Deliberation of the Restricted Committee No. SAN-2023-003 of 16 March 2023 concerning [redacted]

The *Commission nationale de l'Informatique et des Libertés* (CNIL - French Data Protection Authority), met in its Restricted Committee consisting of Mr Alexandre Linden, Chair, Mr Philippe-Pierre Cabourdin, Vice Chair, Ms Anne Debet, Mr Bertrand du Marais, and Mr Alain Dru, members;

Having regard to Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and the free movement of such data, in particular Articles 56 and 60;

Having regard to amended French Data Protection Act No. 78-17 of 6 January 1978, in particular Articles 20 *et seq.*;

Having regard to Decree No. 2019-536 of 29 May 2019 implementing French Data Protection Act No. 78-17 of 6 January 1978;

Having regard to Deliberation No. 2013-175 of 4 July 2013 adopting the internal rules of procedure of the CNIL (French Data Protection Agency);

Having regard to Decision No. 2020-081C of 12 May 2020 of the Chair of the *Commission Nationale de l'Informatique et des Libertés* (CNIL) to instruct the general secretary to carry out or have a third party carry out an assignment to verify all of the processing related to the "[redacted]" application for smartphones;

Having regard to the CNIL Chair's decision appointing a rapporteur before the Restricted Committee of 12 April 2021;

Having regard to the report of Ms. Valérie Peugeot, commissioner rapporteur, notified to [redacted] on 17 March 2022;

Having regard to the written observations made by [redacted] on 02 May 2022;

Having regard to the response of the rapporteur notified to the company on 16 June 2022;

Having regard to the written observations of [redacted] received on 29 July 2022 and the oral observations made at the Restricted Committee meeting;

Having regard to the other exhibits;

The following were present at the restricted committee session on 29 September 2022:

- Valérie Peugeot, commissioner, her report having been heard;

In the capacity of representatives of [redacted]:

- [redacted];
- [redacted].

[redacted] having spoken last;

The restricted committee has adopted the following decision:

I. Facts and proceedings

1. [redacted] (hereinafter "the company") is a French simplified joint stock company [redacted], located at [redacted] and created in 2014. The company estimates that there are [redacted] in its workforce in France. In 2019 it generated a turnover of [redacted] for a net loss of [redacted]. In a letter dated 21 April 2021, the company estimated its turnover for the financial year ended 31 December 2020 at [redacted] and a loss of [redacted].

2. Since 2016, the company has offered a self-service electric scooter rental service that can be accessed from the [redacted] mobile application. It is a "free-floating" vehicle sharing offer, i.e. there are no stations. The scooters are therefore 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 localisation device that allows [redacted] and users, via their mobile application, to know the location of the scooters. Renting an electric scooter from the company requires an account to be created using the mobile application. This is a non-binding service which is charged by the minute.

3. In France, this service is available in the Paris region and in Nice. Furthermore, the company has also expanded its service in certain cities in Italy and Spain through two wholly-owned subsidiaries, [redacted] and [redacted] To date, the company has approximately [redacted] users in France and abroad.

4. An online check was carried out on the website "[redacted]" and the mobile application "[redacted]", on 13 May 2020. Record No. 2020-081/1 drawn up at the end of this audit was notified to [redacted] on 19 May 2020. The CNIL delegation particularly focused on verifying the data collected and the purposes of its collection. The purpose of this check was also to verify the supervision of subcontracting and data security.

5. Three requests for additional information were then sent to the company by recorded delivery letter dated 26 June 2020 and by email dated 27 August and 10 December 2020. The company responded to these requests by letters dated 16 July, 11 September and 15 December 2020.

6. In accordance with Article 56 of the GDPR, on 27 February 2020, the CNIL informed all European supervisory authorities of its competence to act as lead supervisory authority regarding cross-border processing implemented by [redacted], namely the management of user accounts set up by [redacted] derived from the fact that [redacted]'s principal establishment is located in France. After exchanges between the CNIL and the European data protection authorities within the framework of the one-stop-shop mechanism, Spain and Italy are declared to be covered by this processing.

7. In order to examine these items, the CNIL Chair appointed Valérie Peugeot as rapporteur on 12 April 2021, pursuant to Article 22 of the amended French Data Protection Act of 6 January 1978.

8. On 17 February 2022, the rapporteur sent the company an additional request relating to the anonymisation of personal data made by hashing the data and the application of a salt. The company responded in a letter dated 23 February 2022.

9. The rapporteur notified [redacted] on 17 March 2022 of a report detailing breaches of the provisions of Regulation (EU) 2016/679 of the European Parliament and Council of 27 April 2016 (hereinafter "the Regulation" or the "GDPR") and amended Act No. 78-17 of 6 January 1978 on data processing, files and freedoms (hereinafter "the French Data Protection Act" or "amended Act of 6 January 1978") which it considered established in this case. This report also proposed that the restricted committee of the CNIL impose an administrative fine against the Company and that this decision be made public but that the Company not be identifiable by name upon expiry of a period of two years following its publication.

