Deliberation SAN-2022-015 of July 7, 2022 National Commission for Computing and Liberties Nature of the deliberation: Sanction Legal status: In force Date of publication on Légifrance: Friday July 22, 2022 Deliberation of the restricted committee no. SAN-2022-015 of 7 July 2022 concerning the company UBEEQO INTERNATIONAL The National Commission for Computing and Liberties, meeting in its restricted formation composed of Mr. Alexandre LINDEN, president, Mr. Philippe-Pierre CABOURDIN, vice-president, Mrs. Anne DEBET, Mr. Alain DRU, Mr. Bertrand du MARAIS and Mrs Christine MAUGÜÉ, members; Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 relating to the protection of personal data and the free movement of such data, in particular its articles 56 and 60; Having regard to law no. 78-17 of January 6, 1978 relating to data processing, files and freedoms, in particular its articles 20 and following; Having regard to decree no. o 2019-536 of May 29, 2019 taken for the application of law no. 78-17 of January 6, 1978 relating to data processing, files and freedoms; Having regard to deliberation no. rules of procedure of the National Commission for Computing and Liberties; Having regard to decision no. 2020-090C of 12 May 2020 of the President of the National Commission for Computing and Liberties to instruct the Secretary General to proceed or to carry out a mission to verify any processing accessible from the ubeeqo.com domain and the "Ubeeqo" application or relating to personal data collected from them; Having regard to the decision of the President of the National Commission data processing and freedoms appointing a rapporteur before the restricted committee, dated April 12, 2021; Considering the report of Mrs. Valérie Peugeot, commissioner rapporteur, notified to the company Ubeeqo International on October 22, 2 021; Having regard to the written observations submitted by Ubeeqo International on November 22, 2021; Having regard to the rapporteur's response to these observations notified to the company on December 15, 2021; Having regard to the written observations submitted by Ubeeqo International on January 17, 2022, as well as the oral observations made during the restricted training session; Having regard to the other documents in the file; Were present, during the restricted training session of January 27, 2022: - Mrs. Valérie Peugeot, commissioner, heard in her report; As representatives of the company Ubeeqo International:- […] The company Ubeeqo International having had the floor last;After deliberating, the restricted committee adopted the following decision:I. Facts and procedure1. Ubeeqo International (hereinafter "Ubeeqo" or "the company") is a single-person simplified joint-stock company, whose registered office is located at 13 ter boulevard Berthier, in Paris (75017). The company is a subsidiary of the Europcar Mobility Group. This group achieved an average turnover of 2.57 billion euros over the years 2018, 2019 and 2020. In 2019, Ubeeqo achieved a turnover of […] euros, for a net profit [… ] euros. In 2020, Ubeeqo achieved a turnover of […] euros, for a

net profit […] euros.2. Ubeeqo is implementing a digital car-sharing vehicle rental platform that it offers to private and professional customers. As of July 9, 2020, the company had at least […] customers in Europe including, in France, […] individual customers and […] professional customers. Its services are accessible directly by downloading the "Ubeeqo" applications (available on IOS and Android) and the website www.ubeeqo.com. It carries out its activity through its subsidiaries established in particular in France, Belgium, Germany, Spain, Italy and Denmark. At the end of June 2020, the workforce of Ubeeqo and its subsidiaries was 284 employees.3. The company has its own fleet of vehicles that platform users can rent by creating an account on the Ubeeqo website or mobile applications. In 2019, the French subsidiary of Ubeeqo recorded […] reservations.4. For individual customers, the company offers a closed-loop 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 spaces or not, and no Ubeeqo staff is present when picking up the vehicle or when returning it, the service being entirely dematerialized.5. During their rental by customers, the company collects vehicle geolocation data, in particular in order to manage the vehicle fleet for future rentals. The structure of the information system of Ubeeqo and its subsidiaries is composed of two distinct platforms:- Inovia for France, Italy as well as part of the activity in Belgium and Germany;- Phoenix for the Spain, Denmark and the rest of the activity in Germany.7. Pursuant to Decision No. 2020-090C of May 12, 2020 of the President of the CNIL, an online control mission was carried out to verify compliance with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 (hereinafter "GDPR") and the law n ° 78-17 of January 6, 1978 modified relating to data processing, files and freedoms (hereinafter "law of January 6, 1978 amended" or "Data Protection Act") of any processing accessible from the ubeeqo.com domain and the "Ubeeqo" application or relating to personal data collected from them. The report n° 2020-090/1 drawn up following this inspection was notified to Ubeeqo on June 12, 2020.8. On June 17, 2020, the delegation of control sent a questionnaire to the company, to which the latter replied by letter dated July 10, 2020. The delegation of control sent additional requests to the company, by emails of September 28 and October 26 2020. The company responded by emails dated October 7 and November 2, 2020.9. For the purpose of examining these elements, the President of the Commission, on April 12, 2021, appointed Ms Valérie Peugeot as rapporteur, on the basis of Article 22 of the law of January 6, 1978 as amended.10. At the end of her investigation, the rapporteur notified Ubeeqo International, on October 22, 2021, of a report detailing the breaches of the provisions of the Rules that she considered constituted in this case. This report proposed that the restricted committee of the Commission impose an administrative fine on the company and that the decision

