Deliberation of the Restricted Committee No. SAN-2022-015 of 7 July 2022 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. Alain Dru, Mr. Bertrand du Marais, and Ms. Christine Maugüe, members;

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to 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 Act No. 78-17 of 6 January 1978 on data protection;

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

Having regard to Decision No. 2020-256C of 12 May 2020 of the CNIL Chair, instructing the General Secretary to carry out, or have carried out, an investigation of the data processing activities accessible from the "[redacted]" domain and the [redacted] app, or concerning personal data collected from them;

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

Having regard to the report of Ms. Valérie Peugeot, Commissioner rapporteur, notified to [redacted] on 22 October 2021;

Having regard to the written observations made by [redacted] on 22 November 2021;

Having regard to the rapporteur's response to the observations notified on 15 December 2021 to the company;

Having regard to the written observations of [redacted] received on 17 January 2022 and the oral observations made at the Restricted Committee meeting;

Having regard to the other documents in the case file;

The following were present at the Restricted Committee session on 27 January 2022:

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

In their capacity of representatives of [redacted]:

[…]

[redacted] having last spoken;

After having deliberated, the Restricted Committee adopted the following decision:

I. Facts and proceedings

1. [redacted] (hereinafter "[redacted]" or "the company") is a single-member simplified joint-stock company, whose head office is located at [redacted]. The company is a subsidiary of the [redacted]. This group generated an average revenue of [redacted] over 2018, 2019, and 2020. In 2019, [redacted] generated revenue of [redacted], and a net loss of approximately [redacted]. In 2020, [redacted] generated revenue of [redacted] and a net loss of approximately [redacted].

2. [redacted] **implements a digital car-sharing vehicle rental platform which it offers to private customers and business customers.** As at 9 July 2020, the company had at least [redacted] customers in Europe, including [redacted] private customers and [redacted] business customers in France. Its services can be accessed directly through downloading "[redacted]" applications (available on IOS and Android) and via the [redacted] website. [redacted] operates through its subsidiaries based notably in France, Belgium, Germany, Spain, Italy and Denmark. At the end of June 2020, [redacted] and its subsidiaries had [redacted] employees in their workforce.

3. The company has its own fleet of vehicles which the platform users can rent by creating an account on the [redacted] website or mobile applications. In 2019, the French subsidiary of [redacted] recorded [redacted] bookings.

4. For private customers, the company offers a round-trip shared vehicle rental offer: the customer is required to pick up and return their vehicle at the same station. The vehicles are freely accessible, in private or non-private parking areas and no [redacted] staff are present when a vehicle is picked up or when it is returned, the service being completely virtualized.

5. During their rental by customers, the company collects geolocation data from the vehicles, particularly in order to manage the fleet for future rentals.

6. The structure of the IT system of [redacted] and its subsidiaries consists of two separate platforms:

   - [redacted] for France, Italy and part of the activity in Belgium and Germany;
   - [redacted] for Spain, Denmark and the remainder of the activity in Germany.

7. Pursuant to Decision No. 2020-090C of 12 May 2020 of the CNIL Chair, an on-line investigation was conducted in order to verify compliance with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter "GDPR") and of the French Data Protection Act No 78-17 of 6 January 1978 (hereinafter "the amended Act of 6 January 1978" or "the French Data Protection Act") of any processing accessible from the [redacted] domain and the "[redacted]" application or involving personal data collected from them. Record No. 2020-090/1 drawn up at the end of this investigation was notified to [redacted] on 12 June 2020.

8. On 17 June 2020, the supervisory delegation sent a questionnaire to the company, to which the latter replied by letter dated 10 July 2020. The supervisory delegation sent additional requests

to the company, in emails dated 28 September and 26 October 2020. The company responded in emails dated 7 October and 2 November 2020.

9. 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.

10. At the end of her investigation, the rapporteur had a bailiff notify [redacted], on 22 October 2021, of a report detailing the breaches of the GDPR that she considered demonstrated in this case. This report proposed to the Restricted Committee of the Commission to impose an administrative fine on the company and that the decision be made public.

11. Also attached to the report was a notice to attend the Restricted Committee meeting on 9 December 2021 informing [redacted] that it had one month to provide its written observations in accordance with Article 40 of Decree No. 2019-536 of 29 May 2019.