10. On 02 May 2022, the company submitted observations in response to the Rapporteur's sanction report.

11. By letter dated 16 June 2022, the rapporteur's response was sent to the company.

12. On 29 July 2022, the company submitted further observations in response to those of the Rapporteur.

13. In a letter dated 22 August 2022, the rapporteur informed the company of the completion of the investigation.

14. On 23 August 2022, the Chairman of the restricted committee notified [redacted] of a convocation to its meeting on 29 September 2022.

II. Reasons for the decision

15. Pursuant to Article 60(3) of the GDPR, the draft decision adopted by the Restricted Committee was transmitted to the other competent European supervisory authorities on 15 February 2023.

16. As of 15 March 2023, none of the supervisory authorities concerned had raised a relevant, reasoned objection to this draft decision, so that, pursuant to Article 60(6) of the GDPR, they are deemed to have approved it.

A. On the breach of the obligation to ensure the appropriateness, relevance and non-excessive nature of the personal data processed by the company in accordance with Article 5(1)(C) of the GDPR

17. Article 5(1)(c) GDPR provides that personal data shall be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')*". When the data is collected on the basis of the legitimate interest, this collection must also not disproportionately cause a breach of privacy rights regarding the objectives pursued by the company.

18. **The rapporteur** notes that, within the framework of the investigation, the CNIL's inspection delegation was informed that the scooters are equipped with electronic boxes including a SIM card and a GPS geolocation system, embedded on the scooters. She added that these units collect location data from scooters every 30 seconds when the [redacted] is active and its dashboard is on, whether it is moving or ready to be driven. When the [redacted] is not active, the unit collects location data every 15 minutes.

19. This data is then stored in a "scooter database" which contains the following data: the location via GPS and "*a reservation number […] that is collected if the* [redacted] *is reserved, during the rental period*". They are stored in an active database for 12 months, then 12 months in intermediate archiving before being anonymised.

20. The company also stated that the collection of scooter location data, namely the location of the scooter at the reservation departure and arrival points and the location throughout the journey, has the following purposes: handling traffic offences, handling customer complaints, user support (in order to call the emergency services if a user falls off), claims and handling thefts.

21. To end a rental, the user must carry out certain manipulations such as: make sure to be in an authorised area to park the scooters ([redacted] zone), switch off the scooter, press the "END" button located on the scooter or click on "END MY RENTAL" in the mobile application and check that the green diode "FREE" is lit.

22. The rapporteur considers that none of the purposes put forward by the company justify the almost permanent geolocation data collection during the rental of a scooter.

23. **The relevance of collecting this data for each of these purposes should be examined.** First of all, the Restricted Committee points out that, when a vehicle is being rented, geolocation data from the vehicle is associated with an individual and constitutes personal data. However, when the scooter is not rented, geolocation data related to the vehicle alone is not personal data.

24. The restricted committee notes that the company uses three distinct databases:

    - a "scooter database" which contains the data transmitted by sensors fixed to the scooter (scooter location via a GPS, battery status, saddle sensor);
    - a "reservation database" which contains the start and end dates and times of each rental as well as the scooter's condition at the start and end of its rental;
    - a "customer database" which includes data for handling invoicing. This database does not contain scooter data.

25. The restricted committee notes that, while scooters' position data are decorrelated from any information relating to users in the "scooter database" and are kept in a database separate from that storing user data, i.e. the "customer database", which constitutes a choice of privacy-friendly computer architecture (privacy by design), the fact remains that this data may be combined with the data present in the other databases, in particular through the reservation number present in each of the databases, giving extensive and simultaneous access to the databases.

26. The restricted committee therefore considers that the geolocation data collected by [redacted] while the scooter is being rented is personal data when it is possible to combine the different databases, even if such a combination is only one-off, the scooter position data relating to an identified or identifiable natural person.

27. The rapporteur notes that while geolocation data is not sensitive data within the meaning of Article 9 of the GDPR, it is nevertheless considered by the Article 29 Working Party (called the "G29" which became the European Data Protection Board (EDPB)) in its guidelines of 04 October 2017, as being "highly personal data". The EDPB believes that such data is considered to be sensitive data, as the term is commonly understood, insofar as it affects the enjoyment of a fundamental right: collecting position data threatens freedom of movement.

28. By way of clarification, the Restricted Committee also points out that the EDPB considered, in its guidelines 01/2020 on the processing of personal data in the context of connected vehicles and applications related to mobility (Guidelines 01/2020) that "*When collecting personal data, vehicle and equipment manufacturers, service providers and other data controllers should keep in mind that location data is particularly revealing of the life habits of data subjects. The journeys undertaken are very characteristic in that they enable one to infer the place of work and of residence, as well as a driver's centres of interest (leisure), and may possibly reveal sensitive information such as religion through places of worship, or sexual orientation through places visited. Accordingly, the vehicle and equipment manufacturer, service provider and other data controllers should be particularly vigilant not to collect location data except if doing so is absolutely necessary for the purpose of processing*". These guidelines also emphasise that the location data collection is subject to compliance with the principle on which location can be activated "*activating location only when the user launches a function that requires the vehicle's location to be known, and not by default and continuously when the vehicle is started*".

29. Although the company disputes the applicability of the guidelines to the present case on the grounds that they only concern cars, the restricted committee considers that the guidelines are relevant for geolocation data in general.

