Decision no. MED 2021-007 of 28 January 2021 issuing an order to comply to [redacted]

(N° MDM[redacted])

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 the free movement of such data, particularly its articles 56 and 60;

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

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 regulations of the Commission Nationale de l'Informatique et des Libertés;

Having regard to decision no. 2019-080C of 7 May 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 perform an investigation on all processing of personal data, bearing whole or partially on data relating to the marketing and use of products and services attached to the [redacted] product, and encompassing all organisations concerned in their impleme

Having regard to records of investigation nos. 2019-080/1 of 20 June 2019, 2019-080/2 of 4 July 2019 and 2019-080/3 of 1 August 2019;

Having regard to the other items in the case file;

I. The procedure

[redacted] (hereinafter "the company"), located at [redacted], is a simplified joint-stock company established in 2016. The and recorded a turnover of around [redacted] euros in 2018, with a negative result of [redacted] euros.

The company markets the [redacted] children's smart watch, which, via the mobile application published by the company, enables parents to view the geolocation of children wearing the smart watch in real time, send them voice messages, and predefine delimited areas which the children are not authorised to leave.

The company markets the [redacted] in France via its website [redacted], which also has English, Spanish and German extensions, and in the United Kingdom, Spain and Germany via Amazon's website.

Pursuant to decision no. 2019-080C of 7 May 2019 of the Chair of the Commission Nationale de l'Informatique et des Libertés (the French Data Protection Commission, hereinafter the "CNIL"), a CNIL delegation carried out two online investigations on 20 June 2019 and 1 August 2019, and an onsite investigation at [redacted] on 4 July 2019.

These investigations focused largely on information brought to data subjects' knowledge as regards processing of personal data carried out by the company, obligations relating to subcontracting, and the obligation to ensure data security.

On 8 October 2020, in the context of the cooperation procedure, a draft decision has been submitted to the supervisory authorities concerned on the ground of article 60 of the Regulation (EU) 2016/679 of the European Parliament and Council of 27 April 2016.

This draft decision has not given rise to any relevant and reasoned objections.

II. Breaches

A breach of the obligation to inform data subjects of the processing of their data

Articles 12 and 13 of Regulation (EU) 2016/679 of the European Parliament and Council of 27 April 2016 (hereinafter referred to as the "GDPR" or "Regulation") require the data controller to provide data subjects with full information on the processing implemented, and do so in "*concise, transparent, easily intelligible*" fashion.

Firstly, the delegation found that the information provided to the purchaser of a [redacted] smart watch using the [redacted] mobile application is incomplete as it does not contain all the points provided for in Article 13 of the GDPR.

First of all, **the general conditions** of use available on the [redacted] website and the [redacted] mobile application do not contain all the information provided for in Article 13 of the GDPR. Although the general conditions of use identify the data collected (including name, physical address, IP address, email address and geolocation data) and state that they are used "*for the sole purposes of creating the functionalities expected of* [redacted] *SAS Software and monitoring commercial relations with users, for security purposes in compliance with the applicable laws and regulations and to enable improvement and personalisation of the products and services provided to users and the information communicated to them"*, they do not specify the legal basis for their processing, the data retention period or at the very least the criteria used to determine such period, or make mention of the existence of the right to limitation and portability of data or the right to make a complaint to a supervisory authority.

The same is true of **the confidentiality policy**, acceptance of which is required for creating an account on the [redacted] mobile application. Although the delegation found that the confidentiality policy informs [redacted] mobile application users that their personal data is processed by [redacted] in order to provide and improve the service, and in particular to "*process your orders, comply with legal procedures, respond to emergencies, develop and inform you of new products and services, monitor, assess and improve our products, services, systems and networks, and personalise your experience with our services*", it contains no information on the legal basis for the processing, the data retention period or at the very least the criteria used to determine such period, or make mention of the existence of

the right to limitation and portability of data, the existence of the right of objection, access, rectification and erasure (only in the case of the confidentiality policy) or the right to make a complaint to a supervisory authority.

