**Working Notes for STAR D2.2 – report on the findings of the interviews.**

**27 April 2018**

**Substantive questions**

* What counts as a training material? Is a guidance document, info-sheet or copy-pasted Art 29 document? Even if it isn’t targeted at any particular audience? Is anybody actually *trained* by this?
* List of training materials might not just be topics (e.g. DPIA, Breach notification etc), but also scale and size of the delivery (e.g. materials on DPIA for small interactive classes, DPIA for large volume lecture class)
* Need to explore the possibilities of translation (particularly budget, which languages). .

From DPA interviews.

**Q.1 - what training do you offer…**

* Sheer variety of things (might be the way we asked the question)
* Some are limited to infosheets (“passive dissemination”) rather than training
* Some DPAs had more/new training activities planned for the future or as an ambition
* Split between planned/structured or ad hoc/bespoke/response activities
* General or focussed
* Quite a lot of participation in external events
* no real correlation with size: some small dpas do external training, other don’t, however i have the feeling that small dpas are in general more committed to dissemination events
* Perception of demand for training upon DPAs? But some focus only upon internal training (don’t feel compelled to train outside).
* Some DPAs still waiting on national implementation law, which will have impact upon their training activities and materials.

**Q2. to whom is training offered**

* internal/external
* public/private
* DPOs/Controllers role in company
  + Little mention about level in the company - e.g. CISO, CEO etc? [note this is a distinction for the DPOs]
* Specific sector - and some of this was a strategic (e.g. focus on specific industries, or public authorities).

**Q3. Scope of GDPR training…**

* All of them cover the general structure of the GDPR, for audiences with no idea or experience of the GDPR. Information on the website.
* Lots seem to focus on what’s new about GDPR from previous - new concepts, obligations, rights etc. [how this will this change in one-two years time? Or for trainees with no prior data protection experience?]. Fair amount of assumption that the audience had some knowledge of data protection.
  + New topics include DPIA, breach, sanctions, new rights, territorial scope, portability, right to be forgotten, definition of high risk.
* For some DPAs the scope is request driven (but not the majority).
  + But not necessarily very in depth into the specialist areas. [resource constraint]
* Inclusion of national law
* Nothing about operative dimensions - procedures - e.g. how do you set up a data breach notification systems [DPOs would love this]. Perhaps this has been left to the market (more philosophical question about the role of the DPA) - possible tension.

**Q4. type of training**

* (once we exclude the text on websites etc) its (nearly) all face-to-face workshops and conferences of varying scales.
  + (Bulgaria claims an interactive video).
  + Various DPA upload powerpoints used for other purposes.
* Big classes - for DPA around 30 people minimum to make it worthwhile [note - DPO may have very small classes, for example in a small company].
* [getting answers to different questions here]
  + General length of session
  + Complete training course vs one-off events.
* As a general idea, between 1 and 3 days.
* A week to become a DPO?
* Logistics - travel to take the course? Disruption to work day, flexibility of work role etc. - high dependent on audience.
* Lecture format seems very common, but some use more interactive methods
* Q and A seen as very valuable.
  + (have to anticipate what are likely questions from different audiences)
  + Requires certain capacity on the part of the trainer - requirement for experts in the specific field.

**Q5 – which three topics most important**

We can generate from these answers a prioritised list:

* Basics of GDPR including legal framework and key concepts
* Rights of the data subject (and their exercise) =
* Techincal and organisational requirements and measures for data security (inc anonymisation) =
* Role of the DPO =
* Data protection impact assessments
* Duties and obligations of controllers and processors =
* Data breach procedures and notifications =
* Basics theory and concepts and value of privacy /data protection =
* Data protection authorities roles and powers =
* Legal basis for the processing of personal data =
* Privacy by Design =
* National frameworks =
* Data protection register =

But there may be a more philosophical difference in what is seen as a priority

* Split between theoretical/conceptual focus
  + Overviews on the right of the data subject
  + Privacy as a value in corporate culture
  + Privacy by design
* and the practical aspects
  + DPIA
  + Data breach notification
  + Role/Duties of DPOs
  + Checklists (?)
  + Organisational and technical data security measure

[DPOs are, in comparison *extremely* practical, concrete stuff, forms, consent, procedure]

**Q6. - materials**

* Mainly PPT and manuals
* Infographics and checklists
* Very limited interactive materials.
* Case studies and collections of legal materials are ambitions

