SUPPORT SMALL AND MEDIUM ENTERPRISES ON THE DATA PROTECTION REFORM II

Report on WP2 Validation workshop

Deliverable **D2.3** (Version 1.0)

Ms Leanne Cochrane, Dr David Barnard-Wills, Mr Kai Matturi, Dr Filippo Marchetti

Budapest – Brussels – Waterford
July 2019
distribution level: **Public**

Authors	
Name	Partner
Ms Leanne Cochrane	TRI
Dr David Barnard-Wills	TRI
Mr Kai Matturi	TRI
Dr Filippo Marchetti	TRI
Internal Reviewers	
Name	Partner
Lina Jasmontaite	VUB-LSTS
Paul de Hert	VUB-LSTS
Renáta Nagy	NAIH
David Wright	TRI

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

This report has been 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.

Permanent link: TBC

version 1.0
14 July 2019

Table of Contents

1. Background to the STAR II project

The STAR II project (Support small and medium enterprises on the data protection reform II) commenced in August 2018 and is intended to run for a two-year period. It is co-funded by the European Union under the Rights, Equality and Citizenship Programme 2014-2020 and is aimed at: (i) assisting European Union (EU) Data Protection Authorities (DPAs) raise awareness about the General Data Protection Regulation (GDPR) among small and medium enterprises (SMEs); and (ii) assisting SMEs to comply with the GDPR.

There are 22 million SMEs in the EU who form the core of the EU enterprise policy. These SMEs face distinctive challenges from data protection law and can often not afford professional legal advice. As such, they merit special support from public authorities as recognised by Recital 132 of the GDPR which specifies that when undertaking awareness-raising activities addressed to the public, data protection authorities should include specific measures directed towards, among others, SMEs.

The STAR II project outputs will include:

1) A review of the state-of-the-art in DPA awareness-raising activities aimed at SMEs (Deliverable 2.1).
2) Report analysing the SME experience of the GDPR during its first year (Deliverable 2.2)
3) An email hotline run by *Nemzeti Adatvédelmi és Információszabadság Hatóság,*(NAIH the Hungarian National Authority for Data Protection and Freedom of Information) in both Hungarian and English;
4) A guidance document for DPAs on good practices in awareness-raising techniques among SMEs;
5) A handbook for SMEs to help them comply with the GDPR.

At the time of writing, NAIH is currently operating the email hotline and has completed an awareness-raising campaign in Hungary to promote the hotline among SMEs. An analysis of this effort along with Deliverables D2.1 and D2.2. and the validation workshops will ensure that the guidance document for DPAs and the handbook for SMEs is innovative and responsive to the core aim of assisting SMEs comply with their GDPR obligations.

1.1. STAR project, 2017-2019

The STAR II project follows on from the STAR project (Support training activities on the data protection reform), which is nearing completion and focused on providing support to the training activities of DPAs and data protection officers (DPOs) on the EU data protection reform, especially the GDPR. The STAR project was also co-funded by the EU under the Rights, Equality and Citizenship Programme 2014-2020. The outputs from the STAR project have included:

1) Training scenarios for each training category,
2) A Seminars' Topics List, based on the training scenarios,
3) Seminar Material for each one of the seminars,
4) Webinars (selected from the Seminars' Topics List),
5) A training Handbook,
6) A takeaway reference GDPR checklist,
7) A ten-point GDPR introductory list.

2. Executive summary

This report documents a validation workshop for the preliminary results of the STAR II research project, held in Dublin in June 2019. The workshop was intended to present, check, and validate the findings of two studies conducted by the STAR II project:

- A review of the state-of-the-art in Data Protection Authorities (DPAs) awareness-raising concerning the General Data Protection Regulation (GDPR) among small and medium enterprises (SMEs) (Presented in Deliverable D2.1), and
- Research into the experiences of the GDPR of small and medium enterprises (SMEs) (presented in Deliverable D2.2).

To this end, the workshop included presentations of these results, contextual mapping exercises, general discussion with participations and presentations by two DPAs. During discussions, the main findings were confirmed and some additional input was generated.

Key messages that come out of the workshop include:

- For SMEs, the General Data Protection Regulation (GDPR) sits alongside a wider set of compliance requirements (e.g. tax, accounting, health and safety), which are generally seen as important, but not central to the SMEs core business activities, and which may conflict with revenue-generating activities.
- Technology and economic factors are both very important for SMEs and are deeply integrated because of the financial investment often required from SMEs to bolster technological capability, and the way that technological choices are often made on an economic basis. This combination of factors drives many of the choices that SMEs make and strongly influences their data protection posture.
- SMEs face challenges in being a fully informed customer of both technological products and services, and of data protection related advice and support.
    - Managing cloud-based IT and outsourcing personal data processing are two key issues.
    - SMEs face challenges in understanding which technologies and services are appropriate/most suitable for their business.
- Performing risk assessment is a key challenge for SMEs.
- There have been positive outcomes from the GDPR, with new services and business models being created, and some SMEs have used the requirements to update or improve business processes. In some cases this leads to the optimisation of resources and reduced spending on IT.

- SMEs appear to be interested in:
    - Sector-specific interpretation of the GDPR; and
    - GDPR certification options to support SME decision making around IT services and data protection compliance support.

3. List of Abbreviations

DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EC	European Commission
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
ePrivacy Directive	Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (ELI: data.europa.eu/eli/dir/2002/58/oj)
EU	European Union
GDPR	General Data Protection Regulation (Regulation EU 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, ELI: data.europa.eu/eli/reg/2016/679/oj
IT	Information technology
SME	Small and medium enterprise
STAR	Support training activities on the data protection reform
STAR II	Support small and medium enterprises on the data protection reform II
WP29	Working Party on the Protection of Individuals with regard to the Processing of Personal Data set up under Article 29 of Directive 95/46/EC (Article 29 Working Party). WP29 was replaced by the EDPB on 25 May 2018. The EDPB has endorsed many WP29 GDPR-related guidelines.

4. Introduction

This report is the third report which is publicly available as a deliverable in the context of the STAR II Project (Deliverable D2.3). It reports upon a validation workshop required by the grant agreement and held at Chartered Accountants House in Dublin on 24th June 2019. The purpose of the workshop was to validate the information gathering and interview processes and findings represented in Deliverables D2.1 and D2.2.

This report is therefore presented alongside the two other reports referred to as Deliverables D2.1 and D2.2 which concern:

- A review of the state-of-the-art in Data Protection Authorities (DPAs) awareness-raising concerning the General Data Protection Regulation (GDPR) among small and medium enterprises (SMEs) (Deliverable D2.1)
- A review of the SME experience of the GDPR (Deliverable D2.2)

All three reports are intended to inform and direct both the guidance document for DPAs identifying good practices in awareness-raising among SMEs and the handbook for SMEs to help them comply with the GDPR which will be produced later in the project, jointly as Deliverable D4.3.

