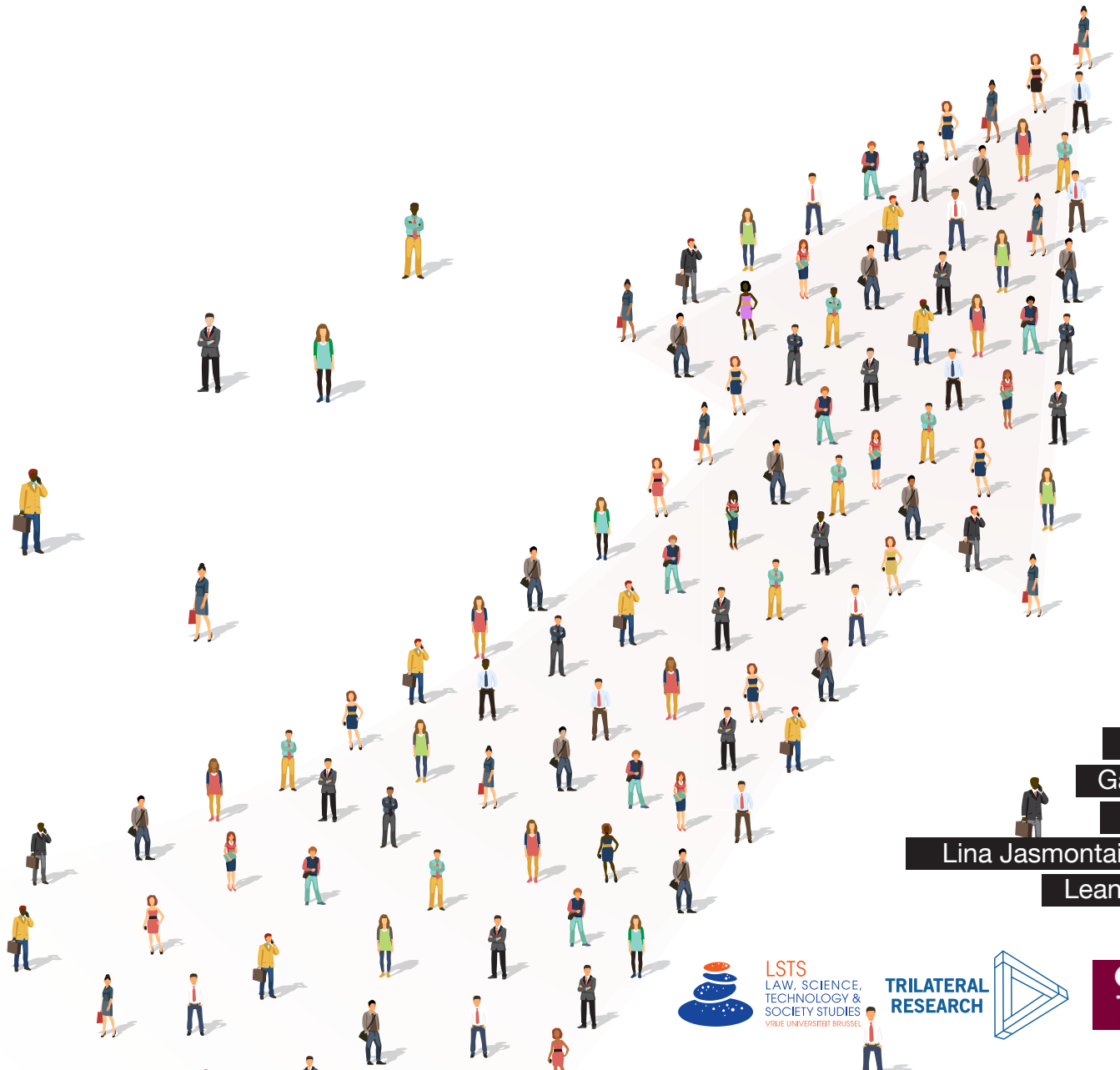
SupporT small And medium enterprises on the data protection Reform II

GUIDANCE FOR DATA PROTECTION AUTHORITIES ON SETTING UP HOTLINES FOR SMEs



prepared by
Gábor Kulitsán
Renáta Nagy
Lina Jasmontaite-Zaniewicz
Leanne Cochrane

LSTS LAW, SCIENCE, TECHNOLOGY & SOCIETY STUDIES VRIJE UNIVERSITEIT BRUSSEL

TRILATERAL RESEARCH

Index

Background to the STAR II project

The STAR II (SupporT small And medium enterprises on the data protection Reform II) project, ran in the partnership between 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 Trilateral Research Limited (TRI IE) between August 2018 and November 2020. The main objective of the project was to promote compliance with the GDPR by assisting both DPAs and SMEs.

There are pressing needs to assist EU data protection authorities (DPAs) in raising awareness among businesses, especially SMEs, on the EU legal framework for personal data protection, particularly the GDPR. At the same time, SMEs often need external assistance to understand the gravity of the regulatory regime applicable for the processing of personal data; they need guidance on how to follow the respective Member State national legislation giving full effect to the GDPR; they need to adapt their routine practices; they need to acquire information, solve new or hitherto unnoticed issues and follow trainings on the new legislation; and they often need to create and execute an action plan to apply the EU data protection framework.

In order to address these needs, the STAR II project has:

1. reviewed the state of the art in DPA awareness-raising activities,
2. analysed SMEs' experience within the first months of the functioning of the GDPR through survey research and interviews;
3. ran an awareness raising campaign for SMEs,
4. ran a hotline (12 months) to respond to SMEs' email queries; based on these queries the project developed a list of the most frequently asked questions;
5. prepared this guidance for DPAs on good practices in running an e-mail hotline and raising SME awareness, and
6. prepared an innovative, FAQ-based handbook (open-access digital and printed) for SMEs on EU personal data protection law.

The STAR II project consulted stakeholders (especially via validation workshops and its External Advisory Board) throughout different stages when drafting its deliverables and guidance documents. All outputs are freely available, openly accessible and copyright-unrestricted, and therefore can be easily reused and adapted.

Disclaimer

The content of this Guidance for DPAs represents the views of the authors only and is their sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

The awareness raising roles and powers of the DPAs under the GDPR

A significant part of the General Data Protection Regulation (GDPR) is devoted to addressing the role and responsibilities of Data Protection Authorities (DPAs). Its Chapter VI on Independent Supervisory Authorities,[1] by taking into account the case law of the Court of Justice of EU (CJEU) that has emerged in response to uncertainties concerning the scope of DPAs tasks and their independence, clarifies the role and responsibilities of DPAs.

The GDPR asserts that the primary responsibility of DPAs concerns the monitoring and consistency of the application of the GDPR 'in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union'.[2] The legislator has foreseen in Article 57 that to attain the objective of monitoring and consistency of the application of the GDPR, DPAs are bound to undertake 22 tasks that range from enforcers, ombudsmen, auditors, consultants to policy advisors, negotiators, standard setters and educators.[3] The list leaves no doubt that DPAs responsibilities reach beyond enforcement. Some suggest that overall all these tasks could be seen through different lenses and DPAs could be regarded as a leader, an authoriser, a police officer and a complaint-handler.[4]

The DPA role of the leader – a policy mainstreamer – and the scope of awareness raising duties to the general public, controllers and processors have received thus far little attention. By engaging in awareness raising activities (e.g. by providing guidance, replying to queries), DPAs can potentially contribute to consistent application of GDPR. To foster the debate on what such awareness raising duties include and how their consistency can be ensured among all European Union (EU) member states, we put forward this guidance document, focusing on one group of recipients of awareness raising activities, i.e. SMEs.

To reflect on this long practiced but only recently formalized duty of awareness raising, we consider the impactions of DPAs as educators.

DPAs & awareness raising

Awareness raising duties of DPAs have been shaped by enforcement powers provided within the scope of the EU personal data protection framework. It can be suggested that to compensate for being awarded with limited enforcement powers to impose the so called 'deterrence' style enforcement and significant fines under the Data Protection Directive, most of DPAs included awareness raising in their enforcement strategies.[5] In view of this, it can be even argued that a big majority of DPAs intuitively followed the recommendation put forward by Baldwin and Cave in their seminal work on understanding regulation. They posited that rules 'have to be employed by enforcers in conjunction with different compliance-seeking strategies – be these prosecutions, administrative sanctions, or processes of persuasion, negotiation, advice, education, or promotion'.[6] By means of opinions, guidelines, public engagements and other similar awareness raising activities, the well-intentioned national regulators sought to reach, on the one hand, individuals, whose rights are affected, and, on the other hand, 'controllers' and 'processors', who handle personal data of individuals. However, diverse approaches emerged among DPAs in terms of their tasks and powers as a result of 'history, case law, culture and the internal organization of the Member States'.[7]

With the adoption of the GDPR lawmakers sought to reduce such diversity and increase harmonisation among DPAs enforcement practices. It could be argued that formalising awareness raising duties of DPAs could be seen as an attempt to ensure that regulators can enforce the applicable framework 'in a more uniform and effective way' and at the same time update enforcement practices of DPAs.[8] While awareness raising duties constitute only part of DPAs tasks, they cannot be considered in isolation from other tasks foreseen in the GDPR. Awareness raising has certainly a direct bearing on how the ones who are regulated cope with applicable rules and it also affects enforcement claims brought by individuals.