be made public.11. Also attached to the report was a convocation to the restricted training session of December 9, 2021 indicating to Ubeeqo International that it had one month to submit its written observations pursuant to the provisions of Article 40. of decree no. 2019-536 of May 29, 2019.12. The company responded to the sanction report with written observations dated November 22, 2021.13. On November 30, 2021, the rapporteur requested a deadline to respond to the observations made by the company. By letter dated December 1, 2021, the chairman of the Restricted Committee notified the rapporteur that she had an additional period of eight days to submit her observations. In a letter dated the same day, the company was informed by the chairman of the Restricted Committee that it also had an additional period of eight days to submit its observations.14. By letter dated December 15, 2021, the rapporteur's response was sent to the company, accompanied by a notice to attend the restricted training session of January 27, 2022.15. By email of December 18, 2021, the company requested a deadline to respond to the observations made by the rapporteur. By letter dated December 21, 2021, the chairman of the Restricted Committee informed the company that it had the benefit of an additional period until January 17, 2022.16. On January 17, 2022, Ubeeqo International produced new observations in response to those of the rapporteur.17. The company and the rapporteur presented oral observations during the session of the restricted committee.II. Reasons for decision18. According to Article 56(1) of the Regulation, "the supervisory authority of the main establishment or single establishment of the controller or processor is competent to act as lead control concerning the cross-border processing carried out by this controller or processor, in accordance with the procedure provided for in Article 60 ".19. As a preliminary point, the Restricted Committee specifies that this deliberation does not cover the processing carried out by the company in the context of its offer to professional clients.20. The Restricted Committee notes that the sole establishment of the company Ubeeqo International is in France and that it has been registered in the trade and companies register in France from the outset, which leads to making the CNIL the authority of competent lead control concerning the cross-border processing carried out by this company, in accordance with Article 56 paragraph 1 of the Regulation.21. Applying the cooperation and consistency mechanism provided for in Chapter VII of the GDPR, the CNIL informed, on December 15, 2020, all the European supervisory authorities of its competence to act as lead supervisory authority concerning the cross-border processing carried out by the company, thus opening the procedure for the declaration of the authorities concerned on this case.22. Pursuant to Article 60(3) of the GDPR, the draft decision adopted by the Restricted Committee was sent to the other competent European supervisory authorities on 3 June 2022. The Restricted Committee notes that the following supervisory authorities are concerned by these

proceedings: Belgium, Denmark, Spain, Italy, Baden-Württemberg and Berlin.23. As of 1 July 2022, none of the supervisory authorities concerned had raised a relevant and reasoned objection to this draft decision, so that, pursuant to Article 60(6) of the GDPR, these latter are deemed to have approved it.A. On the processing in question and the status of Ubeeqo International24 as data controller. The data controller is defined, under the terms of article 4, point 7, of the GDPR, as "the natural or legal person, public authority, service or other body which, alone or jointly with others, determines the purposes and means of the processing ".25. The processing at issue in this procedure is the processing of data relating to the creation of a user account on mobile applications or the ubeeqo.com website and the collection of geolocation data from rented vehicles.26. Firstly, with regard to the responsibility for the processing, it appears from the documents in the file that, with regard to the data collected on the mobile applications or the ubeeqo.com website, the company indicates in its confidentiality policy to be responsible the processing of such personal data. Then, the company determines in particular, for all the subsidiaries, the categories of data that are collected during the registration process, such as contact data. With regard to the processing relating to geolocation data, it appears from the elements provided by the company that this processing is common to all the subsidiaries and that 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 set up two information systems, Inovia and Phoenix, which are each used by several subsidiaries, and the company can access the personal data stored in these two systems.27. Secondly, the Restricted Committee notes that the company Ubeeqo International does not dispute its status as data controller. Moreover, the possibility of joint liability of its subsidiaries has no influence on its own liability with regard to the processing in question. Indeed, this deliberation concerns the liability of Ubeeqo International for the breaches referred to and not that of its possible joint data controllers.28. In view of these elements, the Restricted Committee considers that the company Ubeeqo International determines the purposes and means of processing relating to the creation of a user account on the mobile applications or the ubeeqo.com website and the collection of data from geolocation of rented vehicles. Thus, the company must be qualified as responsible for this processing.B. On the breach relating to the obligation to ensure the adequacy, relevance and non-excessive nature of the personal data processed pursuant to Article 5.1.c of the GDPR29. Article 5, paragraph 1, c) of the GDPR provides that personal data must be “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimization)”. When the data is collected on the basis of legitimate interest, this collection

