**Data Protection Authorities and their awareness-raising duties under the GDPR: *The case for engaging umbrella organisations to disseminate guidance for Small and Medium-size Enterprises***

***Leanne Cochrane[[1]](#footnote-1) & Lina Jasmontaite-Zaniewicz[[2]](#footnote-2)***

**Key words**: awareness raising, compliance, Data Protection Authorities, deterrence, enforcement strategies, General Data Protection Regulation

1. **Introduction**

The effects of the General Data Protection Regulation EU 2016/679 (GDPR) extend beyond changes in business practices concerning personal data handling in the EU and elsewhere. The set of the revised and expanded requirements, rules and obligations of the GDPR also clarified the scope of rights of data subjects and the role of Data Protection Authorities.

A significant part of the GDPR, in fact, is devoted to address the role and functioning of Data Protection Authorities (DPAs). The GDPR in Chapter VI on Independent Supervisory Authorities[[3]](#footnote-3) 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 DPAs responsibilities that could be seen through different lenses, such as that of a leader, an authoriser, a police officer and a complaint-handler.[[4]](#footnote-4)

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’.[[5]](#footnote-5) To attain this objective Article 57 lists 22 tasks for DPAs that range from enforcers, ombudsmen, auditors, consultants to policy advisors, negotiators and educators.[[6]](#footnote-6) While this list leaves no doubt as to whether DPAs responsibilities fall beyond just enforcement, the scope of the role of the educator, as well as the general understanding of DPAs work,[[7]](#footnote-7) to present day has received little attention within the data protection community and therefore with this paper we aim at filling in this knowledge gap. We reflect on the role of DPAs as educators through their engagement in awareness raising campaigns to controllers, processors and the general public. In particular, we focus on DPAs awareness efforts directed to Small and Medium-size Enterprises (SMEs) as in a run for the 25 May 2018 – the date from which onwards the General Data Protection Regulation EU 2016/679 (GDPR) became directly applicable – DPAs and their representatives clearly spelled out that obligations stemming from this legal framework no longer inextricably concern only global technology giants like Facebook and Google, their questionable business practices and other data driven organisation. Any other entities (and individuals) that process personal data in the EU or that process personal data of the individuals based in the EU, with SMEs being no exception, must comply with the obligations stemming from the GDPR.

The enforcement actions undertaken by DPAs leave no doubt about the universal applicability of the GDPR. The most illustrative examples in this regard could be a 15000 EUR fine issued by the Belgian DPA in late 2019 to a SME for not complying with information obligations stemming from the GDPR when using cookies and a 20000 EUR fine issued by CNIL to the translation company after the company has been continuously filming its employees at their workstations and in this way breaching data protection rights of employees.[[8]](#footnote-8)

Recognising that ‘DPAs are multi-taskers’,[[9]](#footnote-9) we deem it necessary to reflect on other DPAs duties concerning monitoring and consistency of the application of the GDPR. To this end, we consider possible approaches DPAs could take in order to satisfy their obligation to raise awareness about data protection and widely disseminated among SMEs. In particular, we question how DPAs could aid SMEs with limited resources with a clear and targeted guidance that would allow to begin their GDPR compliance journey. To answer this question, in this paper we build our argumentation by synthesising our observations extracted during interviews conducted with 18 DPAs, 22 SME association representatives, 52-60 respondents to the online survey and 11 face to face interviews with SME representatives that were conducted within the scope the STAR II research in 2019.[[10]](#footnote-10)

We commence our paper by placing awareness duties within the broader scope of enforcement framework and by reflecting on the legislators’ reasoning behind the explicit inclusion of the awareness raising task among others in the list of Article 57. Before moving on to the part examining state of the art of specific initiatives targeting SMEs developed by DPAs, we introduce reasons for which SMEs should be awarded with a special status (consider legal regimes in other contexts).

Ultimately, we suggest that DPAs should go against the modern efficiency trend of ‘cutting out the middleman’ as a response to the unique pressures on SMEs as “time poor” organisations tend to lack time and resources to communicate their needs to DPAs. Whereas for the DPAs, however, understanding SME needs, it seems imperative to have a direct contact with SME representatives. As this is the case, we suggest that this role could be potentially done by SME Associations.

1. **Enforcement and awareness raising duties of DPAs**

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 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. 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’.[[11]](#footnote-11) 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’.[[12]](#footnote-12)

The legislators with the adoption of the GDPR sought to reduce such diversity and increase harmonisation among DPAs enforcement practices in two ways. First, it aimed at ensuring the ‘complete independence’ of DPAs and the allocation of appropriate funds for them to carry out their duties.[[13]](#footnote-13) While many differences across national DPAs remain, in terms of their size and the rigour of their investigations, they should be now having a better capacity to enforce EU data protection framework to the full extent.[[14]](#footnote-14) Second, by making the awareness raising duty explicit and by providing for a possibility of mega-fines, the legislator has potentially tilted the governance scale which may result in more balanced enforcement strategies of DPAs. Such strategies should represent an equilibrium between hypothetical constructs of ‘deterrence’ and ‘compliance’ (also referred to as ‘advise and persuade’) enforcement strategies that rarely exist in their pure form.[[15]](#footnote-15) Awareness raising duties would fall within the scope of the latter - ‘compliance’ strategies - as they typically seek to prevent harm and damage from occurring; whereas the ‘deterrence’ style enforcement entails issuing fines and sanctions for not complying with the regulation.[[16]](#footnote-16)

This in practice means that it can 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.[[17]](#footnote-17) 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.