Secondly, the delegation found that the information provided by the company in its confidentiality policy and general conditions of use is not concise or easily intelligible within the meaning of Article 12 of the GDPR.

First of all, the confidentiality policy lacks clarity. Its titles tend to be ambiguous and repetitive ("*collection and use of information*", "*use of personal information*", "*authorisations*") and are not clearly prioritised due to lack of graphic consistency: some titles are in bold, while others are underlined.

Furthermore, information on one and the same subject is scattered among several sections, in particular as concerns data recipients, thus hampering its intelligibility.

Finally, the confidentiality policy contains a great deal of vague, generic wording, e.g. "*we may share personal and non-personal information with affiliated entities for approved business purposes*" or "*we may access, monitor, use or divulge your personal information and communications in order to do such things as*: (…) *protect the rights and property of ourselves, our employees, our members, our customers and other persons*, (…) *respond to emergencies, launch, provide, invoice and receive services* (…)". The same is true of the general conditions of use, which, for example, state that data collected are used "*for the sole purposes of creating the functionalities expected of* [redacted] *SAS software"* without it being possible for users to determine the functionalities provided by the smart watch involve processing of personal data.

This results in the user being unable to fully understand the way their personal data is processed by [redacted]

Taken together, these facts constitute a breach of Articles 12 and 13 of the GDPR, which require the data controller to provide, at the time the data are collected and in "*concise, transparent, intelligible and easily accessible*" fashion, information on the legal basis for the processing, recipients of personal data, the personal data retention period and data subjects' rights.

A breach of the obligation to have processing operations carried out on behalf of the data controller governed by a formal legal act

Article 28 of the GDPR provides that processing carried out by a processor on behalf of a data controller must be governed by a contract that sets out the conditions under which the processor undertakes to carry out processing operations on behalf of the data controller, and also contains information on the controller's obligations and rights.

The delegation was informed that [redacted] subcontracted the processing of [redacted] smart watches' geolocation data to the company [redacted] for the purpose of displaying weather forecasts on the watch.

The delegation found that the contract concluded between [redacted] and [redacted] did not contain the clauses provided for by Article 28 of the GDPR.

These facts constitute a breach of obligations of Article 28 of the Regulation.

A breach of the obligation to ensure the security of personal data

Article 32 of the GDPR requires the data controller to ensure a level of security of the processing it carries out appropriate to the risks involved.

On the absence of encryption of communications

During the onsite investigation of 4 July 2019, the delegation was informed that all requests sent to the [redacted] server by the application and the smart watch are in non-secure "http" format.

Yet a connection via a non-secure channel makes all information exchanged vulnerable, including the identifiers and passwords enabling connection to the tool.

The data controller should therefore encrypt the channel used for all requests sent to the [redacted] server by the application and the smart watch in order to protect the confidentiality of data so exchanged.

On the absence of authentication of requests

The online investigation of 1 August 2019 showed that the company has not implemented a system for authentication of communications between the application and the server.

As a result, the origin and authenticity of requests are not guaranteed, which results in a risk of identity theft and access to data by unauthorised individuals.

It is therefore the company's responsibility to implement a system ensuring authentication of requests between the [redacted] application and the [redacted] sever (by means of a TLS protocol, for exampl [redacted] er only accepts legitimate requests, i.e. coming from known users of the server who have right of access to various of its resources.

On inadequate security of passwords

Firstly, the investigation delegation found that the data controller had taken measures to ensure that very simple passwords were refused, both during creation of a user account in the [redacted] application and during employees' connection to the database containing data collected by [redacted] smart watches.

Although such measures may be regarded as best practices, in this case they proved to be inadequate. As regards users, the delegation found that a password composed of nine characters with two types de characters was accepted when an account was created, with no complementary measure such as blocking the account after several unsuccessful attempts at connection. Likewise, as regards employees' access to the database containing data collected by [redacted] smart watches, the delegation was informed that a password composed of ele [redacted] th four types of characters was accepted, with no complementary measure such as blocking the account after several unsuccessful attempts at connection.

