# 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, Lina Jasmontaite-Zaniewicz and David Barnard-Wills**

*In this paper we explore EU data protection authorities' (DPAs) role as leaders and educators, particularly in relation to awareness-raising efforts with Small and Medium-sized Enterprises (SMEs). The GDPR made awareness raising duties of DPAs explicit whilst SMEs face challenges complying with data protection law. We posit that DPAS should make better strategic use of collaboration with SME Associations as intermediaries to better access and understand the needs of SMEs. This collaboration could facilitate dissemination of guidance and information addressed to SMEs. It could also help to overcome concerns expressed by SME representatives about the existing guidance provided by DPAs as being overly generic, focused on legal theory, and in some states arriving too late for implementation. We suggest that by working together SME Associations and DPAs could increase their own working efficiency as well as the one of SMEs. We build our arguments on the findings of an online survey of 52-60 SMEs representatives and semi-structured qualitative interviews with 18 DPAs, 22 SME Association representatives and 11 SME representatives.*

*Keywords: Awareness Raising, Compliance, Data Protection Authorities, Deterrence, Enforcement Strategies, General Data Protection Regulation*

## I. 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 both the scope of rights of data subjects and the role of Data Protection Authorities (DPAs) after 'the role of Data Protection Authorities'.

A significant part of the GDPR, in fact, is devoted to addressing the role and functioning of DPAs. The GDPR in Chapter VI on Independent Supervisory Authorities[1] takes into account the case law of the Court of Justice of the European Union (CJEU) that has emerged in response to uncertainties concerning the scope of DPAs' tasks, responsibilities and their independence. It clarifies and to some extent redefines DPAs' responsibilities such that a DPA can be seen through the different lenses of: a leader, an authoriser, a police officer and a complaint-handler.[2]

DOI: 10.21552/edpl/2020/3/6

* Leanne Cochrane, Senior Research Analyst at Trilateral Research Ltd and Associate Lecturer at the Open University, Faculty of Business and Law, <leanne.cochrane@trilateralresearch.com>. Lina Jasmontaite-Zaniewicz, 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>. David Barnard-Wills, Senior Research Manager, Trilateral Research Ltd, <david.barnard-wills@trilateralresearch.com>.

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

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

The GDPR asserts that the primary responsibility of DPAs concerns the monitoring and consistency of its application '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'.[3] To attain this objective, Article 57 lists 22 tasks for DPAs that range from enforcers, ombudsmen, auditors, consultants to policy advisors, negotiators and educators.[4] While this list leaves no doubt that DPAs' responsibilities fall beyond just enforcement, the scope of their role as educators, as well as the general understanding of DPAs work,[5] has received less attention within the data protection community. This contribution hovers neatly between these topics. We reflect on the role of DPAs as educators through their engagement in awareness raising campaigns targeted at controllers, processors and the general public. In particular, we focus on DPAs' awareness raising efforts directed at Small and Medium-sized Enterprises (SMEs).

The enforcement actions undertaken by DPAs leave no doubt about the universal applicability of the GDPR. The framework applies beyond global technology giants and data driven organisations like Facebook and Google; all entities that process personal data in the EU or that process the personal data of individuals based in the EU, with SMEs being no exception, must comply with the GDPR.[6] The most illustrative examples in this regard include the 15000 EUR fine issued by the Belgian DPA in late 2019 to an SME for not complying with information obligations stemming from the GDPR when using cookies, and the 20000 EUR fine issued by CNIL to a translation company for continuously filming its employees at their workstations and thereby breaching the data protection rights of employees.[7]

Yet recognising that 'DPAs are multi-taskers',[8] we deem it necessary to reflect on DPAs' duties toward SMEs beyond enforcement, such as their duties concerning the monitoring and consistency of GDPR application. To this end, we consider within this contribution how DPAs can appropriately function in their role as educators to aid SMEs with clear and targeted guidance allowing them to begin their GDPR compliance journey. We build our argument within this paper by synthesising our observations from interviews conducted with 18 DPAs, 22 SME association representatives, and 11 SME representatives, as well as a further 52-60 SME responses to an online survey, all conducted within the scope of the STAR II research in 2019.[9]

We commence our paper by placing DPAs' awareness raising duties within the broader scope of an enforcement framework and by reflecting on the legislators' reasoning behind the explicit inclusion of the awareness raising task among others, in the Article 57 list. Before examining the state of the art of specific initiatives targeting SMEs developed by DPAs, we introduce the significant economic role played by SMEs justifying this special status.

