EDPS prior-check Opinion on *"stress screening test based on heart rate variability (Lifestyle assessment)"* at the Committee of the Region.

Brussels, 17 December 2015 (Case 2015-0509)

1. Proceedings

On 11 June 2015, the European Data Protection Supervisor ("the EDPS") received a notification for prior checking under Article 27(2)(a) of Regulation 45/2001 ("the Regulation") from the Data Protection Officer ("the DPO") of the Committee of the Regions ("CoR"). The notification concerns a new processing operation related to the measurement and assessment of the level of stress of staff members based on their heart rate variability and daily habits.

According to Article 27(4) of the Regulation, this Opinion must be issued within a period of two months, that is, no later than 17 December 2015, taking into account suspensions due to requests for further information[1].

2. Facts

Purpose and Data subjects

In the context of the CoR's stress and burnout prevention, its medical service envisages to offer its staff the possibility to undergo a stress level measurement assessment carried out by an external contractor. This test will provide them with an assessment report on how to better manage stress and psychosocial risks in the workplace. Staff members may participate in this program on a voluntary basis.

Legal basis and lawfulness

- Articles 3 and 8 of the Belgian Royal Decree of 10 April 2014 regarding the prevention of psychological risks at work; these provisions oblige the employer to analyse and chart possible psychological risks at work;
- The participation to the test is on a voluntary basis under Article 5(d) of the Regulation.

Procedure and data processed

The CoR will negotiate a service contract for one year with an external Finnish contractor (Firstbeat). A draft contract has been sent to the EDPS as well as other related documents.

The draft contract provides that "*personal data may be processed alone or together with Firstbeat's and its subsidiary companies' personal data files. Any transfer of personal data outside such companies is subject to data subject's separate consent ... Personal data may be*

[1] The case was suspended for further information from 16 June 2015 to 26 June 2015, from 23 July 2015 to 29 September 2015 and 20 November 2015 respectively and for comments from the DPO and the controller from 3rd December 2015 to 10 December 2015.

processed by Firstbeat, its subcontractor or third party service provider (who has obtained from Firstbeat a right to use the Service and offer the Service for its customers as a service provider) by an authorised third party wellness specialist pursuant to the Finnish Data Protection Act. Such authorised third party wellness specialist is entitled to use the Service independently as agreed with Firstbeat. "The "*authorised third party wellness specialist*" mentioned is the CoR's nurse It is also mentioned that personal data will be "*used anonymously for statistical and marketing research purposes*".

Participants have a first contact with the nurse of the CoR's medical service who will attach a measurement device with electrodes on their chest for their heart beat measurement. They may then log in to an online server, select a language and click on "start" providing the following information: first name, last name, date of birth, gender, height, weight, job classification, estimation of aerobic fitness, long-term medication and illnesses, ten questions related to physical activity, eating habits, alcohol consumption, stress, energy level, adequacy of sleep, etc. Participants should then set the date and the time they started their measurement. Furthermore, they are given the opportunity to complete a journal with information for the measurement days and additional information, such as relaxing or stressful moments, or exercise session in order to get more benefits from the assessment. It is up to the participants to provide Firstbeat with their address and phone number or any additional information through the online server.

The device and the online provision of relevant information to the server should last three days and three nights minimum.

When the measurement period is finished, participants will return the measurement device to the CoR's nurse. She will connect the device to the Firstbeat server and upload the measurements. An assessment report will be available to the participants at that moment. Participants can access their report by their own individual account connection that they had created initially when starting the measurements.

The CoR's nurse will be trained by the external contractor in order to be able to explain to the participants the results of their assessment report and coach them how to improve their daily life.

Right of information

Participants will be informed through a "*legal notice regarding data processing in respect of the 'Lifestyle Assessment' test*" (privacy notice). This document will be available on the intranet of the medical service and participants will receive a copy when the heart rate measurement device is handed to them.

Rights of access and rectification

The notification states that participants may exercise their rights of access and rectification by sending an e-mail to the medical service of the CoR. They may correct any inaccurate or incomplete personal data in their medical file. They may ask to remove their assessment report from their medical file..

However, the CoR, in reply to the EDPS' questions, stated that, this is no longer the case, as the CoR Medical Service will not keep the assessment report, only the list of participants' names.

Retention policy
The medical service of the CoR will propose to Firstbeat to adopt a two-year retention period, so that if participants decide to re-do the test within this period, they will be able to compare the results.

Anonymous data will be used for statistical and marketing research purposes. This means that names, e-mail addresses and group information how an individual may be identified will be deleted from the server of Firstbeat. Firsbeat will keep heartbeat readings together with age and sex.

Storage and security measures
No paper files or electronic file will be kept by the Medical Service. The assessment report will be given directly to the participant.

