Deliberation 2021-043 of April 12, 2021Commission Nationale de l'Informatique et des LibertésLegal status: In force Date of publication on Légifrance: Saturday May 08, 2021NOR: CNIL2113933XDeliberation no. of personal data implemented in the context of the designation of drivers who have committed an offense against the highway codeThe National Commission for Computing and Liberties,

Having regard to Convention No. 108 of the Council of Europe for the protection of individuals with regard to automatic processing of personal data;

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, in particular its article 58 ;

Considering the law n° 78-17 of January 6, 1978 modified relating to data processing, files and freedoms, in particular its article 8-I.2°-b;

Considering the decree n° 2019-536 of May 29, 2019 taken for the application of the law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms;

After having heard Mr. Alexandre LINDEN, Commissioner in his report and Mr. Benjamin TOUZANNE, Government Commissioner, in his observations;

Adopts a frame of reference relating to the processing of personal data implemented in the context of the designation of drivers who have committed a traffic offense and set out in the appendix. FRAMEWORK FOR THE DESIGNATION OF DRIVERS WHO HAVE COMMITTED A HIGHWAY CODE OFFENSE (ADOPTED ON APRIL 12, 2021)You can consult the full text with its images from the extract from the authenticated electronic Official Journal accessible at the following address : https://www.legifrance.gouv.fr/download/pdf?id=GBvgUKHKeeZs1ZeR0qI6hMUY8eb3PQb7gVXkk-wrWOs1. Who is this reference for?

This reference system is intended for employers under public or private law providing their employees with vehicles, user companies, professionals providing their customers, for a fee or free of charge, with so-called replacement vehicles, as well as vehicle rental companies short and long term (hereafter organisms).

The term vehicle rental companies refers to all organizations offering, as a main or ancillary activity, a vehicle provision service in exchange for rent, regardless of the duration. Car manufacturers, banking companies and credit institutions offering such a service can thus be considered as vehicle rental companies.

Organizations identifying and designating the driver in the event of a traffic violation must ensure their compliance:

- the provisions of the general data protection regulations (GDPR) as well as those of the amended Data Protection Act of 6 January 1978 (LIL);

- other rules that may apply, in accordance with the regulations in force, in particular the highway code.2. Scope of the reference This reference relates to the processing of personal data commonly implemented by organizations relating to the identification of drivers in the context of the management of litigation related to the recovery of traffic offenses.

Its purpose is to provide a compliance support tool for people and organizations identifying and designating the driver in the event of a traffic offense via the automated infringement control system.

This standard does not relate to the management of the post-parking package (FPS), whose payment procedure does not provide for the designation of the driver to exempt the holder of the registration certificate from payment.

This reference has no binding value. In principle, it makes it possible to ensure the compliance of the data processing implemented by the organizations with the principles relating to data protection, in a context of changing practices in the digital age.

Organizations that deviate from the reference system with regard to the particular conditions relating to their situation may do so.

They may nevertheless be asked to justify the existence of such a need and the measures implemented to guarantee compliance of the processing with the regulations on the protection of personal data.

The repository is not intended to interpret the rules of law other than those relating to the protection of personal data. It is up to the actors concerned to ensure that they comply with other regulations that may also apply, in particular the highway code.

This reference also constitutes an aid to the realization of an impact analysis relating to data protection (DPIA), in the event that this is necessary.

Organizations can also refer to the methodological tools offered by the CNIL on its website in order to facilitate the compliance of the processing implemented. They will thus be able to define the measures to ensure the proportionality and necessity of their processing (points 3 to 7), to guarantee the rights of individuals (points 8 and 9) and to control their risks (point 10) . The organizations will also be able to rely on the CNIL guidelines on DPIA. If the organizations have appointed one, the data protection officer (DPD/DPO) must be consulted.3. Objectives pursued by the processing (purposes) All processing must meet

a specific objective and be justified with regard to the missions and activities of the organization.

Processing relating to the identification and designation of drivers who have committed or may have committed an offense may in particular be implemented in order to: - designate with the National Agency for the Automated Processing of Offenses (ANTAI) the person who was driving or was likely to drive the vehicle when the offense was observed;

- follow the procedure for recovering violations of the highway code for which the public or private bodies referred to above may be liable;

- produce anonymous statistics with a view to adapting road safety training.

