**What does good Data Protection Training look like? The state of the art and requirements for GDPR training.**

Dr Filippo Marchetti, Dr David Barnard-Wills, (Trilateral Research[[1]](#footnote-1))

István Böröcz (Vrije Universiteit Brussel)[[2]](#footnote-2)

Gabor Kulitsán (Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH)[[3]](#footnote-3))

# Abstract

[tbc]

This paper captures the current status of GDPR training

This paper first sets out our combined methodology of interviews supported by documentary search and analysis. It then examines existing GDPR training practices for both DPAs and other stakeholders, covering training methodologies and characteristics, types of training, how training is commonly evaluated, common training topics. It then focuses upon the common GDPR training topics, and evaluates existing GDPR training materials. The paper then presents the future training needs as identified by research participants. A key finding is that the approach and points of view of DPAs and other stakeholders diverge in terms of substantive training as much as they do with regard to the current and prospective training methodologies. On the one hand, authorities tend to deliver (and consider most important to deliver) more institutional, theoretical training on the GDPR, aimed at creating in trainees a clear picture of the legal framework in which both regulat*ors* and regulat*ed* operate. On the other hand, other stakeholder trainers, in particular those who provide training for a profit, tend to focus on more operative aspects, such as procedures and methods to comply with the GDPR provisions.

It concludes by deriving a checklist of positive qualities to look for in data protection training. This provides the designers and deliverers of data protection training guidance on how best to develop this training, and offers those looking for data protection training in this new regulatory context a guide with which they can evaluate what is being offered to them or is available on the market.

# Introduction**[[4]](#footnote-4)**

The purpose of this paper is to map and understand the existing landscape of training by Data Protection Authorities (DPAs) and Data Protection Officers (DPOs), and the existing training material used. It is also intended to capture the training needs of these actors, and thereby inform the developers of new training materials

The General Data Protection Regulation (Regulation EU 2016/679, hereafter "the GDPR") requires European Union (EU) Data Protection Authorities (DPAs) and data protection officers (DPOs) to undertake training activities (Arts 57(1) and 39(1)(b)). These new training responsibilities sit in a potentially awkward relationship with the other elements of their roles. This creates the need to understand both current practices in data protection training, and the perspectives of these actors on their needs for training materials.

Training is defined as a planned, systematic effort to modify or develop knowledge, skill or attitude through learning experiences, to achieve effective performance in an activity or range of activities. The purpose of this activity in professional situations is to enable the trained individual to acquire abilities for the adequate performance of a given task or job.[[5]](#footnote-5) Training materials are those supporting texts, presentations, guides, manuals, and other physical and digital materials that are used in or for those systematic efforts.

Several of the responsibilities for Supervisory authorities set out under Article 57(1) can be understood as creating requirements for training. Notably: (b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing; (d) promote the awareness of controllers and processors of their obligations under this Regulation; and (l) give advice on the processing operations referred to in Article 36(2). DPAs under the GDPR regime have a dual-faceted role, both as knowledgeably authorities in their domain - sources of guidance, advice and information, but also as enforcement authorities, responsible for monitoring and enforcing the regulation, making investigations, placing obligations and orders upon controllers and processors, and issuing administrative fines. Some authorities have exercised this dual role under the old data protection regime, and claim to be comfortable in negotiating the distinction, but for others, this is a new task.[[6]](#footnote-6) Producing and delivering training materials sits in the middle of this dual role as training becomes a version of guidance and will be taken as the view of the DPA and used to made decisions by data controllers and processors. This then has implications for enforcement activity. The risk is that DPAs shy away from firm commitments in their training activity, and that this limits the usefulness of training material. As this paper will show, experiences of DPO's in delivering training to third parties is currently widely varied.

DPO training requirements arise from their task under Article 39 (1)a, "*to inform and advise* the controller or the processor or the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions" and (1)b, "to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising *and training of staff involved in processing operations*, and the related audits" (italics added for emphasis).

The role of the DPO is itself also new. Whilst there have of course been data protection managers and specialists prior to the GDPR, the formal role of the DPO adds some new aspects.

Finally, the European Data Protection Board, also has the responsibility to promote common training programmes amongst the supervisory authorities (Article 71 (1)v).

These training requirements should also be contextualised against one of the policy intents behind the GDPR – Increasing legal certainty and providing a level playing field for data controllers.[[7]](#footnote-7) Effectively, harmonisation of data protection regulation across the EU. Each DPA developing training programmes and materials in isolation increases the overall cost involved, risks undermining the harmonising effect of the GDPR, spreading different sets of competing interpretations and best practices and puts greater pressure on the GDPR consistency mechanisms. Common training programmes would be both an example of increased coordination between data protection authorities, and an aid to this coordination.[[8]](#footnote-8)

This discussion takes places against a context of the introduction of the GDPR. In the run up to its implementation, the number of privately offered training courses increased, as did the number of GDPR consultants and GDPR preparedness efforts.

This paper first sets out our combined methodology of interviews supported by documentary search and analysis. It then examines existing GDPR training practices for both DPAs and other stakeholders, covering training methodologies and characteristics, types of training, how training is commonly evaluated, common training topics. It then focuses upon the common GDPR training topics, and evaluates existing GDPR training materials. The paper then presents the future training needs as identified by research participants. A key finding is that the approach and points of view of DPAs and other stakeholders diverge in terms of substantive training as much as they do with regard to the current and prospective training methodologies. On the one hand, authorities tend to deliver (and consider most important to deliver) more institutional, theoretical training on the GDPR, aimed at creating in trainees a clear picture of the legal framework in which both regulat*ors* and regulat*ed* operate. On the other hand, other stakeholder trainers, in particular those who provide training for a profit, tend to focus on more operative aspects, such as procedures and methods to comply with the GDPR provisions.

In the final section, the paper concludes by deriving a checklist of positive qualities to look for in data protection training. We hope that this checklist provides the designers and deliverers of data protection training with a focus upon the GDPR with guidance on how best to develop this training, and at the same time offers those looking for data protection training in this new regulatory context a guide with which they can evaluate what is being offered to them or is available on the market.

# Methodology

The information supporting this paper derives from two sources. The first source is semi-structured, qualitative interviews carried out in January-April 2018 with representatives of the Member States’ DPAs and public and private sectors’ DPOs. These interviews aimed to identify the current training practices of both categories of stakeholders and assess their foreseeable needs for the future. The second source of information is a collection of existing training materials that the research consortium obtained from the interviewees and by carrying out extensive research on the DPA websites, as well as on the websites of other organisations that provide GDPR training services.