12. The company responded to the sanction report with written observations dated 22 November 2021.

13. On 30 November 2021, the rapporteur asked for time to respond to the observations made by the company. By email dated 1 December 2021, the Chair of the Restricted Committee informed the rapporteur that she had an additional eight days to submit her observations. In a letter dated the same day, the company was informed by the Chair of the Restricted Committee that it also had an eight-day time extension to file its observations.

14. By email dated 15 December 2021, the CNIL sent the company a notice to attend the Restricted Committee meeting on 27 January 2022.

15. By email of 18 December 2021, the company requested time to respond to the observations made by the rapporteur. By letter dated 21 December 2021, the Chair of the Restricted Committee informed the company that it had a time extension until 17 January 2022.

16. On 17 January 2022, [redacted] submitted further observations in response to those of the rapporteur.

17. The Company and the rapporteur presented oral observations at the Restricted Committee meeting.

II. Reasons for the decision

18. According to Article 56(1) GDPR, "*the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60*".

19. First of all, the Restricted Committee points out that the processing operations carried out by the company in connection with its offer to business customers are not covered by this Deliberation.

20. The Restricted Committee notes that the registered office of [redacted] is located in France and has been registered with the Trade and Companies Register in France since the start, which leads CNIL to become the competent lead supervisory authority concerning the cross-border processing carried out by this company, in accordance with Article 56 (1) GDPR.

21. In accordance with the cooperation and coherence mechanism provided for in Chapter VII GDPR, on 15 December 2020 CNIL informed all European supervisory authorities of its competence to act as the lead supervisory authority concerning the cross-border processing carried out by the company and opening the Notification procedure for the relevant authorities in this case.

22. Pursuant to Article 60(3) GDPR, the draft decision adopted by the Restricted Committee was transmitted to the other competent European supervisory authorities on 3rd June 2022. The Restricted Committee notes that the following supervisory authorities are concerned by this procedure: Belgium, Denmark, Spain, Italy, Baden-Wurtemberg and Berlin.

23. On the 1st of July 2022, none of the supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority. The lead supervisory authority and the supervisory authorities concerned are then deemed to be in agreement with that draft decision, pursuant to Article 60(3) GDPR.

A. On the processing in question and the quality of [redacted]'s data controller

24. The rapporteur points out that the data controller is defined under Article 4(7) GDPR, as "*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data*".

25. The processing operations in question in these proceedings are the processing of data relating to the creation of a user account on mobile applications or the [redacted] website and the geolocation data collection from the rented vehicles.

26. Firstly, with regard to the responsibility for processing, it emerges from the documents in the case file that, with regard to the data collected on the mobile applications or the [redacted] website, the company indicates in its privacy policy that it is responsible for the processing of such personal data. Then, the company determines in particular, for all subsidiaries, the categories of data that are collected during the registration process, such as contact data. As regards the processing operations relating to geolocation data, according to the elements provided by the company, such processing operations are common to all the subsidiaries and the company has determined the different purposes (maintenance and performance of the

service, etc.). In addition, the company has established a single data retention period policy, applicable to both the company and its subsidiaries. Finally, the company has implemented two IT systems, [redacted] and [redacted], each of which is used by multiple subsidiaries, and the company can access the personal data stored in these two systems.

27. Secondly, the Restricted Committee notes that [redacted] does not dispute its capacity as data controller. Moreover, the possibility of joint liability of its subsidiaries is without influence on its own liability with regard to the processing in question. Indeed, this Deliberation relates to [redacted]'s liability for the breaches referred to and not that of its possible joint data controllers.

28. In light of these elements, the Restricted Committee finds that [redacted] determines the purposes and means of the processing operations relating to the creation of a user account on the mobile applications or the [redacted] website, and the geolocation data collection from the rented vehicles. Thus, the company must be qualified as the data controller for such processing.

B. On the breach of the obligation to ensure the personal data processed by the company are adequate, relevant and non-excessive, in accordance with Article 5(1)(C) GDPR

29. 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, with regard to the objectives pursued by the company.