**Q.7 - feedback?**

* Highly variable, but standard questionnaire at the end is very common
* Small interactive sessions don’t bother with structured feedback.
* Didn’t seem like they were learning lots from their feedback - did they meet the needs?
* Weren’t able to given much advice on the basis of this - some desire for livestream or webinar.
* See the French answer if necessary

**Q.8 - Variety of training** level  [this question was tricky, sometimes misunderstood, answer may be biased]

* Sector based - raised as an alternate approach to topic-based.
* Audience wanting the materials for reference
* One DPA expressed the desire to basically have DPO able to answer the basic and common questions in the future.
* Some wanted to dispel myths about the GDPR

**Q.9 – desirable Length**

* Obviously variable, but generally the same as what they are currently offering (plus a little bit of desirable time).
* 1-3 days for courses and workshops
* Length of single module - webinar - 30+15Q&Q - single mo
* Italy is an interesting variation - few hours spread over time.

**Q.10 - According to your observations and expertise what would you suggest keeping in mind when preparing the STAR training materials?**

* Easily understandable - no legalese , or “decode” the legal (and IT).
* Separate materials for the general public or other audiences [contrast with STAR objectives]
* Disagreement over focus - some said not too focused and generally accessible vs others who want very specific, targeted to audience and in-depth. On balance seem to be more wanting targeted , specific training.
  + [reading between the lines, what they \*need\* is somebody to take on the things they don’t have time to do - researched and enriched  materials for specific situations and concepts - case studies, invented situations etc.]
* Disagreement in  need(please do internal training Vs DPAs already know everything)
* Can the content be re-used within organisations? E.g. by the DPO or other employees. [mainly tone/register/compexity]
* Practical approaches, examples, case, studies, solutions, directions to guidance, FAQ, templates, to-do lists etc.
* Need to consider the level of knowledge of the audience,
* New concepts may be difficult to cover in short, and generalised training
* Need to support discussions as these were seen as very valuable (maybe key questions, discussion prompts, exercises etc).
* F.A.Q - [STAR II as a source?]
* Consider what elements of training the market can’t provide - focus on rights and obligations, they can figure out solutions on their own? [to discuss further] .

**Q.11- 11. Would you be willing to test the training materials in actual training sessions (in later stages of the project)?**

n/a

**Q.12 - We aim at identifying best practices and evaluate existing training materials on the following criteria: comprehensiveness, suitability, coherence with the regulatory environment, delivery quality, certification, cross-border relevance, accessibility. Do you consider these criteria as appropriate for a proper assessment of best practices? Are there any other criteria you would recommend for consideration?**

* Generally fine with the criteria - some suggestions around thinking about language, suggestion that cross-border relevance might not be as important, and also consider time/length.

**Q.13 To what extent would DPAs need or could benefit from harmonised training materials?**

* Generally seen as a positive, but:
* Two big concerns
  + Language -
  + National law
* Nice idea, but not sufficient, because GDPR is not complete, they need national law and how can you tackle issues that are still not harmonised in harmonised training materials?
  + [probably statistically - go for scale and leave out the outliers]
  + Do DPAs know where they diverge from the EU “mainstream?”
* DPAs vary still
* National case studies and examples

**From stakeholders with training responsibilities interviews**

General considerations:

* Adapting to target audience comes up lots – classes easier to adapt that online courses.

Q1. Does your organisation provide some training on the GDPR now? If not, are you planning to develop training packages in the future? If yes, please describe the proposed structure and main elements of the packages.

* Some established training schemes
  + There are market providers
    - Targetted at companies' employees / private organisations / in-house training.
    - From inidividuals to global firms
    - Training schemes can be varied depending upon the client
  + (Some) organisations are also doing training internally and/or for subsidiary companies in corporate groups.
    - Focused upon their particular data protection issues either of the industry/sector or the particular teams to be trainied.
    - E.g data protection obligations for non-specialists
    - Training for leadership and management on their data protection responsibilites
    - Internal workshops
  + And some do both internal (compliance) training, and provide external training
  + Also non-profits producing training material
  + Many training schemes for general staff were identified as Introductory training, "the basics of the GDPR" or awareness raising
  + Courses for DPOs/Privacy officers exist
* Other planned programmes at various stages of readiness
  + Waiting on sectoral and national legislation
  + E.g. Ad hoc training with ambition towards a more structured scheme
  + Ambition (for some) to have all employees conduct the basic-level awareness training.
  + Schemes for DPO and auditors in development

Q 2. Does your organisation offer that training to everyone in your organisation? If not, who is the target audience (please define the audience and the reasons thereof)?