30. In this context, the Restricted Committee points out that the assessment of compliance with the principle of data minimisation is based on the limited nature of the data processed regarding the purpose for which it is collected. Its assessment implies performing an analysis of the proportionality of the personal data collection regarding the purposes for which it is intended.

31. In view of the foregoing, the restricted committee considers that only the need for the collection and retention of position data collected every 30 seconds should be analysed when the collection of position data at the beginning and end of the lease is relevant to the purposes pursued.

32. **Firstly, regarding the management of claims related to additional charges**, **the rapporteur** considers that the collection of geolocation data every thirty seconds for the entire duration of the rental is not necessary. The rapporteur specifies that the management of overcharging should be managed by the user's contact when he/she encounters a difficulty in terminating his/her rental or, at the very least, by less intrusive means than almost permanent geolocation of the vehicle throughout the lease.

33. In its defence, **the company** argues that the collection of the position data of the scooters every 30 seconds would be necessary, as part of a service invoiced by the minute for situations that have led to overcharging and claims from users when they have failed to properly terminate their rental, in particular when:

    - the user loses communication with a scooter for technical or human reasons;
    - the user makes a complaint related to unauthorised parking areas;
    - the user does not stop the scooter correctly to end the rental;
    - the scooter is moved by a third party.

34. The collection of position data every 30 seconds would make it possible to go back in 30 seconds steps to identify the number of seconds during which the scooter was stopped. It adds that users very often realize later that a rental was not properly completed and do not contact the company when the rental is terminated. The triggering of geolocation at the time of contact by the user would not therefore suffice because it would not be possible to calculate the additional charge minutes between the time the user wanted to end the rental and could not do so, and the time when the company was able to solve the problem and put an end to the rental.

35. **The Restricted Committee** notes the arguments put forward by the company about managing complaints related to additional charges. However, it notes that, for this purpose, the collection and retention of geolocation data for scooters every 30 seconds is not necessary.

36. Indeed, in three of the situations mentioned by the company (loss of communication with the scooter, difficulty related to unauthorised areas, scooter displaced by a third party), the restricted committee considers that the user can contact [redacted] to resolve the difficulties and complete the rental. Geolocation could therefore be triggered from this generating event.

37. Regarding cases where the user does not stop the scooter correctly to end the rental, the restricted committee points out that the geolocation of the scooter every 30 seconds does not make it possible to determine when the user really wanted to end the rental. Indeed, the static position of the scooter alone does not demonstrate the user's desire not to continue the rental.

38. In addition, the restricted committee states that it would be possible to put in place alternative and less intrusive mechanisms allowing the company to ensure that the user has terminated the rental or, on the contrary, warn it when this is not the case, for example by sending an SMS message or confirmation by an alert via the application that the rental has ended.

39. Although for the month of June 2022 the company claims to have received approximately 11,500 calls for 386,766 journeys relating to additional charge problems, it does not indicate what proportion of the calls related to this specific situation. The restricted committee considers, in the absence of precise statistics, that these cases cannot justify the almost permanent geolocation of all scooters.

40. In general, the rapporteur notes that Article 7.4.6 of [redacted]'s General Terms and Conditions of Use provides that "it is the Users' responsibility to check that their Rental has ended correctly. [redacted] shall not be held liable for prolonged invoicing in the event of incorrect return of the Scooter". It is therefore up to the user to ensure that he/she has properly terminated the rental.

41. **Secondly, regarding 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 an infringement when a check of the time of the infringement and the person who leased it during this period is sufficient to do so.

42. In its defence, **the Company** asserts that collecting scooter positioning data every 30 seconds is necessary to obtain information about the circumstances and context in which the infringement was committed. The objective is to verify whether the infringement identified by the ANTAI ("National Agency for Automated Processing of Offences") has been committed: confirm or disprove the presence of the scooter at the place identified by the notice of violation and verify whether the offence could have occurred in this place. It also considers that the collection of scooters' position data is necessary in order to be able to identify or prove the identity of the driver to the ANTAI, the police or the insurance companies.

43. **The restricted committee** considers, on the one hand, that it is not necessary for the company to collect and retain the position of the scooters every 30 seconds to identify and prove the identity of a driver to the ANTAI, the policy or the insurance companies. In fact, collecting the number and date of the infringement notice, the date and time of the start and end of the lease and the date and time of the infringement is sufficient to meet this purpose. This data, cross-referenced with the registration plate number of the scooter, makes it possible to identify the person who leased said scooter. Moreover, collecting the position data of the scooters does not make it possible to establish as such the identity of the person responsible for the offence since it is not possible to determine whether the scooter was moved by the person who leased it or whether it was moved by a third party to an illegal parking area since scooters can be freely moved with or without the motor in operation.

44. Moreover, the restricted committee considers that collecting scooter positioning data every 30 seconds is excessive in that this data is collected for all the vehicles leased by the company although doing so only meets an incidental purpose when a given user needs the data to dispute a traffic infringement.

45. **Thirdly, regarding the management of vehicle theft, the rapporteur** stresses that, in order to be considered proportionate, the processing of geolocation data must be made necessary for this purpose by a triggering event, such as a reported theft or suspected theft. The geolocation data of the scooters cannot therefore be considered strictly necessary for the pursuit of the purpose related to the risk of theft before any triggering event.

