STAR II SUPPORT SMALL AND MEDIUM ENTERPRISES ON THE DATA PROTECTION REFORM II

Draft versions of the guidance & handbook

Deliverable **D4.1**

version 1.1

Gábor Kulitsán
Renáta Nagy
Lina Jasmontaite-Zaniewicz
Leanne Cochrane

Budapest – Brussels – Dublin
May 2020

Distribution level: **Public**

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

TRILATERAL RESEARCH

A report prepared for the European Commission's Directorate-General for Justice and Consumers (DG JUST).

The STAR II project (*Support small And medium enterprises on the data protection Reform II*; 2018-2020) is co-funded by the European Union under the Rights, Equality and Citizenship Programme 2014-2020 (REC-RDAT-TRAI-AG-2017) under Grant Agreement No. 814775.

Cover image:

Permanent link:

Authors	
Name	**Partner**
Gábor Kulitsán	NAIH
Renáta Nagy	NAIH
Lina Jasmontaite-Zaniewicz	VUB-LSTS
Leanne Cochrane	TRI

Contributors	
Name	**Partner**
Júlia Sziklay	NAIH
Alessandra Calvi	VUB-LSTS
Paul de Hert	VUB-LSTS

Internal Reviewers	
Name	**Partner**
Alessandra Calvi	VUB-LSTS
Lina Jasmontaite-Zaniewicz	VUB-LSTS
Leanne Cochrane	TRI
David Barnard-Wills	TRI

Institutional Members of the STAR Consortium		
Member	**Role**	**Website**
Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH)	Project Coordinator	naih.hu
Vrije Universiteit Brussel (VUB) Research Group on Law, Science, Technology and Society (LSTS)	Partner	https://lsts.research.vub.be/
Trilateral Research Ltd. (TRI IE)	Partner	trilateralresearch.com

Version number	Author	Purpose/Change	Date
1.0	**All authors**	**Initial submission to EC**	**29/02/2020**
1.1	Alessandra Calvi Lina Jasmontaite-Zaniewicz	Updated hotline data; advanced draft Handbook for consultation with EAB and DPA	13/05/2020

Table of Contents

1 Background to the STAR II project

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 enhancing compliance with the GDPR by assisting DPAs and SMEs.

There are pressing needs to assist EU data protection authorities (DPAs) in raising awareness among businesses, especially SMEs, on the new 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 new regulatory regime applicable for the processing of personal data; they need guidance on how to follow their 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; they often need to create and execute an action plan to apply the new framework.

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

1) review the state of the art in DPA awareness-raising activities,
2) analyse SMEs' experience within first months of the functioning of the GDPR,
3) run an awareness raising campaign for SMEs,
4) establish and operate an e-mail hotline (12 months) to respond to SMEs' questions, measuring its performance and the most frequently asked questions,
5) prepare a digital guidance for DPAs on good practices in running an e-mail hotline and raising SME awareness, and
6) draft an innovative, FAQ-based handbook (digital and printed) for SMEs on EU personal data protection law.

These results will be prepared in consultation with stakeholders (especially via validation workshops and the External Advisory Board) and widely disseminated. The outputs will be freely available, openly accessible and copyright-unrestricted, thus easily reusable and adaptable.

2 Summary

This document is comprised from two parts:

Part A - the guidance for DPAs on good practices in raising awareness, especially for SMEs about GDPR issues. The guidance, after situating awareness raising task within the redefined role of DPAs, builds on the experience of NAIH obtained during the timespan of a hotline for SMEs. The guidance provides recommendations on how to set up and run a hotline. It pays special attention to the required infrastructure, resources required, engaged personnel, internal policies, legal implications and ethical considerations.

Part B - an innovative handbook for SMEs on EU data protection law based on the questions SMEs most frequently asked the hotline and the responses given. The responses to be given will help explain to SMEs the basics of data protection law and the GDPR, through illustrations, practical examples, templates and contacts for better understanding and easy utilisation. This handbook will accustom SMEs to the GDPR, and help them ensure that they are GDPR compliant. The handbook will predominantly reflect and build on the issues raised in Activity 3.4. The handbook will also be valuable for DPAs too as it will help them understand which issues are particularly concerning SMEs and where they might wish to be put the emphasis in their own awareness raising activities.

