Decision No MED 2024-066 of 23 May 2024 issuing an order to [redacted]

(No MDM241026)

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 of the Council of 27 April 2016 on the protection of personal data and on the free movement of such data, in particular Articles 56 and 60;

Having regard to Law No 78-17 of 6 January 1978 on data processing, data files and individual liberties, as amended, in particular Article 20;

Having regard to the French Postal and Electronic Communications Code, in particular Article L34-5;

Having regard to Decree No 2019-536 of 29 May 2019, as amended, for the application of Law No 78-17 of 6 January 1978 on data processing, data files and individual liberties;

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

Having regard to decision No 2022-148C of 29 September 2022 of the Chair of the CNIL (French Data Protection Authority) to instruct the Secretary General to carry out or have carried out an audit mission of the data processing implemented by [redacted];

Having regard to online inspection report No 2022-148/1 of 20 October 2022;

Having regard to on-site inspection report No 2022-148/2 of 6 December 2022;

Having regard to the other exhibits in the case file;

I - The context

[redacted] (hereinafter "the company") is a simplified joint stock company specialising in the retail trade of automotive equipment. Created on [redacted] 2008, its registered office is [redacted] ([redacted]). It has 163 employees and in 2022 generated revenue of more than €[redacted] for a net loss of €[redacted]. Since 2015, the company has been a subsidiary of the [redacted].

The company's business is the sale of automotive parts via the internet, from the website [redacted] and its establishment located at [redacted]

Pursuant to Decision No 2022-148C of 29 September 2022 of the Chair of the Commission nationale de l'informatique et des libertés (hereinafter "the Commission" or "CNIL"), on 20 October 2022, the CNIL carried out an inspection of the website [redacted] and on 6 December 2022 an inspection mission at the company's premises, at [redacted], to verifycompliance of the processing implemented by the latter with all the provisions of Law No 78-17 of 6 January 1978 on information technology, files and freedoms, as amended (hereinafter "LIL") and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter the "Regulation" or "GDPR").

Additional requests were sent by the CNIL on 24 April 2023, to which the company responded by email on 5 May 2023. On 7 July 2023, the company informed the CNIL that it had appointed a data protection officer who was also the DPO of [redacted]

On 15th April 2024, as part of the cooperation procedure, a draft was submitted to the relevant authorities on the basis of Article 60 GDPR.

This project did not give rise to relevant and reasoned objections.

The company collects personal data such as the last names, first names, addresses, email addresses, phone numbers and bank details / IBAN of its customers or prospects, from its website [redacted] and phone conversations from customer service, for the following purposes, specified in its privacy policy updated on 17 July 2023:

- order management;
- accounts receivable management;
- management of the [redacted] loyalty programme;
- assistance with choosing parts compatible with the vehicle;
- the fight against fraud involving means of payment and unpaid amounts;
- recording phone conversations with Customer Service;
- management of customer/product reviews;
- commercial prospecting;
- organisation of competitions;
- statistical analyses to optimise the website and marketing campaigns;
- statistical studies with a view to personalising the offer;
- managing contacts outside the scope of an order;
- processing of requests to exercise rights of access, rectification, deletion, limitation, objection and portability.

II – On breaches relating to GDPR

1 - A breach of the obligation to define a specific, explicit and legitimate purpose of the processing

In law, Article 5-(1)(b) GDPR provides that data must be *"collected for specified, explicit and legitimate purposes".*

In the case in point, the company collects the email address entered by users when registering for the newsletter from the dedicated insert on the home page of the website [redacted]. However, the delegation noted that the company did not send the newsletter to users who had registered.

In fact, the company kept their email addresses in the database and in the strategic customer relationship management tool (CRM [redacted]).

Under these conditions, the company retains the email addresses of certain users of its website registered for the newsletter without a specified, explicit and legitimate purpose.

These facts constitute a breach of Article 5(1)(b) GDPR.

It follows from the foregoing that [redacted] must cease collecting the email address of users when they register for the newsletter if this address is not communicated to them.

2 - A breach of the obligation to collect adequate, relevant and limited data

In law, Article 5(1)(c) GDPR states that personal data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')".

Compliance with the principle of minimisation in the context of the implementation of the processing of personal data is assessed in particular with regard to a requirement of subsidiarity, as confirmed by Recital 139 GDPR, according to which "[p]ersonal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means".

In the case in point, the delegation noted that, when creating a customer account, the registration fields relating to the postal address and phone number must be filled in by the user. However, the delegation found that it was possible to place an order without creating a customer account, in "visitor" mode.
In this sense, the postal address and phone number are not necessary information when creating a customer account, since this action is not systematically associated with the fulfilment of an order.