5. Methodology

5.1. Invitees/Attendees

Just under 100 invitations were sent out to individuals to attend the validation workshop. All persons from DPAs and SME Associations who were either interviewed or who responded to the questionnaire which formed the research data for Deliverables D2.1 and D2.2. were invited to attend the validation workshop. This did not include SMEs that responded to the online survey. In addition, all members of the STAR II advisory board were invited.

Beyond these invitees, invitations targeted the Irish Data Protection Commission and SME associations based in the Dublin area. These invitees were identified by using Trilateral Research Ltd.'s mailing list, online research and field referrals.

In total, including the facilitators, fourteen people attended the workshop including three persons from a data protection authority, five from business associations (SME or sector specific), two DPO specialists, three researchers and one GDPR consultant. Out of these fourteen: seven participants were predominantly focused on the SME context in Ireland; two on Hungary; and five on the EU wide context.

5.2. Workshop Agenda

The workshop agenda was sent to participants the Friday before the workshop and was structured as follows:

14.00 - Welcome and Overview of STAR II project
14.10 - Exercise - A typical SME
14.35 - Exercise - The External Environment
15.00 - Presentation of STAR II findings: SMEs and the GDPR – Trilateral Research
15.15 - Tea and Coffee
15.30 - Presentation of STAR II findings: DPAs and raising awareness among SMEs – Trilateral Research
15.45 - "The Irish Data Protection Commission and awareness-raising among SMEs" - Mr Garrett O'Neill, Head of Private and Financial Sector Consultation and Assistant Commissioner, Data Protection Commission

16.00 - "The Hungarian DPA (NAIH) and the SME hotline"- Dr Júlia Sziklay, Head of the Freedom of Information Department, *Nemzeti Adatvédelmi és Információszabadság Hatóság*
16.15 - Open Discussion
17.00 - Thanks and Close

The main findings presented in draft versions of Deliverables D2.1. and D2.2. were reported to and discussed with participants during the workshop. Before doing so however, the workshop agenda was structured to commence with two exercises. The purpose of these exercises was to set the scene for the workshop in terms of outlining the internal and external factors affecting SMEs with which the participants engage. It was also an opportunity to brainstorm with participants prior to influencing the outcomes through the presentation of the project findings. Presenting the project findings in the middle of the workshop then allowed some opportunity for the participants to reflect and provide feedback.

6. Exercise 1: A Typical SME

In our first exercise, we worked with the participants to assemble a picture of a "typical" SME[1], focused upon the general (non-data protection specific) challenges that they face – understood as pain points – and a general sense of what a positive situation looks like for an SME – areas for gains and opportunities. Whilst there is huge diversity within the SME sector, the intent was to anchor our discussion around data protection challenges and issues in the day-to-day experiences of SMEs.

The discussion around the exercise engaged with the topics of general SME challenges and these related to challenges SMEs have with the GDPR, as well as some of the positive aspects of the GDPR as experienced by small business.

Figures 1 and 2 below show how the 'typical' SME exercise was conducted during the workshop and the information discussed above captured. Figure 1 is an example of the flip-chart image which can be used to conduct this exercise. Figure 2 shows the populated image from the discussions on the day. As is apparent from the Figure 2 and the writing below which tries to capture the narrative verbatim, participants identified many more 'pains' for SMEs than 'gains'.

[1] Modelled on the 'Pain-Gain Map'. See, Dave Gray, Sunni Brown & James Macanufo, *Game storming: A Playbook for Innovators, Rulebreakers and Changemakers* (O'Reilly, 2010), 190.

Figure 1: The 'pain-gain' template on which 'A typical SME' exercise was modelled.[2]

[2] Ibid., 191.

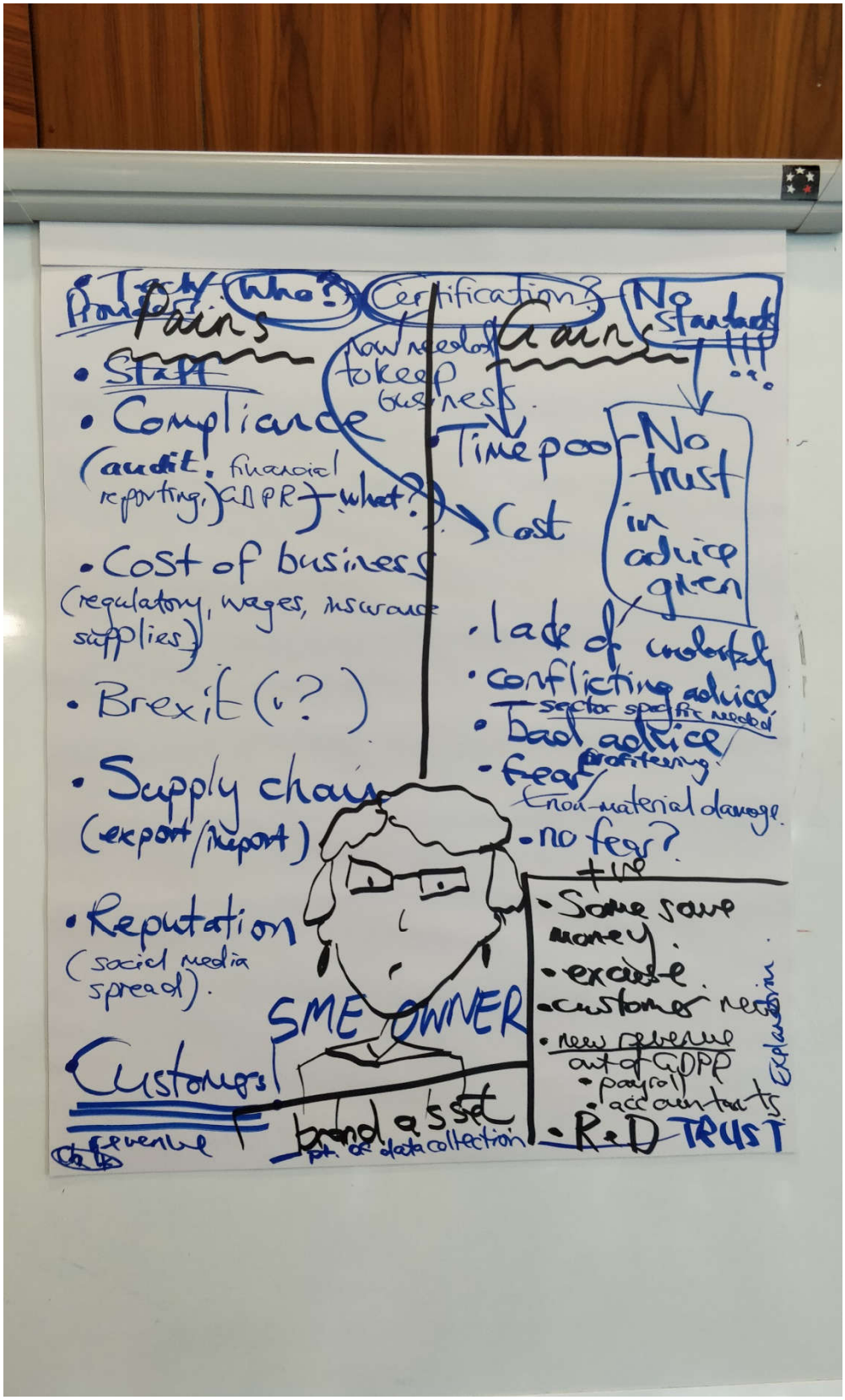

Figure 2: Results of the 'A typical SME' exercise

The following narratives try to convey the verbatim flow of the discussion that accompanied the information captured in Figure 2.