3 Guidance for DPAs on setting up hotlines for SMEs

3.1 The role and powers of DPAs under the GDPR

A significant part of the General Data Protection Regulation EU 2016/679 (GDPR) is devoted to address the role and the daily functioning of Data Protection Authorities (DPAs). The GDPR in 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, responsibilities and their independence, clarifies and, to some extent, redefines 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] It has been observed that the consistency obligation found in the GDPR does not have an equivalent in the Data Protection Directive 95/46/EC (DPD) that it has repealed.[3] Nonetheless, it can be suggested that this obligation related to the requirement for DPAs to 'cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information' that was set in the DPD.

The legislator has foreseen in Article 57 that to attain the objective of monitoring and consistency of the application of the GDPR, DPAs should undertake 22 tasks that range from enforcers, ombudsmen, auditors, consultants to policy advisors, negotiators and educators.[4] The list leaves no doubt that DPAs responsibilities fall beyond enforcement.[5] 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.[6]

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 little attention. To foster the debate on what do such awareness raising duties include and how their consistency can be ensured among 27 European Union (EU) member states, we put forward this guidance document.

In an attempt to reflect on this long practiced by only recently formalized duty, we will consider the impactions of DPAs as educators.

3.2 DPAs & awareness raising

Dynamics of enforcement powers provided within the scope of the EU data protection framework have shaped awareness raising duties of DPAs. It can be suggested that to compensate for being

[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] Kuner C., Bygrave L., Docksey C., The EU General Data Protection Regulation (GDPR): A Commentary (OUP; 2020), 866.
[4] Cross reference to Bennett, Colin and Charles Raab, The Governance of Privacy: Policy Instruments in Global Perspective, MIT Press, Cambridge MA & London, 2003, p.109–114. in 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.
[5] The list is included at the end of this guidance.
[6] Centre for Information Policy Leadership, 'Regulating for Results Strategies and Priorities for Leadership and Engagement: A Discussion Paper' (2017) p. 7-8.

awarded with limited enforcement powers to impose the so called 'deterrence' style enforcement and significant fines under the Data Protection Directive 95/46/EC, for most of DPAs awareness raising duties have long been part of their enforcement strategies.[7] In view of this, it can be even argued that most of the DPAs followed intuitively the recommendation put forward by Robert Baldwin and Martin Cave in their seminal work on understanding regulation 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, negotiation, education, or promotion'.[8] By means of opinions, guidelines, public engagements and other similar awareness raising activities, the well-intentioned national regulators sought to reach, one 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'.[9]

The legislators with the adoption of the GDPR 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 a way update enforcement practices of DPAs.[10] This being said, it should be added that 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 a direct bearing on how the ones who are regulated cope with applicable rules and it also affects enforcement claims brought by individuals.

3.3 Advantages of awareness raising

Awareness raising duties of DPAs should be considered to be instrumental to attain the objective of monitoring and consistency of the application of the GDPR because of several reasons.

First of all, 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 the regulation that can be understood in a comprehensive manner, carries the potential to result in the desirable behavior of addressees. In this sense, awareness raising activities could be key enablers to promote a data protection culture among the general public.

Secondly, 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 General Data Protection Regulation in a specific national context.[11]

Third, awareness raising practices of DPAs, similarly to other enforcers across the EU regulatory domains,[12] allow to mainstream the overall policy objective to the wider audience and in this way minimize disparities in information – the so called information asymmetries – that have been reported among entities, organizations 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 in order to empower data subjects with control over their personal data, and on the

[7] 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.
[8] Robert Baldwin and Martin Cave, *Understanding Regulation: Theory, Strategy, and Practice* (OUP 1999), p. 101.
[9] 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.
[10] 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.
[11] 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.
[12] 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.).

other hand, they have to facilitate data flows within the internal market for controllers and processors.

Finally, the awareness raising duties of DPAs could be seen as a tool reducing 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 favorable regulatory set-up.[13]

3.4 Awareness raising practices

DPAs reported to use different mediums to reach out the target audience with their awareness raising campaign as well as to learn their distinct needs.[14] DPAs identified the print media, social media and events as the most common general awareness-raising methods. DPAs typically opt-in for the multi-method approach that allows 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 the DPAs' websites for information on recent data protection issues, guidelines and decisions. Therefore, the DPAs should be encouraged to share information on decisions, opinions, guidelines, practical examples on data protection, etc. on their website. The information to be provided must be as practical as possible, as especially SMEs reported to be interested in detailed practical information.[15] Arguably, this could be done in coordination with SME associations to avoid duplication of effort and maximise resources. The emphasis here is again on follow-up and mapping the change.