* Training delivered to
  + Executive level
  + Management
  + Operators in charge of data processing
  + DPOs (public and private)
  + Employees with other privacy-related or data processing roles
  + Everyone (either basic training/awareness or all employees in "data-intensive" organisation/industry)
* A relatively commonly reported pattern is organisations starting with targeted training internally (top management and DPOs), but then progressing to general training across the organisation. One respondent described attempting to role out training for employees with any involvement in data processing across a large organisation, but because of lack of capacity, this was rolled-back to mid-level data processors and management with decision making responsibilities related to personal data.
* General public (uncommon)

Q3. Please describe the type of training with special attention to its attributes, such as form of contact (online, face-to-face, etc.), size of groups, length of sessions, length of the whole training, evaluation process, further trainings, etc.

Formats include:

* Face to face classroom / seminar
* Webinar
* Pre-recorded training / video presentation
* Telephone training
* Larger scale event
* Combination (e.g. online foundation, then face-to-face practitioners)
* Supplementary written material
* On-the-job training/mentorship/review and quality control
* Simulated games
* Fact sheets

Lengths

* Classes - 1 day, half day, 4 hours, 2 x 1.5 hrs
* Webinars - 30-35 minutes (basic training for all), 1.5 hours
* Certification courses much longer – 5 days, with exam, 10 days

Participants

* 1 to 1
* 6-8
* 25-30 people
* Up to 100
* Group size dependent upon targets (see below), and numbers of a specific speciality within the organisation (e.g. how many in marketing? How many in admin?)

Other observations

* Several organisations structured their training so that executives, data specialists or management were more likely to have classroom/face to face training, with webinars available to the rest of the employees. The management sessions are likely to be somewhat longer than the general training, but with a limit to the amount of time that senior management (C-level) can devote to this.
* Acknowledgement that online learning is not as effective as F2F, but better than no training.
* Resource constraints identified as part of the reason for these choices (would use e-learning material if available).

4. What is the scope of the training you provide? What topics or issues do you cover?

* Split between general course for management and detailed training for particular operators on their duties. Also a similar split, but general for beginners, and then specialised training.
* Others however have gone more detailed for top managers and how this will change relationships to suppliers, partners etc, and what contracts/documetns need updated, whilst general staff have had a more general introduction.
* General course, then specific data handling model adopted by the company or otherwise adapted to the specific audience. (e.g. complaint procedures). Some training is entirely about the implications of GDPR for a businesses specific practices.
* Specific Topics mentioned
* Procedures to comply with new rights of data subjects
* How to use IT tools
* Why EU regulation is useful
* Legal basis / lawfulness of processing
* EU law
* Obligations for controllers and processors
* Innovations in the legal environment
* DPO
* Record of DPA activities
* DP in employment contracts
* Big data
* Data deletion
* Mobile device management
* SAP
* Direct marketing
* Principles
* Complaint procedures
* Data lifecycle management
* Data processing audit
* Regulatory and compliance gap analysis
* 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

Q. 5. What are three topics you consider most important for trainees?

Single prioritised list (with grouping of related topics)

* Organisational Procedures and data protection in practice
  + Forms
* General overview, definitions and basic concepts of GDPR
  + Principles of data protection
* Purposes and legal grounds for data processing
* Security and technical elements of data protection
* Risks and risk management
  + Sanctions
* Data breach notification and procedures
* Communication with the data subject and the customers's perspective
* Rights of the data subject
* Responsibility of the data controller
  + Accountability
  + Data registers
* Consent
* Data protection impact assessments
* International data transfers
* Privacy by design
* Contracts
* DPO role
* How to get a competitive edge from compliance

Q6. What kind of materials do you currently use for your training activities (slides, brochures, essays, books, case studies, legal materials etc.)? Would you be willing to share with us some of your current training materials for best-practices-identification purposes (even materials addressing the directive)?

The following materials were reported as being in use

* Slides of presentations
* Handouts
* E-learning courses
* Text of the regulation
* Documents from national DPA
* Documents from Article 29 Working Party
* Video
* Books/handbooks
* Online knowledge centres and databases (for large law firm)
* Wiki
* Research studies

Most commercial respondents were unwilling to share their training materials with STAR.