must also not cause a disproportionate invasion of privacy, with regard to the objectives pursued by the company.30. The rapporteur notes that, as part of the investigation, the CNIL's delegation of control was informed that, during the rental of a vehicle by an individual, the company collects geolocation data, every 500 meters , when the engine starts and stops or when the doors open and close. Geolocation data is collected by internal vehicle systems and then transmitted via the GSM network to the service provider's information system and then communicated to Ubeeqo's platforms. 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 has indicated that vehicle geolocation data is collected for various purposes:- to ensure the maintenance and performance of the service (checking that the vehicle is returned to the right place, monitoring the state of the …),- to find the vehicle in the event of theft,- to provide assistance to customers in the event of an accident.32. The rapporteur considers that none of the purposes put forward by the company justifies an almost permanent collection of geolocation data during the rental of a vehicle.33. It is necessary to examine the relevance of the collection of this data for each of these three purposes. As a preliminary point, the Restricted Committee points out that, when a vehicle is being rented, the geolocation data from this vehicle is associated with a person and constitutes personal data. Although geolocation data is not sensitive data, within the meaning of Article 9 of the GDPR, it is nevertheless considered by the Article 29 working group (known as "G29" which has become the European Data Protection Board (EDPS)) in its guidelines of 4 October 2017, as "highly personal data". The G29 considers that these data are considered sensitive, in the common sense of the term, insofar as they have an impact on the exercise of a fundamental right. Indeed, the collection of location data involves freedom of movement.34. By way of clarification, the Restricted Committee also recalls that the EDPS considered, in its guidelines 01/2020 relating to the processing of personal data in the context of connected vehicles and mobility-related applications (guidelines 01 /2020) that "When collecting personal data, vehicle and equipment manufacturers, service providers and other data controllers should bear in mind that location data is particularly indicative of habits The journeys made are very characteristic in that they can make it possible to deduce the place of work, the residence as well as the centers of interest (leisures) of the driver, and can possibly reveal sensitive information such as the religion, through place of worship, or sexual orientation, through places frequented. nt, vehicle and equipment manufacturers, service providers and other controllers should take particular care not to collect location data unless absolutely necessary for the purpose of the processing". These guidelines also emphasize that the collection of location data is subject to compliance with the principle that location can be activated "only when the user initiates a feature that requires knowing the location of the

vehicle, and not by default and continuously when starting the car ".35. In this context, the Restricted Committee recalls that the assessment of compliance with the principle of data minimization is based on the limited nature of the data processed to what is necessary with regard to the purpose for which they are collected. Its assessment involves carrying out an analysis of the proportionality of the personal data collected with regard to the intended purposes.36. Firstly, with regard to the management of the vehicle fleet and rental contracts, the rapporteur considers that the collection of geolocation data throughout the duration of the rental is not necessary. She considers 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 range of services it offers is based on the immediate availability of vehicles and flexibility involving adaptation to the needs of the user which evolve during the rental period. It recalls that the system is entirely dematerialized and that it operates in a closed loop: the vehicle must be picked up and brought back to the same station. It argues that limiting the collection of geolocation data to the scheduled rental end time would deprive it of the possibility of managing the fleet in a flexible way, depending on the actual location of the vehicles. The company also claims that it does not know in advance the actual end time of a rental and that customers can return the vehicle early simply by returning it to the departure station. Consequently, geolocation at regular intervals would be the only means of determining the vehicle's return time.38. The company argues, with regard to rental contracts, that geolocation allows it to deal with cases where the vehicle would be returned to somewhere other than its starting location, in particular to be able to end the rental or recover a vehicle parked at a wrong place. In addition, it maintains that it must be able to monitor the proper performance of the contract, for example during prohibited use of the vehicle outside motorable roads or outside national territory. Geolocation would also be necessary to control the entry and exit of a vehicle from urban toll zones (particularly in Madrid) and thus provide the customer with an immediate and automated billing service.39. The company maintains that it needs to know immediately if a vehicle has been used outside of the rental terms and conditions in order to prevent the vehicle from being put back into circulation, for safety reasons or "for reasons of good administration. of the service" (particularly insurance).40. The Restricted Committee takes note of the arguments put forward by the company to manage its fleet efficiently and flexibly.41. The Restricted Committee notes, however, that, for this purpose, the collection of vehicle geolocation data throughout the journey (every 500 meters when the vehicle is moving but also when the vehicle's engine is switched on or off and when the doors are opened or closed using a badge or the application) is not necessary.42. Indeed, the Restricted Committee notes that, on the one hand, to return the