DPAs reported a variety of ways in which they became aware of the needs of SMEs concerning the GDPR. This being said, it should be added that DPAs referred to events as the most effective awareness-raising strategy for SMEs, which also provides better insights into the specific challenges faced by SMEs. The consultation feedback provided by SME representative bodies was mentioned, however, it appeared that the one-to-one interaction that a DPA has with individual SME representatives[16] in a consultation or advisory context provided DPAs with the most substantial benefit in terms of understanding the needs of SMEs. Such interactions reported to occur through established engagement channels such as the public-facing hotline or helpdesk service, participation 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. Individual comments made by various DPAs which appear more context specific also help to highlight some other ways in which DPAs can engage at a personal level with SMEs

3.5 An overview of hotlines run by DPAs

The interviews carried out with 18 DPAs by the Consortium on their awareness-raising activities among SMEs about the GDPR concluded that all DPAs operated a form of telephone or email and telephone advice service SMEs can use to contact the DPA. However, in most cases, this service was not an SME specific hotline/helpdesk service.

Overall, it is deemed that a helpdesk or hotline service can be a very useful tool for DPAs to establish connection between the DPA 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 an adequate

[13] Kuner C., Bygrave L., Docksey C., The EU General Data Protection Regulation (GDPR): A Commentary (OUP; 2020), 930.
[14] STARII, D.2.1.
[15] STARII, D2.2.
[16] Within the scope of this guidance we consider 'SME representative' to include individuals working for and running SMEs.

platform to give legal advice in a specific issue due to liability issues as well as operating an e-mail hotline/helpdesk service can also face the issue of liability, therefore DPAs tend to give general guidance on the data protection legislation.

It appeared that most DPAs do not use internal guidance to direct hotline/helpdesk advisers (i.e., personnel). This a surprising finding given 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. However, such documents were deemed to be subject to confidentiality and were not shared with the Consortium. Most calls/queries were facilitated in the national language of the respective country which was also the language in greatest demand from SMEs. While some DPAs provided services in multiple languages, English was the most widely used across the EU DPAs in addition to the national language. 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.