6.1. General SME Challenges

- **Compliance** – not just with the GDPR but beyond this, such as obligations relating to auditing and financial reporting. A combined set of costs, seen not really as a revenue earner but as a 'necessary evil'. Overcoming that and turning it into a positive mindset. GDPR seen as an addition on top of the rest of the requirements upon SMEs.
- The general **cost of doing business** is seen as high and increasing – some participants reported some savings with the GDPR, but the general cost of wages is going up, cost of regulation is going up. General issues identified here included: regulation, wages, insurance, finance, supplies.
- **Threat of Brexit** – the cost is unknown, there is much uncertainty and issues of UK/IE border routes, importers and exporters.
- **Reputation** – the GDPR is about people. Companies that deal with a lot of individuals as clients are wary of making any mistake with the GDPR. There can be differences between how the GDPR is understood by companies and how it is understood by the public. Companies have fears concerning being spoken about negatively on social media. They worry about the impacts upon reputation with direct impacts upon profits.
- **Uncertainty and where do I get advice?** about what has to be done – how to invest, what changes to make to forms, websites etc.
- **New technologies** – desire for new technologies (biometrics etc) and often they don't know the impacts. Some companies might be out there buying new technologies and not thinking about the privacy or data protection issues.
- **Customers** – the key motivator for SMEs is who are their customers, how do they get them, how do they retain them. With regard to GDPR, the big question was about keeping and using existing mailing lists – related to this key concern about keeping customers. Higher than compliance in hierarchy.
- **Staff** – costs of recruitment, hiring and retaining the right people.
- **Service providers** – one of key questions to regulator is who is the best service provider for a particular IT need (including GDPR compliance), but they can't answer this question, because it's a marketplace, its anticompetitive, and that is not their role, but a very regular question. Lots of IT security providers, but don't necessarily have the right qualifications.

6.2. GDPR Challenges

- **Certification and standardisation** - The GDPR certification process (as envisaged in Articles 42-43) is not yet mature, but the ambition is a process through which you will know what you're getting, that standards are being met, that the cost isn't excessive – like hiring a plumber or an electrician. SMEs have desire for a way to show that they meet the minimum standard – barriers for this include mainly cost, but also time. There are no national courses for example, and DPOs have only existed for a short period. Nobody has yet had the time to do a proper training course on what a DPO is, what their functions are, how to exercise independent functions. Nobody has assessed what is a professional GDPR expert, and how they would do a DPIA for a business. Or how they would risk assess a business, what harms could be done by its data management processes, that's a huge undertaking – business that are in contact with us (IE DPA) did a data mapping exercise, a big spring clean, to see how they were handling personal data, and that was a huge undertaking for them. Time and cost, expense – third parties do it for a small fortune. Standards are not there, haven't been set yet. There aren't certifications that exist yet. But on the other hand, some businesses feel that they must show some form of certification or gold standard just to keep the business/customers that they currently have, or generate business with certain customers/clients. In fact, **SMEs can be locked out of service contracts**. Recently, some of the large multinationals that the SMEs sell to are now starting to require standards or certifications of some sort. If you don't have these, you don't get in the door - it is becoming a roadblock. Some SMEs have stopped working with the multinational because of the level of requirements and the process to be accepted as a vendor. Similar requirements have also been seen in local government procurement.
- **Potential for misinformation** – Participants discussed their experience of SMEs being provided with misleading information:
    - When SMEs are buying services from suppliers for example, purchasing CCTV equipment or data management solutions, they often ask the supplier "will this make me GDPR compliant?" The advice received may be misleading, such as the experience of one coffee shop with 32 cameras because they were upsold. This situation illustrates that being able to get objective, neutral advice is a challenge. SMEs are desperate to be compliant and are therefore vulnerable to this form of exploitation.
    - Sometimes they don't understand the reports they get from the consultants they do hire and are contacting organisations for support with this. The reports can be factually correct but written in a way that you have to

understand the GDPR before understanding the report. All an SME owner/manager wants is a checklist at the start to say what is needed – so consultant reports can raise confusion. This came up again and again.

  - Combination of where SMEs are going for advice, people trying to sell them things and because no set standards, will often ask 2-3 people for advice, and will get three different answers. This was communicated as 'a real problem'. It leads to confusion and frustration.
  - Huge proliferation of GDPR consultants that leapt out of the woodwork. Created a bandwagon effect. Some are giving wrong advice.
  - IT providers trying to sell SMEs something they just don't need. Isn't the role of the organisations (DPA or sector bodies) to recommend specific suppliers? They can give some advice about standing back and deciding if you really need these technologies or services, using common sense. Don't need to spend 4x on IT equipment and overkill.

- **Need for sector specific interpretation –**SMEs across every sector, e.g. retail, construction etc – they need sector specific advice. Some consultants are starting from the general and trying to interpret for specific sectors. The Chartered Accountants organisation in Ireland did this, trying to interpret for their members. The provision of sector specific guidance can be a challenge for DPAs and any regulator – it will take a long time to roll out specific interpretations of the GDPR for big multinationals and SMEs different sectors. Coupled with SMEs being scared by consultants and consultants' own individual interpretations, there have been 'real problems here'. The absence of sector specific interpretations again offers an opportunity for profiteering.
- **Lack of clarity around the meaning of legal provisions**–There is a degree of fear about what will happen if an individual complainant claims immaterial damages. In Ireland, nothing has come through the circuit courts, at least nothing is going through to a judgement (potentially the matter is settled earlier), so there are no precedents. Judges therefore appear unsure concerning immaterial damages. If somebody threatens – "I'm really upset with what you did with my data, but €2,000 will settle it – what are you going to go? It's cheaper than going to court." Some service providers have treated such situations as a failure of service provision and then offered a

discount to clients on next years' service. There is no book of quantum[3] as there would be in the insurance industry, and we're a long way away from that. What is the appropriate penalty – there's a lot fear about this, and this is driving need for information. Have seen it the other way around – some companies don't see that the fines are going to come. Some expectation that it will plateau – anxiety when GDPR came into force but hasn't happened yet.

6.3. GDPR Positives

There were also some GDPR positives – **space** due to cleaned up lists, **better processes** in place so more **efficiencies**. Some people reported that the GDPR has helped some SMEs deal with certain situations, for example, finding information they have. (Some people do use GDPR as an excuse to limit the use of personal data saying for example, "I'm sorry, I can't do that because of GDPR", but in other ways it has been useful.)

Prior to the GDPR era, several companies didn't have a defined query or complaint process. Default was that this is a SAR, so hand it over to somebody else. But intentions to comply with the GDPR facilitated the development of a good customer complaint/query handling processing. It's actually **improved the relationship** of some SMEs **with their customers**.