Advantages of awareness raising

Awareness raising duties of DPAs are instrumental to attain consistent application of the GDPR for the following four reasons:

First, awareness raising activities undertaken by DPAs complement the applicable legislative framework by providing additional explanation of different provisions (e.g., what does the purpose limitation principle entail?). Only regulation that can be understood in a comprehensive manner, carries the potential to result in the desirable behaviour of addressees. In this sense, awareness raising activities could be essential when promoting a data protection culture among the general public.

Second, DPAs, when explaining rules applicable to controllers, processors and data subjects, do so by taking into account the national law background and specificities. In this way, DPAs interpret and apply the GDPR in a specific national context.[9]

Third, awareness raising practices of DPAs, similarly to other enforcers across the EU regulatory domains,[10] allow the mainstreaming of the overall policy objective to the wider audience and in this way minimise disparities in information – the so called information asymmetries – that have been reported among entities, organisations and individuals that process personal data, or are subject to the processing operations. For DPAs, this task is particularly challenging as on the one hand they must act to empower data subjects with control over their personal data. On the other hand, they have to facilitate data flows within the internal market for controllers and processors.

Finally, awareness raising duties of DPAs could be seen as a tool to reduce divergence in enforcement practices, which if not managed, could potentially result in a forum shopping, where the concerned entities (i.e. controllers and processors) would look for the most favourable regulatory set-up.[11]

Awareness raising practices

During the interviews within the STAR II project, EU DPAs reported using different mediums to reach out the target audience with their awareness raising campaigns as well as to learn their distinct needs.[12] DPAs identified the print media, social media and events as the most common general awareness-raising methods. DPAs typically opt for the multiple methods that allow combination of different mediums.

One of the most effective mediums available for DPAs to spread information is their own website. It also could be considered the most appropriate information platform for the addressees of the information, as they presumably visit their DPAs' websites for information on recent data protection issues, guidelines and decisions. Therefore, DPAs should be encouraged to share information on decisions, opinions, guidelines and practical examples on data protection, on their websites. The information to be provided must be as practical as possible because SME representatives reported being interested in detailed and practical information.[13] Arguably, this could be done in coordination with SME associations to avoid duplication of effort and to maximise resources. The emphasis here is again on follow-up and mapping the change to accommodate interests of SMEs.

Apart from the use of their websites, DPAs reported a variety of ways in which they become aware of the needs of SMEs concerning the GDPR. DPA representatives suggested that by participating in events and by engaging in the one-to-one interaction with individual SME representatives, they obtained better insights into the specific challenges faced by SMEs.[14] Such interactions were reported to occur through established engagement channels such as the public-facing hotlines or helpdesk services, participation in and presentations at events organised by third parties, or other consultation and advisory services. In these contexts, individual SMEs were approaching DPAs with very practical questions that required specific answers. Some DPAs also reported that they have consulted SME representative bodies about the needs of SMEs. However, DPAs referred to events as the most effective awareness-raising medium for SMEs. More detail about the awareness raising methods of DPAs can be found in STAR II deliverable 2.1 – Report on DPA efforts to raise awareness among SMEs on the GDPR.

An overview of hotlines run by DPAs

Based on the interviews carried out with 18 DPAs by the STAR II Consortium on their awareness-raising activities among SMEs about the GDPR, it can be concluded that all DPAs operated a form of advice service that SMEs can use. Typically, such advice service is provided by telephone or email. Some DPAs respond to queries via both email and telephone. However, in most cases, this service is not an SME specific hotline/helpdesk service.

DPAs receive most calls/queries in the national language of the respective country. While some DPAs provided responses in multiple languages, English is the most widely used across the EU DPAs, in addition to the national language/s. A small number of DPAs, however, expressed that it would be beneficial to develop their English language capacity in order to respond to the incoming queries.

Overall, DPAs deemed that a helpdesk or a hotline service can be a very useful tool for DPAs to establish connection between themselves and the general public, including the data subjects and SMEs. The interested parties are provided a continuously available source of up to date and trustworthy information. However, a telephone hotline/helpdesk is not always regarded to be an adequate platform to give legal advice in a specific issue due to liability issues. DPA personnel are not aware of all the circumstances concerning the processing of personal data, only of those the SME has shared in the inquiry, therefore the replies offered by a DPA can only be based on the information it has obtained via the communication of the hotline user. Therefore, such replies should not be turned against the DPA during the investigation or court proceedings. It is also essential that individuals can fully understand the information they receive in order to avoid the misinterpretation of the reply received. Perhaps in order to overcome such issues, DPAs tend to give general guidance on the data protection legislation and include disclaimers in their communication.

It appeared that the majority of interviewed DPAs do not use internal guidance to direct hotline/helpdesk advisers (i.e., personnel). This a surprising finding given that in order to ensure a consistent application of the GDPR, it is important that answers provided by DPAs to reoccurring or similar questions are provided in a standardised and systematic way. We found that just over a quarter of DPAs did have such documents in place. Such documents were deemed to be subject to confidentiality and were not shared with the STAR II Consortium.

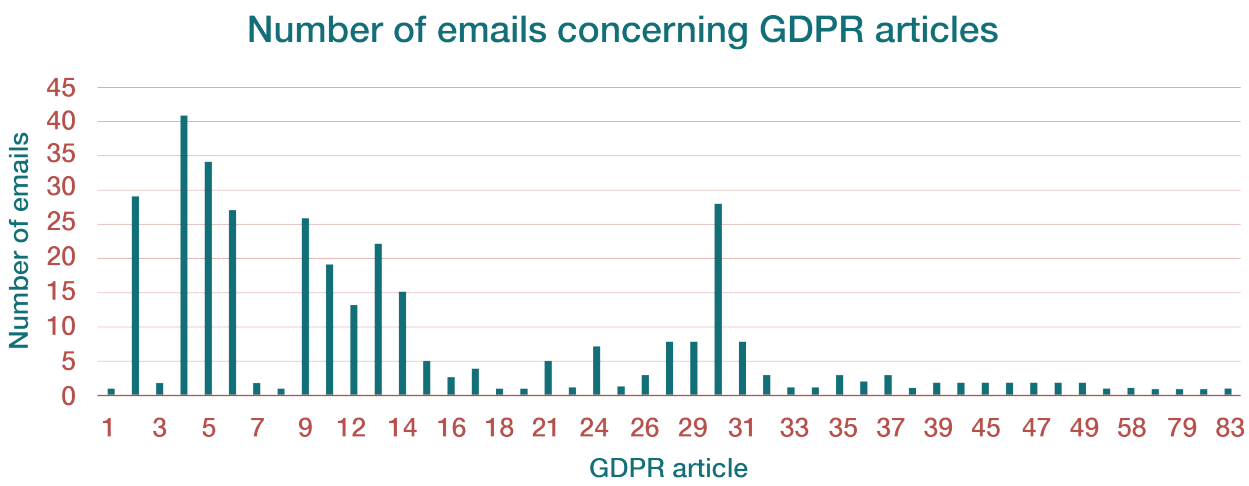
NAIH's hotline for SMEs

Within the scope of STAR II project, NAIH launched a hotline dedicated to SME enquiries. NAIH operated the hotline between 15 March 2019 and 15 March 2020 to assist SMEs with questions and uncertainties concerning compliance with the GDPR. NAIH welcomed questions from SMEs based or functioning across the European Union (EU) about the interpretation and application of the GDPR provisions. NAIH received queries in Hungarian and in English. Out of 148 inquiries, only three inquiries were submitted in English. Out of these, only one fell within the scope of the hotline dedicated to SMEs. This initiative indicates that a considerable uncertainty remains concerning the application of GDPR provisions, especially for SMEs.

Key findings

The added value of this initiative is that it allowed NAIH to obtain better insights about the specific difficulties and questions SMEs face. In particular, it allowed NAIH to identify questions that SMEs commonly have and GDPR provisions that require further clarification. From the graph below, it appears that SMEs have questions concerning the scope of the GDPR (Article 2), the definitions (Article 4) and data processing principles (Article 5). SMEs also frequently required guidance on transparency obligations foreseen in Articles 12, 13 and 14. Article 13 was the most commonly invoked of the three suggests that most SMEs with questions for the regulator were primarily thinking about their data collection directly from the data subject (customer databases, marketing efforts and employee data).

The data from the email hotline offered the STAR II Consortium the opportunity to compare the self-reported interests during interviews with the actual questions that SMEs asked of the regulator in the real-world. Whilst the topic categories do not correlate on a one-to-one basis there is substantial overlap, despite the localisation of the hotline data in comparison to the survey data.



SMEs asked mostly practical questions concerning compliance with a particular GDPR requirement in a specific context. This suggests that while SMEs are aware of the GDPR, this awareness does not equate to the full understanding and comprehension of their obligations when processing personal data.