**Scoping awareness raising duties to SMEs**

Awareness raising duties of DPAs under the GDPR can be divided into two groups following the rationale embedded in Article 57.1. The first group includes the DPAs obligation to ‘promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing’,[[18]](#footnote-18) whereas the second group requires regulators to engage in activities furthering ‘the awareness of controllers and processors of their obligations’.[[19]](#footnote-19) Recognising that there are great differences in compliance capacity of controllers and processors to whom the GDPR applies, the obligation to raise awareness among them should be considered in light of Recital 132.[[20]](#footnote-20) The Recital notes that such awareness efforts ‘should include specific measures directed at controllers and processors, including micro, small and medium-sized enterprises, as well as natural persons in particular in the educational context’. Requiring DPAs to focus on SMEs as a specific target group of awareness raising campaigns should not come as a surprise because SMEs constitute the backbone of European economy and their roles is continuously reaffirmed by the European Commission reports.[[21]](#footnote-21) At the same time, for these enterprises compliance with the GDPR, poses distinctive challenges – apart from lack of awareness, they rarely can afford professional legal advice.

Interpretation of what awareness raising duties entail is at the discretion of DPAs. The GDPR does not list what actions and activities would be deemed to be part of awareness raising duties. Various examples of activities that could fall within the scope of such duties may include but are not limited to ‘issuing press releases, briefings and commentaries; disseminating reports, studies and publications; […] working with the media; holding public meetings and events; convening conferences and workshops; and creating and contributing to educational materials’.[[22]](#footnote-22) Such activities can be communicated through different mediums.

During the interviews with 18 DPAs we found that mediums through which awareness raising activities are communicated range from traditional tools such as radio, television, print media, video to the use of internet websites, dedicated social media accounts and engagement of influencers.[[23]](#footnote-23) DPAs repeatedly identified the print media, social media and events as the most common general awareness-raising methods, however, several DPAs argued for the use of a multi-method approach to raise awareness, in particular where SMEs are targeted as they tend to be varied in nature and have different needs. During the interviews, it was also noted that participation at events dedicated to SMEs was one the most effective ways to develop and adjust awareness-raising strategies as often presentations and question sessions at such events would facilitate face to face exchanges about the pressing needs and compliance hurdles of SMEs. Furthermore, during interviews we observed that DPAs claim to understand SME needs better if they had personal interactions with SME representatives, for example, via on-site consultation and helpline/helpdesk advisory services or participation at events dedicated to SME needs.

When considering the scope of awareness raising duties of DPAs to SMEs, apart from DPAs positions, views of academics and practitioners provide insightful remarks. In principle, they suggest that as far as DPAs’ role of awareness-raising among SMEs, is concerned, it should be regarded that of leader,[[24]](#footnote-24) ‘where the emphasis is on the expertise, authority, influence of and information from the DPA’.[[25]](#footnote-25)

Professor Christopher Hodges asserts that successful leadership, and consequently success of awareness raising duties of DPAs depend on trusted relationships which entail constructive engagement by DPAs with regulated entities; a term that includes SMEs is of great relevance.[[26]](#footnote-26) In his view, supportive and responsive regulation based on more profound understanding of ‘how and why business seek to comply’ requires reconsidering the strict ‘deterrence’ approach.[[27]](#footnote-27) Hielke Hijmans, the renowned data protection expert, partially shares this view, however, he notes that enforcement of the regulatory framework to be successful, regulators should have sufficient resources and capacity to issue a strong sanction.[[28]](#footnote-28) It could be suggested that the conceptual debate among the two experts, has been in fact resolved by the legislator who opted-in for a more balanced and practical enforcement strategy that would include both deterrence and compliance approaches. Indeed, observations made during interviews with 22 SME associations, in fact, support Hijmans’ point given that information on the imposition of fines was one way how to capture the attention of SMEs. That said, SMEs, however, are not always preoccupied with fines and a perception was identified among some SMEs that DPA hard enforcement, in particular imposition of fines, was instead a concern of much larger companies.

In view of this, in the following sections we explore the role that DPAs play in terms of the GDPR awareness campaigns for SMEs, which, as noted above, often have distinct GDPR related needs and merit special support from public authorities in comparison with bigger players in the market that have compliance teams. To this end, we provide an overview of the state of art and guidance documents that have been issued to ease the GPDR compliance for SMEs and therefore exhibit the DPA role of leader, rather than police officer. While no interviewed DPAs shared the same view on their role of the leader,[[29]](#footnote-29) this is the narrative that will pursue.

1. **The State of the Art of DPAs awareness raising efforts targeting SMEs**
2. **Guidance materials**

Publishing expert advice on data protection issues is an activity that that is pursued by DPAs on a regular basis. DPAs engage in preparation of such advice independently, in cooperation with other DPAs, or within the framework of the European Data Protection Board (EDPB). This acclaimed expert advice contributing to the consistent application of the GDPR can be presented in different forms: guidelines, recommendations, and best practices. While guidance provided by the EDPB ‘on its own initiative, on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices’ receive by far most attention, independent initiatives carry a potential to encourage in a similar vein consistent application of the GDPR - the principle-based regulation, which is technology neutral and which is often are criticised for being too vague and triggering legal uncertainty.