The information collected for one of these purposes cannot in principle be reused to pursue another objective which would be incompatible with the initial purpose. Any new use of data must in fact respect the principles of protection of personal data, in particular the principle of the purpose of the processing (for example, the processing implemented for the purposes set out above must not give rise to interconnections or exchanges other than those necessary for the accomplishment of these).4. Legal bases of the processingEach purpose of the processing must be based on one of the legal bases set by the regulations (article 6 of the GDPR). (See for an explanation of the rule: Lawfulness of processing: the main points on the legal bases provided for by the GDPR).

It is up to the data controller to determine these legal bases before any processing operation, after having carried out a reflection, which he can document, with regard to his specific situation and the context. Having an impact on the exercise of certain rights, these legal bases are part of the information that must be brought to the attention of the persons concerned.

The table reproduced below aims to provide data controllers with assistance in identifying the legal bases likely to be used in the most common cases.

These elements must be adapted to the specific situation of each organization concerned. Thus, for example, depending on whether the body in question is in the private or public sector, certain processing operations that nevertheless serve the same purpose may be based on different legal bases (for example, legitimate interest in the private sector and performance of a mission of public interest in the public sector).

Purposes

Legal basis

Designation and identification of the driver

Legal obligation in accordance with the provisions of Article L. 121-6 of the Highway Code

Follow-up of the procedure for recovering traffic violations and management of litigation

Legitimate interests

Realization of anonymous statistics

Legitimate interests5. Personal data concerned5.1. Principles of relevance and minimization of data Under the principle of minimization of data, the data controller must ensure that only the data necessary for the pursuit of the purposes of the processing are actually collected and processed. Data relating to:

a) The procedure for designating the driver;

b) Monitoring the collection procedure. The table reproduced below provides illustrations of the data that the CNIL considers to be in principle suitable according to the purposes of the processing.

Data categories

Sample Data

To the procedure for designating the driver (these are the data transmitted to the ANTAI)

Driver information

Name, usual name, first names, sex and, where applicable, title of the person; date and place of birth, postal address and, if applicable, e-mail address;

driver's license number.

Vehicle Information

Registration number of the vehicle concerned.

Information relating to the employer when he rents his fleet of vehicles

Surname, first names and contact details of the data controller and, where applicable, of a contact within the organization concerned.

Rental Information

Number and date of the notice of contravention;

If applicable, date and time of the start and end of the rental;

If applicable, date and time of the offence.

Monitoring of the recovery procedure by the data controller

Number, date and time of the vehicle rental or provision contract; vehicle registration number; possible file number communicated by ANTAI; date and method of designation; customer identification data: surname, first names, date of birth, postal address; amount of the fine.5.2. The processing of data relating to offenses and convictionsCertain data processed in the context of the designation of drivers calls for increased vigilance due to their particularly sensitive nature. Benefiting from specific protection, they can only be collected and processed under conditions strictly defined by the texts.

Such data may only be processed in compliance with the legal provisions relating to offense data (art. 46 of the LIL). In this case, their processing is authorized by specific provisions of national law, namely Articles A. 121-1 et seq. of the Highway Code.6. Recipients of data and access to information Personal data can only be made accessible to persons authorized to know it with regard to their duties.

In general, access authorizations must be documented by the organizations, and access to the various processing operations must be subject to traceability measures. See point 10 relating to safety.

The data controller who wishes to use a subcontractor must ensure that he only uses organizations that offer sufficient guarantees. A contract, defining the characteristics of the processing as well as the different obligations of the parties in terms of data protection, must be established between them (article 28 of the GDPR). A subcontractor's guide, published by the CNIL, recalls these obligations and gives examples of clauses to be included in the contracts.6.1. Persons accessing the data on behalf of the data controllerOnly persons authorized by virtue of their missions or functions may access the personal data processed, and this within the limits of their respective attributions and the accomplishment of these missions and functions.

It may be, for example, people responsible for the administrative management of staff.6.2. Recipients of dataThe GDPR defines recipients as any organization that receives the communication of data.

In the context of this repository, the following may in particular be recipients of the data:

- ANTAI;

- the public prosecutor's officer;

- temporary employment companies.7. Data retention A precise retention period for the data must be set according to each purpose: this data cannot be kept for an indefinite period.

The data retention period or, when it is impossible to set, the criteria used to determine this period, is part of the information

that must be communicated to the persons concerned.

It is the responsibility of the controller to determine this duration before implementing the processing.7.1. Storage periods It is recommended that the data collected and processed for the purposes of designating drivers be kept in the active database for a period of forty-five days from receipt of the ticket, unless legal or regulatory provisions to the contrary or particular case.