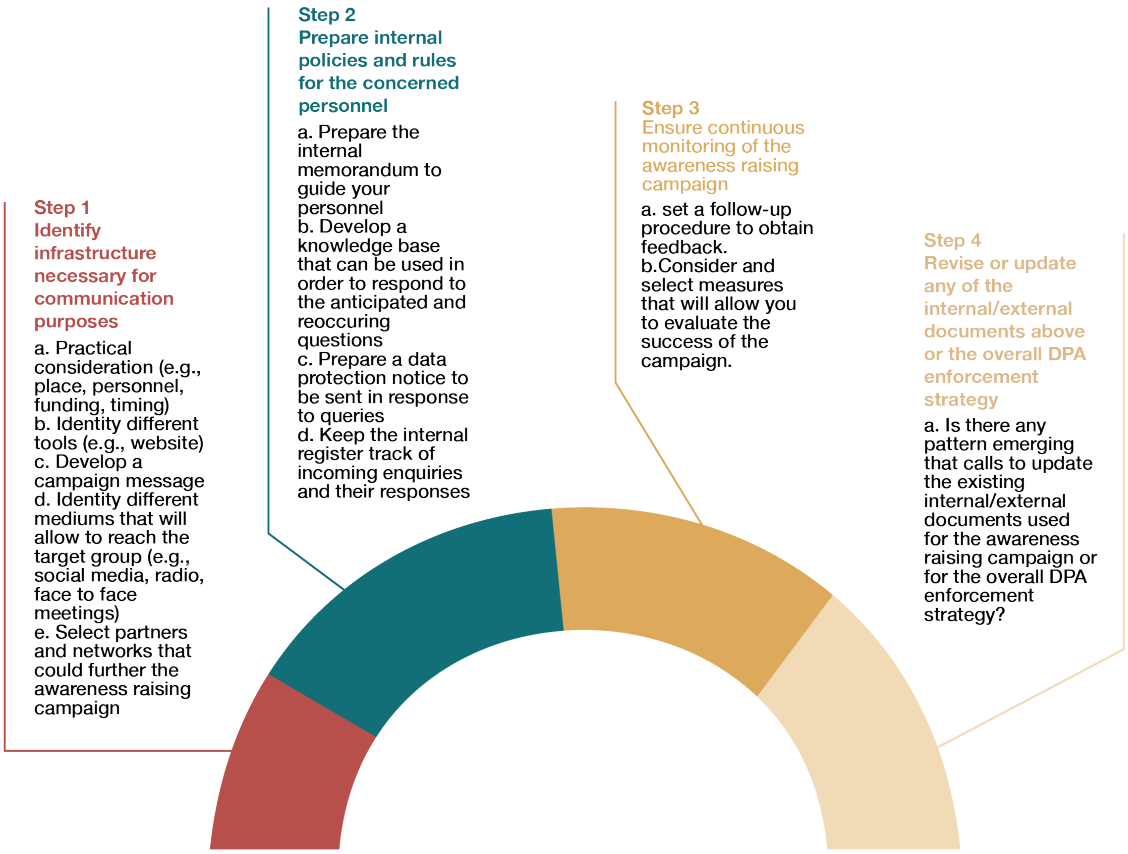
Recommendations for setting up a hotline for SMEs

Based on the experience with the hotline dedicated to SMEs, NAIH has put forward recommendations on running an awareness raising campaign for a specific target group.

The first two issues that need to be addressed before moving on to the peculiarities of running a hotline concern the selection of a target group and the formulation of the overall goal of a particular awareness raising campaign. In case of STAR II project, the overall goal was to enhance GDPR compliance among SME representatives. NAIH suggests taking the following steps in order to develop a comprehensive plan for a successful awareness raising campaign. These steps can be aligned with most project management methodologies that an organisation may use. A detailed description of NAIH's experience is provided in the next section.

Planning an Awareness Raising Campaign

A DPA Hotline for SMEs



1 Identify infrastructure necessary for communication purposes

a. *Practical considerations.* For an effective set up of a hotline, it is necessary to anticipate the time it is going to consume and allocate funding. Then it is important to find a physical location where the hotline can be run. Competent personnel must be appointed, either part-time or full time. Personnel responding to queries must have expertise in GDPR related issues. Additionally, they could receive training on soft communication skills (e.g. empathy, active listening as well other oral and written communication practices to make communication more pleasant).

b. *Identify necessary tools.* There are several tools through which a hotline can run. Websites and e-mail addresses may be the most common and effective tools. Nevertheless, it may be desirable to provide a phone number or a physical address where queries may be sent in a paper form. The latter may be of use for SMEs lacking technological literacy.

a. *Develop a campaign message.* Communicating in a simple and easy to understand language the scope of the hotline and making clear what type of questions will be answered should reduce the number of questions that are out of scope. It may contribute to increasing satisfaction by managing user expectations as well. An example of such communication is in the section on Radio campaign.

b. *Identify communication medium to reach the target group.* This may include social media, radio, and face to face meetings. In each case, the chosen communication medium has to be suitable and include parts of the population that may lack digital literacy.

c. *Select partners and networks that could further the awareness raising campaign.* They can be, for example, sector specific SME associations or business networks, consumer organizations and chambers of commerce.

2 Prepare internal policies and rules for the concerned personnel

Such policies and rules may include:

a. *an internal memorandum to guide your personnel.*

The memorandum should set the internal rules for the operation of the hotline and specify the tasks of the engaged personnel, the internal policies (including deadlines, conditions of assistance, languages used, etc.) and liability issues. An example of such a memorandum is provided in Annex I.

Ideally, people with different seniority would be responding to hotline queries. Queries received may be divided into different groups according to their complexity and then assigned to staff members, taking into account their expertise and seniority level. Also, the memorandum may contain a chain of responsibilities and approvals as well as recommendations concerning replies to queries.

Table 1: Queries can be divided in the following groups:

Difficulty 1:	A question answerable on the basis of the knowledge base, OR, a rejected question (e.g. on the basis that it was too specific and amounts to a request for the lawfulness of a specific piece of data processing)
Difficulty 2:	A question not answerable on the basis of the knowledge base but answerable unequivocally by the Hotline Expert on the basis of the law-enforcement practice of the Authority and the supervisory authorities under the General Data Protection Regulation, the relevant case law of the courts, and the documents of the European Data Protection Board assisting the application of law
Difficulty 3:	Hotline request poses a new or especially complicated question which cannot be answered unequivocally on the basis of the law-enforcement practice of the Authority and its associate authorities, the relevant case law of the courts, and the documents of the European Data Protection Board assisting the application of law, the Hotline Expert shall involve other experts of the Authority in accordance with executive guidance where necessary.

b. *a knowledge base* that can be used to respond to the anticipated and reoccurring questions. Ideally, the knowledge base should be prepared before launching the hotline. It has to be kept up to date, in the light of incoming queries. On a regular basis, it must be reviewed and updated with the reoccurring questions that were not included in the initial knowledge base. This document also should take into account the national and European case law as well as guidance issued by authoritative EU bodies such as the European Data Protection Board (EDPB). Such a knowledge base may be particularly helpful to ensure standardisation of responses to similar questions / scenarios.

c. *a data protection notice* was available on the NAIH's website embedded in the announcement on the launch of the SME hotline. The data protection notice could be sent in response to queries. An example of a data protection notice is available in Annex II.

d. *an internal register* to track incoming enquiries and their responses. Generalised questions received (not referring to individuals or specific organisations) are going to be added to the knowledge base.

Table 2: Examples of issues that could be included in the internal register:

1.	**Number:** serves as an identification number for the e-mails received.
2.	**Date of receipt:** an indicator for the project assistant to set the deadline for the processing of the enquiry and the latest date of reply.
3.	**Member State:** information on the origin MS of the hotline user.
4.	**Language:** the language of the e-mail sent to the SME hotline.
5.	**Nature of the issues raised:** whether the enquiry concerns a theoretical interpretation of the provisions of the GDPR or is a concrete question concerning the practical application of a related provision (theoretical or practical issue).
6.	**Number of issues raised:** the number of the questions the e-mail contains.
7.	**Issues raised:** short summary of the questions received.
8.	**Topic:** to which field of data protection the issue is related.
9.	**Difficulty of the issue:** the answers to questions are classified in three groups according the level of difficulty of formulating them (estimated difficulty of the answer). This should be per question, rather than per email.
10.	**Keywords:** keywords of the enquiry to foster the quick search in the Register.
11.	**Provisions of the GDPR concerned:** this column also can contain the relevant provisions of the national legislation and the WP29, the EDPB or any other relevant guidelines.
12.	**Date of answer:** the date when the answer was sent to the hotline user.
13.	**Case worker:** name of the person that answered the query.
14.	**E-mail:** e-mail address of the hotline user, this information is only stored for the time frame laid down in the data protection notice.
15.	**Status:** the actual status of the response (in progress, finished)
16.	**Time spent** working on the query (e.g. person hours)

3 Ensure continuous monitoring of the awareness raising campaign

a. Set a follow-up procedure to obtain feedback from your target group. Having a follow up procedure to gather comments and suggestions from users is important in order to understand how to further improve the hotline. To this end, a DPA could request SMEs that submit queries concerning personal data processing operations fill in a satisfaction survey. An example of a satisfaction survey is available in Annex III.

b. Consider and select measures that would allow you to evaluate the success of the campaign (e.g., the number of questions, response time, etc.). Based on the statistical analysis, the functioning of the hotline can be periodically refined and adjusted to the needs. Follow up procedures and continuous monitoring allow the identification of issues that need to be addressed.