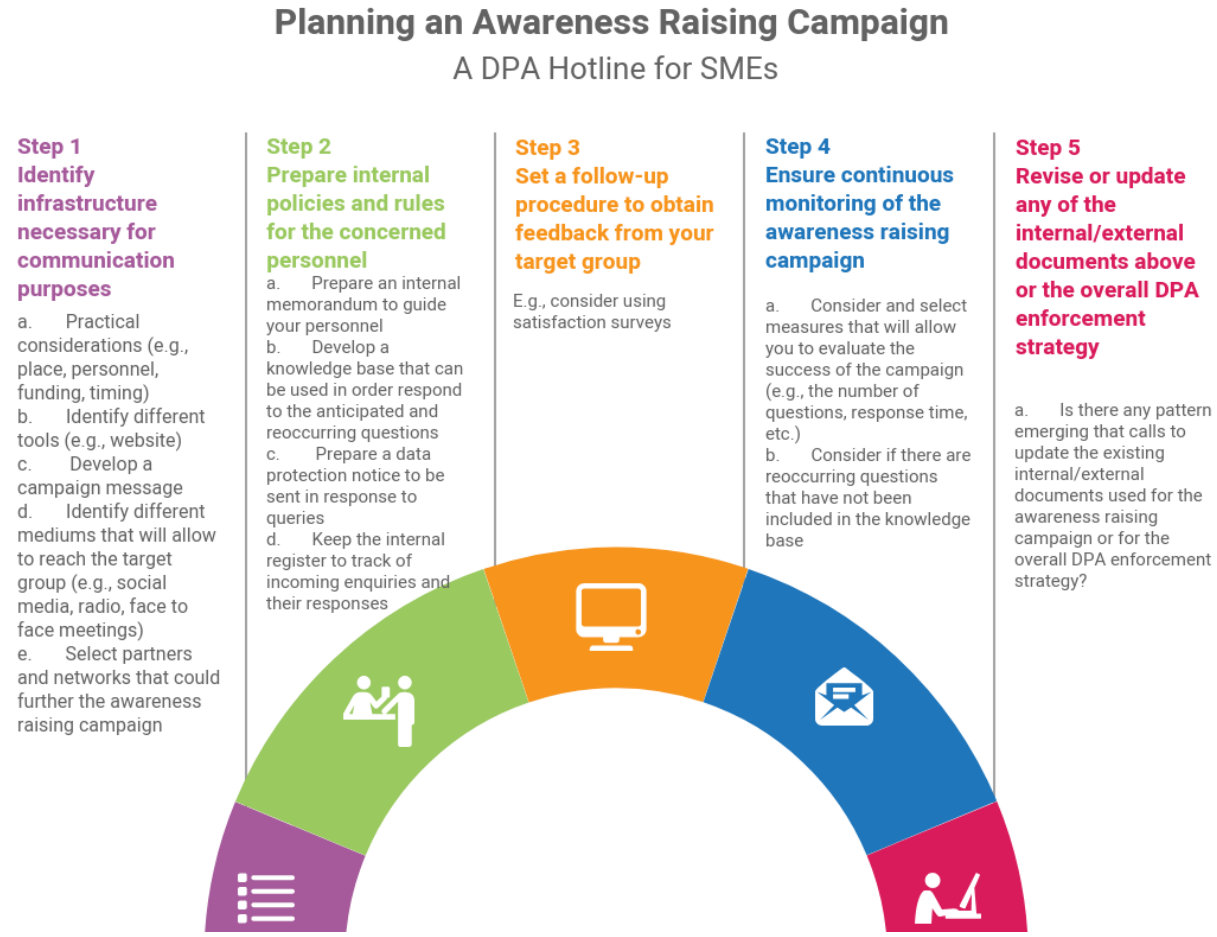
4 NAIH's hotline for SMEs

Within the scope of STARII project, NAIH launched a hotline dedicated to SME enquiries. NAIH operated the hotline between 15 March 2019 and 15 March 2020 in order 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. This initiative allowed to confirm that indeed a considerable uncertainty remains concerning the application of GDPR provisions, especially, for SMEs. The added value of this initiative is that it allowed to obtain better insights about the specific difficulties and questions SMEs face and that it allowed to draw recommendations on running an awareness raising campaign for a specific target group.

After providing an overview of recommendations, a more detailed description of each of them will be provided in the following sections.

4.1 Recommendations for setting up a hotline for SMEs

After selecting a target group and defining the objective of a particular awareness raising campaign, in our case enhancing GDRP compliance among SME representatives, we believe that by taking the following steps a comprehensive plan for a successful awareness raising campaign, can be developed:



1. **Identify infrastructure necessary for communication purposes**

    a. Practical considerations. For an effective set up of the hotline, it is necessary to allocate funding and to find a physical location where this can be run. Personnel to be appointed, either part-time or full time, it has to be trained.
    b. Identify different tools. There are several tools through which a hotline can be run. Websites and mail addresses may be the most common and effective tools and they were the one chosen by NAIH for running the hotline. Nevertheless, it may be desirable to provide a phone number or a physical address where queries may be sent in paper form to avoid excluding those SMEs with lack of technological literacy.
    c. Develop a campaign message in a simple and easy to understand language.
    d. Identify different mediums that will allow to reach the target group (e.g., social media, radio, face to face meetings). Even in this case, the medium chosen has to be suitable to avoid excluding part of the populations that may lack digital literacy.
    e. Select partners and networks that could further the awareness raising campaign. They can be, for example, sector specific SME associations or networks.

2. **Prepare internal policies and rules for the concerned personnel**. Such policies and rules may include:

    a. Prepare an internal memorandum to guide your personnel. Ideally, people with different seniority will be providing responses in the hotline. Queries received may be divided into different categories according to their complexity and assigned to different officials depending on expertise and seniority level. The memorandum may contain also recommendations concerning the replies, the deadlines for providing answers etc.
    b. Develop a knowledge base that can be used in order respond to the anticipated and reoccurring questions. Ideally, the knowledge base has to be prepared before starting to run the hotline and has to be kept up to date, in the light of the queries received and of the national and European case law developments and issuance of guidance by for example the European Data Protection Board. Such knowledge based may be particularly helpful in order to ensure standardisation of responses to similar questions / scenarios.
    c. Prepare a data protection notice to be sent in response to queries.
    d. Keep the internal register to track of incoming enquiries and their responses. Albeit the questions received will feed the knowledge base, it is best practice to ensure the anonymization of the persons forwarding the request.