Ultimately, we suggest that DPAs should go against the modern efficiency trend of 'cutting out the middleman': in the current context SME Associations are an appropriate 'middleman'. Although DPAs report the imperative of having direct contact with SME representatives to understand SME needs, we argue that

3 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), Art 51.

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

5 This observation is shared by Charles D. Raab and Ivan Szekely, 'Data Protection Authorities and Information Technology' (2017) Computer Law and Security Review 33, 421–433.

6 In the EU, SMEs constitute 99% of all business in the EU, and provide 2/3 of all private sector employment. It is an EU policy priority to promote new business, particular in areas of technology, which often have particularly salient data protection issues.

7 For more information on the Belgian DPA decision see here: <https://www.insideprivacy.com/data-privacy/belgian-supervisory-authority-imposes-website-cookie-fine/> and the CNIL decision, see here: <https://privacylawblog.fieldfisher.com/2019/videosurveillance-cnil-issues-fine-of-20-000-euros-against-a-small-company-in-france> accessed 1 September 2020.

8 Charles D. Raab and Ivan Szekely, 'Data Protection Authorities and Information Technology' (2017) Computer Law and Security Review 33, 421–433.

9 David Barnard-Wills et al, 'Deliverable D2.1 Report on DPA efforts to raise awareness among SMEs on the GDPR' (Version 1.1; 2019), available: <https://www.trilateralresearch.com/wp-content/uploads/2020/01/STAR-II-D2.1-DPA-awareness-raising-v1.1.pdf> accessed 14 July 2020; STARII, Deliverable D2.2 Report on the SME experience of the GDPR (2019), available <https://www.trilateralresearch.com/wp-content/uploads/2020/01/STAR-II-D2.2-SMEs-experience-with-the-GDPR-v1.0-.pdf> accessed 14 July 2020. Please note that the UK was a Member State of the EU during 2019. The ICO was therefore an EU DPA during the STAR II research. At the time of writing, the GDPR still applies in the UK based on the 'Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community, 2019/C 384 I/01, see Arts 70 and 71.

SME Associations are often better placed to identify and communicate such needs to DPAs on behalf of SMEs. This is because SMEs, unlike SME Associations, tend to lack the time and resources necessary to communicate their business needs to DPAs. We additionally argue that SME Associations can assist DPAs in disseminating information to SMEs through what is essentially the strategic leveraging of existing communications networks. The paper therefore suggests a wider re-examination of the role SME Associations can play in assisting DPAs in the fulfilment of their leadership, education and awareness raising functions towards SMEs. While more immediately applicable to some EU member states than others, this strategy has the potential to better represent the interests of SMEs and increase the working efficiency of all relevant entities, ie SMEs, SME Associations and DPAs throughout the EU.

## II. Enforcement and Awareness Raising Duties of DPAs

There is a broad consensus among regulatory scholars that 'enforcement' can be deterrence or compliance driven. Awareness raising duties mostly fall within the scope of 'compliance' and strategies accompanying it - as they typically seek to prevent harm and damage from occurring. The 'deterrence' style enforcement requires those regulated to be aware of the possibility of enforcement and it entails issuing fines and sanctions for not complying with the regulation.[10]

The 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 through significant fines under the Data Protection Directive 95/46/EC, most DPAs awareness raising activities formed part of their enforcement strategies. In view of this, it can be even argued that most of the DPAs acted in accordance with 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] By means of opinions, guidelines, public engagements and other similar awareness raising activities, the well-intentioned national regulators sought to reach, on the one hand, individuals, whose rights are affected, and, on the other hand, 'controllers' and 'processors', who handle personal data of individuals. However, diverse approaches emerged among DPAs in terms of their tasks and powers as a result of 'history, case law, culture and the internal organization of the Member States'.[12]

The adoption of the GDPR was intended to reduce such diversity and increase harmonisation among DPAs enforcement practices in two ways. First, it aimed to ensure the 'complete independence' of DPAs and the allocation of appropriate funds for them to carry out their duties.[13] While many differences across national DPAs remain, in terms of their size and the rigour of their investigations, they should now have better capacity to enforce the EU data protection framework to the full extent.[14] Second, by making the awareness raising duty explicit and by providing for a possibility of significant fines, the EU legislator has potentially tilted the governance scale which may result in more balanced enforcement strategies of DPAs.[15] 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.[16]

---

10 For more on enforcement strategies see: Robert Baldwin and Martin Cave, *Understanding Regulation: Theory, Strategy, and Practice* (OUP 1999) 96-117 and Neil Gunningham, 'Enforcement and Compliance Strategies', 120-145.