4 Revise or update internal/external documents above and the overall DPA enforcement strategy

a. Consider if there is any pattern emerging that indicates the need to update the existing internal/external documents used for the awareness raising campaign or for the overall DPA enforcement strategy. The results obtained from the hotline could orient DPAs in issuing further guidance on recurrent queries.

NAIH's experience of running a hotline dedicated to SMEs

Infrastructure for communication purposes

Prior to the launch of the hotline, NAIH considered the necessary infrastructure for an awareness raising campaign. This included practical questions concerning the place from where the hotline will be managed and personnel who will be in charge of this task as well as the identification of different tools that could be used throughout the campaign (e.g., a website page and an enquiry form). Then, NAIH in consultation with the consortium partners developed a campaign message that was used to reach out to the target audience – SMEs representatives. It should be added that NAIH engaged with the target audience through different mediums, including social media, radio, and face to face meetings. The latter proved to be particularly valuable as they allowed to further the awareness raising campaign among the concerned audience, even though the correlation between the participation in events and received queries has not been possible to establish.

1 Website

NAIH regularly publishes final decisions and opinions on its website. All available decisions, opinions and recommendations can be searched by topic and are freely available for the public. Considering the engagement with the website and its regular updates with the latest documents issued by the authority, it was decided to dedicate part of it for the awareness raising campaign.

Following on from this decision, besides all relevant up to date information on the activity of the authority and general guidance for data controllers and data processors, such as a 12 bullet-point introductory guidance for the GDPR compliance for controllers,[15] the website was updated and now provides information for SMEs on GDPR compliance via the form of brochure that has been updated on a regular basis (see Annex IV). To advertise the STAR II project and the SME hotline the NAIH published an announcement on its website on the launch and operation of the SME hotline on 15 March 2019.

Additionally, the website was used to further spread information on the progress and results of STAR II and especially on the operation of an SME hotline. To this end, the NAIH prepared three press releases on the actual status of the project that have been published on NAIH's website. 13 information booklets have been

prepared on the SME hotline in Hungarian (6 of those on a specific issue that emerged on the SME hotline often) and 2 booklets in English. Some of them were published on our website, some of them have been disseminated at conferences and informational events.

NAIH's website has been considered to be the most appropriate information platform for the stakeholders of the project as the end-users (i.e. SME representatives) presumably visit the NAIH's website for information on recent data protection guidelines and decisions issued by the authority and other information on the activity of the authority. The website offers an opportunity for users to "self-answer" common questions before escalating to the hotline. As a rule of thumb, if a question can be answered by a staff member copy-and-pasting an answer from a document, that information should be made available to the SME online. If a hotline is going to effectively shut down over a holiday period then this should be communicated to users.

2 Radio campaign

The radio campaign has played a vital role in reaching out to the target audience. Radio as the communication channel, the length of the campaign (one month), and the frequency of broadcasting (two plus one spots per day) were based on the previous positive experience gained in the ARCADES project.[16]

The radio campaign raised awareness regarding the data protection obligations by drawing attention to the new regulatory framework concerning the processing of personal data. The campaign also explained the particular form of assistance STAR II will provide. In particular, it referred to the hotline for SMEs and the subsequent recommendations on how to run hotline for other DPAs as well as the handbook for SMEs. A one-month-long campaign with three spots (50 seconds) per day was deemed to be appropriate to deliver the message for a significant number of people, including the target audience.

While there is a good reason to believe that the campaign reached the target group widely and has increased the awareness of GDPR obligations among the SMEs, statistical information on the extent to which such campaign has changed compliance practices and behaviour is not available.

NAIH requested quotes from the Hungarian Media Service Support and Trust Fund (MTVA) on the expected costs of the recording and one-month-long broadcast, and later a contract has been signed.

NAIH drafted the text and the scenarios of the radio campaign in English and in Hungarian and then validated them with the STAR II Consortium. The Consortium Partners reviewed the message in English. The final text for the radio spot was recorded in Hungarian in December 2018. The following text was recorded:

"Do you know that small and medium-sized enterprises represent 99% of all businesses in the EU? Rules and obligations of the new EU data protection regulation (coming into force as of May 2018) affect generally these data controllers, too and there are also some specific rules of the GDPR which apply to SMEs. For more information please, contact the National Authority for Data Protection and Freedom of Information, which has set up a special hotline: kkvhotline@naih.hu. This Public Social Advertising has been prepared upon the request of NAIH and co-financed by the Rights, Equality and Citizenship Programme of the European Union under the supervision of the DG JUST of the Commission."

The radio campaign was broadcasted by Petőfi Rádió, a countrywide available public radio that has the most listeners per day among the entire adult population in Hungary. According to the data published by the National Media and Infocommunications Authority, Petőfi Rádió had about 1,3 million listeners per day in average in the first quarter of 2019. The radio spot was broadcasted 86 times between 15.03.2019 – 15.04.2019 (17 times in the morning hours, 37 times in the afternoon hours and 32 times in the evening hours).

3 Face to face interactions

In line with findings of the STAR II project interviews with DPAs, NAIH has found face to face interactions to be particularly useful in order to obtain a better understanding of SME distinct needs concerning the GDPR compliance.[17] Primarily because face to face meetings often result in a more open discussion concerning the context of the processing operations in question than it is possible over the phone.[18]

Within the scope of the STAR II project, NAIH interacted with SME representatives at the following events:

- a validation workshop for the preliminary results of the STAR II research project. The event was held in Dublin in June 2019. The report on the first validation workshop can be found in Deliverable D2.3 Report on WP2 Validation workshop.
- an information event for SMEs on the GDPR organized by the Somogy Chamber of Commerce and Industry in June 2019. The Chamber invited the representatives of the NAIH and all SMEs registered at the Chamber. The attending SMEs were provided the opportunity to ask questions they are most interested in concerning the GDPR compliance.
- an information event for SMEs on the GDPR organized by the Budapest Chamber of Commerce and Industry in October 2019. The Chamber invited the representatives of the NAIH and all SMEs registered at the Chamber. The attending SMEs were provided the opportunity to ask questions concerning the GDPR compliance.

Additionally, the President and other representatives of NAIH presented the project and the launch of the SME hotline at several conferences, such as Hungarian Decision maker Think Tank Conference, Infoszféra Conference, Data Protection Case Handling Workshop.

4 Internal rules and procedures

After addressing practical considerations, it has proved to be useful to set internal rules and procedures for personnel handling incoming enquiries.

NAIH prepared **an internal memorandum** that laid down the detailed rules for the responses to be given including deadlines, conditions of assistance, liability issues (see Annex I). For example, personnel were required to provide responses in a manner that would provide comprehensible assistance in the interpretation of law applicable relevant to the merit of the question and that would go beyond the mere reference to the provisions of law. Personnel were requested to highlight the relevant aspects in the application of law related to the received question, the factors to be considered among them, and their significance. At the same time, personnel had to ensure that the answer shall contain no opinion as to the lawfulness of any concrete data processing.

NAIH developed **the knowledge base** before launching of the hotline. It included anticipated questions that the DPA expected to receive. The document was updated and revised following up on the statistics provided by the incoming questions and the answers given to them on a monthly basis. More specifically, the knowledge base was developed on the basis of the law-enforcement practice of the Authority and the documents of the EDPB. The knowledge base was prepared in a question–and–answer structure, and contained abridgments of law-enforcement practice in pairs of questions and answers, providing relevant quotations and keywords to assist searches.

NAIH also prepared **a data protection notice**, which was available on the website. A copy of this notice is included in the Annex II.

To keep track of enquiries, NAIH maintained **the internal register of enquiries**. This allowed to ensure that responses are provided in a timely manner and at the same time it allowed to ‘tag’ and group enquiries and in this way collect statistical data needed for the project. It was apparent that during the functioning of the hotline the difficulty of incoming enquiries reduced. The register included the e-mail address of the requester as personal data only in order to monitor the fulfilment of the request, and according to the data protection notice the personal data required for other products by the Project shall be deleted five years after the conclusion of the Project.



5 Continuous monitoring of the awareness raising campaign

During the functioning of the SME hotline, the encountered issues and the answers were continuously monitored (qualitatively and quantitatively). The statistical analysis also served as necessary data for the monitoring and evaluation of SME awareness-raising strategies and the success of the knowledge base.

As mentioned above, NAIH developed the internal register of enquiries that allowed to keep track of the campaign (e.g., the number of questions, response time, etc.) and to identify recurring questions that have not been included in the knowledge base. By the end of the hotline, the knowledge based amounted to 129 pages.