3. **Set a follow-up procedure to obtain feedback from your target group**

    a. In our case, SMEs who submitted queries concerning personal data processing operations were asked to fill in satisfaction surveys. Setting up a follow up procedure to gather comments and suggestions from users is important to understand how to further improve the hotline.

4. **Ensure continuous monitoring of the awareness raising campaign**

    a. Consider and select measures that will allow you to evaluate the success of the campaign (e.g., the number of questions, response time, etc.). As follow up procedures, continuous monitoring enables to identify the criticalities of the hotline and to correct them.

b. Consider if there are reoccurring questions that have not been included in the knowledge base. Ideally, every time a new query is presented, it should be included in the knowledge base.

5. Revise or update any of the internal/external documents above or the overall DPA enforcement strategy

a. Consider if there is any pattern emerging that calls 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 issues further guidance on recurrent queries.

4.2 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 different tools that will be used throughout the campaign (e.g., website page, enquiry form). Then, NAIH in consultation with the consortium partners developed a campaign message that was used to reach out to the target audience. It should be added that NAIH engaged with the target audience different mediums, including social media, radio, and face to face meetings. The latter provide particularly valuable as it allowed to further the awareness raising campaign among the concerned audience.

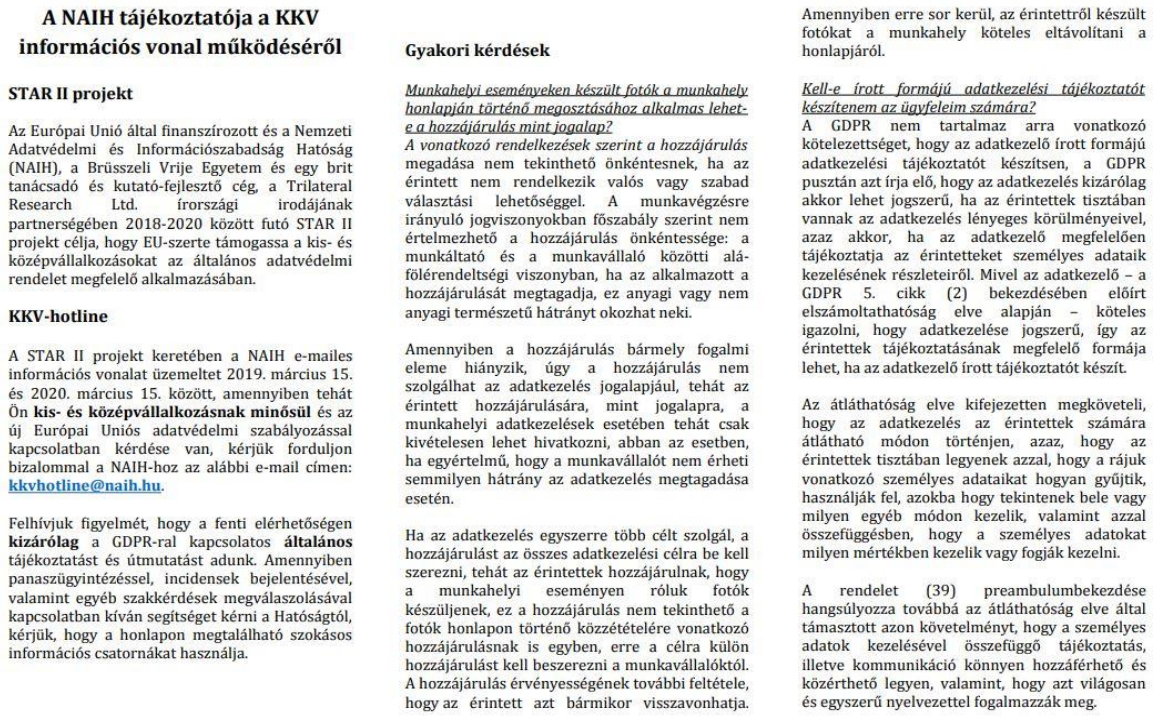
4.2.1 Website

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,[17] the website was updated and now provides information for SMEs on the GDPR compliance via the form of brochure that has been updated on a regular basis. 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 14.03.2019.

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 2 press releases on the actual status of the project that were published on NAIH's website and also 3 information booklets on the SME hotline (so far). NAIH's website has been considered to be the most appropriate informational 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 issues, guidelines and decisions issued by the authority and other information on the activity of the authority.