Yet authentication based solely on use of an inadequately robust password may lead to associated accounts being compromised and attacks by unauthorised third parties, brute force [redacted] for example The processing carried out by the [redacted] application and the [redacted] server makes data identifying minors accessible, so carrying a major risk for data subjects in the event of illegitimate access to such data.

As an illustration, in its deliberation no. 2017-012 of 19 January 2017, the CNIL considered that, in order to meet password robustness requirements and ensure adequate levels of security and confidentiality, a password must contain at least twelve characters and include at least one uppercase letter, one lowercase letter, one figure and one special character. When a password is composed of eight characters, containing three of the four categories of characters, it must be accompanied by a complementary security measure (such as blocking the account after several unsuccessful attempts at connection) in order to ensure adequate levels of security and confidentiality.

Secondly, the delegation was informed that no password renewal policy had been implemented.

Thirdly, the delegation found that the application account's password hashing algorithm used in the database and the password modification URL is the MD5 algorithm, which is now deemed obsolete in terms of security insofar as it has widely known vulnerabilities that make it easily reversible in the event of passwords being divulged in their hashed form.

On lack of traceability of accesses

The delegation was informed that access to the base containing data collected by smart watches was via a "root" account (an account possessing the system's highest level of rights) shared by two of the company's employees.

Allowing two technicians to share an account giving access to the database containing data collected by smart watches is a practice that does not reliable authentication of users and, in consequence, makes management of authorisations and traceability of accesses and individual actions impossible. Such lack of traceability also makes it impossible to identify individuals gaining fraudulent access to, damaging or erasing data.

These facts go to show that the security measures implemented do not ensure an adequate level of security of the personal data processed and that they therefore constitute a breach of obligations of Article 32 of the Regulation.

In light of the above, the company , located , is hereby given an order to comply, within six (6) months from the notification of this decision and subject to measures it may already have adopted, to:

- **inform the individuals from whom personal data is collected, in compliance with the provisions of Articles 12 and 13 of the GDPR,** in particular by providing them with full, easily intelligible information on the legal basis for the processing, personal data recipients, data retention periods or at the very least the criteria used to determine such periods, the existence of the right to limitation and portability of data, the existence of the right of objection, access, rectification and erasure (only in the case of the confidentiality policy) and the right to make a complaint to a supervisory authority;

- **make additions to the contract** concluded between and so that it includes all the in icle 28-3) of Regulation (EU) 2016/679;

- **for all personal data processing operations implemented, take all necessary security measures to enable maintenance of such data's security and prevent unauthorised third parties accessing them,** in particular:
    - by encrypting the channel used for connection to the production database, e.g. by using the HTTPS protocol;
    - by implementing a system ensuring authentication of requests between the [redacted] application and the [redacted] server, and only authorising those that are legitimate (e.g. by means of a TLS protocol);
    - by implementing a binding policy on passwords, in particular in terms of complexity, in line with the following modalities:
        - passwords composed of at least 12 characters, containing at least one uppercase letter, one lowercase letter, one figure and one special character; or
        - passwords composed of at least 8 characters, containing 3 of the 4 categories of characters (uppercase letters, lowercase letters, figures and special characters) and accompanied by a complementary measure such as delaying access to an account after several failures, inclusion of a mechanism protecting against intensive automated attempts (e.g. "captcha") and/or blocking the account after several unsuccessful attempts at authentication (10 at most);
    - by providing for renewal of passwords (every six months, for example);
    - by ensuring that each technician logs on to the base containing data collected by [redacted] smart watches using their own individual identifier and password;
- **justify, to the CNIL, compliance with all of the above requests within the time-limit set.**

After this time-limit, if the company [redacted] has complied with this order to comply, this procedure shall be considered closed and a letter shall be sent to it to this end.

However, if the company [redacted] has not complied with this order to comply, a rapporteur shall be appointed and may request that the restricted committee issue one of the penalties set out under Article 20 of the Act of 6 January 1978, amended.

The President

Marie-Laure DENIS