In our survey, we found that around 80% of surveyed SME representatives have accessed guidance provided by DPA at least once in the period of last six months, with a small group of SMEs who were accessing guidance from their DPA on a very regular basis (i.e. more than 10 times in last six months).[[30]](#footnote-30) The reasons for relatively low engagement with guidance materials provided by DPAs varied from the observation that such guidance documents are overly generic and that the organisation must infer from it and make assumptions about how it should be interpreted in their specific situation.[[31]](#footnote-31) Some of the respondents note that such guidance more often raises more questions than it answers and that it arrives too late – after the time the legislation should have been implemented. Furthermore, some SME representatives shared an opinion that DPA guidance is too academic and focused on legal theory to be useful for everyday use, particularly for SMEs. This point was highlighted by on interviewee as ‘the rules and guidance are designed for much bigger companies, where there is one or two specialist people just dealing with the issue. They are not for people doing paperwork late at night at the kitchen table after being in the field all day.’

Despite criticism directed towards general guidance documents, overall about 45% of respondents found the guidance to be somewhat useful. Consequently, it can be suggested that there is place for improvement and that more tailored DPA guidance taking into account distinct needs of SMEs would be appreciated.

1. **Guidance tailored to SMEs**

Based on the information provided by the STAR II DPA interviews as well as desktop research of all EU DPA websites, it appears that slightly less than one third of EU DPAs currently provide GDPR guidance that is specifically tailored for SMEs; upon last review this included the DPAs from Belgium (APD),[[32]](#footnote-32) France (CNIL),[[33]](#footnote-33) Ireland (DPC),[[34]](#footnote-34) Lithuania (VDAI),[[35]](#footnote-35) Slovenia (IP),[[36]](#footnote-36) Spain (AEPD),[[37]](#footnote-37) Sweden (Datainspektionen)[[38]](#footnote-38) and the UK (ICO).[[39]](#footnote-39) Some of these DPAs further distinguish guidance for micro-businesses.[[40]](#footnote-40)

The guidance provided through the DPA websites and takes the form of either a downloadable document, a section of the DPA website or indeed a separate dedicated website. The approach taken in the SME specific guidance is usually holistic in terms of the issues covered, often presented in the same order as an SME might logically need to commence addressing data protection within their organisation. The issues typically include, in various presentation styles: key concepts of the GDPR (e.g. what is (not) personal data and the difference between personal data and special categories or the so called sensitive data), principles (e.g. accuracy, data minimisation, limited retention); data security obligations concerning technical and organisational set up of the processing; obligations concerning data subject rights; and the appointment of a Data Protection Office (DPO), among others. These issues were often usefully identified to SMEs by the asking of positive questions or activity-based steps rather than approaching the issue in terms of the GDPR obligations.

a) Self-assessments

Two illustrative examples[[41]](#footnote-41) in this regard of guidance documents addressing SMEs include ‘GDPR Guide’ of the Datainspektionen, which asks businesses the following nine “quick” questions[[42]](#footnote-42) and that of the ICO which sets out eight questions for small businesses and sole traders so they can conduct an initial self-assessment before immersing themselves further in the numerous guidance pages.[[43]](#footnote-43) It can be noted , that the Swedish DPA questions are more applied than that of the UK authority, although ‘more information’ is readily available beside each ICO question with applied examples. Both sets of questions in the order they appear are in the tables below:

|  |  |
| --- | --- |
|  | **Datainspektionen** |
| 1 | Do you have a list of what types of personal information is in your company and how you use this information?  |
| 2 | Do you have a customer register? |
| 3 | Are you sending out newsletters or other marketing to your customers?  |
| 4 | Do you have any kind of booking system where customers can book time with you? |
| 5 | Do you have a register of your suppliers? |
| 6 | Do you have employees and save data in a payroll system? |
| 7 | Do you have contact information and maybe a photo of some of your employees on your web? |
| 8 | Have you decided how long information about your customers, suppliers and employees should be stored? |
| 9 | Do you protect the information about, for example, customers, suppliers and employees so that unauthorised persons cannot access them? |

|  |  |
| --- | --- |
|  | **ICO** |
| 1 | Do you have a record of what personal data you hold? Do you know what you use it for? |
| 2 | Do people know you have their personal data and understand how you use it? |
| 3 | Do you only collect the personal data you need? |
| 4 | Do you only keep personal data for as long as it is needed? |
| 5 | Do you keep personal data accurate and up to date? |
| 6 | Do you keep personal data secure? |
| 7 | Do you have a way for people to exercise their rights regarding the personal data you hold about them? |
| 8 | Do you and your staff (if you have any) know your data protection responsibilities? |

b) Templates

In terms of tools and templates however, the SME specific guidance was variable. The ICO provides a *privacy notice* template easily accessible from the SME section of its website,[[44]](#footnote-44) VDAI provides a link in its guidance to a sample *data protection impact assessment form*,[[45]](#footnote-45) and the IP includes templates of the: *Notice to individual of processing activities* (Articles 13 and 14 GDPR); *Record of Processing Activities* (versions for both Controllers and Processers) under Article 30 GDPR; *Notification of Breach* (Article 33 GDPR);and, *Appointment of DPO*.[[46]](#footnote-46)