46. In its defence, **the company** asserts that the collection of scooter data in the event of theft does not mean that this data is matched with the identity of the users. The company adds that it only needs scooter location data to be able to locate scooters in order to find and recover them in the event of theft.

47. The company states 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 (flat battery, technical problem or when the scooter is in a car park or an area in which geolocation cannot be triggered) may prevent it from triggering remote geolocation. It also states that the collection of scooters position data every 30 seconds significantly reduces 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 seeking to steal the scooter.

48. **The restricted committee** points out above all that, even if the company does not match the position data of the scooters and the user's data to find stolen vehicles, the possibility of this matching between the different databases justifies the position data of the scooters being considered personal data and subject to the requirements of the GDPR.

49. The rapporteur also points out that before any triggering event, vehicle geolocation data cannot, as a rule, be regarded as strictly necessary for pursuing this purpose and its continuous collection or collection at very close intervals must be considered excessive.

50. By way of clarification, the Restricted Committee finds that the Guidelines 01/2020 state that location data can only be passed on after a reported theft and cannot be constantly collected for the rest of the time. In this respect, the EDPB also recommends that the data controller should clearly inform the data subject that the vehicle is not permanently tracked and that geolocation data can only be collected and transmitted after a reported theft.

51. In addition, the Restricted Committee stresses that assessing if processing is limited to what is necessary, within the meaning of Article 5(1)(c) GDPR, is informed by the provisions of recital 39 GDPR, according to which, "*Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means*". The existence of less intrusive means of achieving the same purposes must thus be taken into account, whether processing data by alternative means or processing less data, or processing it less frequently.

52. Above all, the restricted committee 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 identify an individual. This is therefore not personal data and such a situation is therefore outside the scope of this procedure.

53. The restricted committee then goes on to consider that no theft scenario justifies collecting position data every 30 seconds. On the one hand, cases, for which the company has not established the frequency, where the scooter is stolen during use, i.e. when the user is him/herself on the functioning scooter, does not justify the quasi-permanent collection of scooter position data. On the other hand, scooters can be stolen when users takes a break during the rental. In this situation the user may contact [redacted] immediately upon confirmation of the theft at the end of the break, which will inform the company of the last position of the scooter.

54. Questioned on the number of vehicles found thanks to the latest known position of the scooter, the company was unable to provide statistics showing the effectiveness of geolocation every 30 seconds.

55. Thus, the Restricted Committee points out that, in view of the above considerations, cases where, on the one hand, geolocation is the only way of knowing the last known position of the vehicle and where, on the other hand, the last known position is actually close to the location of the vehicle, appear to be limited. In such situations, the Restricted Committee does not call into question the need to know the last known position of the vehicle using the latest geolocation data. But this assumption is not sufficient to justify the collection of all geolocation data for all users' journeys.

56. In the light of all these considerations, the Restricted Committee considers that, in many use cases, collection of geolocation data every 30 metres during the scooter rental is not necessary for managing theft of vehicles. The fact of systematically carrying out this collection for situations where it could actually be useful on the basis of the legitimate interests of the company, appears to be a disproportionate breach of privacy rights. Indeed, as pointed out above, the company's collection and retention of all vehicle user journeys lead it to handling and retaining highly sensitive data (cf. CNIL, FR, 7 July 2022, Sanction, [redacted], No. SAN-2022-015, published).

57. **Fourthly, regarding the management of accidents**, **the rapporteur** argues that the collection of geolocation data for this purpose can only take place from a triggering event, particularly technical notification when the scooter is at an excessively steep angle or there is a request for assistance by the customer, making such collection necessary.

58. In its defence, the company maintains that it is necessary to collect scooter location data every 30 seconds and to cross-reference it with the user data, to be able to contact the user when the detector has sent a technical warning relating to an accident and to assist the user with declaration and reporting formalities. The company adds that accidents do not necessarily trigger a technical notification, particularly when the scooter is not at a sufficiently steep angle. The company states that it is regularly contacted by insurance companies after a claim to obtain additional information such as the precise location of a scooter at the time of an accident.

59. **The Restricted Committee** first points out that it is entirely legitimate for the company to wish to assist users who are victims of traffic accidents during the rental of a vehicle. However, in order to provide such assistance to users, the company must be aware that an incident or accident has occurred.

60. The Restricted Committee considers that, as soon as the company becomes aware of the occurrence of an accident concerning a rented vehicle, it may geolocate this vehicle in order to assist the user if necessary.

61. The restricted committee considers that, in the vast majority of cases, a triggering event allows the company to be aware of an accident, whether it is the technical notification of the scooter being at an excessively steep angle or a call from the user.

62. On the other hand, the Restricted Committee considers that geolocation every 30 meters of all scooters throughout the rental term, prior to receiving any information relating to an accident, is not necessary to provide assistance to a user. The near permanent geolocation data collection is therefore neither appropriate nor relevant to this purpose.

63. **It follows from all of the above that the Restricted Committee considers that none of the purposes advanced by the company justify collecting geolocation data every 30 metres during the rental of a vehicle. Such a practice is indeed very intrusive to the privacy of users insofar as it can reveal their movements, the places they visit, and all the stops made during a journey, which amounts to calling into question their freedom to move freely.** The Restricted Committee notes in this respect that it is clear from the foregoing that the company could offer an identical service without near constant geolocation data collection.

