Decision no.MED 2021-013 of 1st April 2021 issuing an order to comply to the company [redacted]

(No. MDM211014)

The Chair of the *Commission Nationale de l'Informatique et des Libertés* (French Data Protection Authority),

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

Having regard to Act no.78-17 78-17 of 6 January 1978 amended, on information technology, data files and liberties (French Data Protection Act), its Article 20 in particular;

Having regard to Decree no.2019-536 of 29 May 2019, implementing Act no.78-17 of 6 January 1978 on information technology, data files and civil liberties;

Having regard to Deliberation no.2013-175 of 4 July 2013 adopting the Internal Rules of Procedure of the *Commission Nationale de l'Informatique et des Libertés*;

Having regard to decision no.2019-13C of 27 December 2019 of the Chair of the *Commission Nationale de l'Informatique et des Libertés*, tasking the Secretary-General with performing or assigning a third party to conduct an investigation of the [redacted] company;

Having regard to Online Investigation Record no.2020-013/1 of 15 January 2020;

Having regard to Onsite Investigation Record no.2020-013/2 du 23 January 2020;

Having regard to Referral no.19018488;

Having regard to the other items in the case file.

I. Context

The [redacted] (hereinafter, the "Company"), better known under its former trade name [redacted], runs a platform for rental of vehicles (cars and motorbikes) which puts vehicle owners in contact with private individuals. It employs about 133 people at its head office, located at [redacted]. Its turnover in 2018 was [redacted] euros.

In the context of its activity, the Company publishes [redacted] website and the [redacted] mobile application, which target consumers living in France and other European Union countries.

The platform provides two ways of renting vehicles:

- using the [redacted] technology, which enables the customer to unlock the hired car using a smartphone (via a unit installed in the vehicle) without meeting the owner. Identity documents and driving licenses, which are required for rentals, are checked directly by the application, as are driver records. If the check of supporting documents fails (due to poor quality document or suspicion of fraud), the user can have them checked manually by sending an email to the Company's customer service. The

email is automatically turned into a ticket by the [redacted] company, a subcontractor specialising in management of customer relations, utilised by [redacted];
- without [redacted]: in this case, users have to make physical contact with car owners, who check the supporting documents and hand them the car keys in person.

On 15 October 2019, a complaint was referred to the *Commission nationale de l'informatique et des libertés* (hereinafter, the "CNIL" or the "Commission") from one of the Company's customers, who reported that his driving license was accessible via any browser with no authentication required, by entering an URL that connected to the [redacted] software tool. The complainant also stated that despite his making several requests for deletion to the Company's services, his driving license was still freely accessible on the date of the referral.

Pursuant to The Chair of the Commission's Decision no.2020-13C of 27 December 2019, a CNIL Delegation conducted an online investigation of the Company's website on 15 January 2020 and an onsite investigation at the Company's premises on 23 January 2020, in order to check whether the personal data processing operations it implemented were in compliance with Regulation no.2016/679 of the European Parliament and the Council of 27 April 2016 on personal data protection (hereinafter, the "GDPR").

In a mail sent on 14 February 2020 subsequent to the onsite control, the Company stated that it "*had been able to get the [redacted] tool's configuration modified so that any documents sent by [its] users via email would no longer generate the URL link. Users who send documents by email now receive a confirmation email with the said document as a simple attachment"*.

On 27 May 2020, following the Company's communication of documents requested in the context of the onsite investigation, the CNIL's departments conducted a complementary investigation on the documents, in the context of which the Company was requested to complete a questionnaire before 1 July 2020.

On 3 July 2020, the Company sent the CNIL's departments the completed questionnaire.

On 3 September 2020, in the context of the cooperation procedure, a draft decision was submitted to the authorities concerned on the basis of Article 60 of the GDPR.

II. Breaches of the GDPR's provisions

A. A breach of the obligation to define and comply with a retention period proportionate to the purposes of the processing

Pursuant to Article 5, Paragraph 1, e) of the GDPR, "personal data shall be *kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed*".

In this instance, although the onsite investigation showed that the Company had defined a policy on data retention periods in a document entitled "*Privacy deletion policies*", the Company's representative nonetheless told the Delegation that, in practice, there had been no restrictions on retention periods for users' data relating to creation of their accounts on the [redacted] platform since the Company's creation.

In its letter of 3 July 2020, the Company stated that its database contained the accounts of 874,000 users whose last connection had been in 2016 but that it was able to specify the number of users who had connected for the last time before 2016.

Finally, the Company's representatives stated that there was no intermediate archiving of data.

The aforementioned facts constitute a breach of the obligations of Article 5, Paragraph 1, e) of the GDPR. It is therefore the company's responsibility to define and enforce retention periods for user data.

B. A breach of the obligation to comply with requests for erasure of data

Under Article 17, Paragraph 1, a) of the GDPR, "*The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed*".

In this instance, the case file shows that, since 30 August 2019, the complainant at the origin of Referral no. 19018488 has requested the Company on several occasions to erase his driving license, which had been made freely accessible via a link automatically generated by the [redacted] software tool.