vehicle, the engine must necessarily be switched off and, on the other hand, that this event triggers the geolocation of the vehicle. Thus, when a user turns on or off the engine of the vehicle, this vehicle transmits its geolocation to the company. If the company then finds that the vehicle is back at its starting point and that it is closed, it can end the current rental. The geolocation of the vehicle at this instant therefore makes it possible to determine whether the vehicle is at its starting point, ready to be returned. Conversely, the collection of geolocation data during the rest of the journey is not necessary to determine whether the vehicle has returned to its departure station in order to be returned.43. With regard to the case where the vehicle is returned to somewhere other than its starting 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 can only take place after the customer has contacted the company. In addition, the collection of the geolocation of the vehicle when the vehicle stops, at a place other than its starting point, combined with the information that the latter was not subsequently switched on, makes it possible, in this case , to have data allowing the end of the rental to be established, in connection with the user's telephone call. Furthermore, the Restricted Committee considers that, once the company is aware of the customer's wish to return the vehicle to another location, it can activate geolocation in order to manage this situation.44. With regard to compliance with the general conditions of use and in particular the use of the vehicle off roadways and outside national territory, the company, questioned on this subject during the restricted training session, did not provided elements relating to its effective use of geolocation data to detect such uses, nor to draw any consequences. In particular, it is not established whether geolocation data is used for these purposes and, if so, how and to what extent. In particular, the company has given no indication of the actions implemented when a vehicle leaves national territory. The Restricted Committee stresses in this respect that, in any event, the customer could be held responsible for any use of the vehicle outside the general conditions of use. The Restricted Committee notes, superabundantly, that the use of regular geolocation to identify the movement of a rented vehicle outside motorable roads is not usual 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 the geolocation of vehicles every 500 meters.45. With regard to the use of geolocation to control the entry and exit of a vehicle from a congestion charge zone, the Restricted Committee notes first of all that this does not concern (in the Member States of the Union concerned by the processing in question) than the city of Madrid. Next, an almost permanent collection of geolocation data on all rented vehicles, on the basis of legitimate interest, necessarily appears

disproportionate to the advanced purpose which is that of immediate and automated billing of costs to customers. . The Restricted Committee observes that this applies all the more so as regards the hiring of vehicles in cities other than Madrid.46. Secondly, with regard to the fight against vehicle theft, the rapporteur emphasizes that, in order to be considered proportionate, the processing of geolocation data must be rendered necessary for this purpose by a causal event, such as a declaration theft or suspected theft. Vehicle geolocation data cannot therefore be considered strictly necessary for the pursuit of the purpose linked to the risk of theft, before any triggering event.47. In defence, the company maintains that the collection of geolocation data every 500 meters makes it possible to find the vehicle in the event of theft or suspicion of theft, in particular when there are inconsistencies between the actual location of the vehicle and its intended place of return. Indeed, geolocation would be the only effective means of meeting the legitimate objective of preventing theft. The company maintains that it cannot ask customers about the location of the vehicle because, in 60% of the cases identified by Ubeeqo International in France in 2021, the customer is the author of the theft. In addition, the use of geolocation from a generating event would at best make it possible to obtain information that is too late, or even no information. Indeed, the geolocation systems would either be deactivated or rendered useless by placing the vehicle in an area where the signal could not emit (underground parking, etc.). Knowing the last known position of the vehicle would therefore make it possible to reduce the search area for the vehicle if it were stolen and no longer transmitted a signal.48. The Restricted Committee stresses that, as the rapporteur points out, before any triggering event, the geolocation data of vehicles cannot, in principle, be considered as strictly necessary for the pursuit of this purpose and their collection permanently or very closely must be regarded as excessive.49. By way of clarification, the Restricted Committee notes that the 01/2020 guidelines indicate that location data can only be fed back from the theft declaration and cannot be collected continuously the rest of the time. In this respect, the EDPS also recommends that the data controller clearly informs the data subject that there is no permanent tracking of the vehicle and that geolocation data can only be collected and transmitted from the declaration of vol.50. In addition, the Restricted Committee emphasizes that the assessment of the limited nature to what is necessary, within the meaning of Article 5.1.c of the GDPR, is informed by the provisions of recital 39 of the GDPR, according to which "[t]he personal data should only be processed if the purpose of the processing cannot reasonably be achieved by other means". The existence of less intrusive means to achieve the same purposes must therefore be taken into account, whether they are alternative means or data processed less frequently or in smaller numbers.51. The Restricted Committee takes note of the company's observations and in particular of the fact that, in

60% of cases of theft in France, the theft is caused by the user of the vehicle. In these cases, this user would therefore not report, or at least in a timely manner, the theft in question and would not provide the company with the last known position of the vehicle. However, in these hypotheses, the company has in principle the identity of this person, which was verified during the user's registration process, by collecting copies of an identity document and the conduct of that person.52. The Restricted Committee also notes that, therefore, in 40% of cases in France, the user not being the thief of the vehicle, he can communicate to the company the last known position of the vehicle before it disappears.53 . The Restricted Committee then notes that in the event that the vehicle disappears and the last known position is not communicated by the user, the company can in principle activate the geolocation of the vehicle remotely. It is only in cases where either the vehicle is in an area where the signal does not emit (white area or underground car park in particular), or the