64. The Restricted Committee therefore considers that these facts constitute a breach of Article 5(1)(c) of the GDPR.

B. On the failure to define and respect a personal data storage period, which is porportionate to the pruposes of the processing, in accordance with Article 5 (1)(e) of the GDPR (storage limitation)

65. Article 5(1)(e) of the Regulation requires that personal data shall be *"kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')".*

66. **The rapporteur** pointed out, in her report, that it appears from the exchanges with the company that the position data are kept in the scooter database without any time limitation, while the company also specifies that these data are anonymized after twenty-four months. The rapporteur considered that keeping user's geolocation data for an unlimited period of time or for twenty-four months in the active database exceeds the period of time necessary for the purposes for which the data concerning management of customer complaints and management of fines, damages and thefts are processed.

67. **In its defense, the company** explained that, contrary to what was stated in the report, it doesn't keep personal data *"without time limitation"* and not during twenty-four months in active database. It specified that the scooters' position data are kept for twelve months in active database, and that after twelve months, the scooters' position data are no more kept in active database but are archived in an intermediate database. After this storage of twelve months in intermediate filing, the data are anonymized.

68. **During the session,** given the information communicated by the company as part of the investigation, the rapporteur considered that the period and conditions of retention comply to the GDPR, in view of the purposes mentioned.

69. The restricted committee considers that the breach of Article 5(1)(e) of the GDPR is not constituted.

C. On the failure to provide a formal legal framework for the processing operations carried out by a sub-contractor in application in article 28, paragraph 3 of the RGPD

70. Article 28 of the GDPR requires that the processing carried out by a subcontractor for a data controller be governed by a contract which sets out the aim and duration of the processing, the nature and purpose of the processing, the type of personal data, the categories of data subjects concerned and the obligations and rights of the data controller. This contract also provides for the conditions under which the subcontractor undertakes to perform the processing operations on behalf of the data controller.

71. **The rapporteur** found that [redacted] uses fifteen subcontractors with access to or hosting of personal data. Of these fifteen contracts, she considers that the contracts with [redacted], [redacted], [redacted] and [redacted] do not contain all the information provided for in the GDPR. The contract with [redacted] only generally provides for the security obligations incumbent on the subcontractor and it does not mention the obligation on the subcontractor to make all information available to the data controller to demonstrate compliance with the obligations provided for, enable audits to be carried out and contribute to these audits. The contract with [redacted] does not stipulate a procedure for the deletion or return of the subcontractor's personal data to the data controller upon expiry of the contract. The contract with [redacted], which is very incomplete, does not state the purpose of the processing or its duration. Finally, the contract with [redacted] does not cover the category of data subjects concerned by the processing.

72. In its defence, **the company** states that the contracts with [redacted] and [redacted] have been amended following inspections by the CNIL in order to comply with the GDPR. Regarding the contract with [redacted], the company considers that the subcontractor undertakes to implement the measures required by Article 32 of the GDPR and that the contract provides for the conditions under which the subcontractor makes the necessary information available to [redacted]. Regarding the contract with [redacted], the company states 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, which is 14 months before anonymisation.

73. **The restricted committee** points out, as a preliminary point, that in its guidelines 07/2020 of 7 July 2021 on the concepts of controller and subcontractor in the GDPR, the EDPB states that *"while the elements referred to in Article 28 of the Regulation constitute the essential content of the contract, the contract should allow the controller and the subcontractor to further*

clarify how these essential elements will be implemented by using detailed instructions. Therefore the processing agreement should not merely reproduce the provisions of the GDPR; it should include more specific and concrete information on how the conditions will be met and on the level of security required for the processing of personal data that is the subject of this agreement" (paragraph 112). Therefore the information referred to in Article 28(3) must not only be included in the subcontracting contract, but must also be sufficiently precise and detailed to ensure that the personal data is processed in a compliant manner.

74. Regarding the contract concluded with [redacted], the "accountability" clause effectively provides that the subcontractor must answer the data controller's questions and provide any document requested. However, it is not clearly stated that the subcontractor must, upon request, make all information available to enable audits to be carried out and take part in these audits.

75. The rapporteur also considers that the "*security clause, which requires that the subcontractor implement technical and organisational measures to ensure a level of security suited to the risk, should be more specific*". Indeed, by way of illustration, in its guidelines 07/2020, the EDPB states that *"the agreement should avoid merely repeating these assistance obligations and should contain details on how the subcontractor is invited to assist the controller in fulfilling the obligations listed. For example, standard procedures and forms may be attached as appendices to the agreement to enable the subcontractor to provide the controller with all necessary information* […] *the subcontractor is first required to assist the controller in complying with the obligation to adopt appropriate technical and organisational measures to ensure the security of the processing. Although this may, to some extent, encroach on the requirement that the subcontractor itself adopt appropriate security measures where the subcontractor's processing operations fall within the scope of the GDPR, these two obligations remain distinct, one referring to measures specific to the subcontractor and the other to those of the controller*". Here, only the security objectives to be achieved are described, without specifying how to achieve it, such as a description of the processes or mechanisms developed in appendices to the contract. In the absence of clarification on the means to fulfil the obligation to implement technical and organisational measures to ensure a level of security appropriate to the risk, the restricted committee considers that the contract does not meet the requirements of the GDPR.