The data obtained from the internal register provided insights about the needs and difficulties SMEs are facing in order to comply with the GDPR. Based on the register the most frequently asked questions were identified, which has been an important indicator of SME concerns and apprehensions about the GDPR.

Based on the statistical analysis, the functioning of the hotline was periodically refined and adjusted to the needs of SMEs. The statistical analysis of the data collected in the register also enabled the DPA to identify the most compelling needs of the SMEs in their compliance efforts. Also, having this overview resulted in a more accurate assessment of the GDPR issues that need to be clarified.

Operators of an SME hotline should ensure from the start that they are capturing the knowledge they are gaining about the SME experience of the GDPR and the particular problems being encountered. Such hotlines serve as a real-world indicator of what SMEs want information on. This can then serve as a guide for prioritizing training.

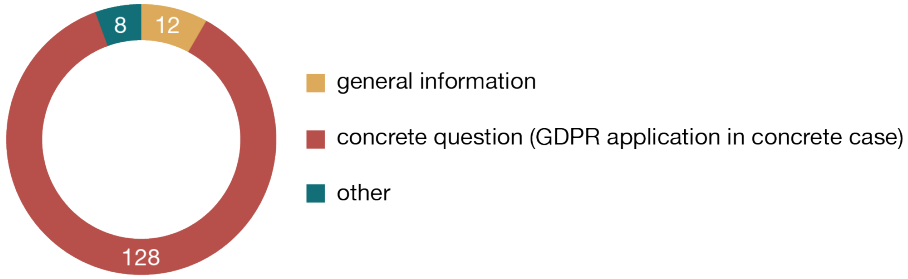
NAIH found it be useful to receive feedback from SMEs who submitted queries concerning personal data processing operations. NAIH decided to do so through the means of a satisfaction survey that was sent by email.

The most significant result of the awareness raising campaign was that it encouraged and incentivised the development of the informational strategies that meet the needs of the SMEs representatives. We are inclined to believe that the statistical data analysis of the hotline can facilitate the customization of the DPA's training program and to monitor changes in SME concerns/queries over time.

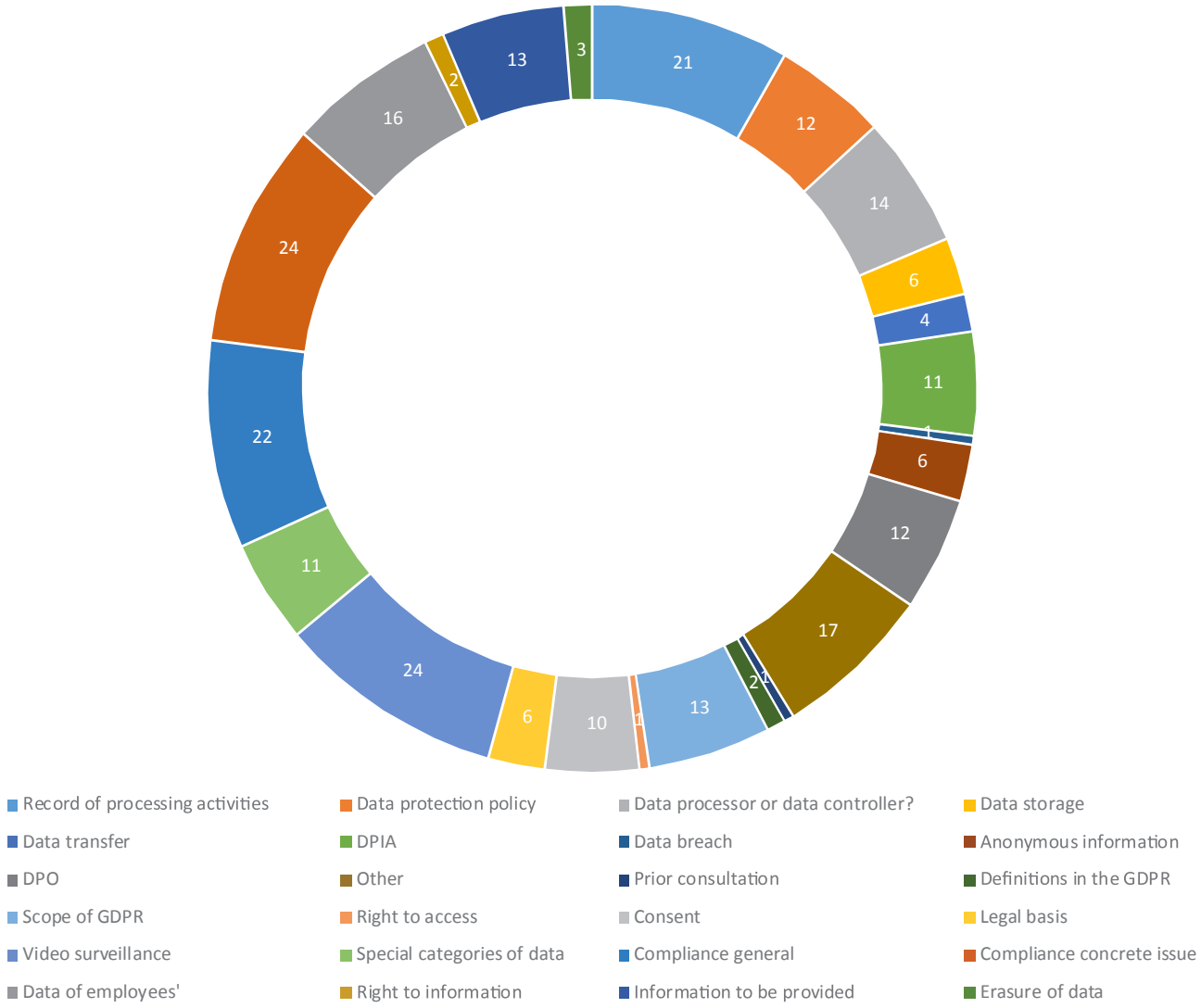
Statistical data

The NAIH has experienced a relatively high interest among SMEs during the hotline's operation, but it must be noted that only Hungarian SMEs have used the hotline so far. Three e-mails were received in English, however two of those were out of the scope of the SME hotline.

The distribution of questions as per type of question:



Distribution of questions by theme



Concluding remarks

NAIH considers the awareness raising campaign a success as the increased interest of the SMEs on the GDPR compliance was recorded. During the operation of the hotline NAIH had an opportunity to engage with SME representatives through different mediums and found that the majority of the SMEs that sent enquiries learned about the campaign after finding a notice on the website of NAIH; a smaller part referred to the radio campaign. In awareness raising various efforts and modes are complementary and interlinked.

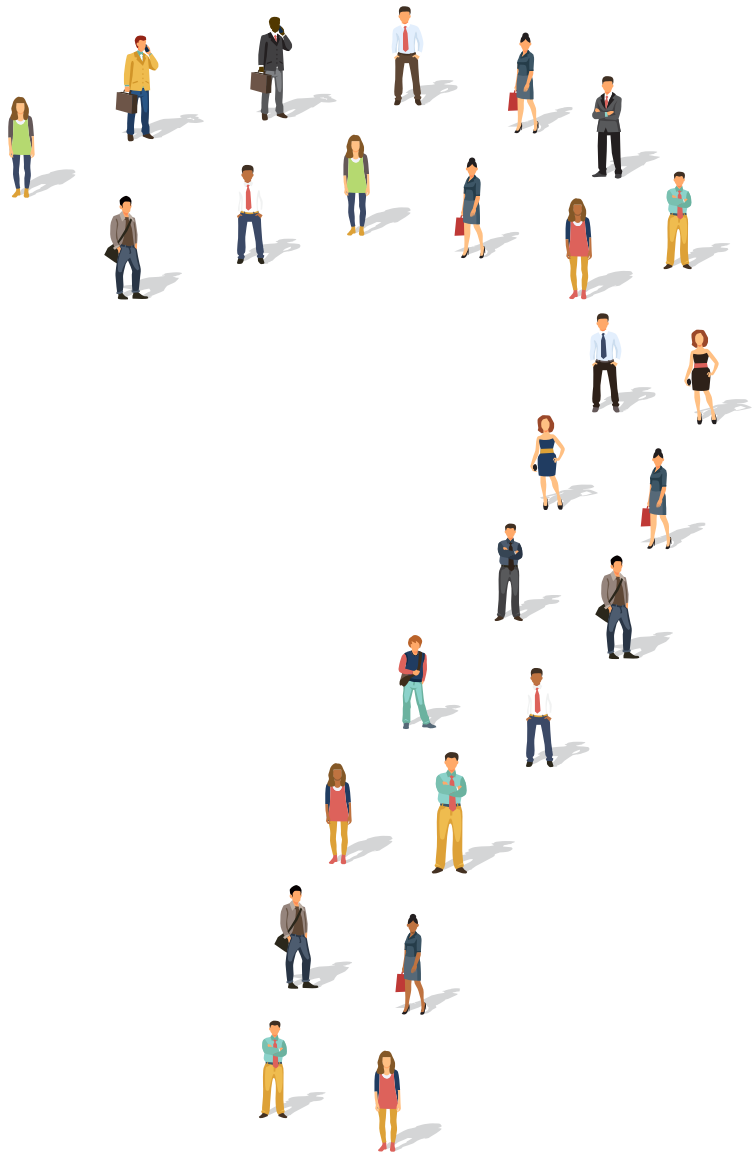
While the NAIH was able to draw some recommendations of best practices concerning the set-up of a hotline for SMEs, it recognises that each DPA is independent in it actions as they concern fulfilment of the leader orientated obligations stemming from Article 57 of the GDPR. SMEs are primarily interested in information from “their” national regulator, even if this information is already available elsewhere from another regulator. Significant ground could be gained for SMEs by either DPAs either directly adopting and translating, or actively endorsing support material created by their peers.