To develop this report, the authors conducted a series of semi-structured, qualitative interviews with a) senior representatives of several Member States’ DPAs and b) DPOs, data protection experts, and other stakeholders between January and April 2018. These oral or written interviews lasted between 25 and 60 minutes and were based upon an interview guide developed and validated by the research consortium in January 2018. The interview templates for interviewing DPAs and other stakeholders were carefully planned to map the current training practices and investigate the potential training needs of the stakeholders. Consequently, all questions intended to solicit key information required for evaluating or designing an effective training scheme.

The stakeholder interview approach had been validated in previous research projects, such as PHAEDRA I and II, where the methodology had proved a suitable way of collecting and understanding DPA perspectives.[[9]](#footnote-9) The semi-structured approach using agreed templates allows for flexibility and adaptation to particular interviewees[[10]](#footnote-10), but also consistency across the different interviewers. The interview research process takes participants perspectives as valid perspectives, which can feed into a larger discussion. The interview is a "social event", based on interactions between interviewer and interviewee.[[11]](#footnote-11) This means that even where there is potentially disagreement about factual issues, these perspectives are meaningful for the DPAs involved. The semi-structured approach allows for flexibility and adaptation to particular interviewees, but also consistency across the various interviewers. As a semi-structured method was used, some DPAs or DPOs offered opinions or perspectives on issues that were not anticipated in the interview protocol, and at this point it was not possible to confirm if other interviewees would have been in agreement or disagreement with this perspective.

The interviews were carried out either by phone, by Skype, or by making resort to other conference call services as requested by the interviewees. Upon explicit request, as well as when a “live” interview could not be arranged – mainly due to time constraints of DPAs that are now extremely busy in view of the GDPR applicability deadline – the interview questions were provided to the participating stakeholder institution to be completed as a written questionnaire.

Where circumstances allowed, and participants gave their consent, the interviews were audio recorded. All interview answers were inserted in a single file, and anonymised to ensure confidentiality by removing any reference to the interviewee name, title, or contact detail from this file. A few interviewees requested the opportunity to see and approve their interview transcript. In these cases, the answers were extracted from the abovementioned file and sent to the interviewee directly. In all cases, we received the interviewee’s approval.

The authors contacted all Member States’ DPAs to present the project and ask their availability to be interviewed. The majority of them replied positively and were interviewed in the abovementioned timeframe. A few DPAs showed interest in the project but declined to participate due to work overload in the months prior to the 25 May 2018 deadline or to the limited training activities carried out. The consortium did not receive any response from a limited number of DPAs despite multiple attempts to contact them, by email and phone. In total, the consortium was able to interview 17 DPAs, including two German State DPAs (*Landesbeauftragter für Datenschutz*).[[12]](#footnote-12)

With regard to the interviews with other stakeholders, the consortium managed to interview a sample of 15 DPOs and data protection experts who are in charge of training activities in their organisations. They mainly operated in the banking, educations, legal services, and consultancy sectors, giving a good cross-section of DPO concerns relative to the sample size. Moreover, a few additional interviews have been carried out with stakeholders without training responsibilities, such as civil servants and similar officers. In addition, the consortium tried to get in contact with the main DPO associations operating in the Member States, and despite several attempts, only one association responded and was interviewed.

With regard to the analysis of the existing training materials, a critical analysis has been carried out to detect the current best practices, as well as to pinpoint the characteristics that training materials should have for them to be 1) easily adaptable to each training situation and, 2) easily understandable by audiences with different education, experience, and cultural backgrounds.

Some of the existing materials have been directly provided by the interviewees upon the interviewer’s request. Where the circumstances did not allow the interviewees to share those materials, an open source search has been carried out on several DPAs’ and organisations’ websites. A total number of 87 sample materials has been collected and catalogued, and a sample of 60 of such documents[[13]](#footnote-13) have been analysed and evaluated based on the criteria of accuracy, comprehensiveness, suitability, coherence with the regulatory environment, delivery quality and clarity, certification, cross-border relevance, accessibility.[[14]](#footnote-14) The results of this analysis now converge into this article to enrich the analysis of the interview.

# Existing GDPR training practices

The purpose of this mapping exercise was to gather information from DPAs and other stakeholders on the scope of the existing training on the GDPR; to investigate best practices; and ultimately to allow for the development of materials that can easily be incorporated in an existing training environment. To this end, the consortium developed questions that aimed to assess two key aspects of training. On the one hand, interview questions investigated methodological aspects of training, including but not limited to the nature of the provided training, the target audience, the materials and technological means used. On the other hand, other questions investigated the substance of the existing training, including covered topics and training priorities.

## Training methodologies

In relation to the current data protection training context, our findings are as follows:

**Most Data Protection Authorities have some involvement in training, but training approaches are highly variable across the EU.** In general, most EU DPAs at national or subnational level[[15]](#footnote-15) informed us that they were engaged in training, dissemination, or awareness-raising activities with a view to the applicability deadline of the GDPR on 25 May 2018. However, the approach to training activities varies greatly from authority to authority.

**Not all DPAs see external training as a current duty.** Some authorities training priorities were currently focused upon carrying out internal training to ensure all their staff were prepared to deal with the new legislation when it became applicable. This preparative training is carried out in different ways depending on the size of the authority and its internal organisation. Internal training for the smaller authorities (in terms of number of staff) involved most, if not all, of the personnel in the same, interactive and relatively information session, due to the ease of engaging activities in small groups. A few bigger authorities tend to organise internal training sessions that are attended by a selected audience of officers of different departments. External training (i.e. providing training to non-staff e.g. companies, government departments) is not unanimously perceived as a current duty by the EU DPAs interviewed. While most – if not all – DPAs provided or are providing internal training, answers on external training were more diversified. Some of the interviewed DPAs do not consider themselves currently compelled to train externally, and some of them argued that any GDPR training needs were being addressed by private-sector services. Others report engaging in some sort of training, although the level of planning differs. Curiously, the authors observe that there is limited correlation between the size of the authority and its choice to engage in external training: a few smaller DPAs provide external training, though their size of course influences the nature of the training provided. However, it has also been observed that smaller DPAs expressed a strong commitment to taking part to dissemination events, including giving presentations to specialised audiences in industry sector associations’ meetings and take part in conferences at national and international level. We might provisionally understand this as a strategy to maximise limited resources by making use of the knowledge held by DPA staff in multiple externally-hosted settings.