76. Regarding the contract concluded with [redacted], the rapporteur considers that while the contract provides for a personal data retention policy, no mention is made 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 references under Article 28(3) of the GDPR and must therefore be specifically and separately referred to in the contract. Article 28(3) (g) provides that the contract must indicate that the subcontractor "at *the choice of controller, delete all personal data or return it to the controller at the end of the provision of services relating to the processing, and destroy existing copies*". Therefore this phrase must therefore be specifically and separately referred to in the contract.

77. Regarding the contracts with [redacted] and [redacted], the restricted committee takes note of the fact that the company has ensured that the contracts comply with the requirements of the GDPR. However, at the date of the audits, the said contracts did not meet these requirements. Indeed, the contract with [redacted], which is very incomplete,

did not concern in particular the purpose of the processing, the duration of the processing or the type of personal data processed. As concerns the contract entered into with [redacted], it did not specify the category of persons covered by the processing.

78. Therefore regarding all of these facts, the Restricted Committee considers that the breach of Article 28 (3) of the GDPR is established.

D. Regarding the breach of the obligation to notify users and obtain their consent before recording and reading data from their electronic communications devices, in violation of Article82 of the French Data Protection Act.

79. Article 82 of the French Data Protection Act provides that "*any subscriber or user of an electronic communications service must be informed in a clear and complete manner, unless he/she has been previously informed by the data controller or its representative, of: 1) the purpose of any action aimed at electronically accessing information already stored in his or her electronic communications terminal equipment, or recording information on this equipment; 2° The means available to him or her to object to it. Such access or recording may only take place provided that, after receiving such information, the subscriber or user has expressed his or her consent which may result from the appropriate parameters of his/her connection device or any other device under his or her control. These provisions shall not apply if access to the information stored in the user's terminal equipment or the recording of information on the user's terminal equipment: 1° Is for the exclusive purpose of allowing or facilitating electronic communication; 2° Or is strictly necessary for the provision of an online communication service at the express request of the user*".

80. **The rapporteur** considers that [redacted], as the publisher of the website "[redacted]" and the mobile application [redacted], has a responsibility for compliance with the obligations of Article 82 of the French Data Protection Act for the operations of reading and/or writing data performed in users' terminals via the reCaptcha mechanism provided by Google when creating an account on the mobile application as well as when logging in and using the forgotten password procedure on the website. The rapporteur notes that [redacted] does not provide any information, in particular through a consent window, regarding the collection of information stored on user equipment or the means to refuse such collection. Furthermore, the user's consent regarding accessing information stored on his/her equipment or recording information on his/her equipment is not collected at any time.

81. In its defence, [redacted] states that it uses the reCaptcha mechanism for the sole purpose of making the user authentication mechanism secure It states that setting up such a mechanism complies with CNIL deliberation No. 2017-012 of 19 January 2017, which does not specify that it is mandatory to obtain the consent of users. It adds that the use of reCaptcha must be covered by the second exemption provided for in Article 82 of the French Data Protection Act in that the service is requested by the user - namely registration or connection to the [redacted] service - and that the actions to read and write data on the terminals are necessary to ensure the security of the service. Lastly, the company states that as it is not required to obtain the consent of its users for its own use of the reCaptcha mechanism, it cannot be required to

obtain the consent of its users on behalf of Google. It states that the Google reCaptcha mechanism, which is directly integrated into the website, provides a link that refers to Google's privacy policy, implying that Google considers itself a data controller and informs users itself. Furthermore, [redacted] cannot itself modify the presentation or configuration of the mechanism and therefore does not have the ability to integrate a check box or another information link. The company states that deliberation No. 2020-092 of 17 September 2020 is later than the control procedure and cannot be applied to judge whether user consent has been obtained, such judgement being carried out on the regime prior to the said deliberation. However, it concludes that it will no longer use this mechanism as of October 2022.

82. **The restricted committee** notes, **firstly**, that the Council of State ruled (CE, 6 June 2018, *Editions Croque Futur*, No. 412589, Rec.), that under the obligations incumbent on the publisher of a site that places "third-party cookies", include that of checking with its partners, on the one hand, that they do not issue trackers through the site that do not comply with the regulations applicable in France, and on the other hand, to take any useful steps with them to put an end to any breaches. In particular the Council of State judged that *"website publishers who authorise the placing and use of said "cookies" by third parties when their website is visited must also be considered as data controllers, even though they are not subject to all the obligations imposed on third parties who have issued a "cookie", particularly when they retain sole control of compliance with its purpose or retention period. In respect of the obligations incumbent on the website publisher in such cases, the obligation to ensure with its partners that they do not issue, through its website, "cookies" that do not comply with the regulations applicable in France and that of taking any useful steps with them to put an end to breaches*" (see also CNIL, FR, 27 September 2021, Sanction, [redacted] Company, No. SAN-2021-013, published).