During the onsite investigation conducted on 23 January 2020, the Delegation found that the Company had not erased the driving license, which was still accessible via the aforementioned link.

Although, in its letter of 14 February 2020, the Company stated that any documents that users sent by email would no longer generate a URL link, in its response of 3 July 2020 to the questionnaire sent by the Delegation it nonetheless wrote that it was "*unable to delete the links that had previously been created and that these therefore still exist*".

This most recent statement makes it clear that the Company has not yet erased the complainant's driving license.

Moreover, during the onsite investigation and in their letter of 14 February 2020, the Company's representatives stated that when it receives a request for erasure, the Company "*anonymises"* the data subject's customer record in the customer management tool. However, the Investigation Delegation found that, despite such "anonymisation", the user's number was still in the database.

In its Opinion 05/2014 of 10 April 2014, which provides useful hints on assessment of a piece of data's identifiable character, the Article 29 Working Party (WP29) defined anonymisation as the result of "processing personal data in order to irreversibly prevent identification".

In this case, customer records created by the Company are not anonymised within the meaning of the GDPR, as it is still technically possible to re-identify customers from their

user numbers. For example, an attacker who managed to unlawfully infiltrate the Company's servers would be able to take note of these numbers, which are also stored unencrypted, and cross-reference them with other indirectly identifying personal data in their possession in order to try to discover the identities of the individuals behind such data.

It follows that the general data erasure procedure implemented by the Company does not guarantee data subjects' right to erasure.

The aforementioned facts constitute a breach of the obligations resulting from Article 17 of the GDPR. It is the company's responsibility to comply with requests for the deletion of personal data that are made to it.

C. A breach of the obligations relating to data processors

Under Article 28, Paragraph 3of the GDPR, all processing implemented by a data processor must be governed by a contract, concluded between the data controller and the processor which binds both parties, "*sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller"*. Hence, the contract must include a series of mandatory terms, as detailed in points a) to f) of the same Article.

In this instance, during the onsite investigation, the Delegation was informed that the Company had entrusted verification of the identities of its users' profiles to two service providers, [redacted] and [redacted].

[redacted] has developed a robot responsible for validating the various supporting documents provided by users (driving license, identity document and video selfies). When the robot does not validate a profile (e.g. because of the poor quality of a photo), the check is carried out manually by a [redacted] employee.

It follows that [redacted] and [redacted] process personal data on behalf of [redacted] and therefore act as data processers for the Company.

However, the Inspection Delegation found that the service provision contract concluded with [redacted] on 9 July 2019 and the one concluded with [redacted] on 25 July 2019 do not specify all the terms provided for by Article 28, Paragraph 3 of the GDPR.

The contract concluded with [redacted] does not define the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, or the obligations and rights of the controller. Nor does it specify that the processor undertakes to:

- process the personal data only on documented instructions from the controller (Article 28, 3. a));
- respect the conditions […] for engaging another processor (article 28, 3. d));
- assist the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 (Article 28, 3. f));
- delete or return all the personal data to the controller after the end of the contract (Article 28, 3. g));

- make available to the controller all information necessary to the carrying out of audits (article 28, 3. h)).

Although the contract concluded with [redacted] defines the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, it does not include any of the terms listed in Article 28, Paragraph 3 of the GDPR.

The aforementioned facts constitute a breach of the obligations resulting from Article 28 of the GDPR. It is the responsibility of the company to complete the subcontract.

D. A breach of the obligation to keep a record of processing activities

A combined reading of Paragraphs 1 and 5 of Article 30 of the GDPR makes it clear that a data controller with over 250 employees and/or which carries out processing of personal data on a regular basis must maintain a record of processing activities carried out under its responsibility.

Such record must contain the following information:
- the name and contact details of the controller,
- the purposes of the processing,
- a description of the categories of data subjects and of the categories of personal data,
- the categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organisations,
- the envisaged time limits for erasure of the different categories of data,
- a general description of the technical and organisational security measures referred to in Article 32, Paragraph 1 of the GDPR.

In this case, although the Company has fewer than 250 employees, it carries out a variety of personal data processing operations regarding prospects and customers, for such purposes as marketing, customer management and combating fraud. Insofar as the Company's main activity is based on a platform that puts vehicle renters and owners in contact with each other, there can be no doubt that such processing is carried out on a regular basis.

However, statements made by the Company's representatives make it clear that, on the date of the onsite investigation, the Company did not keep a record of processing activities.

The aforementioned facts constitute a breach of the obligations resulting from Article 30 of the GDPR. It is the company's responsibility to set up this record of processing activities.

E. A breach of the obligation to ensure data security and confidentiality

Under Article 32 of the GDPR, "*the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk [including by guaranteeing] the ongoing confidentiality, integrity, availability and resilience of processing systems and services*".

Firstly, as regards the security measures applied to supporting documents that platform users send by email, in its letter of 14 February 2020, the Company stated that it had requested its

processor to modify the [redacted] tool's configuration so that any documents emailed by users would no longer generate the URL link, and that users who send supporting documents by email now receive a confirmation email with the said documents as attachments.