**When external training is conducted by DPAs, it is not always conducted in a strategic manner.** These external training activities are sometimes organised and planned in advance by the issuing authority as part of a strategy, and some other times are developed on an ad-hoc basis in response to specific requests from external stakeholders (for example, from part of the national government) to provide training. While this difference may be due to a different approach to training, the amount of resources and staffing also has its weight in deciding if and to what extent a planned training programme must be organised.

**Most "training" material is essentially passive dissemination.** In our data collection, the authors took a broad and encompassing scope for what could constitute training material. With regard to dissemination and awareness-raising activities, most DPAs developed and made informative materials available on their websites to ensure that organisations and citizen in need of information on the GDPR innovations may access knowledge for free and from an official source. These materials are mostly means for passive dissemination, such as handbooks and info-sheets, but they also sporadically included videos. In a very limited number of cases, DPAs engaged in information sessions or awareness-raising activities with schools.

**An issue that arose during the DPA interviews is that (at that point in time) some DPAs were still waiting on national legislation before developing any specific training (or advisory) initiatives. S**ome Member States have not yet issued national laws to complete the parts of the GDPR that require the latter to do so. Therefore, a few DPAs are still waiting for these regulations to be issued to plan a comprehensive training or awareness-raising scheme.

**Nature of the training organisation is critical for the type of training.** While the distinction between internal and external training is relevant when investigating the DPAs activities, it has limited relevance when dealing with other stakeholders, such as DPO associations, DPOs, and officers with data protection responsibilities. This is due to the fact that the nature of the organisation’s activities plays a key role in determining whether they will be in need or encouraged to engage in internal or external training activities. For instance, banks will be more inclined in engaging in internal training to ensure their employees are well aware that the privacy culture is changing but will not be inclined to engage in external training. At the same time, consultancy firms and law firms are more inclined to enter the market of GDPR training for business reasons, as their staff may include professionals GDPR experts able to provide such training as a service. At this end of the market, the line between training and consultancy becomes blurred. A few non-DPA organisations stated that they provide training for subsidiaries or parent organisations, that is focused on their specific needs, especially with regard to data protection obligations for non-privacy-specialists. As a result of this landscape, we anticipate internal training will shift from general purpose "this is the GDPR" training, to more bespoke training on internal procedures, policies and requirements ("this is how we do our GDPR compliance") as these become more mature and more established.

### Methodological characteristics

As said, though the landscape is not homogeneous, DPAs offer both internal and external training. Internally, they reported carrying out training activities to prepare their staff for the entry into force of the GDPR. As anticipated, the target group for smaller DPAs tends to include most – if not all – of the authority’s staff. Bigger DPAs carried out the internal training in different ways, including seminars with a restricted audience to ensure interaction among participants. In this latter case, each DPA department is represented by one or more officers, while a DPA experts gives a presentation on a specific topic.

Externally, DPAs carry out training activities both with public and private sector organisations. In many cases, these activities seem to be focused on training the public sector first. On the one hand, this seems reasonable due to the fact that public bodies – especially in some countries – have limited possibilities to make resort to private services due to bureaucracy or limited resources. On the other hand, this risks the private sector lacking consistent training from public authorities and becoming reliant on private services only.

As expected, the approach of external trainers[[16]](#footnote-16) in the private sector is complementary to that of DPAs, as they tend to focus on training companies and other organisations in the private sector as a priority. Of course, as anticipated, some stakeholders also provide training internally. Up to a certain extent, this data may be interpreted as to highlight the market-orientation of non-institutional trainers. Their approach is market-led and profit-oriented, and as a consequence, they focus their training on the market segments that are willing to pay for training. If the DPAs focus on training in the public sector and on awareness-raising activities, private organisations may fill the gap in offering training to other categories of stakeholders.

While the DPAs training activities usually avoided defining target-groups based on their role in the target organisation (they often mention training DPOs and IT officers), the training carried out by non-DPA stakeholders is highly tailored and aims to cover all corporate functions. Indeed, in addition to DPOs and IT officers, most trainers mentioned bespoke training sessions for C-level executives, managers, and even employees without data protection tasks but who may be in a position to detect privacy-related issues in the company operations. These employees have been defined in an interview with an Italian privacy expert as “privacy antennas”.

With regard to priority in training specific target groups, private organisations offering training tend to first train C-level executives and DPOs, and then progressing to a more spread and general training across the organisations. To this purpose, though, economic and organizational capacity plays an important role. One of our interviewees explained the fact that their organisation had first attempted to roll out a general training course for all employees, and then rolled back to focus only on mid-level management due to lack of capacity.

#### Type of training

Concerning the type of training offered, different trends have been observed among DPAs vis-à-vis other stakeholders. Exempting passive, informative-dissemination and awareness-raising campaigns on DPA websites, in terms of active training both stakeholder categories expressed a general preference for in-class, face-to-face lectures. Reasons given for this preference included the effectiveness of face-to-face interaction, increased attention of trainees as opposed to lack of attention and distraction when attending webinars or online modules, and the possibility of asking questions directly and obtaining an answer straight away.

DPAs rely almost solely on face-to-face delivery methods for training, either at their premises or in other locations. A very limited number of authorities engaged in different types of trainings, such as the creation of videos, webinars, or other forms of distance learning. Interactive training is also practiced, mainly by organising seminars with a restricted number of participants in order to ensure interaction among participants and with the instructor. This is especially done in smaller DPAs for the purposes of their internal training.

Non-DPA stakeholders with training responsibilities appear keener to engage in innovative forms of training. Interviewees often mentioned webinars, distance live lectures, online training platforms, telephone training, on-the-job/mentorship training or work review, and simulated games, in order to reach bigger audiences or make the training more flexible and adaptable to every work situation (a few trainers also mentioned that some trainees take this kind of courses during breaks). At the same time, a few stakeholders acknowledge that distance learning is less effective than in-class training (noting problems with distractions or "multitasking"), noting that it is still better than no training in cases of limited resources.

Across-the-board, interviewees appreciated methods such as Question and Answer (Q&A) sessions and the creation of written Frequently Asked Questions documents (FAQs), as these were considered an efficient method to achieve satisfaction among participants and – at the same time – to investigate the actual needs of the trainees to refocus future trainings on the most relevant topics.