11 Robert Baldwin and Martin Cave, *Understanding Regulation: Theory, Strategy, and Practice* (OUP 1999) 101.

12 Art 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) 22-23.

13 ibid

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>.

15 It should be noted that many DPAs were already deeply engaged in awareness raising practices, and therefore for them adding this obligation to the DPA responsibility list was a reasonable step to make. The EU legislator includes three co-legislating institutions: the European Commission, the Council of the European Union and the European Parliament.

16 Neil Gunningham, 'Enforcement and Compliance Strategies' in Robert Baldwin, Martin Cave, and Martin Lodge (eds), *Oxford Handbook of Regulation* (OUP 2010) 122.

In practice this means 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 in a way that updates the enforcement practices of DPAs.[17] This being said, it should be added that while awareness raising duties constitute only a 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.

## III. Scoping DPAs' Awareness Raising Duties to SMEs

Under Article 57.1 of the GDPR, the awareness raising duties of DPAs can be divided into two categories. 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] whereas the second group requires DPAs to engage in activities furthering 'the awareness of controllers and processors of their obligations'.[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] The Recital notes that such awareness raising 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: SMEs constitute the backbone of the European economy and the significance of their role is continuously reaffirmed by European Commission reports.[21] At the same time, compliance with the GDPR poses distinctive challenges for SMEs – apart from a lack of awareness, the revision of existing practices is often time consuming and they can rarely afford professional legal advice.[22]

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 based upon general communications practice 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'.[23] Such activities can be communicated through different mediums (see section IV.1).

When considering other evidence for the scope of awareness raising duties DPAs have towards SMEs, the views of academics and practitioners supplement the perspective of DPAs themselves. In principle, some among this group suggest that DPAs' awareness-raising role among SMEs should be regarded as a form of *leadership*,[24] 'where the emphasis is on the expertise, authority, influence of and information from the DPA'.[25] Christopher Hodges asserts that successful leadership, and consequently the success of awareness raising activities of DPAs, depends on trusted relationships which entail constructive engagement by DPAs with regulated entities.[26] In his view, supportive and responsive regulation based on

17 Art 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) 4.

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, Art 57.1 (b).

19 ibid Art 57.1 (d).

20 Note, recitals are not legally binding, yet they are used to interpret the binding provisions.

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.

22 David Barnard-Wills et al, 'Report on the SME experience of the GDPR, Deliverable D2.2, STAR II project, 2019.

23 SDG Accountability Handbook, 'Raising Awareness through Public Outreach Campaigns What is it?' (2018).

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.

25 Centre for Information Policy Leadership, 'Regulating for Results Strategies and Priorities for Leadership and Engagement: A Discussion Paper' (2017) 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> accessed 1 September 2020.

26 Christopher Hodges, 'Delivering Data Protection: Trust and Ethical Culture' (2018) 4 European Data Protection Law Review 65.

a more profound understanding of 'how and why business seek to comply' requires reconsidering the strict 'deterrence' approach, which it will be recalled from the section above focuses on fines and sanctions.[27] Hielke Hijmans partially shares this view, however, he notes that for enforcement of the regulatory framework to be successful, regulators should have sufficient resources and capacity to issue a strong sanction.[28] It could be suggested that the conceptual debate among the two experts, has been in fact resolved by the EU legislator who opted-in for a more balanced and practical enforcement strategy that includes both deterrence and compliance approaches. Indeed, observations made during interviews with 22 SME Associations, support Hijmans' point given that information on the imposition of fines was one regularly-cited way of capturing the attention of SMEs. That said, there is evidence that SMEs are not preoccupied with fines, with the perception identified among some SMEs that a hard enforcement approach by DPAs, in particular the imposition of fines, was instead a concern for much larger companies. Some SME interviewees expressed the belief that they were 'below the radar' of data protection regulators.

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 expressed the view that their role is one of a leader,[29] the contribution pursues this narrative to emphasise the influential role DPAs can and should play beyond deterrence strategies.