An especially notable tool is *Facilita* (in Spanish) provided by the AEPD. This tool goes to the length of generating the minimum documents necessary for GDPR compliance for businesses or persons that process personal data where there is a low risk to the rights and freedoms of data subjects. These documents include everything from information clauses, information signs such as for video surveillance, register of processing activities and contracts for third party processors, and are generated already populated with the company information provided.[[47]](#footnote-47) The documents also include an information annex outlining data subject rights and the minimum organisational and technical measures that should be implemented, including relevant links such as to the National Institute for Cyber Security. Before using the tool to generate the tailored documents, *Facilita* first takes businesses through a series of questions to confirm that the organisation is not engaged in sensitive data or higher risk processing activities.

1. **Hotline Advice Services**

In addition to guidance materials prepared independently or in cooperation with others that are made available through websites of national data protection authorities, most of the DPAs have set up hotline advice services. Such services, while developed taking into account capacity and resources of national DPAs, contribute to the overall awareness raising effort concerning the GDPR compliance.

As with the GDPR guidance materials, most of the interviewed DPAs responded that they did not consult with other DPAs when establishing their respective hotline/helpdesks. Similar references were made to cooperation at EU level and awareness of other services but only a small number stating directly that they consulted other DPAs before setting up the hotline/helpdesk.

All interviewed DPAs had a public facing helpline or helpdesk service which SMEs could use to contact the DPA. For all DPAs, a telephone service was in operation. Just under half of the interviewees/respondents also referred to an additional email service which for some could then also lead to an in-person consultation depending on the specific issue raised. No DPAs referred to an email service without the existence of an accompanying telephone service. Importantly, however, one DPA did not frame their service as a helpline or helpdesk but rather informed the project that they answer queries through their general contact details.[[48]](#footnote-48) This DPA emphasised that they did not provide legal advice, nor even specific advice but rather a response to the general question. This was considered important so as not to limit the SME’s individualised solution or give the impression that there was only one available solution.

Although the overwhelming majority of these services were also accessible to the general public, data controllers, and SMEs on an equal basis, a few interviewees/respondents suggested that SMEs account for a large proportion of these calls and that it is a key way they have become familiar with the issues of concern to SMEs. The clear lack of an SME specific hotline or helpdesk however does not appear to equate with a perceived need for one.

Furthermore, DPAs even hypothetically do not consider a possibility of having an SME focused advice service if provided with additional resources. DPA representatives in general believe that such effort from their side is not necessary as there exists demand for the specialised advice service and that the limiting factors on its success are capacity and expertise rather than awareness or indeed the need for an SME specific advice.

Interestingly, the DPA perception of success of hotline services differed greatly from the experience shared by SMEs representatives. They claimed that DPAs are hard to reach and that in response to their queries they do not receive concrete and timely answers. The other remark put forward was that knowledge level of the DPA staff responding to queries tends to vary and therefore there are situations when conflicting guidance is provided in response to the same matter (either internally contradictory or a national DPA contradicting guidance from the EPBD, for example).

In the following section we consider how the position of DPA representatives could be reconciled with disappointments over DPA awareness raising efforts that we learned from SME representatives. We build this section on the findings of the interviews with DPAs and SME representatives, which seem to indicate that communication between DPAs and SMEs has not followed a smooth road. For DPAs reaching out to SMEs concerned with the GDPR compliance has not always been easy because of numerous reasons, such as the DPAs are not aware about existence of SMEs across different sectors or they are overwhelmed with the enforcement or they lack resources for such awareness campaigns. Yet it seems that without having any direct contact with SMEs, it is difficult for DPAs to identify distinctive needs of controllers and processors representing these enterprises. Consequently, it means that isolated DPAs efforts to overcome SMEs disappointment over general guidance issued by DPAs and the functioning of hotlines may have little impact.

1. **Outlook for raising awareness through nourishing relations between DPAs and SME Associations**

While it is evident that DPAs should seek for an alternative way to satisfy their obligation to raise awareness about data protection and widely disseminated among SMEs, the question remains open: how DPAs could aid SMEs with limited resources with a clear and targeted guidance that would allow to begin their GDPR compliance journey.

The answer to this question to some extent became apparent during the STAR II interviews with SME Associations. There is a good reason to believe they could play a crucial role in assisting DPAs to maximise awareness of these resources and indeed other DPA awareness raising efforts. Although SME Associations do not form a significant part of the SME architecture in all EU Member States (e.g. Hungary or Lithuanian), in others, such as Denmark or the UK, SME Associations form an integral part of the SME landscape leading to the conclusion concerning their potential to assist DPAs in fulfilling their awareness raising obligations.

In terms of the benefit SME Associations can bring, the point is two-fold. First, the activities in which SME Associations have a stake overlap with the obligations placed on DPAs to raise awareness about the GDPR among SMEs. Second, SME Associations have open communication channels with SMEs, which can be exploited to raise awareness of the GDPR. We further advance these arguments in the following sub-sections.