In case of face-to-face training, the size of classes varies. In general, DPAs tend to organise external training for classes of over 30 and up to 100 participants. This may be related to the need to train as many people as possible while operating with limited human resources. DPO trainers, however, tend to train smaller classes, mostly because due to the more tailored nature of training, the size may be tied to the amount of people with a certain role in a company (number of C-level executives, number of IT experts, etc.). When the size of the classes increases, they tend to resort to webinars and other alternative means, as webinars allow more participants to take part to the training without requiring a further logistic effort. A few interviewees also claimed to offer one-to-one training sessions, especially to top management of private sector companies.

In terms of length of the training, there is a general understanding that a general, foundational GDPR training to set the bases for future trainings or for self-study may be carried out in around one working day (7 hours with breaks). However, this preparation would not equip the trainee with the tools to work independently without further study. The 2- or 3-day format is preferred by the majority of DPAs and other stakeholders for external training, as they claim it allows them to provide an adequate substantive preparation in a time that is respectful of logistics and other aspects (travel time to and from the venue, time away from normal job roles for trainees). Concerning internal training, they tend to be shorter in terms of hours or days. Seminars may last up to 4 hours, but a few DPAs tend to organise shorter sessions, however distributed over a wider period of time (akin to continuous professional development). Finally, a small number of DPO trainers offer a more structured, typically 1-week training that leads to some sort of certification, such as DPO certification or GDPR professional certification.

## Training evaluation

In the interviews, we explored with participants the extent to which feedback on training was collected and used. Feedback is normally collected as standard end-of session or end-of-training questionnaire to monitor quality and to get the trainees’ perspective. DPAs mostly rely on this tool or on more informal feedback collection, such as an oral unstructured feedback session at the end of the seminars. In many cases however, interviewees reported that feedback was not collected at all.

Other stakeholder trainers rely on the same tools but reported more structured collection and analysis system for feedback. A limited number of them rely on their Human Resource departments for developing and then extracting information from the questionnaires regarding their internal training.

# Existing training topics

In terms of substantive scope, nearly all of the interviewed DPAs that provide training have focused or are focusing on the general structure of the GDPR, targeting audiences with little to no experience in data protection. Such sessions aim at setting the grounds for further self-study or training with the DPA or other training providers.

Outside this general training, most of the DPAs heavily focus on the innovations of the GDPR compared to the old legislation (national implementations of Directive 95/46/EC (DPD) and others). This includes teaching the new concepts and tools introduced with the Regulation (e.g. the DPIA, sanctions, territorial scope, etc.), the new obligations for data controllers and data processors (e.g. risk-based approach and accountability, data breach notification, etc.), as well as the new rights of the data subjects (e.g. data portability). In this case, there is a general assumption that, despite not having any prior preparation on the GDPR, their audience is at least acquainted with data protection law and with the concepts guiding the regime of the DPD, or that the primary concern of their audience, is transitioning from the old regime to the new.

Nearly all interviewed DPAs mentioned the fact that they are also including information on national legislation in the training. Indeed, though the GDPR is directly applicable in all Member States, a small but relevant number of rules require national legal systems to enact legislation to complete or define a few aspects (for instance, it is still national law that defines what a Public Authority is under EU data protection law). DPAs, as well as nearly every interviewed stakeholder, underlined the necessity of taking national law into account when designing a data protection training scheme. The understood priority for end-users was that the scheme covers the relevant law for their context and operations, not that it be conceptually driven by the legal instrument.

A very limited number of DPAs are determining the scope of their training activities based on requests from their trainees. Indeed, while this is a very common approach in the private sector where training activities are reconfigured based upon the needs of the "customer", DPAs tend not to organise request-driven training sessions. This coupled with the relative lack of feedback collected by DPAs from training sessions, potentially leaves DPA training at some distance from its potential users.

A limited number of DPAs did however report organising bespoke training for specific industries, such as the financial sector, the health sector, or the public education sector.

It is to be highlighted that one of the most relevant differences between DPAs and other trainers is the approach to the operative dimension of GDPR compliance. While DPAs seem to adopt a more theoretical approach for conveying GDPR knowledge, such as the reading and explanation or comment of the GDPR legal text, DPO trainers tend to focus on the practical aspects of the new legislation. This includes operative instructions to carry out and deliver adequate DPIAs, impact of the GPDR on contracts with suppliers and clients, how to update the documentation on data transfers, the record of processing activities (data registers), the function of binding corporate rules (not without criticisms about the slowness of DPAs to provide guidance on this point), the practical obligations for the newly-appointed DPOs.

Additional, specific, practical training topics mentioned by non-DPA trainers included procedures to comply with new rights of data subjects; obligations for data controllers and processors; lawfulness of processing; how to use privacy-related IT tools; DPO – appointment and role; record of DPA activities; data protection in employment contracts; Big data and the GDPR; anonymisation; mobile device management; SAP[[17]](#footnote-17); direct marketing; complaint procedures; data lifecycle management; data processing audits; regulatory and compliance gap analyses; training clients staff on GDPR and compliance; structuring data processing methods; preparing compliance strategies and action plans; compliance documentation; data protection impact assessment; notification of personal data breach.

# Existing GDPR training materials.

The materials collected and analysed by the authors cover almost all of the European DPAs. As mentioned before, materials have been analysed based on the previously-determined criteria of comprehensiveness, suitability, coherence with the regulatory environment, delivery quality, certification, cross-border relevance, and accessibility.

While the materials issued by a few countries have not been analysed in full due to linguistic barriers, they have still been analysed, together with all other materials, in terms of structure, key elements, and accessibility.

While most of the private-sector interviewees were reluctant to share their training materials – even samples of them – with the authors for commercial reasons, it has been still possible to collect a limited number of materials online. This analysis can provide the following observations:

**Presentation slides and documents are the industry norms.** As is the norm across many industries and sectors, digital presentation slides are by far the most used training material in this context, both by DPAs and by other stakeholders. Due to the prevalence of in-class training, such an outcome was expected. Handouts, such as legal texts, documents and guidelines issued by the Article 29 Working Party (WP29) or by DPAs are also often used as in coordination with slides. Both DPAs and DPO trainers make regular use of infographics, checklists, FAQs, and similar materials to ensure easier understanding and access to information, and to give participants a reference to take away from the training.