30. **The rapporteur** notes that, in the context of the investigation, CNIL's supervisory delegation was informed that, during the rental of a vehicle by an individual, the company collects geolocation data every 500 metres, when the engine turns on and off, or when the doors open and close. Geolocation data is collected by systems internal to the vehicles and then transmitted by the GSM network to the service provider's IT system and then communicated to [redacted] platforms. The operational teams also have a button to refresh the position of the vehicle and locate it in real time.

31. The rapporteur notes that the company stated that vehicle geolocation data were collected for different purposes:
    - Ensuring maintenance and the performance of the service (making sure that the vehicle is returned to the right place, to monitor the condition of the fleet, etc.),
    - Finding the vehicle if it is stolen,
    - Assisting customers in the event of an accident.

32. 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 vehicle.

33. **It is necessary to examine the relevance of the collection of this data for each of these three purposes.** First of all, the Restricted Committee points out that, when a vehicle is in the process of being rented, geolocation data from this vehicle is associated with an individual and constitutes personal data. While geolocation data are not sensitive data, within the meaning of Article 9 GDPR, they are nevertheless considered by the Article 29 Working Party (called the "WP29" which became the European Data Protection Board (EDPD)) in its guidelines of 4 October 2017, to be *"highly sensitive data"*. The WP29 believes that such data are considered to be sensitive data, as the term is commonly understood, insofar as they affect the enjoyment of a fundamental right. Indeed, the location data collection calls into play the freedom of movement.

34. By way of clarification, the Restricted Committee also recalls 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 are particularly revealing of the life habits of data subjects. The journeys carried out 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 the place of worship, or sexual orientation through the places visited. Accordingly, the vehicle and equipment manufacturer, service provider and other data controller 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 that location can be activated "*only when the user launches a functionality that requires the vehicle's location to be known, and not by default and continuously when the car is started*".

35. In this context, the Restricted Committee recalls that the assessment of compliance with the principle of data minimisation is based on the limited nature of the data processed with regard to the purpose for which it is collected. Its assessment involves an analysis of the proportionality of the personal data collection with regard to the intended purposes.

36. **Firstly, with regard to the management of the fleet of vehicles and leases, the rapporteur** considers that geolocation data collection for the entire duration of the rental is not necessary. She believes that the company may need this data to manage the start and end of the rental but that such collection is not justified over the entire rental period.

37. In defence, **the company** argues that the service offering it provides is based on immediate availability of vehicles and flexibility involving adaptation to the needs of the user that evolves during the rental period. It recalls that the system is completely virtualized and that it operates in a closed loop: the vehicle must be taken from and brought back to the same station. It argues that limiting the geolocation data collection to the scheduled end time would deprive it of the possibility of managing the fleet in a flexible manner, depending on the actual location of the vehicles. The company also contends that it is not aware in advance of the actual end time of a

rental and that customers can return the vehicle in advance simply by reporting it to the departure station. Therefore, geolocation at regular intervals would be the only way to determine the time of return of the vehicle.

38. The company argues, with regard to rental agreements, that geolocation allows it to deal with cases where the vehicle is returned outside of its departure location, in particular to be able to close the rental or recover a vehicle parked in the wrong location. In addition, it argues that it must be able to carry out supervision of the proper performance of the contract, for example during a prohibited use of the vehicle off-road or outside the national territory. Geolocation would also be necessary to supervise the entry and exit of a vehicle from urban toll areas (particularly in Madrid) and thus provide the customer with an immediate and automated billing service.

39. The company argues that it needs to know immediately whether a vehicle has been used outside the rental general terms and conditions in order to prevent the vehicle from being put back into service, for safety reasons or *"for reasons of proper administration of the service* " (including insurance).

40. **The Restricted Committee** notes the arguments put forward by the company to manage its fleet efficiently and in a flexible manner.

41. However, the Restricted Committee notes that, for this purpose, the geolocation data collection from the vehicle throughout the journey (every 500 metres when the vehicle moves but also when the motor of the vehicle is started or stopped, and when the doors are opened or closed using a badge or application) is not necessary.

42. Indeed, the Restricted Committee notes that, on the one hand, in order to return the vehicle, the engine must necessarily be shut off and, on the other hand, that this event triggers the geolocation of the vehicle. Thus, when a user starts or stops the engine of the vehicle, this vehicle sends the company the geolocation of the vehicle. If the company finds that the vehicle is back at its starting point and is closed, it can end the current rental. The geolocation of the vehicle at this time therefore makes it possible to determine whether the vehicle is at its starting point, ready to be returned. *Conversely*, the geolocation data collection during the rest of the journey is not necessary to determine whether the vehicle is returning to its departure station in order to be returned.