Thus the collection of this personal data does not appear adequate, relevant and limited to what is necessary when creating a customer account.

Under these conditions, the collection of the postal address and phone number of website users who create a customer account without placing an order does not comply with the principle of minimisation.

These facts constitute a breach of Article 5(1)(c) GDPR.

It follows from the foregoing that the company must collect data relating to the customer's postal address and phone number only when the customer makes a purchase requiring delivery.

3 - Obligation of transparency and provision of information to individuals

In law, Article 12(1) GDPR provides that "[t]he controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and […] relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language […] The information shall be provided in writing, or by other means, including, where appropriate, by electronic means.*"*

The principle of transparency in processing requires controllers to inform all data subjects of their inclusion on an exclusion list as soon as it is implemented, as well as the associated reason, the means of contesting the decision or rectifying the situation and the existing means of redress. The controller must also inform these data subjects when they are no longer included on the blacklist.

In the case in point, as part of the fight against fraud, the company collects and reconciles its customers' personal data via scoring processing, which enables it to verify orders with a view to identifying errors, potential fraud and unpaid amounts.

According to the website's privacy policy, the legal basis for the processing is based on the legitimate interest of the company in protecting itself against fraud and non-payment.

When an alert is detected, the customer's order is blocked and the consistency of the buyer's profile, the level of risk associated with the order and its possible history are checked. Depending on the buyer's profile and the fraud score calculated by the company, customer information, such as bank card payment attempts, IP address, postal address and email address and phone number, is escalated for further verification. In case of doubt about the order, customer service contacts the buyer by phone to confirm certain information.

Users of the [redacted] website are informed of the implementation of this processing within the company's privacy policy.

However, in the event of confirmed fraud, the customer can be placed on a blacklist so that he/she can no longer place an order on the [redacted] website. This list includes his/her billing and delivery address, which may correspond to his/her home address, email address, phone number and bank details. It thus constitutes the processing of personal data.

However, the delegation found that data subjects were not informed of their inclusion on the exclusion list, of the associated reason, of the means to challenge the decision or regularise the situation as well as of the existing means of appeal and of their possible withdrawal. Under these conditions, the principle of transparency of processing is not respected.

These facts constitute a breach of Article 12 GDPR.

It emerges from the foregoing that [redacted] must inform any data subject of his/her inclusion on an exclusion list as soon as it is implemented as well as the associated reason, the means to challenge the decision or regularise the situation, the existing remedies and his/her withdrawal from the blacklist.

4 - A breach of the obligation to ensure data security and confidentiality

In law, Article 32(1) GDPR requires that the controller, "[t]aking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, […] shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk".

It follows from these provisions that the controller is required to ensure that the automated data processing it implements is sufficiently secure. The sufficiency of the security measures is assessed (a) with regard to the characteristics of the processing and the risks it entails, and (b) with consideration of the state of knowledge and the cost of the measures.

a) Regarding the robustness of passwords

In law, the CNIL recalled that the implementation of a robust authentication policy constituted an elementary security measure that contributed to compliance with the obligations of Article 32 GDPR (CNIL, FR, 24 November 2022, Sanction, No SAN-2022-021, published). Thus it was necessary to ensure that a password that could be authenticated on a system could not be disclosed.

In its Deliberation No 2022-100 of 21 July 2022 adopting a recommendation on passwords and other shared secrets, which is not mandatory but which provides relevant information on the security measures that should be taken, the CNIL recommends that, to ensure a sufficient level of security and confidentiality, if authentication is based solely on an identifier and a password, the password be composed of at least 12 characters including upper case, lower case, numbers and special characters to be chosen from a list of at least 37 possible special characters, or be composed of at least 14 characters including upper case, lower case and numbers, without any mandatory special character, or, when it corresponds to a sentence comprising words in the French language, be composed of at least seven words.

Failing this, the CNIL considers that a sufficient level of security and confidentiality can also be ensured by authentication based on a password at least eight characters long, made up of three different categories of characters but accompanied by an additional measure such as, for example, a temporary ban on access to the account after several unsuccessful attempts, the duration of which increases with each attempt, the implementation of a mechanism to protect against automated and intensive submissions of attempts (e.g. "captcha") or the blocking of the account after several unsuccessful authentication attempts (maximum 10).

In the case in point, on the one hand, with regard to user access passwords to the [redacted] website, the delegation noted that authentication required an identifier and a password, the latter being able to be composed of only six characters. In addition, no additional measures to restrict access to the account, such as a blocking measure in the event of repeated failed login attempts, are implemented.