Some SMEs created a **whole new business**, such as in payroll context. The GDPR can be a huge benefit to their bottom line with new hires and revenue up. Some SMEs have taken a strategic view of the GDPR, to make it a core part of their business. They started two years before it came out and identified it as a business opportunity. It benefited, for example, certain accountancy firms of a certain size, to have an IT department and data protection expertise in house. All the big four were all over this to offer advice and there are opportunities for smaller firms – the choice is there to build ancillary and add on services to your revenue stream. Lots of companies are doing this. Some include research and development e.g. Enterprise Ireland and others who help business to do R&D have seen a slight stimulus to R&D.

[3] See for example, https://www.piab.ie/eng/forms-guidelines/Book-of-Quantum.pdf

In the data and marketing industry, some SMEs see making privacy a **brand asset** – the way larger organisations have done, e.g. the guardian, the BBC etc are drawing attention to their privacy policy, using video and other ways of communicating the information. SMEs could do this. In the charity sector too, some organisations have made a huge deal about making sure everybody has the right opt-ins; they built campaigns around this. **Personal reputation** is an important asset for SMEs. As they realise that it can be affected by personal data breaches, the importance of compliance with the GDPR increases.

7. Exercise 2: Context mapping – the external environment

The context map exercise has been designed to show external factors, trends and forces at work surrounding an organisation.[4] Providing a systematic view of the external environment that SMEs are acting with provides greater context for their actions and needs around data protection and the GDPR. The aim of the exercise is to gain a holistic view of the external environment and business landscape.[5]The identified factors may not be on the daily mind of SMEs, but they affect SMEs significantly. The aim of using the exercise during the workshop was to connect participants and STAR II partners with the wider landscape within which SMEs function beyond the GDPR.

Figure 3: The 'context map' template on which the 'External Environment' exercise was modelled.[6]

Modelled on Figure 3, we pinned to the wall six large pages as shown in Figure 4 with the following headings:

[4] Ibid., 84. Gray et al. attribute the 'context map' exercise to The Grove Consultants International's Leader's Guide to Accompany the Context Map Graphic Guide (1996–2010).
[5] Gray (n 1), 84-86
[6] Ibid., 85.

- Trends
- Technology factors
- Economic factors
- Political factors
- Customer needs
- Unknowns

The facilitators role is to ask intelligent and thought-provoking questions to stimulate and focus the discussion of participants where necessary. To do so, we drew upon the research conducted in the STAR II project. The aim of the exercise was to portray a context as rich and accurate as possible. Participants were able to populate the categories in any order.

Figure 4: Validation Workshop, Dublin 24 June 2019 - Starting the 'External Environment' exercise

Political factors (essentially Brexit) dominated the early part of the discussion, before the group moved on to discuss technological trends, and the close relationship between technological trends and economic factors.

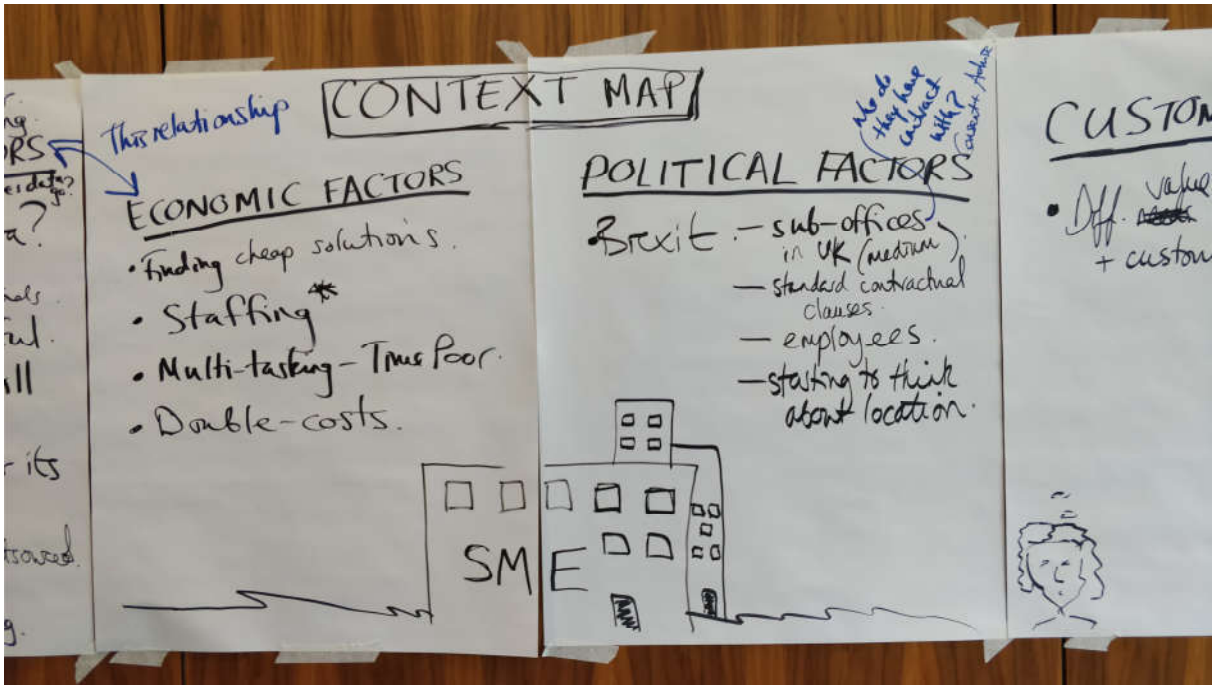

Figure 5: Validation Workshop, Dublin 24 June 2019 – Showing Economic and Political Factors

The discussion had an organic ease involving almost all workshop participants. The issues focused on were the political, technological and economic factors. One overarching trend was the issue of SME understanding of the GDPR, both in terms of what the GDPR means and requires but also then the run-on effect this lack of clarity creates concerning the ability of SMEs to assess appropriate technical and organisational measures for implementation – a feature that is also challenging in the non-GDPR circumstances (see Figure 6). The following narrative describes how the issues were raised by participants:

7.1. Political Factors

- The issue of **Brexit** was particularly salient for Irish SMEs. It created uncertainty and sits in the background of many SMEs minds:
    - Some are taking actions – there have been awareness campaigns about: opening sub-offices in the UK; the implications of selling online; how to access customer data; changing currency, etc.
    - There are some support structures in place to help business adapt to it, but an issue for SMEs remains knowing about these, getting access to and making the most use of them.
    - There are voices saying Brexit is never going to happen, so there's uncertainty there too.
    - The situation of employees post-Brexit was a big issue for SMEs.

Some associations have done specific webinars on data protection and Brexit in an attempt to fill this information gap. Concerning the GDPR, a particular Brexit issue is the transfer of personal data (either staff or customer) between the UK and the EU in the event of no-deal Brexit. In this circumstance, UK will be a third country, outside the EEA, and for transfer of personal data to the UK will need a lawful basis. This was seen as a real challenge for SMEs that operate across the border. SMEs were seen as not being familiar with **standard contractual clauses**, whilst binding corporate rules were seen as very complicated. This was perceived as a harsh situation for SMEs to be in.