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



A NAIH tájékoztatója a KKV információs vonal működéséről

STAR II projekt

Az Európai Unió által finanszírozott és a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH), a Brüsszeli Vrije Egyetem és egy brit tanácsadó és kutató-fejlesztő cég, a Trilateral Research Ltd. írországi irodájának partnerségében 2018-2020 között futó STAR II projekt célja, hogy EU-szerte támogassa a kis- és középvállalkozásokat az általános adatvédelmi rendelet megfelelő alkalmazásában.

KKV-hotline

A STAR II projekt keretében a NAIH e-mailes információs vonalat üzemeltet 2019. március 15. és 2020. március 15. között, amennyiben tehát Ön **kis- és középvállalkozásnak minősül** és az új Európai Uniós adatvédelmi szabályozással kapcsolatban kérdése van, kérjük forduljon bizalommal a NAIH-hoz az alábbi e-mail címen: kkvhotline@naih.hu.

Felhívjuk figyelmét, hogy a fenti elérhetőségen **kizárólag** a GDPR-ral kapcsolatos **általános** tájékoztatást és útmutatást adunk. Amennyiben panaszügyintézéssel, incidensek bejelentésével, valamint egyéb szakkérdések megválaszolásával kapcsolatban kíván segítséget kérni a Hatóságtól, kérjük, hogy a honlapon megtalálható szokásos információs csatornákat használja.

Gyakori kérdések

Munkahelyi eseményeken készült fotók a munkahely honlapján történő megosztásához alkalmas lehet-e a hozzájárulás mint jogalap?
A vonatkozó rendelkezések szerint a hozzájárulás megadása nem tekinthető önkéntesnek, ha az érintett nem rendelkezik valós vagy szabad választási lehetőséggel. A munkavégzésre irányuló jogviszonyokban főszabály szerint nem értelmezhető a hozzájárulás önkéntessége: a munkáltató és a munkavállaló közötti alá-fölérendeltségi viszonyban, ha az alkalmazott a hozzájárulását megtagadja, ez anyagi vagy nem anyagi természetű hátrányt okozhat neki.

Amennyiben a hozzájárulás bármely fogalmi eleme hiányzik, úgy a hozzájárulás nem szolgálhat az adatkezelés jogalapjául, tehát az érintett hozzájárulására, mint jogalapra, a munkahelyi adatkezelések esetében tehát csak kivételesen lehet hivatkozni, abban az esetben, ha egyértelmű, hogy a munkavállalót nem érheti semmilyen hátrány az adatkezelés megtagadása esetén.

Ha az adatkezelés egyszerre több célt szolgál, a hozzájárulást az összes adatkezelési célra be kell szerezni, tehát az érintettek hozzájárulnak, hogy a munkahelyi eseményen róluk fotók készüljenek, ez a hozzájárulás nem tekinthető a fotók honlapon történő közzétételére vonatkozó hozzájárulásnak is egyben, erre a célra külön hozzájárulást kell beszerezni a munkavállalóktól. A hozzájárulás érvényességének további feltétele, hogy az érintett azt bármikor visszavonhatja.

Amennyiben erre sor kerül, az érintettről készült fotókat a munkahely köteles eltávolítani a honlapjáról.

Kell-e írott formájú adatkezelési tájékoztatót készítenem az ügyfeleim számára?
A GDPR nem tartalmaz arra vonatkozó kötelezettséget, hogy az adatkezelő írott formájú adatkezelési tájékoztatót készítsen, a GDPR pusztán azt írja elő, hogy az adatkezelés kizárólag akkor lehet jogszerű, ha az érintettek tisztában vannak az adatkezelés lényeges körülményeivel, azaz akkor, ha az adatkezelő megfelelően tájékoztatja az érintetteket személyes adataik kezelésének részleteiről. Mivel az adatkezelő – a GDPR 5. cikk (2) bekezdésében előírt elszámoltathatóság elve alapján – köteles igazolni, hogy adatkezelése jogszerű, így az érintettek tájékoztatásának megfelelő formája lehet, ha az adatkezelő írott tájékoztatót készít.

Az átláthatóság elve kifejezetten megköveteli, hogy az adatkezelés az érintettek számára átlátható módon történjen, azaz, hogy az érintettek tisztában legyenek azzal, hogy a rájuk vonatkozó személyes adataikat hogyan gyűjtik, használják fel, azokba hogy tekintenek bele vagy milyen egyéb módon kezelik, valamint azzal összefüggésben, hogy a személyes adatokat milyen mértékben kezelik vagy fogják kezelni.