83. The restricted committee also notes that while the recommendations issued by the Commission on cookies have recently evolved to take into account the developments induced by the GDPR in terms of consent, in particular, these changes have no impact in this case and it has been continuously considered, as indicated in deliberation No. 2013-378 of 5 December 2013 adopting a recommendation on cookies and other trackers referred to in Article 32-II of the Act of 6 January 1978, since repealed, that *"when several players intervene in the storage 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 Act of 6 January 1978]". This deliberation specifies that this is the case *"of publishers of websites (or mobile app publishers, for example) and their partners (advertising agencies, social networks, publishers of audience measurement solutions, etc.). Indeed, insofar as website publishers often constitute the sole point of contact for Internet users and that the deposit of third-party Cookies depends on browsing their website, it is their responsibility to proceed, alone or jointly with their partners, with the prior information and the collection of consent explained in Article 2 of this recommendation*". The restricted committee also states that it has already enshrined the responsibility of publishers of websites in several decisions (see on this point, Deliberation SAN-2021-013 of 27 July 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 when logging in performing the

forgotten password procedure on the website. The restricted committee considers that it was indeed the publisher of the website - in this case [redacted] - who chose to use the reCaptcha mechanism and therefore allowed the actions of reading and writing data present on users' terminals.

85. In view of the foregoing, the restricted committee considers that the company is not justified in arguing that it is under no obligation or responsibility for the operations carried out by Google via reCaptcha aimed at accessing information already stored on users' electronic communications terminal equipment, or at recording data in this equipment without their consent when they visit its website. It therefore considers that the company is also responsible for compliance with the provisions of Article 82 of the French Data Protection Act when using Google's reCaptcha mechanism.

86. **Secondly**, the restricted committee considers that while a data controller can claim an exemption from information and collection of consent when the read/write operations performed on a user's terminal are for the sole purpose of securing an authentication mechanism for the benefit of users (see on this point CNIL, FR, 27 September 2021, Sanction, [redacted] Company, No. SAN-2021-013, published), the opposite is true when these operations also pursue other purposes that are not strictly necessary for the provision of a service. However, the purpose of the Google reCaptcha mechanism is not for the sole purpose of securing the authentication mechanism for the benefit of users but also allows analysis operations by Google, which Google itself specifies in its General Terms and Conditions of Use.

87. The restricted committee notes that GOOGLE informs companies using reCaptcha technology, under the General Terms and Conditions of Use available online, that the functioning of the reCAPTCHA API is based on the collection of hardware and software information (such as data on devices and applications) and that this data are transmitted to Google for analysis. GOOGLE also states that such companies are responsible for informing users and requesting their permission regarding the collection and sharing of data with GOOGLE.

88. In this case, it emerges from these elements that [redacted] should have informed users and obtain their consent, which is not the case here.

89. Whilst [redacted] informed users, within the framework of its privacy policy, that *"when you visit our Site or Application, browsing and location data from cookies or similar technologies will be collected."*, the precise purposes of the cookies used, the possibility of objecting to them or that the continuation of the visit constitutes a form of consent is not part of the information provided by the company. Thus the information, accessible via the privacy policy on the website was only provided after cookies and other trackers had been stored and in a non-specific manner, whereas the recommendation resulting from deliberation No. 2020-092 of 17 September 2020 clearly provided that the information should be specific and prior to said storage. Therefore it cannot be considered that users were informed and consent validly obtained in light of the recommendations of deliberation No. 2020-092 dated 17 September 2020.

90. **Lastly**, as concerns the enforceability of deliberation No. 2020-092 dated 17 September 2020 as concerns analysing the obtaining of users' consent, the restricted committee points out that deliberation No. 2020-092 for adopting a recommendation proposing practical compliance procedures in the event of the use of "cookies and other trackers" aims to interpret the applicable legislative provisions and to inform stakeholders on the implementation of concrete measures to ensure compliance with these provisions so that said stakeholders implement these measures or measures having an equivalent effect. On this point it is stated in the recommendations that they *"are primarily intended to recall and explain the law applicable to the reading and/or writing of data (hereinafter "trackers") on the subscriber's or user's (hereinafter "users") electronic communications terminal equipment".*

91. The Commission pointed out, in the context of its recommendation of 17 September 2020, that "when none of the exceptions provided for in Article 82 of the French Data Protection Act applies, users must, on the one hand, receive information in accordance with this article, supplemented, where applicable, by the requirements of the GDPR, and, on the other hand, be notified of the consequences of their choice".

92. The rapporteur notes that the CNIL has not created in its recommendation new obligations incumbent on the stakeholders but merely illustrated in concrete terms how Article 82 of the law must be applied.

93. In this respect, the fact that the recommendation of 17 September 2020 would not be enforceable against the company, in view of the methods for obtaining consent applicable on the date of the audit, has no impact since Article 82 of the French Data Protection Act provides that *"any user of an electronic communications service must, unless it has been informed beforehand, be informed in a clear and complete manner by the data controller or its representative: 1. Of the purpose of any action aimed at electronically accessing information already stored on their electronic communications terminal equipment, or writing information to this equipment; 2. Of how said user can object to it".*

94. However, the company did not inform users even regarding the provisions of the former recommendation resulting from deliberation No. 2013-378 of 5 December 2013, prior to the provisions of deliberation No. 2020-092, of the precise purpose of the cookies, the possibility of objecting to said cookies and that continuing browsing constitutes agreement to the storage of cookies on users' terminals.