The data may be kept longer than the durations mentioned above, in intermediate archiving, in certain specific cases, for example if the data controller has a legal obligation (for example, to meet accounting, social or tax) or if he needs to constitute proof in the event of litigation and within the limit of the applicable limitation/foreclosure period (for example, the duration of the prescription in contraventional matters is twelve months). The duration of the intermediate archiving must however respond to a real need, duly justified by the data controller after a preliminary analysis of various factors, in particular the context, the nature of the data processed and the level of risk of a possible dispute.

Within the framework of an agreement with the ANTAI, all exchanges of information between the organization and the ANTAI on the drivers of vehicles who have committed a traffic offense should be suppressed by the organization once the designation made.

When the employee's missions involve driving a vehicle as their main activity (driver, delivery man, ambulance driver, etc.) or when frequent travel is necessary for the proper performance of the contract (salesperson, technician, etc.) and provided that the employee has freely consented to it, the body should be able to keep the elements necessary for the designation of a driver longer in order to avoid the latter having to provide the same data many times for possible subsequent designations .7.2. Retention of anonymized data The regulations relating to the protection of personal data do not apply, in particular with regard to retention periods, to anonymized data. These are data that can no longer be linked to the identified natural person to whom they relate.

Anonymization must be distinguished from pseudonymization. In the latter case, it is technically possible to trace the identity of the person concerned using third-party data. The pseudonymization operation is reversible, unlike anonymization.

Thus, the data controller can keep the anonymized data without a time limit.

To find out more, you can refer to the CNIL guides:

- Security: Archive securely;

- Limit the retention of data;

- Practical guide: retention periods. Anonymization is a process that consists of using a set of techniques in such a way as to make it impossible, in practice, to identify the person by any means whatsoever and this in an irreversible manner. Also, once anonymised, the data can no longer be linked to a person (For more information, you can refer to the EDPS guidelines on anonymisation).8. Information of persons Processing of personal data must be implemented in complete transparency vis-à-vis the persons concerned.8.1. Content of the information to be provided The information communicated to the persons concerned must be provided under the conditions provided for in Articles 12, 13 and 14 of the GDPR.

From the stage of the collection of personal data, the persons concerned must in particular be informed of the existence of the processing, of its essential characteristics (including the identity of the person in charge of the processing and the objective pursued) and of the rights they have.

Examples of information notices are available on the CNIL website and can be consulted in the GDPR section: examples of information notices .8.2. Methods of issuing information In order to fully respect the principles of loyalty and transparency, in accordance with the provisions of Articles 13 and 14 of the GDPR, individuals must be directly or indirectly informed at the time the data is collected.

If the GDPR does not impose any specific form, written information should be preferred, so as to be able to justify its content, as well as the time when it was issued.

Within the framework of this standard, the data controller informs the persons concerned by any appropriate means in accordance with the provisions of Article 12 of the GDPR.9. Rights of personsThe persons concerned have the following rights, which they exercise under the conditions provided for by the GDPR (to go further, see the section entitled Understanding my rights on the CNIL website):

- the right of access, allows the person concerned to know if data concerning him are processed by the data controller and, in this case, to obtain details of the conditions of this processing and, at his request, to Obtain a copy of the data concerning him held by this person in charge;

- the right of rectification, allows the person concerned to request the rectification of inaccurate or incomplete information concerning him;

- the right to erasure, allows the data subject to ask an organization to erase personal data concerning him;

- the right to limit processing: for example, when the person disputes the accuracy of their data, they can ask the organization

to temporarily freeze the processing of their data, while it carries out the necessary checks;

- the right to object to the processing of data concerning the person, subject to the conditions for exercising this right pursuant to the provisions of Article 21 of the GDPR. The person concerned may object to the processing of their data at provided that he invokes reasons relating to his particular situation, and only when the processing is implemented on the basis of the legitimate interest of the controller, or for the performance of a task in the public interest or a task under public authority.

The controller may refuse to respond to this request for opposition if he demonstrates that he has legitimate and compelling interests which prevail over the rights and freedoms of the applicant.

With regard to this standard, the data controller appears to be able to refuse to grant such a request in the context of monitoring the recovery procedure, insofar as he has legitimate and compelling interests which prevail over the rights and freedoms of the applicant, except in special circumstances.

Please note: The data controller must respond to requests received as soon as possible and within a maximum of one month. If additional time is necessary to process the request (for example, due to its complexity), the data subject must be informed within this same period of one month. In all cases, a response must be provided within a period which may not exceed three months.

