Support for the SMEs in the GDPR compliance

Financed by the European Union, the STAR II (SupporT small And medium enterprises on the data protection Reform II) project, running in the partnership of the National Authority for Data Protection and Freedom of Information (NAIH), the Research Group on Law, Science, Technology & Society (LSTS) of the Vrije Universiteit Brussel (VUB), and the Trilateral Research Limited (TRI IE) between 2018 and 2020, has the aim of assisting SMEs in applying the GDPR.

Taking the structure and needs of SMEs into account, the project helps the enterprises in question shape an appropriate practice.

In order to interact with SMEs, assist them to ensure compliance with the GDPR and gather valuable information about the difficulties they face NAIH was operating a hotline for SMEs between 15 March 2019 and 15 March 2020. This period the kkvhotline@naih.hu of the NAIH provided information for SMEs throughout the European Union in respect of the interpretation and proper application of the GDPR.

On the basis of the questions and issues raised by the SMES, a handbook will be compiled, which will be accessible and usable throughout the EU, and thus the entities concerned will not need to elaborate their own materials, thereby decreasing their personnel and material expenses.

FAQs addressed to the SME hotline

I. Scope of the GDPR

1. Are SMEs subject to the GDPR?

Yes. If they process personal data, they are subject to the rules of the GDPR.

The data protection reform took the special situation of SMEs into account:

- The majority of SMEs are not obliged to employ a data protection officer;
- The criteria for carrying out data protection impact assessments are significantly limited, and only small portion of SMEs are subject to them;
- SMEs are also exempt from the obligation to document their data processing activities.

2. *Am I, or is my activity, subject to the GDPR even when I process no personal data as part of my main activity, but I do have employees?*

Yes. The processing of the data of employees is prescribed by several laws for various purposes, whereby the enterprise is obliged to process the personal data of its employees.

3. *Does the processing of the telephone numbers of my clients for business purposes qualify as data processing?*

Yes, because it concerns business or professional activity, and does not belong among the exemptions of so-called household data processing not subject to the GDPR.

4. *Is it subject to the GDPR when one contacts a company (a non-natural person) with a direct marketing offer?*

No. Article 4 point 1 of the GDPR defines the concept of personal data. The protection of the data of non-natural persons does not fall within the scope of the GDPR.

5. *Is a company subject to the GDPR when processing of a small number of personal data of contractual partners or their contact persons for the purposes of fulfilling contracts of service?*

Yes, because the frequency, quantity or purpose of data processing are irrelevant from the point of view of scope, unless Article 2 mentions the as exemptions.

6. *Is it considered data processing when I publish my telephone number on my webpage or Facebook profile, and I am thus called by my possible clients?*

No, not until the processing of the personal data of other natural persons takes place (e.g. you are called by natural persons).

II. Lawfulness of data processing

1. *May consent be obtained from the data subject electronically?*

Yes, because the GDPR has no provision on the form of consent; it only defines the requirements of validity. The data controller however is obliged to prove that the data subject had given consent.

2. *If a natural person requests my enterprise to erase his or her personal data, and I thus erase all his or her data, including his or her name, from the records, how can I prove that I had received such a request and fulfilled it?*

The GDPR does not obligate data controllers to keep records of their measures taken in the course of enforcing the rights of data subjects.

Insofar as the data controller wishes to keep record of its fulfilling data subject requests in order to comply with the principle of transparency and in the lack of a provision thereto, it is expedient to define its contents so as not to include personal data.

III. Data breach

1. *Does the data controller have any obligation other than notifying the Authority when a data breach occurs?*

Yes. First, it has to maintain record of data breaches, indicating the facts of the breach, its effects, and the measures taken to redress it. Second, if the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without delay.

2. *What must the data breach notification include?*

As minimum, it must:

- describe the nature of the personal data breach, including, where possible, the scope and approximate number of data subjects concerned, as well as the scope and approximate number of personal data records concerned,
- communicate the name and contact details of the data protection officer or other contact point designated to provide more information,
- describe the likely consequences of the personal data breach, and • describe the measures taken or proposed to be taken by the controller.

IV. Designation of a DPO

1. *As an SME, how am I to assess whether I am obliged to designate a DPO or not?*

Article 37 (1) defines the cases when a data protection officer must be designated.
With respect to SMEs, it is Article 37 (1) b) that is governing, pursuant to which a data protection officer shall be designated where 'the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require **regular and systematic monitoring of data subjects on a large scale**' The notification shall include the names of the data controller and data processor, their contact details, the name, postal and electronic address of the data protection officer.

V. Data processing record

1. *Must a data processor also maintain a data processing record?*

Yes. Article 30 (2) of the GDPR defines the content of such a record. Accordingly, each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller.

2. *In what form must such a record be maintained?*

Pursuant to Article 30 (3) of the GDPR, such a record shall be in writing, including in electronic form.

VI. Processing of employees' data

1. *May an enterprise use GPS in its company cars?*

An indispensable condition of lawful data processing is that data processing has a legal basis under Article 6 of the GDPR; according to Article 6 (1) f), data processing may be lawful when it is necessary for the purposes of the legitimate interests pursued by the controller. If the employer has also a legitimate interest in using tracking system, the first issue to be examined is whether the data processing is by all means necessary for the purposes designated by the employer, and whether its implementation by a GPS device is proportionate to the limitation on rights.

It is particularly important that employers inform their employees of installing tracking devices in the company cars their employees drive, and that while they use the vehicle, their movements are recorded.

It is adjudged differently when employees may also use company cars for private purposes; in this case, there can be no legitimate interest of the employer in controlling the progress and circumstances of work.

2. *Under what conditions may employers process the certificates of good conduct of employees?*

In the opinion of the Authority based on the relevant provisions of the GDPR and the Privacy Act, employers may process the personal data of their employees concerning criminal actions, the related security measures, and their having no criminal record, first, on the basis of Article 6 (1) c) of the GDPR (processing is necessary for compliance with a legal obligation to which the controller is subject) and, second, based on the authorisation of an Act detailing the processing.

Note, however, employers may only require their employees to show them their certificates of good conduct; they may not make copies of them.

**Allow me to call your attention to the fact that the information provided by the Authority herein—being consultation answers without a procedural framework—shall not be construed as law or any legal instrument, or as to have any normative feature, legal effect or binding content. The interpretation of law by the Authority on the basis of the information provided in these questions shall bind no other authority, the courts or the data controller, and it merely serves the purposes of guidance. The position outlined and the information provided herein shall not exempt the addressee from having to shape its own legal opinion or the data controller from the liability for processing data.*

the data protection reform II; 2018-2020) which is co-funded by the European Union under the Rights, Equality and Citizenship Programme 2014-2020 (REC-RDAT-

Nemzeti Adatvédelmi és Információszabadság Hatóság

LSTS LAW, SCIENCE TECHNOLOGY & SOCIETY STUDIES VRIJE UNIVERSITEIT BRUSSEL

TRILATERAL RESEARCH

The SME hotline is operated by the National Authority of Data Protection and Freedom of Information under the STAR II project (Support small and medium enterprises on TRAIAG-2017) under Grant Agreement No. 814775.