geolocation system has been dismantled for the purpose of theft, that the company does not will not have access to the geolocation of the vehicle. However, the proportion of these assumptions was not disclosed by the company.54. In this respect, the Restricted Committee considers that when the geolocation system has been knowingly rendered unusable, the information represented by the last known position of the vehicle has relative value with a view to searching for the vehicle.55. Thus, the Restricted Committee emphasizes that, in the light of the foregoing considerations, the cases where, on the one hand, geolocation is the only means of knowing the last known position of the vehicle and where, on the other hand, this last known position is actually close to the location of the vehicle, appear limited. In these situations, the restricted training does not call into question the usefulness of knowing the last known position of the vehicle thanks to the last geolocation data. However, this assumption is not sufficient to justify the collection of all geolocation data from all user 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 stresses that the absence of alternative means of preventing theft, which are less intrusive to the privacy of users, tends to reinforce the conclusion that it is disproportionate to base the prevention of vehicle theft on the quasi-permanent collection of geolocation data.57. In view of all of these considerations, the Restricted Committee considers that, in a large part of the cases of use, the collection of geolocation data every 500 meters during the rental of the vehicle is not necessary for the purpose of preventing vehicle theft. The fact of systematically carrying out this collection for use cases where it could be effectively useful, when other means of preventing and combating theft exist, on the basis of the legitimate interest of the company, appears disproportionate invasion of privacy. Indeed, as pointed out above, the company's

collection and storage of all the journeys of vehicle users leads it to handle and store highly personal data.58. Thirdly, with regard to the location of the vehicle in the event of an accident, the rapporteur maintains that the collection of geolocation data for this purpose can only take place after a causal event, in particular a request for assistance by the client, making this collection necessary.59. In defence, the company maintains that limiting the triggering of geolocation to the hypothesis of a request for assistance would be tantamount to depriving it of the possibility of providing assistance to its client even though it would be impossible for him to request it. . Also, identifying the last known location of the vehicle would be important when the vehicle is in an accident in a "white" area.60. The Restricted Committee first stresses that it is legitimate for the company to want to provide assistance to users who are victims of a traffic accident while renting a vehicle. However, 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, when the company becomes aware of the occurrence of an accident involving a rented vehicle, it can geolocate this vehicle in order, if necessary, to provide assistance to the user.62. On the other hand, the Restricted Committee considers that geolocation every 500 meters of all vehicles throughout the rental period, prior to any information relating to an accident, is not necessary to provide assistance to a user. The collection of quasi-permanent geolocation data is therefore neither adequate nor relevant with regard to this purpose.63. It follows from all of the above that the Restricted Committee considers that none of the purposes put forward by the company justifies the collection of geolocation data every 500 meters 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 frequentation, all the stops made during a daily journey, which amounts to putting in causes their freedom of movement. The Restricted Committee notes in this regard that it is apparent from the developments above that the company could offer an identical service without collecting geolocation data on an almost permanent basis.64. In addition, the Restricted Panel notes that the company has stated that its practice has evolved and that it no longer keeps a history of geolocation data. The Restricted Committee considers that this is a good practice, insofar as the risk of breaching the privacy of users is less significant. However, on the date of the inspections, the company kept a history of geolocation data in the Inovia.65 information system. The Restricted Committee therefore considers that these facts constitute a breach of Article 5.1.c of the GDPR.C. On the breach of the obligation to define and respect a retention period for personal data proportionate to the purpose of the processing pursuant to Article 5.1.e of the GDPR66. Under the terms of Article 5.1.e of the Regulation, personal data must be “kept in a form allowing the identification of the persons concerned for a period not

exceeding that necessary with regard to the purposes for which they are processed; personal data may be stored for longer periods insofar as they will be processed exclusively for archival purposes in the public interest, for scientific or historical research purposes or for statistical purposes in accordance with Article 89 , paragraph 1, provided that the appropriate technical and organizational measures required by this Regulation are implemented in order to guarantee the rights and freedoms of the data subject (limitation of storage) ".1. With regard to the retention period of geolocation data67. The rapporteur notes that it emerges from the company's data retention policy that the geolocation data of private customers are kept on an active basis for the duration of the commercial relationship and then for three years from the date of last activity. of the user. 