43. With regard to the case where the vehicle is returned elsewhere than at its departure location, it appears from the company's statements that it is not the mere geolocation of the vehicle that allows the rental to be terminated, as in the case of end of rental at the departure station. In the absence of an automatic process, the end of the rental may only take place after the customer has contacted the company. In addition, the collection of the vehicle's geolocation when the vehicle stops, at a location other than its starting point, combined with the information that it was not started again after that, makes it possible, in this case, to have data to establish the end of the rental, in connection with the telephone call from the user. In addition, the Restricted

Committee considers that, as soon as the company is aware of the customer's desire to return the vehicle to another location, it may activate geolocation in order to manage this situation.

44. With regard to compliance with the general terms and conditions of use and in particular the use of the vehicle off-road and outside the national territory, the company, questioned on this subject during the Restricted Committee session, did not provide any information relating to its effective use of geolocation data to detect such uses or to draw any consequences therefrom. In particular, it is not established whether the geolocation data is used for such purposes and, where applicable, how and in what proportions. In particular, the company has not given any indication of the actions taken when a vehicle was taken outside the national territory. The Restricted Committee underlines in this regard that, in any event, the customer may be held liable for any use of the vehicle outside of the general terms and conditions of use. The Restricted Committee notes, for the sake of completeness, that the use of regular geolocation to identify a movement of a rented vehicle off-road is not customary and raises questions of proportionality. Under these conditions, the company's desire to ensure compliance with the general conditions of use by users cannot justify geolocation of vehicles every 500 metres.

45. With regard to the use of geolocation to monitor the entry and exit of a vehicle from an urban toll area, the Restricted Committee notes first of all that this only concerns (in the States of the European Union concerned by the processing in question) the city of Madrid. Then, an almost permanent geolocation data collection on all rented vehicles, on the basis of legitimate interest, necessarily appears disproportionate to the purpose advanced, which is that of immediate, automated invoicing of costs to customers. The Restricted Committee notes that this is especially applicable with regard to the rental of vehicles in cities other than Madrid.

46. **Secondly, with regard to the fight against 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 vehicles cannot therefore be considered strictly necessary for the pursuit of the purpose related to the risk of theft, before any triggering event.

47. In its defence, **the company** argues that the geolocation data collection every 500 metres makes it possible to find the vehicle in the event of a theft or suspected theft, particularly when there are inconsistencies between the actual location of the vehicle and its scheduled return location. Indeed, geolocation would be the only effective way of meeting the legitimate objective of preventing theft. The company argues that it cannot ask customers about the location of the vehicle because, in 60% of cases identified by [redacted] in France in 2021, the customer is the perpetrator of the theft. In addition, the use of geolocation starting from a triggering event would at best make it possible to obtain information too late, or even no information at all. Indeed, geolocation systems would be either deactivated or rendered inoperable by placing the vehicle in an area where the signal could not be emitted (underground parking lot, etc.). Knowing the vehicle's latest known position would therefore reduce the vehicle's search area if it were stolen and no longer emitting a signal.

48. **The Restricted Committee** points out that, as the rapporteur found, before any triggering event, vehicle geolocation data cannot, as a rule, be regarded as strictly necessary for pursuing this purpose and their continuous collection or collection at very close intervals must be considered excessive.

49. By way of clarification, the Restricted Committee finds that the Guidelines 01/2020 state that location data can only be passed on after of 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 the reported theft.

50. 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 to achieve the same purposes must thus be taken into account, whether processing data by alternative means or processing less data, or processing it less frequently.

51. The Restricted Committee notes the company's observations and particularly the fact that, in 60% of theft cases in France, the theft is committed by the user of the vehicle. In such cases, this user would therefore not report, or at least not in a timely manner, the theft in question and would not provide the company with the last known position of the vehicle. However, in such cases, the company theoretically has the identity of the individual, which was verified during the user's registration process, by collecting copies of an identity document and the driving licence of that individual.