NAIH noted that for more efficient handling of queries it is important that the internal memorandum sets up a chain of responsibilities and approvals that includes only one department. In case of NAIH, due to the fact that the hotline was operated under the project, the involvement of personnel from different departments was involved in responding to queries. Based on the NAIH’s experiences this prolonged the response time. Therefore, it is advisable that responses are handled by one department, for the administrative – professional – approval process to remain as simple as possible.

At the same time, NAIH considered the division of the workflow to be useful for speeding up the response time. The knowledge base has proved to be particularly helpful in optimising the work effort. It allowed the less experienced personnel to answer the simple enquiries, whereas the more complex enquiries were directed immediately to the hotline expert. Furthermore, it was observed that a knowledge base may be particularly helpful in order to ensure standardisation of responses to similar questions / scenarios. The majority of staff effort and time in such a service will be taken up by responding to concrete questions where the GDPR needs to be applied to concrete operational context and activities of an SME. These are the most common questions, and tended to have a higher than average difficulty. This means data protection expertise remains important in handling these emails, and they to a large extent cannot be handed off to a knowledge base.

The most significant result of the awareness raising campaign was that it encouraged and incentivised the development of the informational strategies that meet the needs of the SMEs representatives. The results obtained from hotlines dedicated to a particular group could potentially orient DPAs in issuing further guidance on recurrent queries as well as select topics for training activities.

This means data protection expertise remains important in handling these emails, and they to a large extent cannot be handed off to a knowledge base.



References

[1] *When referring to Independent Supervisory Authorities we use the following terms: Data Protection Authorities, DPAs and regulators.*

[2] *European Union Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/ EC (GDPR), Article 51.*

[3] *Bennett, Colin and Charles Raab, The Governance of Privacy: Policy Instruments in Global Perspective, MIT Press, Cambridge MA & London, 2003, p.109–114. David Barnard-Wills, Cristina Pauner Chulvi and Paul De Hert, 'Data Protection Authority Perspectives on the Impact of Data Protection Reform on Cooperation in the EU' (2016) 32 Computer Law & Security Review 587, 587 <https://linkinghub.elsevier.com/retrieve/pii/S026736491630084X> accessed 3 August 2019.*

[4] *Centre for Information Policy Leadership, 'Regulating for Results Strategies and Priorities for Leadership and Engagement: A Discussion Paper' (2017) p. 7-8.*

[5] *Within the scope of this guidance enforcement strategies are understood as policy documents setting out DPAs' priorities concerning audits, investigations, and awareness raising activities. We recognize that DPAs also have other influential powers, such as the possibility to intervene into processing operations by request blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing.*

[6] *Robert Baldwin and Martin Cave, Understanding Regulation: Theory, Strategy, and Practice (OUP 1999), p. 101.*

[7] *Article 29 Working Party and the Working Party on Police and Justice joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, The Future of Privacy (2009 WP 168), p. 22-23.*

[8] *Article 29 Working Party and the Working Party on Police and Justice joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, The Future of Privacy (2009 WP 168), p. 4.*

[9] *It should be noted that some differences in the interpretation of the GDPR occur due to the fact that it has been translated into all EU languages. All officially translated versions of the GDPR are enforceable.*

[10] *Awareness raising is a horizontal issue that resurfaces across the range of EU policy areas (e.g. national competition authorities; Telecommunications national regulatory authorities etc.).*

[11] *Kuner C., Bygrave L., Docksey C., The EU General Data Protection Regulation (GDPR): A Commentary (OUP; 2020), 930*

[12] *Cochrane, L., Barnard-Wills, D., & Matturi, K., Report on DPA efforts to raise awareness among SMEs on the GDPR, STARII D2.1, Budapest, Brussels & Waterford, July 2019.*

[13] *Barnard-Wills, D., Cochrane, L., Matturi, K., & Marchetti, F., Report on the SME experience of the GDPR, STARII D2.2, Budapest, Brussels & Waterford, July 2019.*

[14] *Within the scope of this guidance we consider 'SME representative' to include individuals working for and running SMEs*

[15] *See: https://naih.hu/felkeszueles-az-adatvedelmi-rendelet-alkalmazasara.html*

[16] *The principal objective of the ARCADES project is raising awareness in schools in the European Union about data protection and privacy and in this way reinforcing children's protection of personal data in the online environment. In order to achieve this objective, the data protection and privacy related content will be introduced at schools in the European Union by means of providing training on privacy and data protection (two-day seminars for teachers) and disseminating the gained information among pupils. For more information see: http://www.arcades-project.eu/index.php.*

[17] *Cochrane, L., Barnard-Wills, D., & Matturi, K., Report on DPA efforts to raise awareness among SMEs on the GDPR, STARII D2.1, Budapest, Brussels & Waterford, July 2019.*

[18] *Callers tend to be reluctant to share information over the phone as this may trigger a DPA to act. For example, in case a caller poses a question about a personal data breach to some DPAs (i.e. ICO), such action will trigger the registration of a personal data breach. Approaches, however, differ among DPAs.*

[19] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).*

[20] *GDPR 57: '1. Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory: […] (b) | promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention; […] (d) | promote the awareness of controllers and processors of their obligations under this Regulation'.*

[21] *For the definition of recipient see Article 4 (9) of the GDPR.*

Annex I — Annex I — Memorandum on running the hotline for SMEs

Memorandum

Recipients:
Dr Júlia Sziklay, Head of Department
Dr. Györngyi Balogh, Head of Department
Dr Attila Mátyásfalvi, Head of Department
Eszter Szamosközi, Mrs. Orbán, Head of Department
Dr. Kata Nagy, General Secretary
Szilvia Urbán, Head of Department

Administrators: Dr. Júlia Sziklay, Dr. Tamás Számadó
Subject: The order of fulfilling the 'SME Hotline' task within the STAR II Project
Date: '' March 2019

I hereby establish the order of fulfilling/implementing the task of providing prompt, electronically accessible information services for the duration of a year for small and medium enterprises (hereinafter: 'SME Hotline') within the framework of the 'SupporT small And medium enterprises on the data protection Reform II'—the so-called STAR II project, identification number: 814775 – STAR II – REC-AG-2017/REC-RDAT-TRAI-AG-2017(hereinafter: 'the Project')—of the National Authority for Data Protection and Freedom of Information.

1. The duration of fulfilling the SME Hotline task by the Authority within the Project shall be March 15 2019 and March 15 2020.

2. The SME Hotline task shall constitute: answering requests for general information coming to the dedicated functional e-mail address (kkvhotline@naih.hu; hereinafter: 'hotline'), as published on the NAIH website and advertised over the radio, from small and medium enterprises (hereinafter: 'hotline requests') on the application of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), as well as the creation of a related Knowledge Base, and the collection of statistical data.

3. The duty of professionally supervising and directing the SME Hotline task operation shall be borne by the Head of the Freedom of Information Department (Project Coordinator), who may instruct colleagues participating in the fulfilment of this task but not belonging directly under her direction—via informing, if necessary, the colleague's direct superior.

4. The Project Assistant colleague at the Department of Freedom of Information shall coordinate answering hotline requests and ensure the fulfilment of the administrative duties required. Should the Project Assistant be incapacitated, the head of the Department of Freedom of Information shall designate and commission a colleague to perform the task as a deputy.

5. Hotline questions shall be answered within 8 workdays of receiving them in the way defined by this instruction. The response shall be sent to the requester's e-mail address. The response shall include:

    a. the summary of the question or questions;

    b. the concrete answer to each question, with references to sources used apart from citations of law, and

    c. the disclaimer in Annex 1 a).

6. The answers to the hotline requests in Hungarian or English, as well as the languages designated by consortium members and EU languages, shall be in the language of the request, under the condition that the Project Assistant shall send the non-English or non-Hungarian requests to the designated consortium member, redacting the personal data in the request and stating the expected deadline, and shall then dispatch the response by the consortium partner to the requester.

7. The Project Assistant shall draft responses to questions that can be answered on the basis of the Knowledge Base under point 18, and shall forward the draft response to colleague designated by the Head of the Data Protection Department (hereinafter: 'the Hotline Expert'), who shall signal within a day if he or she disagrees with and suggests changes to it on its merits; the Project Assistant shall dispatch the response taking into account the possible suggestions by the Hotline Expert.