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 are collected are linked to a rental contract for a specific vehicle and not to the entire commercial relationship, which lasts until the last expression of interest at the commercial relationship of the user (in particular: a rental or reservation in progress, the fact of clicking on a link in a newsletter, registration for a Ubeeqo offer or connection to the Ubeeqo account).68. In view of these elements, the rapporteur criticizes the company for not linking the retention period of geolocation data to each rental contract 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 contract is taken into consideration to start the retention period. It therefore considers that the geolocation data collected during the rental of a vehicle are kept for a period that exceeds the purposes for which they are processed.69. In defense, the company argues that it does not keep any geolocation data history. It argues that each geolocation data collected replaces the data previously collected, both in the Inovia information system and in the Phoenix information system. Thus, only the last known position of a vehicle is kept. Consequently, in her view, she cannot be criticized for retaining the geolocation data which she collects for an excessive period of time.70. The Restricted Committee recalls that the retention period for personal data 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 subject to intermediate archiving, for a fixed period, when their retention is necessary, for example for compliance with legal obligations or for pre-litigation or contentious. The Restricted Committee also stresses that the effectiveness of the implementation of a policy of data retention periods is the necessary counterpart to its definition and makes it possible to ensure that the data is kept in a form allowing the identification of persons concerned for a period not exceeding that necessary with regard to the purposes for which they are processed. This also makes it possible, in particular, to reduce the

risks of unauthorized use of the data in question, by an employee or by a third party (see CNIL, FR, October 29, 2021, Sanction, n° SAN-2021-019, published) .71. In this case, the Restricted Committee notes that it appears from the documents in the file that, on the date of the controls by the CNIL delegation, the company kept, in the Inovia information system, a history of geolocation data. Geolocation data was kept, in application of the retention period policy, on an active basis for three years from the date of the user's last activity. The starting point of the retention period for this data was thus linked to the end of the commercial relationship between the company and the user. This practice concerned part of the company's activity, i.e. the data collected in the countries where the Inovia information system was used (France, Italy and, partially, Belgium).72. However, the Restricted Committee notes that the purposes for which geolocation data are collected are not linked to this entire commercial relationship but to each vehicle rental contract. Indeed, with regard, firstly, to the purpose linked to the management of the fleet of vehicles and the rental contract, the geolocation data of the vehicle are no longer necessary for this purpose once the vehicle has been returned and the tenancy has ended. Secondly, with regard to the purpose linked to the prevention of theft, the geolocation data would only be necessary in the event of the theft of the vehicle, while the case is being examined by the competent judicial authorities or until the outcome of the a procedure for removing doubts that did not lead to confirmation of the theft of the vehicle. Thirdly, with regard to the purpose linked to the assistance of users in the event of an accident, if the geolocation data of vehicles may be necessary for the performance of an assistance service, they are no longer necessary from then on. that this service or the procedures related to it end.73. The Restricted Committee emphasizes that, where applicable, following procedures related to the theft of a vehicle or an accident, geolocation data in connection with these procedures may be retained by the company, in particular pursuant to obligations or to constitute evidence in the event of litigation and within the limit of the applicable limitation period. However, this data must be sorted and then kept in a dedicated archiving database, separate from the active database, for a period linked to the purposes sought. In addition, the starting point of the retention period for this data must be linked to the situations and events justifying the collection of this data and cannot, in this case, depend mechanically and systematically on the end of the commercial relationship. with the customer.74. Consequently, the Restricted Committee considers that the fact that the starting point of the retention period for geolocation data is linked not to the rental contract but to the end of the commercial relationship with the user did not make it possible to comply with the principle according to which personal data should not be kept for longer than is necessary for the purposes for which they are processed.75. In addition, it appears from the elements of the file that the company has modified

its geolocation data retention policy. Thus, on the date of the control by the CNIL delegation, the company kept, in the Inovia information system, a history of geolocation data. The Restricted Committee notes that the company maintains that this practice evolved during the present sanction procedure and that, from now on, no geolocation data history is kept. Indeed, each geolocation data collected would replace the data previously collected in the information system. The last data collected would therefore erase the previous one. Consequently, at a given moment, only the last known position of the vehicle is recorded in the information system.76. While the Restricted Committee takes due note of this development, it notes that this is not the practice that was observed during the review.77. The Restricted Committee concludes that the company has kept the geolocation data in question for a period that exceeds that necessary with regard to the purposes for which they are processed and has thus disregarded its obligations with regard to Article 5.1.e of the GDPR. 2. Regarding the effective implementation of the data retention policy78. The rapporteur criticizes the company for not respecting its retention policy insofar as it was found during the check that personal data relating to users who have been inactive for more than eight years were present in the information system. Inovia. The rapporteur maintains that the data are thus kept for a period exceeding the purposes for which they are processed.79. In defence, the company argues that the data in question would relate to its activity in the context of the offer 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 