On the other hand, with regard to passwords for access to the CRM [redacted] application, the internal customer relationship management tool, the additional information received by the CNIL on 9 May 2023 indicated that the passwords for access to the CRM [redacted] application had to meet the following complexity requirements:

- be at least eight characters long;
- contain upper and lower case characters;
- contain at least one numeric character and one special character.

In addition, no additional measures to restrict access to the account, such as a blocking measure in the event of repeated failed login attempts, are implemented.

However, such configurations do not make it possible to guarantee in an optimal manner the security of the personal data processed (postal address, mobile phone number, email address), to which the password allows access by logging into the user account. Indeed, a password composed of six or eight characters is characterised by a low level of complexity, which is not sufficient to guarantee robustness against attempts to connect by third parties and, contrary to deliberation No 2022-100, the company has not implemented additional measures aimed at ensuring a similar level of security, which would have allowed the use of entropy passwords lower than the level required by the aforementioned deliberation.

Under these conditions, the insufficient complexity of the passwords used to authenticate customer accounts on the one hand and the CRM [redacted] application on the other hand does not comply with the principle of data security and confidentiality.

These facts constitute a breach of Article 32 GDPR.

It follows from the foregoing that more restrictive security measures should be adopted regarding access to customer accounts and the CRM [redacted] application in order to prevent access to data by unauthorised third parties.

b) Regarding the procedures for storing passwords

In law, it follows from Article 32 GDPR that the controller must store user passwords in a sufficiently secure manner in order to avoid their compromise and to protect the personal data that may be consulted and collected by accessing the databases.

In its deliberation No 2022-100 of 21 July 2022 adopting a recommendation on passwords and other shared secrets, the CNIL recalled that the use of the hash function made it possible not to store passwords in clear text in the database but only in the form of an imprint.

In particular, it recommends that any password useful for authentication verification and to be stored on a server be previously transformed by means of a non-reversible and secure cryptographic function. By way of illustration, this should be a reputable public algorithm whose software implementation is free of known vulnerabilities, such as HMAC functions using SHA-256, bcrypt, scrypt or PBKDF2, incorporating the use of a salt or key.

In the case in point, with regard to the hash function used to store customer passwords in the database, the delegation noted that [redacted] uses the hash function SHA-256.
However, this function is not designed to allow the secure storage of passwords as such. Indeed, the speed of calculation of this hash function could allow an attacker with access to the hashed passwords to create a correspondence table between all the most common passwords and their derivative resulting from the execution of the SHA-256 function in order to find the original passwords from their hashed version in the database.

Under these conditions, [redacted], by using the hash function SHA-256 for storing passwords, does not comply with the principle of data security and confidentiality.

These facts constitute a breach of Article 32 GDPR.

The company must therefore transform passwords before their storage into a database, including passwords generated on its websites, using a specialised, non-reversible and secure cryptographic function.

c) Regarding the management of identifiers and access rights to the production environment

In law, the CNIL recalls that pursuant to Article 32 GDPR, the controller must put in place appropriate measures to ensure the confidentiality of data and prevent it from being processed illegally by persons who do not have a need to know it (CNIL, FR, 29 October 2021, Sanction, No SAN-2021-019, published).
In the current state of the art, the ANSSI has drawn up specific recommendations in its guide on the secure administration of information systems, specifying in particular that *"Individual administration accounts must be allocated to each administrator".*

In its guide on the security of personal data, the CNIL also recommends *"defining a unique identifier per user and prohibiting accounts shared between several users."*

In this respect, common (or shared) accounts do not allow proper application of the authorisation policy, which is a fundamental element of information system security, aimed at limiting access to only the data that a user needs. Thus only individual accounts allow the traceability of the accesses and actions carried out by each operator on the database. Indeed, shared accounts make it much more difficult to attribute an action and complicate the investigation work in the event of fraudulent access, deterioration or deletion of personal data.

In addition, in accordance with the basic rules relating to the security of information systems, to be effective a password must remain secret and individual.
In the case in point, with regard to accounts providing access to the production environment, the delegation noted that the database's production environment was accessible via registered accounts and an administrator account. Access to the administrator account was stored in a digital safe and reserved for three people. However, the use of non-individual accounts meant that it was not possible to accurately identify users' connections to and use of the administrator account.

However, the non-individualised access to the database production environment by the administrator account did not guarantee the proper application of the authorisation policy, a fundamental element of information system security, and was therefore not compliant with the state of the art.