As to the question whether an information security risk assessment has been carried out regarding the subcontracting of the processing to Firstbeat, the CoR replied that no such assessment had been carried out, as Firstbeat is a reputable Finnish company having its servers in Finland.

3. Legal aspects

3.1. Prior checking

The processing of personal data under analysis is carried out by an EU institution, the CoR. Furthermore, the processing is both manual - which forms part or is intended to form part of a filing system (assessment report printed out in paper) - and automatic (information provided by the participants through the online server of Firstbeat assessment tool and production of the assessment report). The Regulation is therefore applicable.

The processing operation involves the processing of data relating to health, such as heartbeat readings, chronic diseases, medication and eating habits. The purpose of the processing is to assess the participants' level of stress and to provide them with coaching from the CoR's nurse on how to better manage their daily life. Due to the sensitive nature of the data processed, the processing is likely to present specific risks to the rights and freedoms of the applicants and it is therefore subject to prior checking by the EDPS[2].

The EDPS will identify below the CoR's practices which do not seem to be in conformity with the principles of the Regulation and provide the CoR with relevant recommendations.

3.2 Consent

The processing under analysis is based on the voluntary participation of the CoR's staff members. The EDPS reminds the CoR that in an employment situation, consent is a sensitive

[2] Article 27(2) of the Regulation contains a list of processing operations that are likely to present risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, including point (a) processing of data relating to health.

matter as it is doubtful that such consent is freely given. It is therefore important that the CoR ensures that each participant will "unambiguously" give his or her consent before his/her participation to the test, as Article 5(d) of the Regulation requires. This means that the participants' consent must be freely given, specific and an informed indication that they agree that their data are collected through all different steps of the processing[3]. The CoR should therefore adequately inform all participants that their participation and their data collected are voluntary (Article 11(1)(d) of the Regulation) and that they can withdraw their consent at any time.

3.3 Concept of controller and processor and Article 23 of the Regulation

As explained above, the CoR will sign a contract with a Finnish external contractor, Firstbeat, with the purpose of carrying out a measurement and assessment of the level of stress based on the participants' heart rate variability and daily habits.

In light of Article 23 of the Regulation, Firstbeat will act on behalf of the CoR and is therefore to be regarded as processor, whereas the CoR is the controller of the processing operation. This means that the CoR is the EU institution responsible for determining the purposes and means of the processing (Article 2(d) of the Regulation) and Firstbeat is obliged to carry out the processing only on instructions from the CoR (Article 23(2)(a)).

In particular, the CoR, being the controller (Article 4(2) of the Regulation), should indicate in the draft contract the following terms and conditions:
i) Firstbeat should process only adequate, relevant and not excessive data and that the data processed (heartbeat readings, information provided by the participants and assessment report) are only processed for the purpose for which they are collected;

ii) Firstbeat should not be authorised to transfer any information processed or outsource a service to a subcontractor or third party service, unless the CoR agrees so;

iii) Firstbeatshould not further process data for other incompatible purposes (i.e transferred to other companies for marketing purposes);

iv) Firstbeat should implement the data retention period requested by the CoR, and

v) In case a participant wishes to have access to his/her raw data processed by Firstbeat, the latter should be able to guarantee his/her right.

As to the obligations of Firstbeat regarding confidentiality, data protection and security measures under Article 23(2)(b) of the Regulation, the CoR should ensure that specific provisions are added in the draft contract regarding these obligations. As to the confidentiality and security obligations, considering that the processor is a Finnish company, it should in principle be subject to Article 16 and 17(3), second indent of Directive 95/46/EC, implemented in the Finnish law on data protection (see further in point 3.7).

---

[3] Article 2(h) of the Regulation states that the data subject's consent shall mean *"any freely given specific and informed indication of his or her wishes by which the data subject signifies his or her agreement to personal data relating to him or her being processed"*.

3.4 Rights of access and rectification

In light of Article 4(1)(d) of the Regulation, the CoR should ensure that the participants' data are accurate and kept up to date; it should therefore take every reasonable step to ensure that data which are inaccurate or incomplete with regard to the purpose of the processing, are erased or rectified. This means that the CoR is responsible for ensuring that participants are able to exercise their rights of access (Article 13 of the Regulation) and rectification (Article 14 of the Regulation).

The EDPS notes that the nurse of the CoR will discuss with each participant the assessment report and coach them how to manage their stress and improve their daily life. Participants may also re-do the test and to be able to compare results. The CoR does not wish to keep a copy of the assessment report. However, in case a participant requests that a copy of the report and related possible notes are kept in his/her medical file, the CoR should be able to satisfy this request. Participants should then be able to exercise their right of access to their assessment report at any time and their right to rectify/update it if they wish to carry out the test again.