However, in its letter of 14 February 2020 and in the response on 3 July 2020 to the questionnaire sent by the Delegation, the Company stated that it was "*unable to delete the links that had previously been created [by the* [redacted] *tool] and that these therefore still exist*". Nonetheless, it asserted that the URL links that had been created could not be the subject of brute force attacks as they contained several lines of characters, that such length could not be retrieved and that it therefore applied a robust rule of "*security through obscurity*".

Although it is true that the length of the URLs in question makes it unlikely that a brute force attack against them would succeed, the simple fact that the supporting documents they link to are accessible without prior authentication is a risk factor all too likely to compromise the confidentiality of data subjects' personal data. For example, as the URLs are apparently hosted in [redacted] servers' logs unencrypted, an attacker who unlawfully infiltrated the servers could easily transcribe the web addresses in order to access users' supporting documents and make use of them for the purpose of identity theft.

Secondly, as regards the security measures applied to storage of platform users' passwords, the Company stated during the onsite investigation that it had been using the Bcrypt algorithm since 2013 and that this security measure covers 3,083,296 user accounts.

In its letter of 14 February 2020, the Company stated that 164,394 user account passwords created before 2013 are retained in a database in hashed format, using the SHA1 algorithm with salt. It also stated that, since 27 January 2020, users whose passwords are hashed with the SHA1 algorithm have had to use the "*I've forgotten my password*" functionality when they want to authenticate themselves on their accounts and so obtain a new password hashed under the Bcrypt +salt standard. Hence, accounts operating with SHA1 passwords have not been usable since 27 January 2020.

The above information makes it clear that, although the Company has ensured that authentication on the platform is now only possible in accounts whose passwords are hashed by the Bcrypt algorithm, it still retains the passwords to over 150,000 user accounts in a form that does not ensure their confidentiality.

The SHA1 hashing function has known vulnerabilities that make it impossible to guarantee integrity and confidentiality of passwords in the event of a brute force attack after the servers hosting them have been compromised. Inasmuch as a great many internauts use the same password to authenticate themselves on their various online accounts, attackers could well exploit these 150,000 users' passwords to infiltrate their other accounts in order to perpetrate thefts or scams.

Thirdly, as regards the security measures applied in the context of replies to right of access requests, during the onsite investigation the Company's representatives stated that data to which right of access is requested are communicated to data subjects via two separate emails: one containing a data extract in CSV format, in the form of an encrypted archive, and the other containing the password to the archive.

Although the Company encrypts the archive containing personal data, it sends the password to it by the same channel, so exposing the data communicated to a risk of compromise in the event of an attacker's intrusion into the data subject's inbox or interception of emails by an unauthorised third party.

The aforementioned facts constitute a breach of the obligations resulting from Article 32 of the GDPR. It is the company's responsibility to ensure the security of the personal data it processes.

Consequently, the [redacted] company, located at [redacted], is issued an order to comply, <u>within three (3) months as from notification of this decision</u> and subject to measures that it may already have adopted, by:

- **defining and implementing a policy on a retention period for its customers' and prospects' data** that does not exceed the period necessary for the purposes for which they are collected, pursuant to Article 5, Paragraph 1, e) of the GDPR, in particular by purging or ensuring effective anonymisation of data retained beyond the period defined, and, for example, by implementing an effective procedure for archiving such data with restricted access;
- **defining and implementing an effective right to erasure procedure**, pursuant to Article 17 of the GDPR, and, in particular, deleting the complainant's supporting documents and erasing or ensuring effective anonymisation of customer records on individuals who have requested that all their personal data be erased;
- **completing the contracts with [redacted] and [redacted] by including the missing terms**, pursuant to Article 28, Paragraph 3 of the GDPR;
- **keeping a record of processing activities carried out under its responsibility** pursuant to Article 30 of the GDPR;
- **taking all necessary security measures for all personal data processing carried out, so as to ensure the security of such data and prevent unauthorised third parties from accessing them**, pursuant to Article 32 of the GDPR, in particular:
  - by making all supporting documents still retained in the form of links in the [redacted] tool inaccessible by third parties without prior authentication, possibly by having them communicated in the form of attachments, as has been done for supporting documents sent following modification of [redacted] configuration;
  - by replacing the SHA1 hashing algorithm with salt by an algorithm acknowledged to be strong, for passwords to the [redacted] user accounts concerned, possibly by obliging users to c r by deleting their passwords;
  - by using different channels for sending personal data in the form of encrypted archives and the password, possibly by sending the password by SMS when the encrypted archive is sent by email.
- **justifying to the CNIL that it has complied with all of the above requests within the time-limit set.**

After this time-limit has expired, if [redacted] has complied with this order, this procedure will be considered closed and a letter to that effect will be sent to it.

However, if [redacted] has not complied with this order, a rapporteur will be appointed and may request that the Restricted Committee impose one of the sanctions provided for in Article 20 of the Act of 6 January 1978 amended.

The Chair

Marie-Laure DENIS