One association representative told us that their organisation was one legal enterprise but with offices around the world. Their own GDPR compliance work in relation to international transfers of personal data had not been easy but involved rather a lot of work and challenges to set up, and they were large enough and had resources they could put into it. It was a complicated process to get to this, and so smaller companies will not find this easy. Multinationals formerly based in the UK have set up offices in Ireland and around the EU, not just because of data protection considerations but for many other types of regulation, passporting, movement of goods and services.

We were told that SMEs have agreements in place with service providers, and that many of them have never looked before now into where their data is actually processed. One example was given of a group of companies that processes all of its data “in the cloud” but not in Ireland, none of the individual business have previously ever cared where this data was really being stored. Now they are likely confronted with having to think about this.

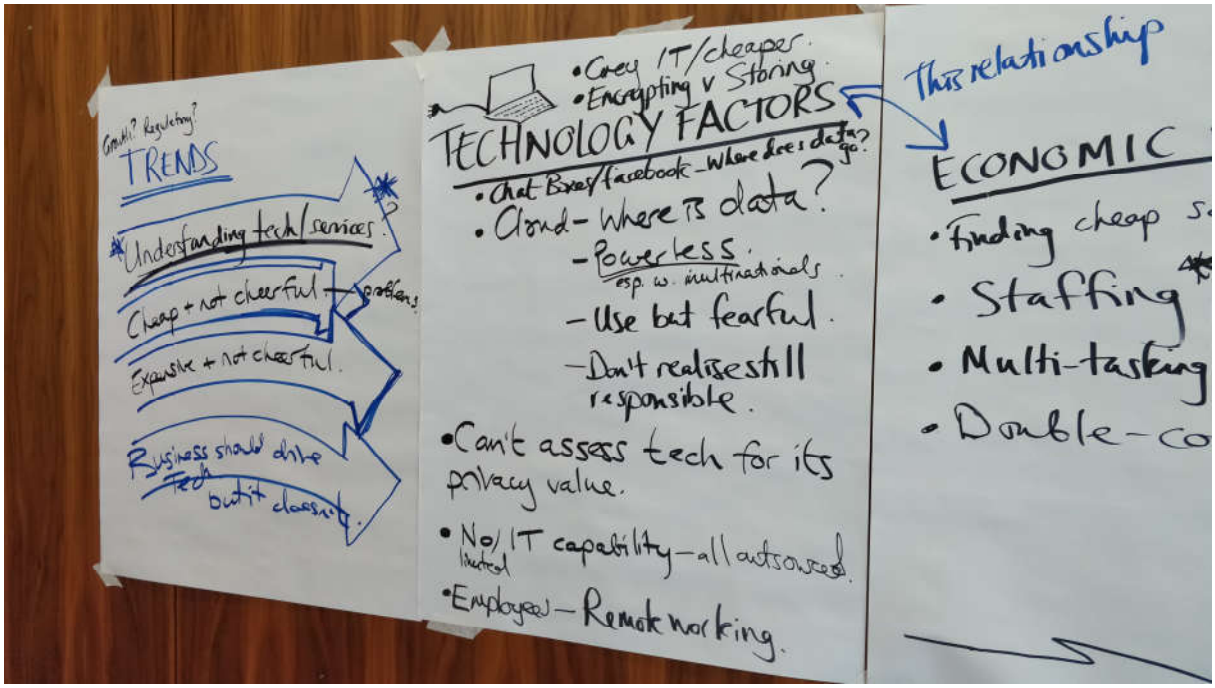

Figure 6: Validation Workshop, Dublin 24 June 2019 – Showing Trends and Technology Factors

7.2. Technological factors

- **Asymmetric negotiating power with larger service providers**–A trend in enterprise IT over the last several years has been moving to the cloud for any type of service. The result of this is that an SME has, most of the time, no idea where your data is. SMEs have little opportunity to talk to the provider and have no power in the negotiations. Companies wish to take advantage of these cloud-based services because they are cheaper. We asked if this would deter SMEs from using these services, and the response was probably not. It was thought SMEs would use the service until it becomes an issue. Some SMEs are communicating that they would rather be non-compliant because it is simply too expensive to move data processing to somewhere else. There are entire SME business models based around Amazon services (for example) because of the essential nature of that provider to their business. In this situation the SME is locked into a standard contract they cannot change and are too small to negotiate.
- **Misunderstanding about responsibility with regard to cloud providers** - some companies have told participants they are GDPR compliant because either Amazon Web Services (AWS) or another services provider is "certified" – the experts have had to say this is a mistake, that Amazon is certified *for themselves,* and that SMEs don't

realise that when they put their business up on the cloud that they're responsible. Ownership transfers to the SME and AWS just has the infrastructure piece. This was seen as hard for SMEs to figure out.

- **Lack of a privacy mindset** - Lack of understanding of the power of personal data and lack of experience in thinking about it, its use, where it is located, what it can do. An example presented was a company that is sold an AI chatbot. The company thinks this is great because it saves times and doesn't cost a staff member to answer question – but the SME hasn't developed a privacy mindset yet – they are not used to asking "what are the privacy implications of this new technology for the business and for customers?".
- **Agile IT** - With IT trends, the traditional model of having IT capability is decreasing or gone. SMEs can go online, use a credit card and then have a service (data storage, CRM, mailing lists, payments etc), keeping no technology in the business. Some SMEs had abandoned all IT knowledge, and all their IT capacity is outsourced – if they have a question, they call the company who provides the service. This creates opportunities, but it also carries risks. The perception was that in the current economy, if an SME does not digitise its business, it will either be closed in a few years, or heavily losing customers. The trends towards outsourcing technological competencies, means that management of SMEs can't make decisions because they do not have somebody with the business' own interests in mind to talk to. Clarity around what is the data for my business is missing. Specifically, technology-based companies are more likely to be ok in this environment.
- **Remote working** -More and more employers are looking at remote working – particular risks of working from home and dealing with personal data, or working outside the EEA, such as data ownership and lack of control. Things can go quite ugly if the employer/employee relationship goes sour. Valuable.
- **Data-focused SMEs –** SMEs are able to do more things with data, some of this is new and innovative and this can bring in risk.
- **Value of data** – service providers holding on to data is a huge risk factor. Maintaining control of digital assets is a challenge, is there a mechanism or procedure in place to retain control. It wasn't key to them because they didn't see the data as being of value. Disjuncture between what data is important to the customer and what is important to the SME.
- **SMEs bootstrapping** – When SMEs are starting up, they are likely to be using any free software they can get access to, including those intended for personal use, free accounts or trial accounts. Even when the company matures, there are likely to still use pockets of these services – e.g. an old Dropbox account somewhere. Because this

service or technology "works" – the company has grown up around it - then it is not seen as an issue, until it causes problems.