A rendelet (39) preambulumbekezdése hangsúlyozza továbbá az átláthatóság elve által támasztott azon követelményt, hogy a személyes adatok kezelésével összefüggő tájékoztatás, illetve kommunikáció könnyen hozzáférhető és közérthető legyen, valamint, hogy azt világosan és egyszerű nyelvezettel fogalmazzák meg.

4.2.2 Radio campaign

The radio campaign was a vital element in reaching out to the target audience – SME representatives. 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.[18]

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 out the target group widely and has increased the GDPR awareness among the SMEs, statistical information on the extent to which such campaign has changed compliance practices and behavior 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 consortium. The final text and the scenarios of the radio spot was recorded in Hungarian language on 20.12.2018. 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

[18] See: http://www.arcades-project.eu/index.php.

Freedom of Information, which has set up a special hotline: kkvhotline@naih.hu. This PSA 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 has 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).

4.2.3 Face to face interactions

In line with findings of the STARII project, NAIH found face to face interactions to be particularly useful in order to obtain better understanding of SME distinct needs concerning the GDPR compliance.[19] 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.[20]

Within the scope of STARII project, NAIH interacted with SME representative at the following events:

- A validation workshop for the preliminary results of the STARII 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 they are most interested in 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.

4.3 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. 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.

[19] STARII, D2.1

[20] 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.

NAIH developed the **"knowledge base"** before the launch 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 European Data Protection Board. 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**.

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. The Register included 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.

4.4 A follow up procedure to obtain feedback

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 satisfaction surveys that were sent by email.

4.5 Continuous monitoring of the awareness raising campaign

The functioning of the SME hotline, the encountered issues and the answers were continuously monitored (qualitatively and quantitatively). Based on the statistical analysis, the functioning of the hotline can be periodically refined and adjusted to the needs. The statistical analysis will also serve as necessary data for the monitoring and evaluation of SME awareness-raising strategies and the success of any knowledge-based resources as well.

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.). reoccurring questions that have not been included in the knowledge base

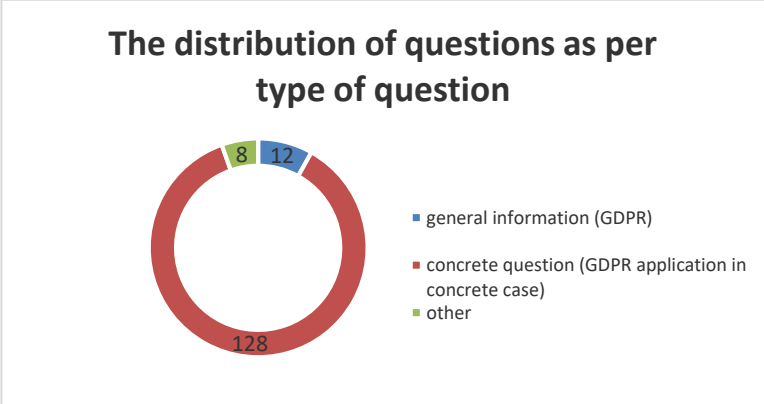
The data obtained from the internal register provided insights about the needs and difficulties SMEs are facing in order to comply with the GDPR. Based on the Register the most frequently asked questions were identified, which was an important indicator of SME concerns and apprehensions about the GDPR.