In general, the materials available on the DPAs websites are PDF-format documents containing thematic guidelines, checklists for compliance, and general guides on the GDPR. Therefore, while introductions usually make clear on the purpose for which each document has been prepared, they only rarely identify a specific target audience. At the same time, due to the fact that such materials are openly accessible online and do not pertain to a comprehensive training scheme or training session, no indication is usually made on what time the reader should dedicate to the study of each material. A small amount of materials are PowerPoint presentations used by authorities in training sessions, conferences, and other dissemination events.

**Alternative delivery methods are rare.** DPAs rarely rely on additional materials beyond the aforementioned, while other trainers reported also making use of e-learning platforms, videos, handbooks, databases and wikis both for internal and for external use. Notably, in a few of these cases e-learning platforms were used relatively passively, as a vehicle for hosting presentation slides online, to enlarge the potential audience, but without setting up a bespoke course (or making use of interactive or assessment features, for example).

**Materials are often generalist.** As to the structure of the materials, most of them included an introductory section aimed at introducing the reader to the topic treated in the document, and the majority of them included a table of contents to assist the reader in identifying the subtopics they are most interested in. However, only a small minority of the materials contained an indication of further readings for those who wish to dive into the topic and achieve a more complete preparation. This seems to be a relevant issue in the current practice, because the more general the documents are, the more indications they might be expected to contain to redirect readers to more specialised materials.

**Training methodologies are missing.** Another missing element in most of the materials, including in the collected PPT presentations, is any mention of the training methodology, a topic that is often addressed in the materials prepared by other stakeholders. There is available material, based upon the relevant legislation, but this material can only rarely be considered to be training material with a pedagogic design.

**Content is mostly relevant and up to date.** In terms of content, the collected materials are usually up-to-date with the new developments in the data protection landscape as should be expected from data protection authorities. A few of them included links to WP29 guidelines and to other regulatory clarifications issued after the entry into force of the Regulation. The content is mostly relevant and will be of use for several kinds of audiences, ranging from private citizens to organisations. However, it must also be noted that a few of the collected general guides were so theoretical, that corporate and organisational stakeholders will likely have to look elsewhere to find more operative, practical guidance on how to comply with the GDPR. Finally, the consortium found the content of these materials mostly accurate and without flawed aspects.

**Material doesn't always cover the full regulatory environment.** Still in terms of content, not every material addressed the entire GDPR regulatory environment. While guidelines usually follow the structure of the GDPR and therefore cover all of its content, most of the remaining materials deal with single topics, such as Data Protection Impact Assessments (DPIAs), DPOs, or the rights of data subjects, and therefore leave other GDPR innovations to be dealt with in other materials issued by the same DPA. This likely supports a user browsing for guidance or information on a specific topic, but with a general grounding already. A relevant aspect to highlight is the general lack of systematic approach in training recipients on the full system that will be in place once the GDPR becomes effective: indeed, in none of the collected materials any reference was found to the other data protection regulations in force, such as Directive 2002/58/EC (ePrivacy Directive) or similar. Furthermore, an extremely limited number of materials contained real life examples, case studies or scenarios.

**International dimension is often missing.** While many materials analysed addressed the topic of international data transfers, very few of them approach data protection taking into account transnational situations beyond data transfers. Indeed, nearly all the materials have a very national approach, and address almost exclusively entities and people in a certain Member State and are drafted in the language of that Member State. This, of course, does not tell the whole story in terms of how these materials might actually have a transnational reach. Especially due to the language in which they are drafted, the materials issued by the UK Information’s Commissioner’s Office (ICO, the UK DPA) were reported as sometimes taken into account by practitioners in other Member States: this happens regardless of the fact that the ICO may or may not have issued them having foreign recipients in mind. The same goes for other materials issued by countries whose language is spoken or understood abroad, and for regulators in countries with a large number of multinational companies, whose guidance becomes relevant across borders.

**Language varies between the general and the legal.** In terms of linguistic register, two different approaches coexist in the current landscape. On the one hand, some DPAs focus on general, non-technical, easily-understandable language, for stakeholders to easily grasp the meaning of the new concepts introduced in the GDPR. On the other hand, a few DPAs opted in favour of offering readers a more technical, precise guidance. In this second case, which is however a minority, materials are drafted using a more legally-solid linguistic register.

**Materials rarely meet accessibility guidance.** Finally, in terms of accessibility, there are a great variety of approaches. While some DPAs do not make any effort to increase the appeal and readability of their documents, resulting in plain text guidelines that are difficult to read, some others embraced a more captivating style in order to make the documents more appealing. The latter often make use of infographics, images, graphs, and tables to aid the explanation of concepts. As a consequence, a document on DPIAs drafted as a plain text essay will be much more difficult to understand than a document in which text is accompanied by graphs and infographics. Nonetheless, it must also be noted that some of the texts falling in the first category are drafted in a more technical and/or legal language, which means that the intended audience for such materials may differ from the intended audience of the more communicative materials. However, the more communicative materials are not necessarily less-useful to a more specialised audience just because of the way they are drafted. Finally, concerning again accessibility, while most of the materials are accessible to hearing impaired, as they are written document, no material has been found that is specifically visually impaired people, with the exception of a few explanatory videos available on the YouTube channels of a few DPAs. However, as one may imagine, very rarely these videos are as detailed as the written documents, as the first ones are mainly conceived for dissemination and awareness-raising purposes. Formatting for accessibility (e.g. through screen readers or text-to-voice software) is mixed within the sample. Some collected documents were easily accessible in this manner (for example, because they are simple text documents) but many other more visually complex documents lacked accessibility features such as alternate text for images, tags, Unicode characters, or language specification, which could cause problems for users of accessibility software.

# Identified GDPR training needs

In addition to questions concerning the existing training practices of DPAs and other stakeholders, the authors asked their interviewees to express themselves on the training practices, contents, and materials they expect would be useful for them, or for the general public, in the near future. These needs can be separated into needs around training methodologies and needs around training topics – how training should be delivered, and what training should cover.

## Needs relating to training methodologies

In most interviews DPAs and other stakeholders were convinced that their current training methodology will continue to prove adequate for further training. Nonetheless, though the majority of stakeholders, both DPA and non-DPA, are convinced that face-to-face classes are still the most effective way to convey knowledge, they also provided several examples of innovative and alternative training, both as a wish for the training designers and experts to explore these areas and as an ambition for them themselves to realise these trainings in the future. They mentioned webinars, online platforms, video series (especially with operative content and practical examples), live-chats, case studies, and Q&A sessions. In nearly all cases, DPAs and other stakeholders strongly desire that future training schemes have a practical approach with examples, case studies and simulations, templates, and checklists. With regard to the audience for these trainings, DPAs expressed the belief that a sector-based approach would be preferable to the more common topic-based approach that currently dominates. In addition, despite their readiness to explore new types of training, DPAs underlined that trainees continue to wish to have the materials as handouts for reference. Therefore, even in future training schemes, the possibility of providing the audience with written handouts should be included.