- **Knowing how to take security/privacy protection actions** – An example that was provided was the possibility of enabling encryption at rest for personal data stored in the cloud. Whilst some SMEs were confident they were using encryption such as using https and the data was encrypted from client to client, they weren't using the optional feature at rest. When told about it, they will enable it, but options and actions like this are not always clear.

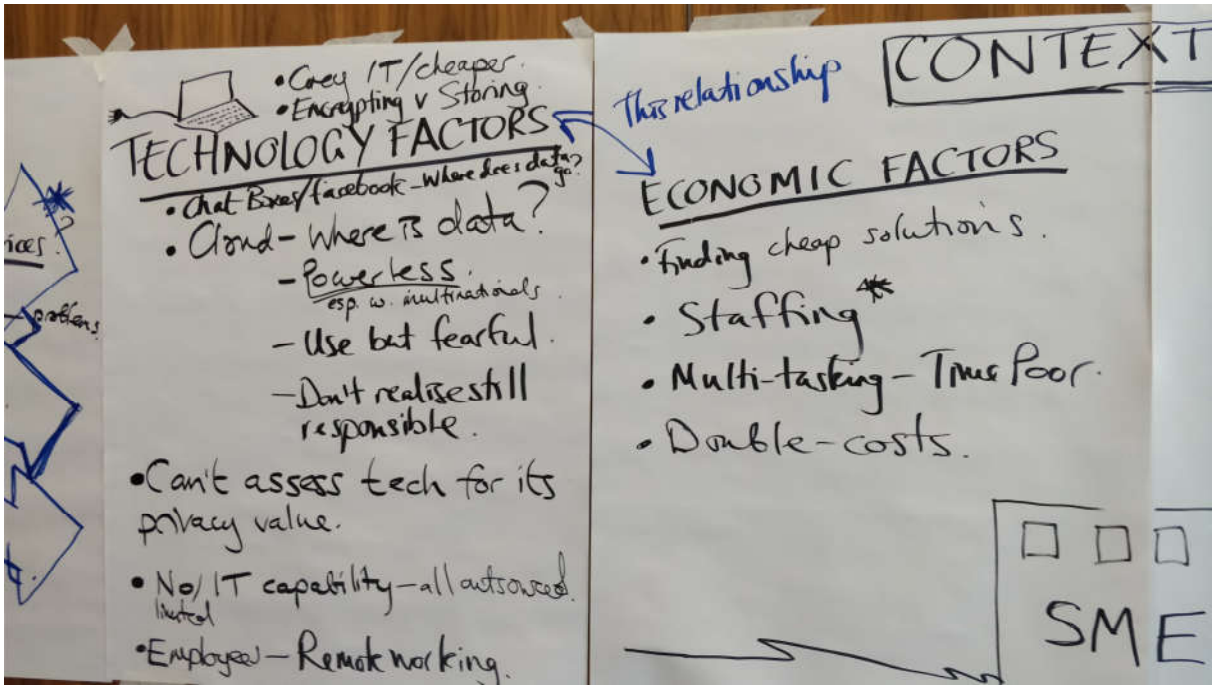

Figure 7: Validation Workshop, Dublin 24 June 2019 – Showing Technology Factors and Economic Factors

7.3. Economic factors

- **Customer driven actions –** SMEs are driven by quick ways to get to and secure a customer and then they worry about data protection afterwards, when they are able. The question for SMEs is how to use new technology, get customers and still comply. They experience a fundamental pressure to "keep the lights on" and stay in business.
- **Staff costs** are vastly increasing, which is a huge economic factor.
- **Limited specialist staff**–SMEs don't have a dedicated team of accountants etc., usually one person doing five to six roles. They just can't allocate more time for doing GDPR related tasks because they don't have it.

- **Customer and client requirements vs inherent business case** - Some companies have experienced clients telling them that if they want to be a data processor for them, then the client wants to see a DPIA of their system. The companies attempted to go and get a DPIA done, without any real idea of what a DPIA *is*. Companies in this situation are asking people to bid to provide this DPIA service, without being able to analyse the responses to that bid. Because it is not defined in their mind what they are trying to buy they often simply go for the cheapest bid. Companies such as these lack basic data protection understanding but will do what is required to meet a customer's requirements - However, because they do not see the value otherwise, they will attempt to pay little for it. SMEs may also ask for DPIAs at the end of a technology development or acquisition process which is not where it is supposed to go and where it cannot really be effective.
- Discussion about the very **strong links between technological factors and economic factors**. SMES are likely to consider technologies and technology services first on price, with strong temptation to go for the cheapest option. This option isn't always enough and can lead to problems further down the line. By this point the SME has already made the expenditure and started using the technology so will find it hard to change and might therefore continue with the sub-optimal service. Simply selecting a more expensive service or technology also doesn't mean better – expensive can sometime be overkill for an SME.
- **Understanding what you need**–Related to the above, knowing how to assess value and find the best fit for their own business is necessary for SMEs. There is a need to identify what an SME really needs, then shop around by talking to multiple providers. In the workshop, an example was given of SMEs saying that they need a particular high-level enterprise solution typically used by large multinationals, because they were told it was "the most compliant" regardless that it did not fit with their business and was very costly. Participants suggested that the business should drive the technology, and not the other way – sometimes SMEs fall down on this, potentially due to being influenced by the vendor or just a general lack of customer knowledge.
- **Planning** – many projects fail due to lack of planning and it is the same with the GDPR.
- **Marketing of technology** – Often technology is marketed in a very lightweight and optimistic way, often with sparse information, focusing on the potential benefits to the user. Finding out what exactly a product of service does can therefore be quite tricky without starting to sign up to it. Finding out about data protection or privacy features is even harder. Fortunately, we're seeing fewer products marketed as "GDPR compliant".