52. The Restricted Committee also notes that, in 40% of cases in France, since the user is not the thief of the vehicle, they can communicate to the company the last known position of the vehicle before it disappeared.

53. The Restricted Committee then notes that in cases where the vehicle disappears and that the last known position is not communicated by the user, the company can theoretically activate the geolocation of the vehicle remotely. It is only in cases where the vehicle is located in an area where the signal is not issued (particularly a telecommunications dead zone or underground car park), or the geolocation system has been dismantled for the theft, that the company will not have access to geolocation of the vehicle. However, the proportion of these assumptions has not been communicated by the company.

54. In this regard, the Restricted Committee considers that when the geolocation system has been knowingly rendered unusable, the information that the last known position of the vehicle represents has relative value in order to search for the vehicle.

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 thanks to the latest geolocation data. However, this assumption is not sufficient to justify the collection of all geolocation data for all users' journeys.

56. In addition, the Restricted Committee notes that other security measures could be put in place to prevent vehicle theft. Indeed, for example, no security deposit is required from the user to rent a vehicle. The Restricted Committee points out that the absence of alternative means of preventing theft, less intrusive of users' privacy, tends to reinforce the conclusion that it is disproportionate to have vehicle theft prevention be based on the near-permanent geolocation data collection.

57. In light of all of these considerations, the Restricted Committee considers that, in many use cases, the geolocation data collection every 500 metres during the car rental is not necessary for the purpose of preventing theft of the vehicle. The fact of systematically carrying out this collection for use cases where it could actually be useful, while other means of preventing and fighting theft exist, on the basis of the legitimate interest of the company, appears to cause 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.

58. Thirdly, with regard to the location of the vehicle in the event of an accident, **the rapporteur** argues that the geolocation data collection for this purpose can only take place from a triggering event, particularly a request for assistance by the customer, making such collection necessary.

59. In its defence, **the company** argues that limiting the triggering of geolocation to the hypothesis of a request for assistance would amount to depriving it of the possibility of providing assistance to its client even though they would be unable to request it. In addition, identifying the last known location of the vehicle would be important when the vehicle is damaged in a telecommunications "dead zone".

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

61. 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, where appropriate, assist the user.

62. On the other hand, the Restricted Committee considers that geolocation every 500 meters of all vehicles 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 adequate 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 500 metres during the rental of a vehicle**. Such a practice is indeed very intrusive in the privacy of users insofar as it is likely to reveal their movements, their places of attendance, all of the stops made during a daily journey, which amounts to calling into question their freedom of movement. 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. In addition, the Restricted Committee notes that the company has stated that its practice had evolved and that it no longer retained geolocation data histories. The Restricted Committee considers this to be a good practice, insofar as the risk of breach of privacy rights for users is less significant. However, as at the date of the investigation, the company retained a history of geolocation data in the [redacted] IT system.

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

C. Regarding the breach of the obligation to specify and comply with a personal data retention period in proportion to the purpose of the processing in accordance with Article 5(1)(e) GDPR

66. According to Article 5.1(1)(e) GDPR, personal data must 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')".*

1. Regarding the geolocation data retention period

67. **The rapporteur** notes that it follows from the company's data retention policy that the geolocation data of individual customers is kept in an active database for the entire duration of the commercial relationship and for three years from the date of the user's last activity. During this business relationship, a customer enters into a new contract with the company for each rental of a vehicle. The rapporteur notes that the purposes for which the geolocation data is collected are related to a rental contract for a specific vehicle and not to the entire commercial relationship, which lasts until the last expression of interest in the commercial relationship by the user (in particular: a current rental or reservation, the fact of clicking on a link in a newsletter, registering for a [redacted] offer or a logging in to the [redacted] account).

68. In view of these elements, the rapporteur accuses the company of not linking the geolocation data retention period to each rental agreement but to the commercial relationship with the customer. Indeed, the date of the last activity of the user and not that of the end of the rental agreement is taken into consideration to start the data retention period. It therefore considers that the geolocation data collected during the rental of a vehicle is kept for a period exceeding the purposes for which it is processed.

69. In its defence, **the company** argues that it does not retain any history of geolocation data. It argues that each piece of geolocation data collected replaces the previously collected data, both in the [redacted] IT system and in the [redacted] IT system. Thus, only the last known position of a vehicle is maintained. Consequently, it cannot be criticised for retaining the geolocation data it collects for an excessive period of time.