## IV. The State of the Art of DPAs Awareness Raising Efforts Targeting SMEs

### 1. Communication Mediums

During interviews with 18 DPAs we found that mediums through which awareness raising activities are communicated range from traditional communication platforms such as radio, television, print media (as well as video), to the use of internet websites, dedicated social media accounts and engagement of influencers.[30] 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, particularly when targeting SMEs, as these enterprises tend to be varied in nature and have different needs. During the interviews, it was also noted that participation at events dedicated to SMEs is one the most effective ways to develop and adjust awareness-raising strategies. This is because presentations and question sessions at such events were understood to facilitate face to face exchanges about the pressing needs and compliance hurdles of SMEs. Furthermore, DPAs claimed to understand SME needs better when 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.

### 2. Guidance Materials

Publishing expert advice on data protection issues is an activity 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 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 in fulfilment of its role to 'examine, 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 the

27 ibid 71.

28 Hielke Hijmans, 'How to Enforce the GDPR in a Strategic, Consistent and Ethical Manner?' (2018) 4 European Data Protection Law Review 80, 82.

29 D2.1, 43, the list of interviewed DPAs include: Belgium, Bulgaria, Croatia, Czech Republic, Estonia, France, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Poland, Romania, Slovakia, and Slovenia.

30 STARII D2.1, 44.

most attention by the data protection community, independent initiatives by DPAs carry the potential in a similar vein to encourage consistent application of the GDPR. As is well known to the current readership, the GDPR is a principle-based regulation, which is technology neutral and which is often are criticised for being too vague and triggering legal uncertainty.[31]

In our survey, we found that around 80% of surveyed SME representatives have accessed guidance provided by a DPA at least once in the six months prior to the survey date, with a small group of SMEs who were accessing guidance from their DPA on a very regular basis (ie more than 10 times in the same six month period).[32] The reasons offered by respondents with relatively low engagement with the guidance materials 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.[33] Some of the respondents noted that the DPA guidance often raises more questions than it answers and further that it arrived too late, ie after the time the legislation should have been implemented. Furthermore, some SME representatives shared the 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 one interviewee who stated that, '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 such criticism directed towards the general DPA guidance documents, overall, about 45% of the survey respondents found the guidance to be 'somewhat useful'. Consequently, it can be suggested that there is room for improvement and that more tailored DPA guidance taking into account the distinct needs of SMEs would be appreciated.

## 3. 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),[34] France (CNIL),[35] Ireland (DPC),[36] Lithuania (VDAI),[37] Slovenia (IP),[38] Spain (AEPD),[39] Sweden (Datainspektionen)[40] and the UK (ICO).[41] Some of these DPAs further distinguish guidance for micro-businesses.[42]

The guidance provided through the DPA websites takes the form of either a downloadable document, a section of the DPA website or indeed a separate ded-

31 GDPR, Article 70.1(e).

32 STARII, D.2.2, 25. The methedology of the survey is defined on 11-13.

33 STARII, D.2.2, 25.

34 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).

35 *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> accessed 1 September 2020.

36 *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> accessed 1 September 2020.

37 *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> accessed 1 September 2020.

38 Informacijski pooblaščenec (IP) meaning the Information Commissioner. See, 'Varstvo Osebnih Podatkov' (*Upravljavec*, 2018) <https://upravljavec.si> accessed 3 October 2019.

39 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.

40 Meaning Data Inspection Board. See, 'GDPR - Nya Dataskyddsregler' (*Verksamt*, 2018) <https://www.verksamt.se/driva/gdpr-dataskyddsregler> accessed 3 October 2019.

41 Information Commissioner's Office (ICO). See, 'Micro, Small and Medium Organisations' (*ICO*) <https://ico.org.uk/for-organisations/data-protection-advice-for-small-organisations/> accessed 3 October 2019.

42 '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.

*Table 1: Swedish DPA, The GDPR Guide*

| | |
|---|---|
| 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? |

icated 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 eg what is (not) personal data and the difference between personal data and special categories or the so called sensitive data, principles (eg accuracy, data minimisation, limited retention period); data security obligations concerning technical and organisational set up of the processing; obligations concerning data subject rights; and the appointment of a Data Protection Officer (DPO), among others. This guidance brought these issues to the attention of SME readers through questions asked in the voice of the SMEs or through proactive actions they could take, rather than approaching the issue in terms of the GDPR obligations.