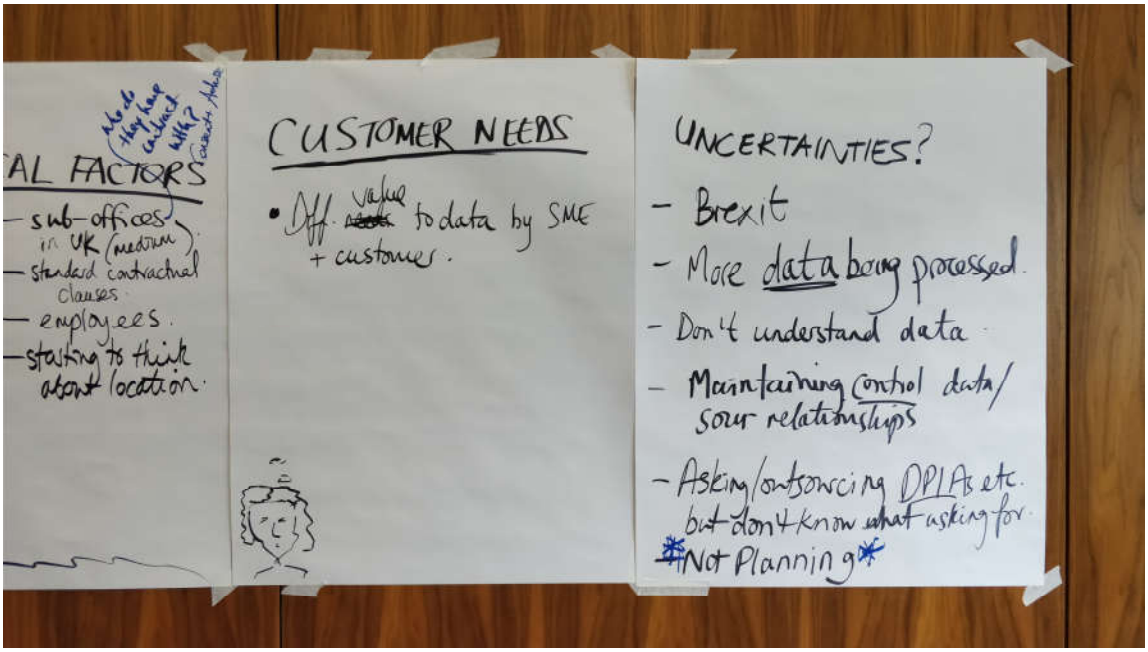

Figure 8: Validation Workshop, Dublin 24 June 2019 – Showing Customer Needs and Uncertainties

The following table depicts the information contained in the populated worksheets from the validation workshop as shown in the photographs contained in Figures 4-8.

Trends	Technology factors	Economic factors	Political factors	Customer Needs	Uncertainties
Understanding technology or services; Cheap and not cheerful; Expensive and not cheerful; Business should drive technology use, but it doesn't'.	Understanding services (e.g. installing a chatbot); Cloud services – where is data?; Powerless to negotiate with multinationals; Use but fear; Don't realise they are still responsible; Can't assess technology for its privacy value; No/Limited IT capability – all outsourced; Remote working and BYOD; Encryption and storage	Finding cheap solutions; Staffing; Multi-tasking (time-poor) Double-costs;	Brexit (Sub-offices in the UK, Standard contractual clauses, employees, starting think about location)	Different values ascribed to data by SME and customers	Brexit; More data being processed; Don't understand data; Maintaining control over data and controller/processors relationships; Outsourcing DPIA etc, but don't know what they're asking for; Not planning

Figure 9: Validation Workshop, Dublin 24 June 2019 – Summary of 'External Environment' exercise worksheets

8. Perspective of the Data Protection Commissioner Ireland

The Irish Data Protection Commission (DPC)'s presentation took the approach of short expression of relevant thoughts by the Commissioner following by an informal conversation with participants.

- The Assistant Commissioner pointed out that the DPC used to provide audits to companies but can no longer provide this service. The function of the DPC is not to 'hold the hand' of the company regarding their data protection needs but rather to focus on identifying systemic issues and addressing these through the provision of guidance.
- The Assistant Commissioner commented that small data protection issues are typically addressed in the domestic courts whereas the bigger issues tend to arrive at the European Court of Justice (ECJ). The ECJ was considered sympathetic to the issue of data protection and data subject-rights.
- In response to one question, the Assistant Commissioner was of the mindset that it would be false to convey a message that the GDPR is simple. The GDPR along with the issue of data protection more widely is not simple.
- It was also considered that alignment across the EU is a challenge. In discussion with participants, it was considered that the DPC's job would be easier if it was able to draft legislation in a similar manner to the French data protection authority (CNIL).
- Furthermore, the DPC conveyed that getting an opinion from the EDPB is not easy because all members must agree. EDPB meetings are not always the place to flesh out issues in depth and have an open discussion because of this need for agreement and time restrictions.
- It was noted that the case-law in other countries regarding data protection remains relevant to the DPC and would be used as a reference point.
- In terms of Brexit, the DPC is advising Irish companies to look beyond the UK for business opportunities. At present, there is an obsession with Brexit among SMEs in Ireland. For data protection however, they need to be aware that local regulations are diverse.

9. Overview of the SME hotline provided by the Hungarian data protection authority (15 March 2019 – 21June 2019)

Nemzeti Adatvédelmi és Információszabadság Hatóság,(NAIH - The National Authority for Data Protection and Freedom of Information)presented a presentation on the operation of the email hotline specifically for SMEs which has been running since 15 March 2019.

NAIH informed the workshop that in Hungary there has been 6/7 fines to date but none have been to SMEs. In Hungary there is also an SME Act which permits the issuing of a warning first from the Authority before a fine. This is currently still the case but there is a feeling that the GDPR will change this status quo.

In terms of the hotline, the Authority advised that its preferred approach is to given written advice so they never give oral advice. They also advocated a short deadline. In terms of the statistics, NAIH informed the workshop that up until 21 June, the hotline had responded to 52 SME queries, with 5 more in progress. In addition, 7 extra queries had been made to the hotline but these were outside the scope of the GDPR (see Figure 10).

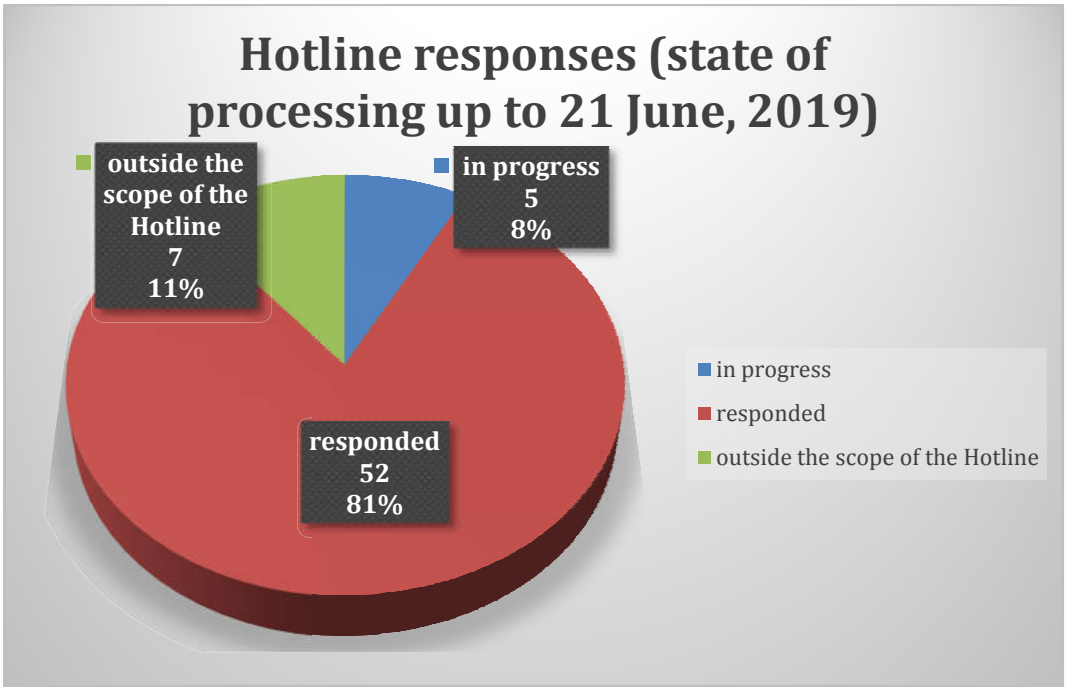

Figure 10: NAIH presentation on hotline responses between 15 March 2019 and 21 June 2019

NAIH also reported on the type of questions received from SMEs during this period. These were broken down into 11 categories as shown in Figure 10. The most frequent type of question (by quite some distance) received by the Hungarian Authority concerned how SMEs should comply with the GDPR. The second largest category shown in Figure 11 is 'Other' which includes a range of individual specific questions. The second and third most frequent specific questions after compliance queries therefore concerned the need for a data protection register and questions concerning employee data.