70. **The Restricted Committee** recalls that the personal data retention period must be determined according to the purpose pursued by the processing. When this purpose is achieved, the data must be deleted or anonymised, or be the subject of intermediate archiving, for a specified period, when data retention is necessary for example for compliance with legal obligations or for pre-litigation or litigation purposes. The Restricted Committee also points out that the effectiveness of the implementation of a data retention period policy is the necessary counterpart to its definition and helps ensure that the data is kept in a form allowing the identification of data subjects for a period not exceeding that necessary for the purposes for which the data is processed. This also makes it possible, in particular, to reduce the risks of unauthorised use of the data in question, by an employee or by a third party (see CNIL, FR, 29 October 2021, Sanction, No. SAN-2021-019, published).

71. In this case, the Restricted Committee notes that it follows from the documents in the case file that, as at the date of the investigation by the CNIL supervisory delegation, the company retained a history of geolocation data in the [redacted] IT system. The geolocation data was retained, in accordance with the data retention period policy, in an active database for three years from the date of the user's last activity. The starting point for the data retention period of this data was thus linked to the end of the business relationship between the company and the user. This practice concerned part of the company's activity, i.e., data collected in countries where the [redacted] IT system was used (France, Italy and, partially, Belgium).

72. Yet, the Restricted Committee notes that the purposes for which geolocation data is collected are not linked to this entire business relationship but to each vehicle rental agreement. In fact, as regards, firstly, the purpose related to managing the vehicle fleet and the rental agreement, the vehicle geolocation data are no longer necessary for this purpose once the vehicle has been returned and the rental has ended. Secondly, with regard to the purpose related to the prevention of theft, geolocation data would be necessary only in the event of theft of the vehicle, the time of the investigation of the file by the competent judicial authorities or until the end of a procedure for the removal of doubt which does not result in the confirmation of the theft of the vehicle. Thirdly, with regard to the purpose of assisting users in the event of an accident, while

vehicle geolocation data may be necessary for providing an assistance service, they are no longer necessary when this service or the associated procedures end.

73. The Restricted Committee points out that, where appropriate, at the end of vehicle theft or accident procedures, geolocation data related to these procedures may be retained by the company, in particular by virtue of legal obligations or to build up evidence in the event of litigation and within the limits of the applicable limitation period. However, such data must be sorted and stored in a dedicated archive database, separate from the active database, for a period related to the intended purposes. Furthermore, the starting point for the data retention period of such data must be linked to the situations and events justifying the collection of such data and cannot, in this case, depend mechanically and systematically on the termination of the business relationship with the customer.

74. Therefore, the Restricted Committee considers that the fact that the starting point for the data retention period of geolocation data is linked not to the rental agreement but to the end of the commercial relationship with the user did not make it possible to comply with the principle that the personal data should not be kept for a period that exceeds that necessary for the purposes for which it is processed.

75. Furthermore, it follows from the evidence in the case file that the company modified its geolocation data retention policy. Thus, as at the date of the investigation by the CNIL supervisory delegation, the company retained a geolocation data history in the [redacted] IT system. The Restricted Committee notes that the company argues that this practice has evolved during this sanction procedure and that, now, no geolocation data history is maintained. Indeed, each piece of geolocation data collected would replace the data previously collected in the IT system. The last data collected would therefore overwrite the previous data. Therefore, at a given moment, only the last known position of the vehicle would be recorded in the IT system.

76. While the Restricted Committee takes note of this change, it notes that it was not the practice observed during the investigation.

77. The Restricted Committee concludes that the company retained the geolocation data in question for a period exceeding that necessary for the purposes for which it is processed and has thus disregarded its obligations under Article 5(1)(e) GDPR.

2. Regarding the effective implementation of the data retention policy

78. **The rapporteur** accuses the company of not complying with its data retention policy insofar as it was found during the investigation that personal data relating to users inactive for more than eight years had been present in the [redacted] IT system. The rapporteur maintains that certain personal data are thus retained for a period exceeding the purposes for which they are processed.

79. In its defence, **the company** argues that the data in question relates to its activity in the context of the offering of services to professionals (B2B) and that the retention policy mentioned in the report does not apply in the context of the offer to professionals.

