data affected by the breach.100. The Restricted Committee first considers that the company has demonstrated serious failures in the protection of personal data since breaches of the fundamental and elementary principles of the GDPR and the "Informatique et Libertés" law are constituted, such as the principles of data minimization and the collection of user consent before registering and reading information on its electronic communication terminal equipment.101. The Restricted Committee then notes that the infringement of the rights of individuals resulting from the breach of the principle of minimization of personal data is particularly significant, given the particular nature of geolocation data. Indeed, the company proceeds to an almost permanent collection of geolocation data from the users of the scooters it rents. Such collection is particularly intrusive for users. Indeed, it makes it possible to follow all the journeys made by the user, to identify the places where he goes, thus being able to reveal information on his behavior, his habits of life, which is likely to affect his private life and his freedom of movement anonymously.102. The Restricted Committee also points out that the personal data processed by the company concern approximately 247,000 users, spread over the territory of three Member States of the European Union.103. The Restricted Committee also notes that certain contracts concluded by the company CITYSCOOT with its subcontractors are incomplete and do not contain all the information provided for in Article 28, paragraph 3 of the GDPR or do not provide sufficiently precisely for the obligations incumbent to the subcontractor.104. With regard to the reCaptcha mechanism, the Restricted Committee considers that the breach relating to Article 82 of the "Informatique et Libertés" law is characterized by the fact that the company did not comply with the requirements in terms of information and collection of consent, which had the effect of depriving users of the choice they should be able to express as to how their personal data will be used.105. Consequently, the Restricted Committee considers that an administrative fine should be imposed with regard to the breaches of Articles 5, paragraph 1, c) and 28, paragraph 3 of the GDPR and Article 82 of Law no. 78-17 of 6 January 1978 relating to data processing, files and modified freedoms.106. Secondly, with regard to the amount of the fine, the Restricted Committee recalls that administrative fines must be effective, proportionate and dissuasive.107. In this case, the company failed to comply with its obligations under Articles 5, paragraph 1, c) and 28, paragraph 3 of the GDPR and Article 82 of Law No. 78-17 of January 6, 1978 relating to the information technology, files and freedoms modified with regard to approximately 247,000 users.108. However, the restricted committee takes into account the fact that, following the checks carried out by the CNIL delegation, the company has brought itself into compliance with the contracts concluded with the companies […] with regard to the requirements of the article 28, paragraph 3 of the

GDPR.109. It also recalls that the activity of the organization 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 achieved, in 2019, a turnover of 21,882,031 euros, for a net loss of -12,641,302 euros. The company estimated its turnover for the financial year ended December 31, 2020 at an amount of […].110. Therefore, in view of these elements, the Restricted Committee considers that the pronouncement of an administrative fine of 100,000 euros for breaches of the GDPR and 25,000 euros for breach of the "Informatique et Libertés" law appears justified. 111.Thirdly, the Restricted Committee considers that the publicity of the penalty is justified in view of the particular nature of the data concerned which relate to geolocation data and the invasion of the privacy of users.FOR THESE REASONSThe Committee of the CNIL, after having deliberated, decides to: - pronounce against the company CITYSCOOT an administrative fine in the amount of 100,000 (one hundred thousand) euros with regard to the breaches constituted in Articles 5, paragraph 1, c) and 28, paragraph 3 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of personal data and on the free movement of such data and 25,000 (twenty-five thousand ) euros with regard to the breach of Article 82 of Law No. 78-17 of January 6, 1978 relating to data processing, files and modified freedoms; - make public, on the CNIL website and on the site of Légifrance, its deliberation, which will no longer identify the company CITYSCOOT by name at the end of a period of two years from its publication. President Alexandre LINDEN This decision is likely to be the subject of an appeal before the Council of State within two months of its notification.