1. **Overlapping interests: Awareness raising is a shared priority for SME Associations and DPAs**

Findings of interviews allow to conclude that interests of SME Associations overlap with interests and objectives pursued by DPAs: they both seek to raise awareness facilitating the GDPR compliance. A number of interviewed SME Associations reported their own proactive involvement with DPAs and SMEs in terms of gauging their awareness of the GDPR, albeit that this activity was mostly focused on the period just before the GDPR came into force. It was expressed by one EU wide Association that the Nordic countries are on the whole (SMEs and others) most aware of the GDPR. Indeed, the STAR II research identified a number of engaged SME Associations from Norway offering proactive assistance and advice to their members, as well as reporting positive DPA relationships.

STAR II interviews leave no doubt as to the profound role some SME Associations play in providing guidance to SMEs on the GDPR. In particular, the online survey with SMEs reported around two thirds of respondent SMEs having looked to sources other than their DPA for GDPR guidance. It appears that while during interviews SMEs expressed a high degree of scepticism over GDPR consultancy services, guidance provided by trade or sectoral associations and chambers of commerce were among the most consulted.[[49]](#footnote-49)

The perception of these guidelines and their usefulness was not explored within the scope of STAR II questions because originally more narrow focus was placed on the relationship between DPAs and SMEs directly, before the potential for the role of SME Associations emerged. The depth of the data on SME engagement with SME Associations therefore comes from the in-depth interviews STAR II researchers undertook with 22 SME Associations.

Awareness raising for SME Associations extends beyond communication to their members. It is well-documented that SME Association representatives are also the ones informing the regulators and the legislator (e.g. European Commission) about daily challenges accompanying the GDPR compliance for small businesses. In this regard, the work by SMEunited, representing national cross-sectoral Craft and SME federations, stands out. For example, it actively participates in the multi-stakeholder expert group to support the application of the GDPR. In one of the last meeting of this group, SMEunited pointed out compliance challenges for SMEs, which range from the application of specific provisions (i.e. the use of a legitimate interest ground) to general governance matters.[[50]](#footnote-50) The voice of SME Association representing a large number of SMEs when conveying their distinctive needs arguably carries more weight than a voice of a sole SME representative.

Having this background in mind it should be added that the awareness raising for some SME Associations is the priority stemming from the fee-paying dimension of their services, which includes provision of relevant information, such as the one concerning advice on the GDPR. As fee operating entities, SME Associations have a vested interest in ensuring that the membership of their SMEs is worthwhile. Part of this vested interest is not just about awareness raising but is furthermore also concerned with a level of understanding, such that SMEs might emerge as satisfied customers of their Association returning to pay their fee for a further year. For SME Associations operating in this way, the incentive might be considered just as powerful as the GDPR awareness raising obligations on DPAs.

1. **Communication channels**

In addition, SME Associations tend to have open channels of communication with their members. One UK based sectoral association noted:

‘We have lots of communication channels for disseminating this research/guidance for SMEs. We have a quarterly letter and magazine, which we included the Guide to the GDPR in. We are very active on social media; we had a countdown to the GDPR on that. We also spoke at a lot of conferences [and] meetings.’[[51]](#footnote-51)

Indeed, one relatively common channel mentioned by SME Associations was the member mailing list. Albeit not directly asked, there was no mention of a corresponding effort to collect SME contact details for dissemination of guidance materials by DPAs.

Further distinction could be made between communication types based on whether SME Associations function on national or European level. It seems to be beneficial to retain a focus for SMEs on member state organisations (as opposed to multi-national or EU wide organisations), even though guidance at EU level would be welcome too. In general, there seems to be a preference for DPA advice services to be offered at the member state level and in the national language because as one SME Association told us, ‘SMEs default to the national context always’. While SME Associations appeared more at home with transnational advice services than SMEs, they too emphasised the importance of communicating in the context of the national language and laws when addressing SMEs. This narrative in the context of SMEs is important because it provides something of a contrast to the intention behind the GDPR that it would be a harmonised tool for EU data protection applicable across all member states. In this regard, some SME Associations expressed the view that the SME concern was based on more than just cultural unfamiliarity or linguistic prowess, but the reality that member state data protection laws were not always harmonious. Perhaps for a mixture of these reasons, one SME Association expressed that SMEs might view advice services outside the state with suspicion, such as this:

‘Well, I would ask myself why is it not being offered by my own member state? I would ask also is it free? I don't see what it wouldn't or shouldn’t be offered nationally.’

It is therefore not surprising that some of the DPAs have started collaborating more closely and proactively with certain SME associations. For example, the Belgian DPA has recently launched an awareness raising project with associations representing a fintech industry in Belgium.[[52]](#footnote-52) The Italian DPA has been closely collaborating with SME associations in Italy and Bulgaria within the scope of SMEDATA,[[53]](#footnote-53) whereas the European Small Business Alliance, a non-party political European group representing small business entrepreneurs and the self-employed, is a partner to the SMOOTH project.[[54]](#footnote-54) The DPA in Hungary has recently interacted with the Somogy Chamber of Commerce and Industry and the Budapest Chamber of Commerce and Industry.[[55]](#footnote-55) It must be recognised that nearly in all cases interaction between DPAs and SME associations have resulted from project work that is partially funded by the Rights, Equality and Citizenship Programme of the European Union. This seem to suggest that for the trust narrative to emerge and develop between SMEs and DPAs there is a need for an external stimulus and encouragement.