80. **The Restricted Committee** notes that the elements of the case file do not corroborate the company's assertion.

81. In fact, firstly, the Restricted Committee notes that, in its response to CNIL dated 10 July 2020, in response to the questions of the supervisory delegation as to the number of users in the database who have not logged in to their account for more than three years, five years, eight years, the company provided extracts from the database of the [redacted] IT system showing personal data relating to [redacted] users inactive for more than eight years, [redacted] users inactive for more than five years, and [redacted] users inactive for more than three years. The Restricted Committee notes that, although the supervisory delegation requested it to " *distinguish by user type, where applicable "*, the company produced a single result and did not mention the distinction between users of the services offered to individuals and professionals.

82. Secondly, the company had specified, in this same response, that " *This result [would] give rise to additional investigations to understand the reasons justifying this result.* " The Restricted Committee notes that this tends to indicate that the company had then considered this result to be non-compliant with its data retention policy.

83. Thirdly, the assertion that all the data in question relate to data collected in the context of the services offered to professionals implies that data relating to services offered to professionals and data relating to services offered to individuals are kept in the same database in the [redacted] IT system. Questioned on this point during the Restricted Committee meeting, the company did not explain how, in the event that all the data were kept in the same database, it would implement the necessary purges, distinguishing the data relating to services offered to professionals and the data relating to services offered to individuals.

84. The Restricted Committee considers that it is thus not demonstrated that the data in question, kept for more than three years, five years and eight years, respectively, are exclusively data collected within the context of services offered to professionals. Therefore, the data retention periods specified by the company should be applied to such data.

85. Therefore, on the basis of the elements observed by the supervisory delegation and the company's elements in response, the Restricted Committee considers that the company retained the data in question for a period exceeding that necessary for the purposes for which they are processed.

86. With regard to all of these elements, the Restricted Committee considers that the breach of Article 5(1)(e) GDPR is established.

D. Regarding the breach of the obligation to inform data subjects pursuant to Article 12 GDPR

87. Article 12(1) GDPR provides that "*The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing or by other means including, where appropriate, electronically. […]*"

88. **The rapporteur** accuses the company of not providing the data subjects with the information referred to in Article 13 GDPR in a sufficiently accessible manner when conducting personal data collection for the purpose of registering with the [redacted] service.

89. In its defence, **the company** argues that this was a malfunction, which was corrected.

90. The Restricted Committee finds, firstly, that, with regard to the easily accessible nature of the information, the WP29 specifies, by way of illustration, in its guidelines of 11 April 2018 on transparency within the meaning of Regulation (EU) 2016/679, that *"The 'easily accessible' element means that the data subject should not have to seek out the*

information; it should be immediately apparent to them where and how this information can

be accessed, for example by providing it directly to them, by linking them to it […]". "*WP29 recommends as a best practice that at the point of collection of the personal data in an online context a link to the privacy statement/ notice is provided or that this information is made available on the same page on which the personal data is collected*". These guidelines also specify that information *"should be clearly differentiated from other non-privacy related information such as contractual provisions or general terms of use"*. The Guidelines add that " *The data subject must not have to actively search for information covered by [Articles 13 and 14] amongst other information, such as terms and conditions of use of a website […]*".

91. In this case, the Restricted Committee comments that, during the online investigation of 26 May 2020, by following the user registration process on the application, it was found that, in order to register, a user had to fill in various types of personal data (first name, surname, date of birth, contact details) on a registration form. It was also found that the registration form contained a link to the General Terms and Conditions of Use. In this document, there was a link to the company's privacy policy, in which the information provided for in Article 13 GDPR were presented.

92. The Restricted Committee finds that the registration form page does not allow the user to access comprehensive data protection information directly since a multi-click route was necessary to obtain it. It also notes that, in order to read information relating to the protection of personal data, individuals were required to search for it in the General Terms and Conditions of Use.

Yet, the presentation of information on the protection of personal data in a document accessible from a link in the website's General Terms and Conditions of Use cannot be regarded as satisfying the requirements of easily accessible information. Indeed, if it is not necessary to include the information referred to in Article 13 GDPR starting from the standard data collection form, it must, at the very least, present something, such as a hypertext link allowing the user to easily read all the mandatory information.