### a. Self-assessments

Two illustrative examples[43] of guidance documents addressing SMEs include the 'GDPR Guide' of the Datainspektionen (Swedish DPA), which asks businesses the following nine 'quick' questions[44] and that from the ICO (UK DPA) 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.[45] It can be noted, that questions posed by the Swedish DPA 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 presented in the tables below.

### b. Templates

In terms of tools and templates however, the SME specific guidance was variable. The ICO (UK DPA) provides a *privacy notice* template easily accessible from the SME section of its website,[46] VDAI (Lithuanian DPA) provides a link in its guidance to a sample *data protection impact assessment form*,[47] and the IP

43 Other DPAs also take a similar approach.

44 'GDPR-Guiden' (*Verksamt*, 2018) <https://www.verksamt.se/driva/gdpr-dataskyddsregler/gdpr-guiden> accessed 3 October 2019.

45 ICO (n 43).

46 See, <https://ico.org.uk/for-organisations/data-protection-advice-for-small-organisations/> accessed 7 October 2019.

47 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.

*Table 2: ICO, How Well Do You Comply with Data Protection Law: An Assessment for Small Business Owners and Sole Traders*

| | |
|---|---|
| 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? |

(Slovenian DPA) 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*.[48]

An especially notable tool is *Facilita* (in Spanish) provided by the AEPD (Spanish DPA). 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.[49] 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.

## 4. Hotlines and Advice Services

In addition to guidance materials prepared independently or in cooperation with others that are made available through the websites of national data protection authorities, most of the DPAs have set up hotline advice services. Such services, while developed in line with the 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 stated 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 an ac-

48 'Obrazci' (*Upravljavec*, 2018) <https://upravljavec.si/obrazci/> accessed 3 October 2019.

49 'Facilita RGPD' (n 10).

companying telephone service. Importantly, however, one DPA did not frame their service as a helpline or helpdesk but rather informed us that they answer queries through their general contact details.[50] 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. This is a fundamental philosophy around the provision of GDPR advice, which can differ between DPAs.

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 did suggest 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. Most DPAs do not have specialist SME contact methods, because they do not believe it to be necessary or a good investment of resources. The hypothetical limiting factors for success are capacity and expertise rather than awareness or indeed the need for SME specific advice channels.

SME Associations had a different perspective. They claimed that DPAs are hard to reach and that in response to their queries they do not receive concrete and timely answers. Another criticism put forward was that the 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).

DPAs when reaching out to SMEs about GDPR compliance faced difficulties. The reasons are various and include a lack of awareness by the DPAs of the different needs of SMEs across different sectors, a feeling by DPAs of being overwhelmed with enforcement as well as a lack resources for such awareness raising campaigns. Yet it seems that without having any direct contact with SMEs, it is difficult for DPAs to identify the distinctive needs of 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. There is an obvious limit to how much DPAs can meet the desires of SMEs, as unlike SME Associations, they are not service organisations purely for SMEs.

In the following section we consider how the position of DPA representatives could be reconciled with the disappointments over DPA awareness raising efforts expressed by SME representatives.

## V. Outlook for Raising Awareness through Fostering Relations between DPAs and SME Associations[51]

While interviews with SME representatives indicate that DPAs should seek improved and new solutions to contextualise and communicate their guidance to individual SMEs more effectively, and therefore satisfy their obligation to raise awareness about data protection and disseminate information widely among SMEs, the question remains open: how can DPAs with limited resources aid SMEs with clear and targeted guidance that would facilitate their GDPR compliance journey?

The answer to this question became to some extent apparent during the STAR II interviews with SME Associations. There is good reason to believe that such associations could play a crucial role in assisting DPAs to maximise awareness of existing guidance 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 (for example, they are not particularly prominent in 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, SME Associations engage in activities with interests which 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

50 This may explain why such service is not available on all DPA websites.

51 Within the scope of this article we use a term 'SME Association' to refer to different types of organisations that provide a meaningful support, advice, guidance and training services to SMEs on their functioning, ranging from trade and sectoral associations to chambers of commerce. They can be financed through membership fees or through public sources of funding.

the GDPR. We advance these arguments in the following sub-sections.