The exercise of rights by individuals must be facilitated by the data controller and be free of charge. The persons concerned must be informed of their possibility of lodging a complaint with the National Commission for Computing and Liberties if they are not satisfied with the processing of personal data concerning them.10. SecurityThe organization must take all necessary precautions with regard to the risks presented by its processing to preserve the security of personal data and, in particular, at the time of their collection, during their transmission and their storage, to prevent them from being distorted, damaged or that unauthorized third parties have access to it.

In particular, in the specific context of this standard, the organization is invited to implement the following measures, or to be able to justify the implementation of equivalent measures or their absence of necessity or possibility (the individuals processing a small volume of data take, for example, basic security measures to ensure the security and confidentiality of the data they process):

Categories

Measures

Educate users

Inform and raise awareness of the people handling the data

Write an IT charter and give it binding force

Authenticate users

Define a unique identifier (login) for each user

Adopt a user password policy in accordance with the recommendations of the CNIL

Force user to change password after reset

Limit the number of attempts to access an account

Manage authorizations

Define authorization profiles

Remove obsolete access permissions

Carry out an annual review of authorizations

Trace access and manage incidents

Provide a logging system

Inform users of the implementation of the logging system

Protect logging equipment and logged information

Provide procedures for personal data breach notifications

Securing workstations

Provide an automatic session locking procedure

Use regularly updated anti-virus software

Install a software firewall

Obtain the user's agreement before any intervention on his workstation

Securing Mobile Computing

Provide encryption means for mobile equipment

Make regular data backups or synchronizations

Require a secret to unlock smartphones

Protect the internal computer network

Limit network flows to what is strictly necessary

Securing the remote access of mobile computing devices by VPN

Implement WPA2, WPA2-PSK, or WPA3 protocol for Wi-Fi networks

Securing servers

Limit access to administration tools and interfaces to authorized persons only

Install critical updates without delay

Ensure data availability

Securing websites

Use the TLS protocol and verify its implementation

Check that no password or identifier is transmitted in the URLs

Check that user input matches what is expected

Put a consent banner for cookies not necessary for the service

Back up and plan for business continuity

Perform regular backups

Store backup media in a safe place

Provide security means for the transport of backups

Plan and regularly test business continuity

Archive securely

Implement specific access procedures for archived data

Securely destroy obsolete archives

Supervise the maintenance and destruction of data

Record maintenance interventions in a logbook

Supervise by a person in charge of the organization the interventions by third parties

Erase data from any hardware before disposal

Manage subcontracting

Include a specific clause in subcontractor contracts

Provide the conditions for restoring and destroying data

Ensure the effectiveness of the guarantees provided (security audits, visits, etc.)

Secure exchanges with other organizations

Encrypt data before sending

Make sure it's the right recipient

Transmit the secret in a separate send and through a different channel

Protect the premises

Restrict access to premises with locked doors

Install intruder alarms and check them periodically

Supervise IT developments

Offer privacy-friendly settings to end users

Test on fictitious or anonymized data

Use cryptographic functions

Use recognized algorithms, software and libraries

Store secrets and cryptographic keys securely To do this, the data controller may usefully refer to the Personal Data Security Guide.11. Impact analysis relating to data protection (AIPD) Pursuant to the provisions of Article 35 of the GDPR, the controller may have to carry out an impact analysis when the processing it implements is likely to pose a high risk to the rights and freedoms of data subjects.

You should first refer to:

- the list of processing operations for which an impact analysis is not required;

- then, to the list of types of processing operations for which an impact analysis relating to data protection is required;

- if the processing implemented is not present on one of these lists, it is then necessary to question the need to carry out a DPIA. To do this, it is advisable to rely on the criteria established by the European Data Protection Board (EDPB) in the Guidelines on Data Protection Impact Assessment (DPIA).

As soon as it is implemented in a company with less than 250 employees, this processing is on the list of types of processing

operations for which no DPIA is required.

If, on the other hand, it is implemented in a company with more than 250 employees or by a rental company in the context of large-scale processing, the processing must be the subject of an impact analysis as soon as when he meets at least two of the nine criteria established by the EDPS and more particularly those relating to:

- personal data relating to criminal convictions or offences;

- vulnerable people (employees);

- on a large scale. To carry out an impact analysis, the data controller may refer to:

- the principles contained in this reference system;

- the methodological tools offered by the CNIL on its website. If the organization has designated one, the DPD/DPO must be consulted.

In accordance with Article 36 of the GDPR, the data controller must consult the CNIL prior to the implementation of the processing if the impact analysis indicates that he is unable to identify sufficient measures to reduce the risks to a acceptable level.

The president,

M. L. Denis