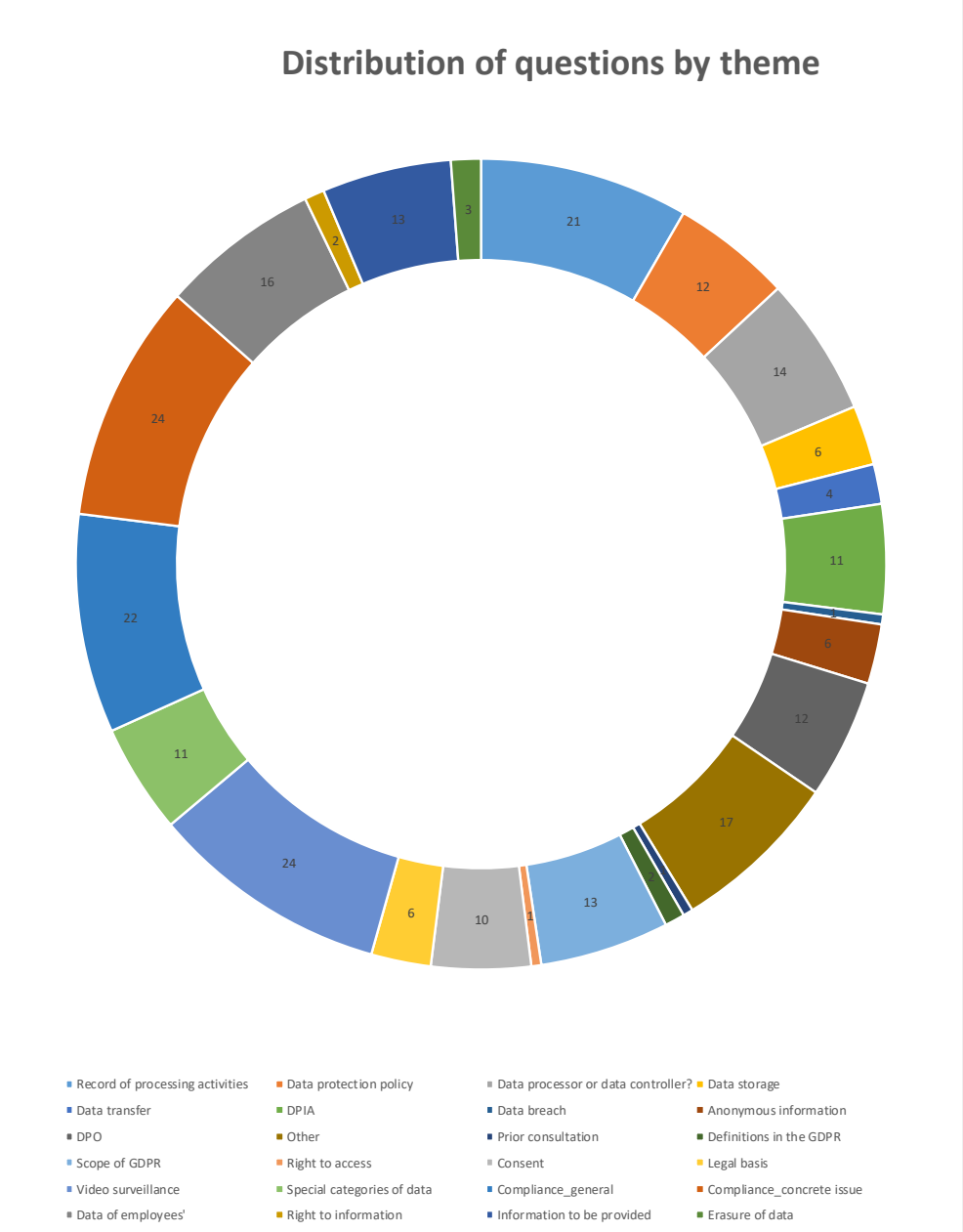
Based on the statistical analysis, the functioning of the hotline was periodically refined and adjusted to the needs of SMEs. The statistical analysis of the data collected in the Register also enabled the DPA to identify the most compelling needs of the SMEs in their compliance and also the assessment of the issues that need to be clarified.

It can be said, that the major outcome of the awareness raising campaign was that encouraged and incentivized the development of the informational strategies that meet the needs of the SMEs representatives. We are inclind 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.)





5 Concluding remarks

NAIH considers the awareness raising campaign a success as the increased interest of the SMEs on the GDPR compliance was reordered. 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.

While the NAIH was able to draw some recommendation 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, such as the ones highlighted in bold.

Article 57

Tasks

1. Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:

(a) monitor and enforce the application of this Regulation;

(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;

(c) advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;

(d) promote the awareness of controllers and processors of their obligations under this Regulation;

(e) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;

(f) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

(g) cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;

(h) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;

(i) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;

(j) adopt standard contractual clauses referred to in Article 28(8) and in point (d) of Article 46(2);

(k) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4);

(l) give advice on the processing operations referred to in Article 36(2);

(m) encourage the drawing up of codes of conduct pursuant to Article 40(1) and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 40(5);

(n) encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Article 42(1), and approve the criteria of certification pursuant to Article 42(5);

(o) where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7);

(p)draft and publish the criteria for accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;

(q)conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;

(r) authorise contractual clauses and provisions referred to in Article 46(3);

(s) approve binding corporate rules pursuant to Article 47;

(t) contribute to the activities of the Board;

(u)keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and

(v) fulfil any other tasks related to the protection of personal data.