8. The questions that cannot be answered on the basis of the Knowledge Base shall be sent by the Project Assistant to the Hotline Expert within 2 days of receipt, who shall then send the draft answer based on the law-enforcement practice of the Authority and the supervisory authorities under the General Data Protection Regulation, the relevant case law of the courts, and the documents of the European Data Protection Board assisting the application of law and in line with the content under point 5 to the Project Assistant within four working days. The latter shall then dispatch the response.

9. Should a hotline request pose a new or especially complicated question which cannot be answered unequivocally on the basis of the law-enforcement practice of the Authority and its associate authorities, the relevant case law of the courts, and

the documents of the European Data Protection Board assisting the application of law, the Hotline Expert shall involve other experts of the Authority in accordance with executive guidance where necessary.

10. The Hotline Expert shall present the draft response he or she formulates to the Head of the Data Protection Department before forwarding it to the Project Assistant.

11. The responses shall be formulated so as to not only include the mere repetition of the provisions of law, but also to provide graspable assistance in the interpretation of law applicable relevant to the merit of the question, and to highlight the relevant aspects in the application of law related to the given question, the factors to be considered among them, and their significance. The answer shall contain no opinion as to the lawfulness of any concrete data processing.

12. Any request that is not general but specific, directed in its content to obtain an opinion on the lawfulness of a given data controller's data processing with a defined purpose shall be rejected by providing the brief notice included in Annex 1 b).

13. The colleagues involved in answering requests shall communicate in between themselves by e-mail.

14. The Project Assistant shall maintain a Register of all hotline requests and the responses to them with the content defined in Annex 2. The aim of the Register shall be to monitor the timely response to requests received and to collect statistical data needed for other products of the Project. The Register shall include the e-mail address of the requester as personal data only in order to monitor the fulfilment of the request, and the personal data required for other products by the Project shall be deleted when the SME Hotline task is concluded. The Cabinet shall be responsible for preparing the data processing notice related to fulfilling the SME Hotline task. The data processing notice shall be published continually alongside, directly beside, other notices accessible on the SME Hotline website.

15. In terms of the statistics and the Register related to the fulfilment of the SME Hotline task and the calculation of the special assignment allowance of the Hotline Expert, the answers to questions shall be classified in three groups according to the level of difficulty of formulating them:

    a. Level 1: a question answerable on the basis of the Knowledge Base or concludable by sending the notice included in point 12;

    b. Level 2: a question not answerable on the basis of the Knowledge Base but answerable unequivocally by the Hotline Expert on the basis of the

law-enforcement practice of the Authority and the supervisory authorities under the General Data Protection Regulation, the relevant case law of the courts, and the documents of the European Data Protection Board assisting the application of law;

c. Level 3: the question is only answerable with the assistance under point 9.

16. The Head of the Freedom of Information Department, the Project Assistant and the deputy Project Assistant shall have read and write access to the kkvhotline@naih.hu e-mail box.

17. Following the conclusion of the SME Hotline task under point 1, the contents of the kkvhotline@naih.hu e-mail box shall be saved and archived on a portable storage device, and the storage device shall be stored filed among the papers of the project until selection for destruction, and otherwise the contents of the e-mailbox shall be deleted.

18. The fulfilment of the SME Hotline task shall be assisted by a Knowledge Base developed on the basis of the law-enforcement practice of the Authority and the documents of the European Data Protection Board assisting the application of law by colleagues selected and instructed thereto by the Head of the Data Protection Department; in its edited form, the Knowledge Base shall have a question–and–answer structure, and contain abridgments of law-enforcement practice in pairs of questions and answers, providing relevant citations and keywords to assist searches. The Knowledge Base shall be accessible to anyone in the „START II" library on drive K:\.

19. Colleagues performing customer service tasks or answering requests (consultation submissions) for information on data controllers or data subjects in connection with the processing of personal data shall take into account, when answering questions already included in the Knowledge Base, the answer included in the Knowledge Base relating to the question as far as they possibly can.

20. During the performance of the SME Hotline task, the Knowledge Base shall be maintained and kept by a colleague selected and commissioned thereto by the Head of the Data Protection Department; she or he shall update it—at least on a monthly basis—on the basis of the information she or he receives in accordance with point 21 or the decision, opinion or any document pertaining to law-enforcement practice the Head of the Data Protection Department transfers to her or him thereto.

21. The Project Assistant and the colleague under point 19 shall record in the data sheet in Annex 3 a question and answer not included in the Knowledge Base, or

an answer that differs in its merits from the one already in the Knowledge Base. The colleague shall forward the data sheet to the colleague in charge of the Knowledge Base within 5 days of dispatching the answer.

22. The Hotline Expert, the colleague in charge of the Knowledge Base, the persons commissioned to deputize for them and the Project Assistant, and the Head of Data Protection Department shall perform their duties related to the SME Hotline task as beyond their normal work duties, as a special assignment in exchange for a special assignment allowance. The conclusion of the agreements on the special assignments shall be in the charge of the Head of the Data Protection Department involving the Department of Management and Human Resources and applying the special assignment definitions in Annex 4.

23. The allowance for special assignments shall be calculated on the basis of actual working hours spent on the special assignment, and the work hours of the Hotline Expert shall be taken into account by weighting the different categories of difficulty so that the hourly fee for a question belonging in the Difficulty Level 2 shall be 200% and one in Difficulty Level 3 shall be 300% of one in Difficulty Level 1.

24. The persons performing special assignments shall keep a record of the working hours spent on the assignment in the Special Assignment Time Sheet included in Annex 5, which they shall submit to the Head of the Data Protection Department within the fifth working day of the last calendar day of the given month. The Head of the Data Protection Department shall approve the Special Assignment Time Sheets of the Hotline Expert, the colleague in charge of the Knowledge Base and those deputizing for them. The Head of the Freedom of Information Department shall approve the Special Assignment Time Sheet of the Head of the Data Protection Department.

25. The performance of the SME Hotline task shall be certified by the Head of the Freedom of Information Department on the basis of the monthly Time Sheets by way of the Performance Certificate included in Annex 6. The payment of the special assignment allowances shall be made upon the inflow of the resources for the Project according to the following schedule as for the performances unpaid but certified before the given dates:

    a. until 30 June 2019;

    b. until 31 December 2019; and

c. until 30 April 2019.

Dr. Attila Péterfalvi
President

Annex 1 of Memorandum NAIH/2019/724/

The Disclaimer and Notice to be Used in SME Hotline Responses

a. The text of the disclaimer referred to in point 5 c) of the Memorandum: 'Finally, please note that the information by the Authority—dispatched outside of any procedural framework, as a consultation answer—shall be construed neither as law nor as any legal instrument, and shall have no normative feature, legal force or binding content. The interpretation of law by the Authority on the basis of the information provided in this case shall in no way bind any other authority, the courts or the data controller; it is serves merely guidance purposes. The opinion and information thus provided shall thus in no way exempt the addressee from the necessity of developing its own legal position or the data controller from its liability for data processing.'

b. The text of the notice referred to point 12 of the Memorandum 'The Authority responds to SME Hotline requests only insofar as they pose general questions of interpreting law, where, beyond the mere repetition of the provisions of law applicable, the requester requires assistance in the interpretation of their content relevant to the question, and the question can be answered by providing information on the relevant aspects of applying law, the factors to be considered among them, and the outlining of law-enforcement practice without any formulation of opinion on the lawfulness of a concrete data processing.

On account of the above, we are not in the position to deliver an opinion as regards the lawfulness of a data controller's data processing with the defined purpose.
I kindly ask you to take knowledge of the information above.'

Amendment of the Memorandum

Memorandum
Ref. no.: NAIH/2019/724/
Recipients:
Dr Júlia Sziklay, Head of Department
Dr. Györngyi Balogh, Head of Department
Dr Attila Mátyásfalvi, Head of Department
Eszter Szamosközi, Mrs. Orbán, Head of Department
Dr. Kata Nagy, General Secretary
Szilvia Urbán, Head of Department

Subject: The amendment of the memorandum on the order of fulfilling the 'SME Hotline' task within the STAR II Project
Date: '' April 2019

The following provision shall replace point 23 of the Memorandum on the order of fulfilling the 'SME Hotline' task within the STAR II Project.

The allowance for special assignments shall be calculated by multiplying the number questions an-swered, the hourly fee defined on the basis of gross salary, and the difficulty factor (the difficulty level defined in the statistical order of the operation of the Hotline), so that the hourly fee for a question belonging to Difficulty Level 2 shall be 200% and one in Difficulty Level 3 shall be 300% of one in Dif-ficulty Level 1, but the allowance shall not exceed half of the gross salary per month. Payment of the special assignment allowance shall be conditional on submitting the monthly time sheet.