1. **Concluding remarks**

DPAs have a well-established record of various activities to raising awareness, ranging from publishing press releases, educational materials and commentaries to holding public meetings and events. Such activities have allowed DPAs to shape application of law practices by controllers, processors. Indeed, only well-informed and aware data controllers and processors can comply with obligations stemming from the EU data protection framework. The weight of awareness raising as a task has recently changed as with the adoption of the GDPR, where awareness raising activities were formalised into a duty under Article 57. The legislator, however, has not provided any cues as to how such duty could be implemented or facilitated in practice. At the same time, it is clear that awareness raising constitutes a profound part of the compliance focused enforcement, and similarly to the deterrence approach, it requires regulators to consider strategies that could further advance their efforts.

In our contribution we argue that knowledge gathered during the interviews of STARII project on the awareness raising practices of DPAs through the lens of SMEs, offers valuable insights in this regard.[[56]](#footnote-56) We found that while some of the DPAs have issued SME focused guidelines, in general, SMEs and SME associations deem the currently available guidance to be generic, theoretical and they assert that it does not meet their needs. They argue for more practical guidance that would be tailored to their needs, preferably including more templates that could be easy to adapt to specific context of an enterprise. The criticism also extends to hotline services provide by DPAs, even if DPAs themselves are satisfied with the way their hotline services perform. SMEs and SME associations reported such services to provide vague and untimely answers. What this discrepancy seems to indicate is that DPAs when evaluating their performance take into account limitations set by the available financial and human resources, whereas SMEs seek for practical, yet not necessary legally binding compliance advice.

Another important finding is that DPAs claim that for them the direct interaction with SMEs is one of the keyways to learn their data protection needs and compliance challenges. The element of direct interaction is consistent with the previous research that indicates that for DPAs an external input is crucial for developing expertise in a certain area.[[57]](#footnote-57) Following this line of reasoning, in this contribution we consider alternative approaches to reach out and learn concerns of SMEs – the key stakeholders’ that are at the core of the EU economy. Recognising limitations of communication with representatives of single enterprises, we put forward a recommendation for DPAs to work more closely with SME associations. This collaboration provides an opportunity to learn distinctive needs of SMEs across a range of sectors in fast and cost-efficient way.

By taking into account findings of interviews with DPAs and SME associations, we consider possible advantages of a closer collaboration among the two. We suggest that there are good reasons to believe that engaging umbrella organisations to disseminate guidance for Small and Medium-size Enterprises could be benefit and assist DPAs in their role of a leader. This collaboration in practice could help to develop a stronger trust-based relationship between the regulators and SME. Some steps have been taken in this regard, and we are able to point out instances where SME associations and DPAs interact, albeit such interaction has been partially encouraged by external funding.

At the same time, we believe this collaboration could be furthered and mutually beneficial. For DPAs it could facilitate strategic enforcement decisions and optimise financial and human resources. Despite expressions by some DPA representatives that funding provision for them had been improved in their member state, DPAs like many public sector organisations, remain resource limited and sometimes such as in the case where interviews could not be facilitated, heavily resource restricted. For SME associations, such collaboration would provide a possibility for wider and more nuanced SMEs interest representation of their members.

**Annex**

**Article 57**

**Tasks**

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

1. monitor and enforce the application of this Regulation;
2. 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;
3. 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;
4. promote the awareness of controllers and processors of their obligations under this Regulation;
5. 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;
6. 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;
7. 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;
8. conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;
9. 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;
10. adopt standard contractual clauses referred to in Article 28(8) and in point (d) of Article 46(2);
11. establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4);
12. give advice on the processing operations referred to in Article 36(2);
13. 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);
14. 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);
15. where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7);
16. 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;
17. conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;
18. authorise contractual clauses and provisions referred to in Article 46(3);
19. approve binding corporate rules pursuant to Article 47;
20. contribute to the activities of the Board;
21. keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and
22. fulfil any other tasks related to the protection of personal data.

2. Each supervisory authority shall facilitate the submission of complaints referred to in point (f) of paragraph 1 by measures such as a complaint submission form which can also be completed electronically, without excluding other means of communication.

3. The performance of the tasks of each supervisory authority shall be free of charge for the data subject and, where applicable, for the data protection officer.

4. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may charge a reasonable fee based on administrative costs, or refuse to act on the request. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

1. Senior Research Analyst within the Policy, Ethics and Emerging Technologies (POET) team at Trilateral; leanne.cochrane@trilateralresearch.com. [↑](#footnote-ref-1)
2. Legal researcher at the Faculty of Law and Criminology of the Vrije Universiteit Brussel (VUB), the Research Group Law, Science, Technology and Society (LSTS), lina.jasmontaite@vub.be. [↑](#footnote-ref-2)
3. When referring to Independent Supervisory Authorities we use the following terms: Data Protection Authorities, DPAs and regulators. [↑](#footnote-ref-3)
4. Centre for Information Policy Leadership, ‘Regulating for Results Strategies and Priorities for Leadership and Engagement: A Discussion Paper’ (2017) p. 7-8. [↑](#footnote-ref-4)
5. 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. [↑](#footnote-ref-5)
6. 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. [↑](#footnote-ref-6)
7. This observation is shared by Raab, Charles D. and Szekely, Ivan, Data Protection Authorities and Information Technology (May 5, 2017). Computer Law and Security Review 33 (2017) p. 421–433. [↑](#footnote-ref-7)
8. For more information on the Belgian DPA decision see here: <https://www.insideprivacy.com/data-privacy/belgian-supervisory-authority-imposes-website-cookie-fine/>, for more information on the CNIL decision see here: <https://privacylawblog.fieldfisher.com/2019/videosurveillance-cnil-issues-fine-of-20-000-euros-against-a-small-company-in-france>. [↑](#footnote-ref-8)
9. Raab, Charles D. and Szekely, Ivan, Data Protection Authorities and Information Technology (May 5, 2017). Computer Law and Security Review 33 (2017) p. 421–433. [↑](#footnote-ref-9)
10. STARII, Deliverable D2.1 Report on DPA efforts to raise awareness among SMEs on the GDPR (Version 1.1; 2019); STARII, Deliverable D2.2 Report on the SME experience of the GDPR (2019). [↑](#footnote-ref-10)
11. Robert Baldwin and Martin Cave, *Understanding Regulation: Theory, Strategy, and Practice* (OUP 1999), p. 101. [↑](#footnote-ref-11)
12. 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. [↑](#footnote-ref-12)
13. Ibid. [↑](#footnote-ref-13)
14. European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law* (2018) 193–194 <https://fra.europa.eu/sites/default/files/fra\_uploads/fra-coe-edps-2018-handbook-data-protection\_en.pdf>. [↑](#footnote-ref-14)
15. Neil Gunningham, ‘Enforcement and Compliance Strategies’ in Oxford Handbook of Regulation, edited by Robert Baldwin, Martin Cave, and Martin Lodge (OUP 2010), p. 122. [↑](#footnote-ref-15)
16. For more on enforcement strategies see: Robert Baldwin and Martin Cave, *Understanding Regulation: Theory, Strategy, and Practice* (OUP 1999), p. 96-117 and Neil Gunningham, ‘Enforcement and Compliance Strategies’, p. 120-145. [↑](#footnote-ref-16)
17. 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. [↑](#footnote-ref-17)
18. 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) 2016, Article 57.1 (b) [↑](#footnote-ref-18)
19. Ibid, Article 57.1 (d) [↑](#footnote-ref-19)
20. Note, recitals are not legally binding, yet they are used to interpret the binding provisions. [↑](#footnote-ref-20)
21. For example, Annual Report on European SMEs 2018/2019: Research & Development and Innovation also Infographic: Presents the latest data on European SMEs based on the annual report (2019). Additionally, see: Annual Report on European SMEs 2014/2015: SMEs start hiring again; Annual Report on European SMEs 2013/2014: Partial and Fragile Recovery. [↑](#footnote-ref-21)
22. SDG Accountability Handbook, Raising Awareness through Public Outreach Campaigns What is it? (2018) [↑](#footnote-ref-22)
23. STARII D2.1, p. 44. [↑](#footnote-ref-23)
24. The role of a leader in this context concerns education, awareness, feedback, guidance and assistance to concerned parties and should not be confused with the notion of a lead authority. [↑](#footnote-ref-24)
25. Centre for Information Policy Leadership, ‘Regulating for Results Strategies and Priorities for Leadership and Engagement: A Discussion Paper’ (2017) p. 29 <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl\_final\_draft\_regulating\_for\_results\_-\_strategies\_and\_priorities\_for\_leadership\_and\_engagement.pdf>. [↑](#footnote-ref-25)
26. Christopher Hodges, ‘Delivering Data Protection: Trust and Ethical Culture’ (2018) 4 European Data Protection Law Review 65. [↑](#footnote-ref-26)
27. Ibid, 71. [↑](#footnote-ref-27)
28. Hielke Hijmans, ‘How to Enforce the GDPR in a Strategic, Consistent and Ethical Manner?’ (2018) 4 European Data Protection Law Review 80, 82. [↑](#footnote-ref-28)
29. D2.1, p. 43, List Interviewed DPAs include [↑](#footnote-ref-29)
30. STARII, D.2.2, p. 25. [↑](#footnote-ref-30)
31. STARII, D.2.2, p. 25. [↑](#footnote-ref-31)