## 1. Overlapping Interests: Awareness Raising is a Shared Priority for SME Associations and DPAs

The findings of the interviews suggest that despite the different mandates of SME Associations and DPAs, whether statutory or otherwise, as concerns SMEs, their interests to a reasonable extent overlap in this case: 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 was applicable. 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, seeing them as over-compliant and primarily generating work for the consultant, guidance provided by trade or sectoral associations and chambers of commerce were among the most consulted.[52]

The perception of these non-DPA generated guidelines and their usefulness was not explored within the scope of STAR II research questions because of the initially narrower focus on the relationship between DPAs and SMEs. The potential for the role of SME Associations emerged during the stint of the project which conducted in-depth interviews with 22 SME Associations: a research group that was identified after engagement with SMEs proved more difficult than originally anticipated.

Awareness raising by 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 (eg 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. It actively participates in the multi-stakeholder expert group supporting the application of the GDPR. In one of the meetings of this group, SMEunited pointed out several compliance challenges for SMEs, which ranged from the application of specific provisions (ie the use of a legitimate interest ground) to general governance matters.[53] The voice of SME Associations which represent a large number of SMEs when conveying their distinctive needs arguably carries more weight than the voice of a sole SME representative.

This close cooperation also raises the possibility of DPAs and SME Associations co-creating guidance for SMEs. The associations bring knowledge of the aggregated concerns and questions of their members as well as knowledge of the best formats to reach their members. DPAs have the legal authority and the wider expertise in the data protection context. Guidance produced in close collaboration, which is acceptable to and endorsed both by the DPA and (sectoral) associations would potentially have the high level of authority and specificity that SMEs are seeking. If successful, this could even become an ongoing process.

Having this background in mind it should be added that the awareness raising for some SME Associations is a priority stemming from the fee-paying dimension of their services, which includes provision of relevant information, such as advice on the GDPR. Potential conflicts of interest could emerge around SME associations wanting to restrict their guidance to members, and the DPAs duty to engage with both member and non-member SMEs. As fee operating entities, SME Associations have a vested interest in ensuring that the membership of their association is worthwhile. Part of this vested interest is

52 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.

53 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>.

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.

## 2. Communication Channels

In addition, effectively functioning SME Associations will have established and 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, in which we included the Guide to the GDPR. 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.'[54]

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 by DPAs to collect SME contact details for dissemination of guidance materials – DPAs therefore appear to typically operate on a model of 'we publish it, you find it' in relation to guidance.

A further distinction can be made between communication types based on whether SME Associations function on the national or European level. It seems beneficial for SMEs to retain a focus 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 data protection 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 member state with suspicion. For example, one SME Association stated of the advice provided by another Member States DPA:

'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 why it wouldn't or shouldn't be offered nationally.'

The expressed concern is that SMEs want to know how they will be regulated, and they want guidance that definitely applies to them. Whilst international guidance can be educational in the absence of nationally specific guidance, their ultimate concern is the interpretation of the GDPR and other relevant laws that they will be regulated against, and what they need to do to comply. The existence of the one-stop-shop principle and complaints handling mechanisms did not feature in these SME considerations.

It is therefore not surprising that some of the DPAs have started collaborating more closely and proactively with certain SME Associations.[55] For example, the Belgian DPA has recently launched an awareness raising project with associations representing the fintech industry in Belgium.[56] The Italian DPA has been closely collaborating with SME Associations in Italy and Bulgaria within the scope of SMEDATA,[57] whereas the European Small Business Alliance, a non-party political European group representing small business entrepreneurs and the self-employed, is a partner in the SMOOTH project.[58] NAIH, the DPA in Hungary has recently interacted with the Somogy Chamber of Commerce and Industry and the Budapest Chamber of Commerce and Industry.[59]

54 An excerpt is taken from the interview with an approval of the interviewee.

55 For more information about DPA initiatives see: EDPB, The evaluation of the GDPR under Article 97, adopted on 18 February 2020, 35-45.