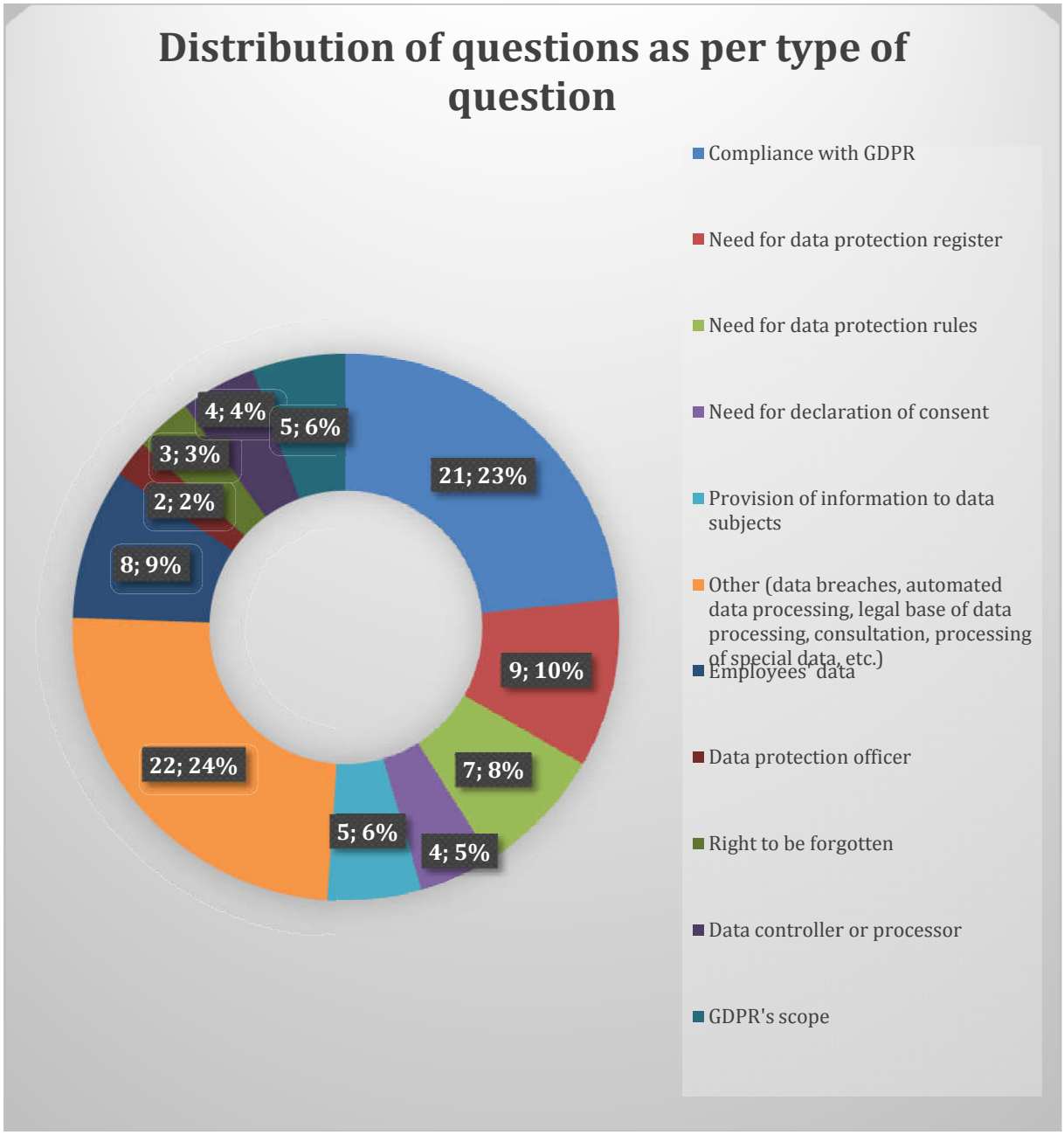

Figure 11: NAIH presentation on the type of question received by the hotline and their frequency between 15 March 2019 and 21 June 2019

NAIH also presented a range of specific examples concerning the type of question asked as well as the written answer provided to the SME. NAIH noted that its aim was to provide concrete guidance but not be overly concrete or specific so as the rationale of the advice can also be understood and therefore assist the SME in re-applying the advice to similar contexts.

10. Additional input to STAR II D2.1 and D2.2

In general, the discussion at the workshop validates the main findings of interviews/questionnaires/surveys from STAR II. Agreement was expressed on many of the issues and challenges we identified as facing SMEs in relation to the GDPR. The workshop also offered the opportunity to deepen our perspectives on some of the issues that emerged in Deliverables D2.1 and D2.2.

One participant suggested that the best way to assist SMEs moving forward was to provide advice on how to **assess risk.** A further participant expressed agreement with this approach. A third party added that it was important to ensure that SMEs are aware that the risk in question is the risk to data subjects and not to the SME. That being said, the **message** needs to come through that the GDPR is **good for businesses too**. In terms of encouraging SMEs to understand the importance of evaluating the risk to data subjects, it was suggested that an effective methodology is to encourage SMEs to **walk in the data subject's shoes**.

In terms of progressing advice on technical and organisation measures, the point was made that **clarity** should be found on whether there is a **desire to ensure technical expertise within the SME.** In this vein it was also pointed out the GDPR is agnostic on technical measures.

Participants strongly agreed that there is a need to ensure that SMEs **do not get hung up on consent** as a legal basis and there was a further warning from the DPC that SMEs should be aware that the **rectification of a problem will cost more than any fine** that may be imposed, e.g. fraud identity services and non-material damage. Reputational damage could also be a factor, but participants noted that this can depend on the nature of the company.

The **culture of the organisation** was also thought to be an important factor, often considered to need development to assist GDPR compliance. Management of SMEs rely on their employees to notify them of a breach but also convey a message of severe repercussions if staff are involved in a breach.

A few participants expressed that they concur with the reasons presented in D2.2 as to why SMEs lose confidence in DPA guidance. It was mentioned that although there is some DPA guidance, it can often just restate that law which should be avoided. **Guidance which does not develop on the law is not always helpful.**

Some participants further identified the issue of certification and standardisation. On the latter point concerning DPAs, ICO/DPC GDPR advice on when to appoint a DPO is for example different. It was expressed that where data protection authorities are awaiting instructions from the EDPB in relation to refining their guidance, this can take time.