evidence in the file does not corroborate the company's assertion.81. Indeed, firstly, the Restricted Committee notes that, in its answer to the CNIL of July 10, 2020, in response to questions from the delegation as to the number of users in the database who have not connected to their account for more than three years, five years, eight years, the company provided extracts from the database of the Inovia information system showing personal data relating to […] users inactive for more than eight years, […] users inactive for more than five years and […] users inactive for more than three years. The Restricted Committee notes that, although the delegation of control asked to "distinguish by type of user, if applicable", the company produced only one result and did not mention the distinction between the users of the services offered to individuals and professionals.82. Secondly, the company had specified, in this same response, that "This result [gave] rise to additional investigations to understand the reasons justifying this result." The Restricted Committee holds that this tends to indicate that the company had then considered this result as not complying with its data retention policy.83. Third, the assertion that all the data in question relate to data collected in the context of 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 Inovia information system. Asked about this point during the restricted training session, 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, in distinguishing between data relating to services offered to professionals and data relating to services offered to individuals.84. The Restricted Committee considers that it has thus not been demonstrated that the data in question, which have been kept for more than three years, five years and eight years respectively, are exclusively data collected in the context of services offered to professionals. Therefore, the retention periods defined by the company should be applied to this data.85. Consequently, on the basis of the elements noted by the delegation of control and the elements of the company's response, the Restricted Committee considers that the company has kept the data in question for a period which exceeds that necessary with regard to the purposes for which they were used. are processed.86. In view of all of these elements, the Restricted Committee considers that the breach of Article 5, paragraph 1, e) of the GDPR is clear.D. On the breach relating to the obligation to inform individuals pursuant to Article 12 of the GDPR87. Article 12.1 of the Regulation provides that "the data controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 as well as to carry out any communication under Articles 15 to 22 and Article 34 with regard to concerns the processing to the data subject in a concise, transparent, comprehensible and easily accessible manner in clear and simple terms, in particular for any information intended specifically for a child. The information is provided in writing or by other means. including, where appropriate, electronically. […] “88. The rapporteur criticizes the company for not providing data subjects with the information referred to in Article 13 of the GDPR in a sufficiently accessible manner when collecting personal data for the purpose of registering for the Ubeeqo.89 service. In defence, the company argues that it was a malfunction, which has been corrected.90. The Restricted Committee notes first of all, by way of clarification, that with regard to the easily accessible nature of the information, the G29 specifies, in its guidelines of 11 April 2018 on transparency within the meaning of Regulation (EU) 2016/679, that "the "easily accessible" criterion means that the data subject should not have to search for the information but should be able to access it immediately: for example, this information could be communicated to the data subjects directly or by means of 'a link that would be addressed to them […] ". It “recommends as good practice that, in an online context, a link to the privacy statement or notice be provided at the point of collection of personal data, or that this information be searchable on the same page where the personal data is collected". These guidelines also state that the information "should be clearly differentiated from other non-privacy information such as contractual terms or general terms of use". The guidelines state that "the data subject should

not have to actively seek the information covered by [Articles 13 and 14] among other information such as the conditions of use of a site […] ".91. In this case, the Restricted Committee notes that, during the online check of May 26, 2020, by following the registration process of a user on the application, it was found that, to register, a user had to enter various personal data (first name, last name, date of birth, contact details) on a registration form. It was also found that the registration form contained a link to the general conditions of use. In this document, there was a link to the privacy policy of the company, in which was presented the information provided for in Article 13 of the GDPR.92. The Restricted Committee notes that the registration form page did not allow the user to directly access exhaustive information relating to data protection insofar as a course of several clicks was necessary to obtain it. It also notes that, to find out about information relating to the protection of personal data, people had to look for it among the general conditions of use. However, the presentation of information relating to the protection of personal data in a document accessible from a link present in the general conditions of use of the website 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 of the GDPR from the collection form, the latter must, at the very least, present a means such as a hypertext link allowing the user to easily take cognizance of all the mandatory information.93. The Restricted Committee notes that the company brought the registration form into conformity on this point during the procedure.94. However, it retains that, on the date of the inspection, the failure relating to the absence of information directly published or accessible on the interface for collecting personal data was characterized with regard to the provisions of Article 12 of the Rules.III. On the penalty and publicity95. Under the terms of III of article 20 of the