Moreover, the EDPS highlights that in case a participant requests to have access to his/her raw data (information processed by Firstbeat), the CoR should ensure that Firtsbeat is in the position to guarantee this right.

The CoR should erase the inaccurate information stated in the notification and clearly set out the above recommendations in both the notification and in the draft contract.

3.5 Data retention

As a general principle, Article 4 (1) (e) of the Regulation states that personal data must not be kept in a form which permits identification of individuals for longer than is necessary for the purposes for which the data were collected or for which they are further processed.

The EDPS notes that Firstbeat is willing to delete the data processed following the CoR's request. If the CoR envisages concluding a one year contract with Firstbeat, the two-year retention period foreseen by the CoR seems excessive to the purpose of the processing. The EDPS recommends that CoR set out a necessary and reasonable retention period, no longer than the length of the contract with Firstbeat, and ensure that the processor implements this retention period. Moreover, the CoR should explicitly state in the draft contract that Firstbeat must adopt adequate safeguards to ensure that these data are not processed for other purposes, or used in support of measures or decisions regarding any particular participant. The notification should be updated accordingly.

In light of paragraph 3.1, the CoR should also adopt a retention period of the assessment report and potential notes by the nurse, in case a participant requests that this information be kept in his/her medical file.

According to the information provided, "anonymised" data will be used by Firstbeat for statistical and marketing research purposes.. Even if names, e-mail addresses and group

information will be deleted, the risk of re-identification of such sensitive data is very high[4]. The data entrusted to Firstbeat, should be considered personal data although the above information will be deleted. The EDPS therefore recommends that the CoR insert a provision in the draft contract highlighting the sensitivity of the data and the high risk of re-identification. Consequently, Firstbeat should not further process any of the data on its server, anonymised or otherwise, for any statistical or marketing purposes.

In case the CoR intends to use anonymous data for statistical purposes only, the EDPS recommends that the anonymised data are not published on internet and they are only used in the sound management of the institution and in the interest of its staff members.

3.6 Information to be provided to the participants

Articles 11 and 12 of the Regulation relate to the information to be given to data subjects in order to guarantee a fair and transparent processing of their personal data. In the present case, some of the data are collected directly from the participants and other information from other entities (i.e. assessment report from Firstbeat and evaluation of the results and coaching by the nurse). Both articles hence apply.

As to the content of the privacy notice, the CoR should
i) clarify the role of the CoR and of Firsbeat, as there is no reference to the latter in the privacy notice;

ii) mention the possibility for the participants to exercise their right of access to and rectification of their assessment report and related notes as well as raw data (information processed by Firstbeat), as explained in point 3.3; and

iii) indicate the retention period of the data kept by the CoR's medical service and by Firstbeat.

The CoR should include all the above recommendations in the privacy notice and publish the updated version on the intranet before the processing is launched.

3.7 Security

Even if the CoR is not processing personal data directly, it is bound by Article 23 of the Regulation: "*Where a processing operation is carried out on its behalf, the controller shall choose a processor providing sufficient guarantees in respect of the technical and organisational security measures required by Article 22 and ensure compliance with those measures*". For that purpose the CoR should obtain formal guarantee (i.e security certification) that Firstbeat indeed complies with its obligations regarding confidentiality and security of the personal data entrusted to them.

---

[4] Please see Article 29 Working party Opinion 05/2014 on Anonymisation Techniques adopted on 10 April 2014 (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf)

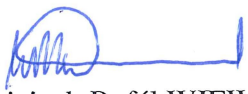
4. Conclusion

There is no reason to believe that there is a breach of the provisions of the Regulation provided that the following considerations are taken into account. In particular the CoR should:

- clarify in the draft contract with Firstbeat the roles of controller and processor and indicate in the draft contract all terms and conditions as explained in point 3.3;
- erase the inaccurate information stated in the notification and state that participants may exercise their right of access to and rectification of the assessment report and other related notes, as well as raw data (point 3.4);
- set out a specific retention period of the data collected for Firstbeat and for the CoR (point 3.5);
- include all information stated in point 3.6 in the privacy notice and publish an updated version on the CoR intranet before the processing is launched;
- obtain formal guarantee (i.e. security certification) from Firstbeat that the information entrusted to them will be kept in accordance with the confidentiality and security requirements present in the Regulation (point 3.7).

In the context of the follow-up procedure, please send to the EDPS a revised version of the notification, privacy notice, draft contract and guarantee of the security of Firstbeat within a period of three months and before the processing is launched, to demonstrate that the above EDPS recommendations have been implemented.

Done at Brussels, 17 December 2015



Wojciech Rafał WIEWIÓROWSKI