In terms of structure and duration of the training, a variety of inputs have been received from DPAs stakeholders. However, in general it can be concluded that DPAs are satisfied with the length they are currently able or willing to offer and they do not expect future training schemes to alter this length: courses and workshops lasting 1-3 days to provide a general knowledge of the GDPR, and 30 minutes for single webinar modules. All sessions should be completed by Q&A sessions as discussion was highly valued by nearly all respondents. This is also supported by most theories of learning and training. This format and length is common across industries and to some extent, the GDPR training available conforms to general corporate training practices, rather than an inherent nature of the content or subject area being trained. Similar but not entirely matching opinion was received from non-DPA trainers. They would prefer to run full courses up to a week and have thematic workshop last half a day to one day (longer than DPA preferences). Webinars would last about 1 hour while e-learning courses may be longer, as they can be paused and resumed. This suggests many trainers feel under pressure in terms of teaching everything they consider important, or necessary for their trainees within the logistical time constraints.

A general request on methodology was that future training should adopt an easily understandable language, that aims at ‘decoding’ the legal and IT language that is used in the GDPR and other related documents. There is a general pressure to move from a legal-theoretical exposition of the GDPR for experts to practical and easily understood material for practitioners (at various levels).

In terms of the degree of focus to adopt in future trainings, there is no convergence among DPAs on whether trainers should focus on providing very specific, in-depth training or more generally-accessible materials for the public. One could argue that this divergence derives from the approach that DPAs have adopted so far: working with limited resources, some DPAs have focused on general information and awareness-raising, while others have focused on getting some key sectors ready for the GDPR; as a consequence, the first group prefer future training to dive deep into specific issues, to complete their work and provide materials they cannot provide due to limited resources, while the second will have the opposite wish, having neglected general information in order to train critical sectors in the national economy. There is demand from both perspectives, but also potential material in both which can be drawn upon in a holistic training scheme. Another point of disagreement is whether future training materials should aim at training non-DPA stakeholders only or DPA staff too.

## Needs relating to training topics

A relevant question in this context of transition from the old DPD harmonised system to the new GDPR unified regime is whether the aforementioned training topics will still be adequate to train data protection professionals in 1- or 2-years time. Indeed, by that time, not only new legislation may have been released alongside the GDPR[[18]](#footnote-18), but also a comparison with the old system, that is now the most common approach to training, will lose its relevance, and, as a consequence, the existing training packages may need reworking. Additionally, as new practitioners enter the workforce or new firms engage in personal data processing, they will have little familiarity with the old regime, and a comparison between the two will not be educationally useful. To this end, it was important to investigate the topics that DPAs and other stakeholders considered most important to train professionals in, to outline accurate and useful training materials for future use. The consortium asked both DPAs and other stakeholders about their expected priorities on training topics.

For DPAs, the consortium’s findings are that the teaching priorities may be reorganised as shown in the following table. This table is organised based on the number of times each topic has been flagged as a priority by interviewed stakeholders. These priorities regard the current training needs of stakeholders, but it may well happen that – with new best practices arising and case-law increasing over time – they could change in the medium-to-long term.

Table 1: DPAs’ teaching priorities

The first observation is that these topics reflect the innovations in the GDPR data protection context. The rights of the data subjects have been increased in number and in the substance and now include ones such as the right to be forgotten, the right to data portability, etc. Even the legal bases for the lawful processing of personal data have been reworked and need organisations to take it into account. The duties and obligations of data controllers and processors are also a part of the GDPR that greatly innovates from the DPD system. This includes enhanced notification duties and processors becoming fully responsible for their processing wrongdoings whenever they or not they remain compliant with their contractual duties. The GDPR also innovates in terms of technical and operational measures to ensure adequate protection of the data subjects’ rights and freedoms: the old Directive, drafted in 1995, was obviously lacking on any contemporary technological tool to protect privacy. Training organisations on the role of the DPO is also an expected priority for DPAs: indeed, DPOs will be the main interlocutors for DPAs in the future, especially in very sensitive fields; at the same time, it is not surprising that DPAs are willing to ensure that all stakeholders are aware of their role and regulatory and sanctioning powers. DPIAs and the records or processing activities are among the most relevant innovations in the GDPR, as they are both a self-assessment and reporting tools for organisation on whether their approach to data processing is correct, and a formidable element to take into account for the purposes of the DPAs’ audits. Moreover, while sanctions took the spotlight as the most ‘fearsome’ innovation for companies, the correct management of data breaches is one of the main tools to avoid being sanctioned. The value of privacy and data protection in the corporate environment is also important, because the GDPR demands a change of approach to the protection of personal data, and concepts such as data protection by design and by default are of paramount importance to this purpose. Finally, as mentioned before,[[19]](#footnote-19) national law is not completely without a role in this new regime: while the GDPR is directly applicable in all Member States, it also need national law to complete its regime.

Based on the outcomes of the interviews and on the data concerning which DPA prioritised each training topic, the abovementioned list may be also reorganised to highlight a more conceptual difference in approaches between DPAs. Indeed, we can identify the existence of two coexisting philosophical or strategic approaches to training. On the one hand, a group of DPAs focused on a more theoretical/conceptual approach to teaching the GDPR. These DPAs focused on giving an overview on aspects such as the new rights of data subjects, the obligations for controllers and processors, the value of the protection of personal data and the data protection by design and by default. On the other hand, a second group of authorities favoured training on more practical aspects of the GPDR. These authorities tended to prioritise training on DPIAs, the management of data breaches, the roles and duties of DPOs and DPAs, and technical and operational measures, including data security.

Although some DPAs favour more practical aspects when mentioning the training they expect to deliver, non-DPA trainers have an even *more* practical approach. Indeed, in addition to the abovementioned topics, non-DPA stakeholders highlighted the importance of training on aspects such as the GDPR impact on contracts; risk management strategies; organisational procedures (including forms and templates); how to practically deal with data subjects’ requests; and how to practically obtain and manage consent.