95. **Finally**, the restricted committee notes that [redacted] intends not to use this mechanism after October 2022. However, at the date of the controls, the mechanism was indeed used.

96. Therefore in view of the foregoing, the restricted committee considers that the company breached its obligations under Article 82 of the French Data Protection Act by allowing the placing of cookies on user terminals via the reCaptcha mechanism provided by Google without informing users and without obtaining their consent.

III. <u>On corrective measures and publicity</u>

97. Under the terms of Article 20 III of the amended Act of 6 January 1978:

"When the controller or its subcontractor fails to comply with the obligations resulting from Regulation (EU) 2016/679 of 27 April 2016 or this law, the chairman of the CNIL may also, if applicable, after sending the warning provided for in point I of this article or, where applicable, in addition to an order provided for in II, contact the CNIL's Restricted Committee with a view to the imposition, after proceedings in which both sides are represented, 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 may not exceed 10 million euros or, in the case of a company, 2% of the total annual global turnover of the previous financial year, whichever is the greater. In the cases mentioned in 5 and 6 of Article 83 of Regulation (EU) 2016/679 of 27 April 2016, these upper limits shall be increased, respectively, to 20 million euros and 4% of the said turnover. In determining the amount of the fine, the Restricted Committee shall take into account the criteria specified in the same Article 83".

98. Article 83 of the GDPR states that *"Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive"*, before specifying the information to be taken into account when deciding whether to impose an administrative fine and when deciding on the value of such fine.

99. **Firstly**, the Restricted Committee notes that, in imposing an administrative fine, it must take into account the criteria specified in Article 83 of the GDPR such as the nature, gravity and duration of the infringement, the measures taken by the data 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 infringement.

100. The restricted committee first considers that the company is guilty of serious failures in terms of the protection of personal data since breaches of fundamental and basic principles of the GDPR and the French Data Protection Act are constituted, such as the principles of data minimisation and the obtaining of users' 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 minimisation of personal data is particularly important, given the special nature of geolocation data. Indeed, the company undertakes near-permanent geolocation data collection from users of the scooters it rents. Such data collection is particularly intrusive for users. In fact, it makes it possible to track all of the journeys made by users and identify the places they go to, thereby possibly revealing information about their behaviour and their life habits, which is likely to infringe their freedom of movement and privacy.

102. The Restricted Committee also points out that the personal data processed by the company concerns about [redacted] users distributed over the territory of three Member States of the European Union.

103. The restricted committee also notes that certain contracts entered into by [redacted] with its subcontractors are incomplete and do not contain all the information provided for in Article 28(3) of the GDPR or do not provide for sufficiently precise obligations incumbent on the subcontractor.

104. Regarding the reCaptcha mechanism, the restricted committee considers that the breach of Article 82 of the French Data Protection Act is characterised by the fact that the company has not complied with the requirements for information and obtaining consent, which has had the effect of depriving users of the choice they must be able to express as to the terms under which their personal data will be used.

105. Consequently, the restricted committee considers that an administrative fine should be imposed regarding the breaches constituted by Articles 5(1)(c) and 28(3) of the GDPR and Article 82 of Act No 78-17 of 6 January 1978 on data processing, files and freedoms as amended.

106. **Secondly**, as regards the value of the fine, the Restricted Committee recalls that administrative fines must be effective, proportionate and dissuasive.

107. In this case, the company breached its obligations under Articles 5(1)(c) and 28(3) of the GDPR and Article 82 of Act No. 78-17 of 6 January 1978 on data processing, files and freedoms as amended regarding approximately [redacted] users.

108. However, the restricted committee takes into account the fact that, at the end of the inspections carried out by the CNIL delegation, the company complied with the contracts entered into with [redacted] and [redacted] regarding the requirements of Article 28(3) of the GDPR.

109. In particular, it considers that the organisation's activity and financial situation must be taken into account when determining the sanction and, in particular, in the case of an administrative fine, its value. It points out in this respect that in 2019 the company generated revenue of [redacted] for a net loss of [redacted]. The company estimated its turnover for the financial year ended 31 December 2020 at [redacted] and a loss of [redacted].

110. Therefore in view of these facts, the restricted committee considers that the imposition of an administrative fine of 100,000 euros for breaches of the GDPR and 25,000 euros for the breach of the French Data Protection Act would appear justified.

111. **Thirdly**, the restricted committee considers that the publication of the sanction is justified in view of the particular nature of the data concerned which relates to geolocation data and the breach of users' privacy.

FOR THESE REASONS

The CNIL's restricted committee, after having deliberated, decides to:

- **impose an administrative fine of 100,000 (one hundred thousand) euros against [redacted] in respect of the breaches constituted by Articles 5(1)(c) and 28(3) of Regulation (EU) 2016/679 of the European Parliament and Council of 27 April 2016 on the protection of personal data and the free movement of such data, and 25,000 (twenty-five thousand) euros regarding the breach constituted by Article 82 of modified Act No. 78-17 of 6 January 1978 on information technology, files and freedoms;**

- **publish its decision on the CNIL and Légifrance websites, which will no longer identify the [redacted] company by name at the end of a two-year period following its publication.**

The Chair

Alexandre Linden

This decision may be appealed before the State Council within two months of its notification.