93. The Restricted Committee notes that the company brought the registration form into compliance on this point during the procedure.

94. However, it holds that, on the date of the investigation, the breach relating to the absence of information directly published or accessible on the personal data collection interface has been established with regard to the provisions of Article 12 GDPR.

III. <u>On the sanction and publicity</u>

95. Under the terms of Article 20(III) of the Act of 6 January 1978 amended:

"*When the controller or his processor 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 restricted committee of the Authority with a view to the announcement, 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 may not exceed €10 million 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 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."

96. Article 83 GDPR further 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 elements to be taken into account when deciding whether to impose an administrative fine and to decide on the amount of that fine.

97. The Restricted Committee notes that, in imposing an administrative fine, it must take into account the criteria specified in Article 83 GDPR, such as the nature, severity, 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 concerned by the infringement.

98. Firstly, with regard to the imposition of a fine, the Restricted Committee first considers that the company has demonstrated serious failures in terms of the protection of personal data since the breaches involve fundamental and basic principles of the GDPR, namely the principles of data minimisation, limitation of the data retention period, and accessibility of information.

99. 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 particular nature of the geolocation data. Indeed, the company conducts near permanent geolocation data collection from users of the vehicles it rents. This near permanent geolocation data collection is particularly intrusive for rental car users. In fact, it makes it possible to track all of the journeys made by the user and identify the places where they go, thereby possibly revealing information about their behaviour and their life habits, which is likely to infringe their freedom of movement and privacy.

100. The Restricted Committee also points out that the personal data processed by the company concern about [redacted] users (customers and prospective customers), spread over the territory of six Member States of the European Union.

101. As regards the data retention period, on the one hand, user geolocation data are retained for an excessive period, which is not linked to the end of the rental agreement, without any particular justification. On the other hand, the company retains personal data beyond the retention periods it has defined, in disregard of the effectiveness of its retention period policy, which reveals a certain negligence in this respect.

102. In addition, it is all the more important, in the context of the geolocation data collection, since the company provides data subjects with information in a transparent and accessible manner, within the meaning of Article 12 GDPR. Indeed, data subjects must be able to understand which data is collected, how this data is used and what their rights are. The Restricted Committee notes in this respect that in view of the growth in the geolocation data collection, particularly within the framework of shared mobility services, data controllers must be particularly vigilant and transparent in the processing of this data.

103. Consequently, the Restricted Committee considers that an administrative fine should be imposed in view of the breaches of Articles 5(1)(c), 5(1)(e), and 12 GDPR.

104. Secondly, with regard to the amount of the fine, the Restricted Committee recalls that Article 83(3) GDPR provides that in the event of multiple breaches, as in the case in point, the total amount of the fine may not exceed the amount set for the most serious breach. Insofar as the company is alleged to be in breach of Articles 5.1(c), 5.1(e), and 12 GDPR, the maximum fine that can be imposed is €20 million or 4% of annual worldwide turnover, whichever is higher.

105. The Restricted Committee recalls that administrative fines must be effective, proportionate and dissuasive. In particular, it considers that the organisation's activity and financial situation must

be considered when determining the sanction and, in particular, in the case of an administrative fine, its amount. In this regard, it notes that the company reports revenue in 2020 of approximately [redacted] with a net loss of approximately [redacted] The Restricted Committee also recalls that the company is a subsidiary of the [redacted] This group generated an average revenue of [redacted] over 2018, 2019, and 2020.

106. Therefore, in view of the relevant criteria of Article 83(2) GDPR mentioned above, the Restricted Committee considers that the imposition of an administrative fine of €175,000 appears proportionate.

107. Thirdly, with regard to the publication of the sanction, the Restricted Committee considers that, in view of the plurality of the breaches identified, their severity, and the particular nature of the data concerned, the publication of this decision is justified.

FOR THESE REASONS

CNIL's Restricted Committee, after having deliberated, has decided to:

- **impose an administrative fine on [redacted] International in the amount of €175,000 (one hundred seventy-five thousand euros) with regard to the breaches set out in Articles 5(1)(c), 5(1)(e), and 12 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.**

- **Make public, on the CNIL website and on the Légifrance website, its Deliberation, which will no longer identify [redacted] International at the end of a period of two years following its publication.**

The Chair

Alexandre Linden

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