Under these conditions, non-individualised access to the administrator account did not guarantee secure management of access rights.

These facts constitute a breach of Article 32 GDPR.

It follows from the foregoing that [redacted] must implement an individual identification method on behalf of the administrator of the production environment.

d) Regarding access to the information system by third-party administrators

In law, the CNIL recalls that pursuant to Article 32 GDPR, the controller must put in place appropriate measures to ensure the confidentiality of data and prevent it from being processed illegally by persons who do not have a need to know it (CNIL, FR, 29 October 2021, Sanction, No SAN-2021-019, published).

In the current state of the art, the ANSSI has drawn up specific recommendations in its guide on the secure administration of information systems, specifying for example that: *"To strengthen the authentication of third-party administrators, the use of a second authentication factor, possibly retained by the entity, is recommended."* (Recommendation 67) or that "*The accounts of third-party administrators must be deactivated by default and activated on request*" (Recommendation 66).

In the case in point, with regard to third-party access to the company's internal tools (CRM), the delegation noted that the service provider [redacted] had administrator access to the CRM application without specific measures to limit the risk presented by providing a third party with an administrator account with extensive powers over the information system. However, access to a company's information system by a third-party structure, generally remotely, constitutes a major risk of compromise when it involves permanent, unsupervised and unrestricted access to maintenance operations.

Under these conditions, the management of third-party administrator accounts does not guarantee the security of third-party access to the CRM application and does not present the required level of security.

These facts constitute a breach of Article 32 GDPR.

It follows from the foregoing that [redacted] must take all necessary measures to guarantee the security of the personal data processed, in particular by strengthening the authentication of third-party administrator accounts for the CRM application.

III. On the breach of Article L34-5 of the French Post and Electronic Communications Code

In law, article L34-5 of the French Post and Electronic Communications Code states that "direct prospecting by electronic mail is authorised if the recipient's contact details have been collected from him/her, in compliance with the provisions of Law No 78-17 of 6 January 1978 relating to information technology, files and civil liberties, in connection with a sale or the provision of services, if the direct prospecting concerns similar products or services provided by the same natural or legal person, and if the recipient is offered, in an express and unambiguous manner, the possibility of objecting, free of charge, apart from those linked to the transmission of the refusal, and in a simple manner, to the use of his/her details at the time they are collected and

each time an electronic canvassing email is sent to him/her in the event that he/she has not refused such use from the outset."

In the case in point, the delegation noted that [redacted] carries out prospecting electronically with its users, whether or not they have a customer account, for products and services similar to the orders they carry out.

However, users may not object in advance, when they place an order, to the receipt of marketing emails for similar products and services. A single mention informs persons that they will be able to object directly by logging into their customer space or from the unsubscribe links present in the messages received.

Under these conditions, the absence of the possibility offered to object in advance and in a simple manner to commercial prospecting based on the exception of similar products and services does not comply with the legal conditions for implementing commercial prospecting.

These facts constitute a breach of Articles L34-5 of the French Postal and Electronic Communications Code.

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

- **delete the email addresses of users without a customer account who have filled in the field dedicated to registering for the company newsletter on the [redacted] website, which are collected without purpose;**

- **collect data that is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed, by ceasing to collect and keep the postal address and phone number of users creating a customer account;**

- **inform the persons when they are registered on the blacklist as well as the associated reason, the means to challenge the decision or regularise the situation, as well as the existing means of appeal and their unsubscription;**

- **take all security measures, for all the processing of personal data that it implements, to preserve the security of such data and prevent unauthorised third parties from having access to it, in particular:**

  - by implementing a binding policy on passwords used by users of the website and the CRM [redacted] application, in particular in terms of complexity or additional authentication measures;

- by transforming passwords before their storage into a database, including passwords generated on its websites, by means of a specialised, non-reversible and secure cryptographic function incorporating salt and time and/or memory settings necessary for its attack;
- by implementing an individual identification method for access to the administrator account of the production environment;
- by taking all necessary measures to ensure the security of the personal data processed, in particular by strengthening the identification of third-party administrator accounts to the CRM application.

- **offer users who place an order a means of objecting before commercial prospecting for similar products and services.**

This order does not require a response from you to the CNIL. On the other hand, if the persistence or repetition of the breaches referred to in the order were found during subsequent verifications, I could appoint a Rapporteur within the CNIL and refer the matter to the Restricted Committee of the CNIL, without a new order being sent to you beforehand, so that one or more of the corrective measures set forth in Articles 20 et seq. of the Law of 6 January 1978 may be pronounced, where applicable.

The Chair

Marie-Laure Denis