modified law of January 6, 1978: "When the data controller or its subcontractor does not comply with the obligations resulting from regulation (EU) 2016/679 of April 27, 2016 or from the this law, the president of the National Commission for Computing and Liberties may also, if necessary after having sent him the warning provided for in I of this article or, if necessary in addition to a formal notice provided for in II, seize the restricted formation of the commission with a view to the pronouncement, after adversarial procedure, of one or more of the following measures: […] 7° With the exception of cases where the processing is implemented by the State, an administrative fine not to exceed 10 million euros or, in the case of a company, 2% of the total worldwide annual turnover of the previous financial year, whichever is higher. mentioned in 5 and 6 of article 83 of regulation (EU) 2016/ 679 of April 27, 2016, these ceilings are increased, respectively, to 20 million euros and 4% of said turnover. The restricted committee takes into account, in determining the amount of the fine, the criteria specified in the same article 83 ".96. Article 83 of the GDPR provides that

"Each supervisory authority shall ensure that the administrative fines imposed in under this Article for breaches of this Regulation referred to in paragraphs 4, 5 and 6 are, in each case, effective, proportionate and dissuasive", before specifying the elements to be taken into account in deciding whether to impose an administrative fine and to decide on the amount of this fine.97 The Restricted Committee recalls that it must take into account, for the imposition of an administrative fine, the criteria specified in Article 83 of the GDPR, such as the nature, gravity and duration of the breach, the measures taken by the controller to mitigate the damage suffered by the data subjects, the degree of cooperation with the supervisory authority and the categories of data to be acts personnel affected by the breach.98. Firstly, with regard to the imposition of a fine, the Restricted Committee considers first of all that the company has shown serious shortcomings in terms of the protection of personal data since breaches are made up of fundamental principles and basic principles of the GDPR, which are the principles of data minimization, limitation of the duration of data retention 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 minimization of personal data is particularly significant, given the particular nature of geolocation data. Indeed, the company proceeds to an almost permanent collection of geolocation data from the users of the vehicles it rents. The almost permanent collection of this geolocation data is particularly intrusive for users of rental vehicles. Indeed, it makes it possible to follow all the journeys made by the user, to identify the places where he goes, thus being able to reveal information on his behavior, his habits of life, which is likely to affect his freedom of movement and his private life.100. The Restricted Committee also points out that the personal data processed by the company concerns approximately […] users (customers and prospects), spread over the territory of six Member States of the European Union.101. With regard to the retention period of the data, on the one hand, geolocation data of the users were kept for an excessive period, which was not linked to the end of the rental contract, 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 area. 102. In addition, it is all the more important, in the context of the collection of geolocation data, that the company provides the data subjects with information in a transparent and accessible manner, within the meaning of Article 12 of the GDPR. Indeed, data subjects must be able to understand what data is collected, how this data is used and what their rights are. The Restricted Committee notes in this regard that in view of the boom in the collection of geolocation data, particularly in the context 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 with regard to the breaches of Articles 5.1.c, 5.1.e and 12 of the GDPR.104. Secondly, with regard to the amount of the fine, the Restricted Committee recalls that paragraph 3 of Article 83 of the Rules provides that in the event of multiple violations, as is the case here, the total amount of the fine cannot exceed the amount set for the most serious violation. Insofar as the company is accused of breaching Articles 5.1.c, 5.1.e and 12 of the Regulations, the maximum amount of the fine that may be withheld is 20 million euros or 4% of the turnover worldwide annual turnover, whichever is higher.105. The Restricted Committee recalls that administrative fines must be effective, proportionate and dissuasive. It considers in particular that the activity of the organization and its financial situation must be taken into account in particular for the determination of the sanction and in particular, in the event of an administrative fine, of its amount. It notes in this respect that the company reports a turnover in 2020 of around […] euros for a net profit […] euros. […] . The Restricted Committee also recalls that the company is a subsidiary of the Europcar Mobility Group. This group achieved an average turnover of […] euros over the years 2018, 2019 and 2020.106. Therefore, in the light of the relevant criteria of Article 83(2) of the GDPR mentioned above, the Restricted Committee considers that the imposition of an administrative fine of 175,000 euros appears proportionate.107.Thirdly, s With regard to the publication of the penalty, the Restricted Committee considers that, in view of the plurality of breaches noted, their seriousness and the particular nature of the data concerned, the publication of this decision is justified.FOR THESE REASONSThe Restricted Committee of the CNIL, after having deliberated, decides to: - pronounce against the company Ubeeqo International an administrative fine of 175,000 (one hundred and seventy-five thousand) euros with regard to the breaches constituted 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 website e of the CNIL and on the Légifrance site, its deliberation, which will no longer identify the company Ubeeqo International by name at the end of a period of two years from its publication. The chairman Alexandre LINDEN This decision is likely to object of an appeal before the Council of State within two months of its notification.