It is to be highlighted that not every abovementioned topic may prove useful in both internal and external training. For instance, while private and public organisations may find it interesting to be trained on procedures and how to draft consent forms and data registers, the same cannot be said for the staff of a data authority. The latter will be more interested in having a clear idea of their prerogative, and of what they can expect from and demand to DPOs. The same can be said with regard to the depth of the training. While DPA staff will find it sufficient to have a less profound training on DPIAs, company data specialists will require a more deep and thorough training not only on the concepts, but also on the practical aspects of DPIAs.

# What does good data protection training look like? A checklist**.**

Based upon the interview and documentary research described in this paper, we now offer a checklist. Our aim here is twofold. We hope that this checklist provides people or organisations designing or delivering data protection training with a focus upon the GDPR with guidance on how best to develop this training. We also hope that this checklist provides those looking for data protection training in this new regulatory context a guide with which they can evaluate what is being offered to them or is available on the market.

**“good” GDPR training:**

* **Covers (at minimum) the following topics:**
	+ *Introduction to the EU GDPR regime* - A topic on the basics of GDPR can be used to start sessions that then move to other specialist areas, and give a holistic overview. general elements are an important precursor to specialised training, and for holistic understanding.
	+ *Purposes and legal grounds for processing personal data* - Explores the main principles and various legal bases for the processing of personal data. Assists trainees in understanding their options in this space, including what is and what is not permitted, and which are the most appropriate legal grounds for their data processing. It also allows them to understand the approach they should have to GDPR compliance as a whole, due to the fact that the entire system is significantly based on these rules.
	+ *The rights of the data subject and their exercise* - the rights of the data subject in relation to the processing of their personal data, how organisations have an obligation to respect these and good practices to implement those rights in data processing. This material will help trainees to understand and protect the rights of data subjects and build systems and structures to help data subjects exercise their rights and minimise their exposure to enforcement actions of administrative and/or contractual/tortious nature. That data controllers understand these rights is a priority topic for EU DPAs.
	+ *Responsibilities of data controllers and processors* - the obligations of data controllers and processors in terms of transparency with data subjects and authorities, organisational measures to ensure compliance with the legislation, and actions to be undertaken in case of pathological situations, such as data breaches. It should also explore the new principle of accountability, a cornerstone of the GDPR regime. This material is also critical for organisations to plan, achieve, and maintain GDPR compliance.
	+ *The role of the Data Protection Officer* - one of the most relevant changes in the new regime is the obligation for some organisations to appoint a Data Protection Officer (DPO), a corporate role tasked with facilitating compliance with the GDPR provisions. Training should give an overview on when and how to appoint one, and what DPOs are tasked with.
	+ *The role of the Data Protection Authority* - Explores the role and responsibilities of the key regulator under the GDPR, the Data protection authority. How can the DPA be of assistance to other data protection professionals? Trainees should be able to understand the role of the DPA and how it likely interacts with their organization, how best to approach and work with the DPA, and what can be expected of it.
	+ *Data protection in practice (including technical and organisational measures)* - explores one of the main subtopics of the responsibilities of data controllers and processors to give depth to one of the main instruments to ensure compliance with the new system, equipping trainees with the adequate knowledge to direct the implementation of these measures by technical experts in their organisation. Should touch upon security of processing, information security, data minimization, anonymisation, pseudonymisation, Privacy-Enhancing-Technologies, data protection by design and by default, encryption, protection from intrusion, protection from loss, audit, penetration testing, and how such measures impact liability.
	+ *Risk management in the GDPR context* - Explores thechange of approach and culture in public and private organisations. Changing corporate cultures around processing of personal data. How does DPIA fit in. Ethics and correct approaches beyond, simple compliance.Accountability and transparency.
	+ *Data Protection Impact Assessments -* The GDPR introduces a new requirement around particular types of processing of personal data – the Data Protection Impact Assessment (DPIA). Essentially, for certain types of personal data processing that can be considered to pose a high risk to the rights and freedoms of data subjects, a data protection impact assessment exercise must be conducted prior to starting that processing. Should include The DPIA concept; DPIA triggers; defining and identifying “high risk” processing; when and how to conduct a DPIA; validating DPIA results, the role of management and DPO, publishing a DPIA, usefulness for DPAs.
	+ Data protection communication - Much of the regulatory regime around data protection involves requirements for various forms of communication, for example, notifying affected parties and authorities in the case of data breach, or providing adequate information to data subjects so they can give informed consent to data process. Guides trainees in understanding their communications obligations and how to execute them.
	+ *GDPR-related laws and special provisions* - The GDPR does not stand alone but is rather accompanied and impacted by other EU legislation, national data protection legislation and decisions, and sectoral legislation. Good GDPR training will embed the Regulation into the context of business and organisations by helping the trainees better understand these connections.
* **Is clear about its target audience, or specifically adapted to its target audience** and its particular training needs. A potential customer of GDPR training should try to understand their particular training needs and select training resources appropriately. GDPR training can be particularly useful if it is designed for use within a particular context or sector, focusing upon common occurrences and practices in that sector, for example, data protection in medical, banking finance, education, marketing industries, or in the law enforcement context.
* **Is Orientated towards longer term use** – Training should bedesigned for longer term use and do not overly focus upon what is “new” in the GDPR, but rather on what is important, complex or otherwise requires training material. This becomes more pertinent over time as fewer data protection professional will have pre-GDPR experience.
* **Is customisable -** Ready for localisation to enable DPAs/DPOs to amend as required (for example, for them to add own logos and trademarks, but also institutional design languages – e.g. corporate colours and fonts) and otherwise interact with as they wish.
* **Is Easily understandable by its target audience**. It should avoid the use of legal jargon where possible, and explain any necessary specialised terminology; define key concepts and terminology; and make good use of graphical elements to support written text.
* **Includes practical examples and case studies**, as these were demanded by GDPR stakeholders[[20]](#footnote-20) and their use is supported by educational theory.[[21]](#footnote-21) Such cases can include synthetic case studies, generated to highlight specific issues or teaching points, but real case studies are particularly desired. Case studies promote vicarious experience for learners.
* **Meets commonly used accessibility standards.** The assessment of existing GDPR training material from various sources, conducted here found that very little of this material meets current accessibility best practices. Users should not be prevented from accessing GDPR training because of visual or other disabilities.
* **Provides practical guidance and instructions** (for example, how-to instructions, Frequently-Asked-Questions lists, to-do lists, best practices, templates and tools).
* **Is Interactive** - Practical exercises for trainees should be included where possible. interactive sessions, facilitate and encourage discussion and interaction between participants. Interaction was strongly identified by stakeholders as a key source of learning and sharing of experience.
* **Is delivered by a subject-matter expert** – whilst introductory training can be delivered by generalist trainers, much GDPR training for specialists in practices involves exploring particular questions, examples and edge-cases and in this, domain expertise and the ability to go beyond the text of training materials remains critical.
* [any others?]