32. The Belgian Data Protection Authority operates in a number of languages. *L'Autorité de protection des données* (APD) is the French abbreviation simply translates as Data Protection Authority in English. CPVP, ‘RGPD Vade-Mecum Pour Les PME (January)’ (2018) <https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/PME\_FR\_0.pdf>. [↑](#footnote-ref-32)
33. *La Commission Nationale de l'Informatique et des Libertés* (CNIL) meaning the National Commission of Information Technology and Freedoms. See, Bpifrance, ‘Guide Pratique de Sensibiliation Au RGPD (April)’ (CNIL 2018) <https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-rgpd\_guide-tpe-pme.pdf>. [↑](#footnote-ref-33)
34. *An Coimisiúm um Chosaint Sonrai/* The Data Protection Commission (DPC). See, ‘Guidance Note: GDPR Guidance for SMEs (July)’ (Data Protection Commission 2019) <https://www.dataprotection.ie/sites/default/files/uploads/2019-07/190708 Guidance for SMEs.pdf>. [↑](#footnote-ref-34)
35. *Valstybinė duomenų apsaugos inspekcija (VDAI)* meaning State Data Protection Inspectorate. See, VDAI, ‘Rekomendacija Smulkiajam Ir Vidutiniam Verslui Dėl Bendrojo Duomenų Apsaugos Reglamento Taikymo (September)’ (2018) <https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomend\_SVV\_BDAR\_2018.pdf>. [↑](#footnote-ref-35)
36. Informacijski pooblaščenec (IP) meaning the Information Commissioner. See, ‘Varstvo Osebnih Podatkov’ (*Upravljavec*, 2018) <https://upravljavec.si> accessed 3 October 2019. [↑](#footnote-ref-36)
37. Agencia Española de Protección de Datos (AEPD) meaning Spanish Data Protection Agency. See, ‘Facilita RGPD’ (*AEPD*) <https://www.aepd.es/herramientas/facilita.html> accessed 3 October 2019. [↑](#footnote-ref-37)
38. Meaning Data Inspection Board. See, ‘GDPR - Nya Dataskyddsregler’ (*Verksamt*, 2018) <https://www.verksamt.se/driva/gdpr-dataskyddsregler> accessed 3 October 2019. [↑](#footnote-ref-38)
39. Information Commissioner’s Office (ICO). See, ‘Micro, Small and Medium Organisations’ (*ICO*) <https://ico.org.uk/for-organisations/in-your-sector/business/> accessed 3 October 2019. [↑](#footnote-ref-39)
40. ‘Guidance Note: Data Security Guidance for Microenterprises (July)’ (Data Protection Commission 2019) <https://www.dataprotection.ie/sites/default/files/uploads/2019-07/190709 Data Security Guidance for Micro Enterprises.pdf>; ‘How Well Do You Comply with Data Protection Law: An Assessment for Small Business Owners and Sole Traders’ (*ICO*) <https://ico.org.uk/for-organisations/data-protection-self-assessment/assessment-for-small-business-owners-and-sole-traders/> accessed 4 October 2019. [↑](#footnote-ref-40)
41. Other DPAs also take a similar approach. [↑](#footnote-ref-41)
42. ‘GDPR-Guiden’ (*Verksamt*, 2018) <https://www.verksamt.se/driva/gdpr-dataskyddsregler/gdpr-guiden> accessed 3 October 2019. [↑](#footnote-ref-42)
43. ‘How Well Do You Comply with Data Protection Law: An Assessment for Small Business Owners and Sole Traders’ (n 13). [↑](#footnote-ref-43)
44. See, <https://ico.org.uk/for-organisations/in-your-sector/business/> accessed 7 October 2019. [↑](#footnote-ref-44)
45. Link provided in the *Rekomendacija* leads here: ‘Pavyzdinė Poveikio Duomenų Apsaugai Atlikimo Forma (2018 M.)’ (*VDAI*, 2018) <https://www.ada.lt/go.php/lit/Pavyzdine-poveikio-duomenu-apsaugai-atlikimo-forma-2018-m> accessed 4 October 2019. [↑](#footnote-ref-45)
46. ‘Obrazci’ (*Upravljavec*, 2018) <https://upravljavec.si/obrazci/> accessed 3 October 2019. [↑](#footnote-ref-46)
47. ‘Facilita RGPD’ (n 10). [↑](#footnote-ref-47)
48. This may explain why such service is not available on all DPA websites. [↑](#footnote-ref-48)
49. Then followed, guidance provide by EU bodies (Article 29 working party guidance, the European Commission or the EDPB) / a general online search; conference and seminars / Foreign data protection authorities’ websites; training providers / Law firms / Auditors / IAP; peers and networks / books/ Peer reviewed journals / and finally, national government. [↑](#footnote-ref-49)
50. For example, see a brief note on one of such meetings: <https://smeunited.eu/news/gdpr-application-discussed-mandatory-monitoring-body-not-fit-for-smes>. [↑](#footnote-ref-50)
51. An excerpt is taken from the interview with an approval of the interviewee. [↑](#footnote-ref-51)
52. Based on the interview with a DPA representative. [↑](#footnote-ref-52)
53. For more information about the project see: <https://smedata.eu/>. [↑](#footnote-ref-53)
54. For more information about the project see: <https://smoothplatform.eu/>. [↑](#footnote-ref-54)
55. STAR II, D4.1 Guidance on hotlines. [↑](#footnote-ref-55)
56. This being said, given the limitations our data sample based on interviews and the survey, we believe our findings should not be overinterpreted. [↑](#footnote-ref-56)
57. A similar argument has been developed in terms of technology take-up by DPAs in Raab, Charles D. and Szekely, Ivan, Data Protection Authorities and Information Technology (May 5, 2017). Computer Law and Security Review 33 (2017) p. 421–433. [↑](#footnote-ref-57)