Dr. Attila Péterfalvi

Annex II — Data Protection Notice

As to the Data Processing by the
National Authority for Data Protection and Freedom of Information
in the framework of the STAR II Project

1. Name of Data Controller

National Authority for Data Protection and Freedom of Information (hereinafter: 'the Authority'); seat: 1125 Budapest, Szilágyi Erzsébet fasor 22/C, Postal address: 1530 Budapest, Pf.: 5; telephone: +36 (1) 391-1400; fax: +36 (1) 391-1410; e-mail address: ugyfelszolgalat@naih.hu

2. The Data Protection Officer and Contact Details

The Data Protection Officer of the Authority: Klára KENDRA ZSIKÓNÉ; direct contact

details: e-mail address: dpo@naih.hu; telephone number: + 36 1 3911 445

3. The Purpose of Data Processing and the Scope of the Data Processed

The purpose of the data processing is to answer the questions on the practical issues of applying the General Data Protection Regulation sent to the Authority through the dedicated electronic information line (kkvhotline@naih.hu) operated for small and medium-sized enterprises (SMEs) in the framework of the STAR II Project between 15 March 2019 and 15 March 2020.
For this purpose, the Authority processes the following data: the name of the contact person provided by the SME, his or her contact details or any other personal data the request might include.

4. The Legal Basis of Data Processing

The data processing is based on Article 6 (1) e) of Regulation (EU) 2016/679 of the European Parliament and of the Council (hereinafter: 'the GDPR') , and is required for fulfilling the duties of the Authority in the public interest with a view to its obligation of performing the tasks under Article 57 (1) b) and d) of the GDPR .

5. The Sources of Personal Data Processed and the Scope of those Personal Data Provided to the Authority not by the Data Subject

Should you turn to the Authority not directly as the contact person of an SME, the Authority shall collect, from the SME as data controller contacting the dedicated electronic line, the following data: the name of the contact person provided by the SME, his or her contact details or any other personal data the request might include.

6. The Recipients of Personal Data and the Categories of Recipients[22]

The Authority shall not transfer personal data to other recipients.

7. The Duration of Storing Personal Data

In accordance with the Project announcement and in view of the obligation laid down in the documentation of the Project, the Authority shall process the electronic documents containing data for five years after the conclusion of the Project.

8. The Data Subject's Rights Concerning Data Processing

8.1. Deadline

The Authority shall fulfil a request to exercise a data subject's rights within one month of its receipt at most. The date of the arrival of the request shall not be included in the deadline.
If need be and in view of the complexity of the given request or the number of requests, the Authority may prolong this deadline by a further two-month period. The Authority shall notify the data subject of the prolongation providing the reasons for the delay within one month of receiving the request.

8.2. Data Subject Rights Concerning Data Processing

8.2.1. The Right of Access

The data subject shall be entitled to request information from the Authority through the contact details under point 1) on whether his or her personal data are being processed or not, and, if such processing is being carried out, he or she shall be entitled to know:

- what personal data,
- on what legal basis,
- for what data processing purpose, and
- for what duration

the Authority is processing;

as well as

- to who, when, on the basis of what law, and what personal data of his or hers the Authority has provided access or transferred;
- what the sources of obtaining his or her personal data were;
- whether the Authority uses automated decision-making, including profiling, and what the logic involved is.

The Authority shall provide a copy of the personal data being processed upon request by the data subject free of charge first; thereafter it may charge a reasonable fee based on administrative costs.
In order to fulfill data security requirements and the protection of the data subject's rights, the Authority shall be obliged to ascertain the identity of the data subject and the person requesting to exercise his or her right of access; for this purpose, the provision of information, access to data, and copies thereof shall be conditional on the identification of the persons involved.

8.2.2. Right to Rectification

The data subject shall be entitled to request the rectification of his or her personal data from the Authority through the contact details under point 1). If he or she can credibly prove the accuracy of the rectified data, the Authority shall fulfill the request within a month at most, and shall notify the data subject thereof at the contact details he or she has given.

8.2.3. The Right to Block (Restrict) Processing

The data subject shall be entitled to request, through the contact details under point 1), that the Authority restrict the processing of his or her personal data (clearly indicating the restricted nature of the processing and ensuring separate processing

from other data) if

- he or she contests the accuracy of the personal data (in this case, the Authority shall restrict processing for the time of verifying the accuracy of the data);
- the data processing is unlawful, and the data subject objects to the erasure of the data, and requests the restriction of their processing instead;
- the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims;
- the data subject has objected to processing (pending the verification whether the legitimate grounds of the controller override those of the data subject).

8.2.4. Right to Object

The data subject shall be entitled to object to the processing of his or her personal data from the Authority through the contact details under point 1) if he or she holds that the Authority processes his or her personal data not appropriately in relation to the purpose laid down in this data protection notice. In this case, the Authority shall demonstrate the compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

8.2.5. Right to Erasure

With regard to the data processing described in this notice, the data subject shall be entitled to exercise his or her right to erasure where processing is not required for the performance of the Authority's tasks in the public interest.

9. Right to Remedy

Should the data subject hold that the Authority has infringed the data protection requirements in effect while processing his or her personal data, he or she
- shall have the right to lodge a complaint with the Authority (National Authority for Data Protection and Freedom of Information; seat: 1125 Budapest, Szilágyi Erzsébet fasor 22/C; postal address: 1530 Budapest, Pf.: 5, telephone: +36 (1) 391-1400; fax: +36 (1) 391-1410; e-mail address: ugyfelszolgalat@naih.hu), or
- may turn to court to protect his or her data, and the court shall hear the case as a matter of priority. In this event, he or she is free to choose to bring the action before the regional court having territorial jurisdiction over his domicile (permanent address), place of residence (temporary address) or the seat of the Authority. He or she can look up the regional court having territorial jurisdiction over his or her domicile or place of residence at the website: http://birosag.hu/ugyfelkapcsolatiportal/birosag-kereso. The Budapest-Capital Regional Court has territorial jurisdiction for actions according to the seat of the Authority.

Annex III — Satisfaction survey

1. How useful do you consider the information provided via the SME hotline?

   ☐ low ☐ medium ☐ high

2. Were you provided with the information in an understandable manner?

   ☐ low ☐ medium ☐ high

3. Were all your questions answered in a satisfactory way?

   ☐ yes ☐ no

4. Are you satisfied with the level of detail of the information?

   ☐ low ☐ medium ☐ high

5. How satisfied are you with the speed of response?

   ☐ low ☐ medium ☐ high

6. Have you looked for other information sources concerning the issue you were interested in before contacting the SME hotline?

   ☐ yes ☐ no

7. If so, where?

   _____

8. How did you find the SME hotline?

   _____

9. Is there anything you were not satisfied with concerning the SME hotline?

   _____

10. Would you consider useful a hotline addressed expressly to SMEs?

    ☐ yes ☐ no

11. Would you consider useful a hotline addressed expressly to specific economic sectors?

    ☐ yes ☐ no

12 Would you prefer a telephone helpdesk?

☐ yes ☐ no

13 What is the activity of your SME?

_____

14 How many employees do you have?

☐ 0 ☐ 1-3 ☐ 4-5 ☐ 6-10 ☐ >10

Annex IV — FAQs addressed to the SME hotline

I. Scope of the GDPR

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.

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.

II. Lawfulness of data processing

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.

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

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.

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

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

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.

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 employee's data

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.

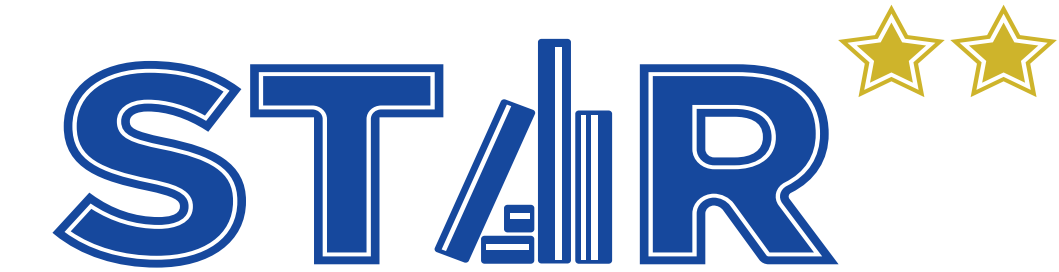
If the employer has also a legitimate interest in using tracking system, the first issue to be examined is whether the data processing is by all means necessary for the purposes designated by the employer, and whether its implementation by a GPS device is proportionate to the limitation on rights.

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.

We want to express our gratitude to the members of the advisory board, our colleagues and data protection professionals, who reviewed and commented on earlier versions of this guidance. In particular, we want to thank:

Dariusz Kloza (VUB-LSTS-d.pia.lab)
Paul De Hert (VUB-LSTS)
Vagelis Papakonstantinou (VUB-LSTS)
Carlotta Rigotti (VUB-FRC)
The Trilateral Data Protection and Cyber Security team
Basile Guley (CNIL)
Jelena Burnik (IP-RS),
Oana Luisa Dumitru (Romanian DPA)
Iva Ivanković (AZOP)
Luc Hendrickx (SME United)
and the representatives of
Belgian, Czech, Latvian, and the United Kingdom
data protection authorities.



SupporT small And medium enterprises on the data protection Reform II

The STAR II project – Support Small and Medium Enterprises on the Data Protection Reform II – has received funding from the European Union's Rights, Equality and Citizenship Programme 2014-2020, under grant agreement No. 814775