56 For more information about the project see: <https://www.autoriteprotectiondonnees.be>

57 For more information about the project see: <https://smedata.eu/>

58 For more information about the project see: <https://smoothplatform.eu/>

59 STAR II, D4.1 Guidance on hotlines.

Communications channels are not just about broadcasting information, but they are also points of interaction. SME Associations reported receiving lots of questions from their (fee paying) members about lots of different types of regulation, including data protection. If DPAs were to work with or even train the SME Association teams responsible for handling these queries, then this would offer a large potential multiplier for dissemination and increase the chances of an improved quality compliance advice getting to controllers and processors. DPAs also have their own communication channels and a mutually beneficial relationship would open these up to SMEs, for example, DPAs have good connections with other EU-based DPAs (many SMEs are not operating internationally), and into larger enterprises which may have data protection practices which SMEs may be able to learn from.[60]

## VI. Challenges

There are some barriers to increased collaboration between DPAs and SMEs, particularly where there is no established relationship or history of cooperation that has been able to build trust. One major challenge is for those DPAs that have a strategic or philosophical approach that stands against giving too specific or too practical advice, or where they are hampered by concerns about not being able to cope with enforcement cases. Practical guidance is essentially what SMEs are seeking, meaning that a close and cooperative interaction but founded on vagueness is unlikely to be appreciated by SMEs.

Such a depth of cooperation would, however, take time and resources and have costs. It must be recognised that in many 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 suggests that for the trust narrative to emerge and develop between SMEs and DPAs, either directly or through SME Associations, there is a need for resources and structures to facilitate initial cooperation, and that this can come from external stimulus and encouragement.

## VII. Concluding Remarks

Many DPAs have a well-established record of various activities to raise awareness, ranging from publishing press releases, educational materials and commentaries, to hosting public meetings and events. Indeed, only well-informed and aware data controllers and processors are in a position to comply with obligations stemming from the EU data protection framework. The weight of awareness raising as a task has of course increased with the adoption of the GDPR, where awareness raising activities are now formalised into a duty under Article 57. In the absence of further direction from the legislator, on how this duty can be implemented or facilitated in practice, regulators must consider strategies to further advance their awareness raising efforts. At the same time, it is clear that awareness raising constitutes a profound part of both the compliance focused and the deterrence focused approach to enforcement.

In our contribution we argue that knowledge gathered during the interviews conducted for the STAR II project on the awareness raising practices of DPAs, especially through the lens of SMEs, offers valuable insights in this regard.[61] 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 the specific context of the enterprise. Their criticism also extends to hotline services provided by DPAs, even if DPAs themselves are satisfied with the way their hotline services perform. SMEs and SME Associations reported that such services provide vague and untimely answers. What this discrepancy of opinion 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

60 During interviews with DPAs, some of them suggested that SMEs could learn from practices developed by large organisations; in Ireland some events were organised to encourage such knowledge exchange.

61 This being said, given the limitations our data sample based on interviews and the survey, we believe our findings should not be over interpreted.

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.[62] 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 the distinctive needs of SMEs across a range of sectors in a fast and cost-efficient way.

DPAs have in recent years been increasing and improving the quality of their collaboration with each other through various mechanisms[63], and also learning from adjacent fields of regulation (eg competition and consumer protection laws).[64] 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 co-create and disseminate guidance for and to SMEs could benefit and assist DPAs in their role as a 'leader'. This practical collaboration could also help to develop a stronger trust-based relationship between the regulators and SMEs. Some steps have been taken in this regard, and we are able to point out instances where SME Associations and DPAs interact, albeit that 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 has 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. Such interaction would necessarily differ across EU Member States but in all cases, it would require initial efforts to build trust and establish relationships between the two categories of organisations. We hope that this article and underpinning research can serve as an initial stimulus for future conversations in this area.

**Note**:This contribution is prepared thanks to the funding made available in the STAR II project (Support small and medium enterprises on the data protection reform II (2018-2020), which is co-funded by the European Union under the Rights, Equality and Citizenship Programme 2014-2020 (REC-RDAT-TRAI-AG-2017) under Grant Agreement No. 814775.

62 A similar argument has been developed in terms of technology take-up by DPAs in Charles D. Raab and Ivan Szekely, 'Data Protection Authorities and Information Technology' (2017) Computer Law and Security Review 33, 421–433.

63 David Barnard-Wills and David Wright, 'Authorities' views on the impact of the data protection framework reform on their co-operation in the EU', D1 PHAEDRA II Project London-Brussels-Warsaw-Castellón, July 2015.

64 Antonella Galetta et al, 'Cooperation among data privacy supervisory authorities by analogy: lessons from parallel European mechanisms', D2.1 PHAEDRA II project, Brussels-London-Warsaw-Castellón, April 2016, 97.