**References**

Barnard-Wills, D., Pauner Chulvi, C., & De Hert, P. "Data protection authority perspectives on the impact of data protection reform on cooperation in the EU", *Computer Law and Security Review*, 32(4), 2016.

Barnard-Wills, D., Vagelis Papakonstantinou, Cristina Pauner & José Díaz Lafuente, *Recommendations for improving practical cooperation between European Data Protection Authorities*, PHAEDRA Project D4.1. Brussels, London, Warsaw, Castellón, January 2017. http://www.phaedra-project.eu/wp-content/uploads/PHAEDRA2\_D41\_final\_20170114.pdf

Blakely, Ruth, Elite Interviews, In Laura Shepherd (Ed.), *Critical Approaches to Security: An introduction to theories and methods*, London & New York, Routledge, 2013.

Clark, Ruth, "Accelerating Expertise with Scenario-based learning", Training and Development, January 2009. <http://www.clarktraining.com/content/articles/ScenarioBasedLearning.pdf>

European Commission, A comprehensive approach on personal data protection in the European Union, Communication from the Commission to the European Parliament, The Council, the Economic and Social Committee and the Committee of the Regions, Com(2010) 609 final. Brussels, 4.11.2010. http://www.europarl.europa.eu/RegData/docs\_autres\_institutions/commission\_europeenne/com/2010/0609/COM\_COM(2010)0609\_EN.pdf

Fielding, N. & H. Thomas, "Qualitative interviewing" in G. Nigel (Ed.) *Researching Social life*, London, Sage Publications, 2001.

Rubin, H.J & I.S. Rubin, *Qualitative Interviewing: The Art of Hearing Data*, London, Sage Publications, 1995.

1. One Kightsbridge Green, London, United Kingdom, SW1x 7QA [↑](#footnote-ref-1)
2. 4C339, Vrije Universiteit Brussel, Pleinlaan 2 1050 Brussels [↑](#footnote-ref-2)
3. [↑](#footnote-ref-3)
4. This paper is based upon research conducted as part of the STAR project (Support Training Activities on the data protection Reform) which is co-funded by the European Union under the Rights, Equality and Citizenship Programme 2014-2020 (REC-RDAT-TRAI-AG-2016) under Grant Agreement No.769138 [↑](#footnote-ref-4)
5. Roger Buckley & Jim Caple, 2007, The Theory and Practice of Training (Revised 5th Edition), London & Philadelphi, Kogan Page Publishers, p.5. [↑](#footnote-ref-5)
6. David Barnard-Wills, Cristina Pauner Chulvi, Paul De Hert, Data protection authority perspectives on the impact of data protection reform on cooperation in the EU, Computer Law & Security Review, Volume 32, Issue 4, 2016, [↑](#footnote-ref-6)
7. European Commission, A comprehensive approach on personal data protection in the European Union, Communication from the Commission to the European Parliament, The Council, the Economic and Social Committee and the Committee of the Regions, Com(2010) 609 final. Brussels, 4.11.2010. http://www.europarl.europa.eu/RegData/docs\_autres\_institutions/commission\_europeenne/com/2010/0609/COM\_COM(2010)0609\_EN.pdf [↑](#footnote-ref-7)
8. David Barnard-Wills, Vagelis Papakonstantinou, Cristina Pauner & José Díaz Lafuente, *Recommendations for improving practical cooperation between European Data Protection Authorities*, PHAEDRA Project D4.1. Brussels, London, Warsaw, Castellón, January 2017. http://www.phaedra-project.eu/wp-content/uploads/PHAEDRA2\_D41\_final\_20170114.pdf [↑](#footnote-ref-8)
9. Barnard-Wills, D., Pauner Chulvi, C., & De Hert, P. "Data protection authority perspectives on the impact of data protection reform on cooperation in the EU", *Computer Law and Security Review*, 32(4), 2016. [↑](#footnote-ref-9)
10. Fielding, N. & H. Thomas, "Qualitative interviewing" in G. Nigel (Ed.) *Researching Social life*, London, Sage Publications, 2001; Rubin, H.J & I.S. Rubin, *Qualitative Interviewing: The Art of Hearing Data*, London, Sage Publications, 1995. [↑](#footnote-ref-10)
11. Blakely, Ruth, Elite Interviews, In Laura Shepherd (Ed.), *Critical Approaches to Security: An introduction to theories and methods*, London & New York, Routledge, 2013. [↑](#footnote-ref-11)
12. Interviewed DPAs: Austria, Bulgaria, Cyprus, Czech Republic, Estonia, France, Germany (Niedersachsen), Germany (Schleswig Holstein), Hungary, Italy, Malta, Poland, Portugal, Romania, Slovakia, Slovenia, United Kingdom. [↑](#footnote-ref-12)
13. The remaining materials have not been analysed due to linguistic barriers. [↑](#footnote-ref-13)
14. These criteria were acknowledged by the majority of interviewees as an appropriate basis for analysis of training materials. See below, para 3.2.2.3. [↑](#footnote-ref-14)
15. The allocation of supervisory powers at national or subnational level depends on the legal system of the EU Member State, provided that also a national DPA exists in countries where such powers are devolved at subnational level. [↑](#footnote-ref-15)
16. On this, see the distinctions made above para 3.2.1. [↑](#footnote-ref-16)
17. SAP is a software that aims at facilitating organisations’ management of business operations and customer relations. [↑](#footnote-ref-17)
18. E.g., the ePrivacy Directive is undergoing a reform process that will probably lead to the enactment of an ePrivacy Regulation to complement and complete the GDPR regime in the online environment (see: ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation). [↑](#footnote-ref-18)
19. See above, para 3.2.1. [↑](#footnote-ref-19)
20. Ibid, p.25 [↑](#footnote-ref-20)
21. Clark, Ruth, "Accelerating Expertise with Scenario-based learning", Training and Development, January 2009. http://www.clarktraining.com/content/articles/ScenarioBasedLearning.pdf [↑](#footnote-ref-21)