Q7. Do you gather feedback on your training courses or training materials? How do you gather such feedback (e.g. online questionnaires, paper questionnaires, e-mail)? Based on the feedback you’ve received, what do you think would be the most effective way to provide training (e.g. webinars, videos, workshops, online courses, etc.) What types of materials would you create?

Types

* Feedback of some sort pretty common across those interviewed.
* Commonly an end-of-course or end-of-session questionnaire to monitor quality – e.g. evaluating the trainer, the course materials and including venue/location, either paper or online.
* Smaller (individual) trainers operating on informal feedback directly from participants
* Others more structured format, collected and processed by HR (not run by the trainers for their own purposes)

Things learnt

* People do like face to face, and trainees prefer personal contact
* Webinars possibly hyped (distractions, lack of attention, "multi-tasking"). Good for "common language" but not the best way for developing advanced knowledge.
* E-learning ok for measuring training (e.g. quiz/assessment).
* Case studies have traction
* Workshops strong for practical training
* Mix of materials is a strength, including reading materials with detail information on the topic.
* Some scepticism that lengthy written materials ever get read.

Interest in developing

* Videos with operative content and practical examples– e.g. how to manage right of access or codes of conduct.
* Tutorials covering the implementation of the GDPR across the EU.

8. What variety of training level do you consider appropriate (e.g., general overviews vis a vis specialised training on selected issues, etc.)? Why?

* Many start with general overview, then move to specific issues or tailored to industry sector or corporate function/business unit.
* Training levels are broken down in several ways
  + The general training may be delivered to any type of trainee, specialised to particular roles (including data protection specialist/DPO).
  + Top management and DPOs may received specialised training different from general employees.
  + Employees with data protection-related roles (involved in processing or accessing personal data) may receive different training from other staff.
* The general training may include specific issues at higher level of resolution because they have been identified as a priority for that organisation (e.g. going into more detail on data breach identification and notification procedures)
* Trainers do not want to do away with the general elements because they feel it is an important precursor to specialised training, and for holistic understanding.
* Others (claim to) entirely tailor based upon the client's needs
* Specialised training can be VERY specialised (e.g. the data protection issues involved in a particular employees day-to-day tasks). And/or can include sectoral legislation other than the GDPR.
* Also some focus on "new and emerging issues in data protection"

Q 9. How long do you think training sessions should last (e.g. an hour-long webinar or a half-day workshop)? All acknowledge that training session length varies, but clustered around:

* "full" Courses – up to a week
* Workshops/seminars – 2 or3 hrs - 1 day, (modules not longer than ½ day) (no longer than 7 hours). Half a day was fairly common.
* Webinars – 1 – 1.5 hours
* E-learning – can be many hours (equivalent to full courses, but can be split up).
* Execs – 30 minutes

To consider

* Longer for more "complicated" topics
* General confidence that you can do basic awareness training in/under an hour (but this doesn't provide the knowledge to actively work with the GDPR).
* For F2F courses, participants travel – suggests 3hr not enough, 2 days too much.
* Suggestion that recurring but shorter is better than "fit all into longer session"

10. Are you aware of any other organisations offering training on the GDPR? Is it free or does it cost?

* Respondents knew about several other organisations offering training, as well as organisations developing their in-house training. There are understood to be lots of sources of general training on the GDPR, but that this doesn't always fit the needs of a particular organisation or industry sector. This market is seen by some to include low quality training (as well as high quality).
* Free training that exists is seen as poor quality, superficial (can do it yourself), doesn't result in certification (seen as less useful?), or is offered by lawyers/DPO as loss-leader (or free initial general training followed by charging for specialist work).
* DPO associations not providing much training
* DPO course costs 12-1500 Euro
* Desire for free training from the DPAs or the EC

11. According to your observations and expertise what would you suggest keeping in mind when preparing the STAR training materials? [largely direct quotes]

* "practice cannot be forgotten based on simple theory." And " It is important that the material shall contain information that are important and useful in everyday use, not only the general explanation of the GDPR."
* It is necessary to pass the message that GDPR is a complex management system and needs a multidisciplinary approach.
* one should develop materials on DPIA without reducing it to a mere exercise of cybersecurity. Everyone focuses on that but it is instead also a cultural thing, as we must talk about the risks to rights and freedoms
* most important is to keep it as short and simple as possible and to focus on why it is important to behave in a compliant way in a company.
* It is not only substantive training, but also a cultural thing
* even elearning in a complex group is difficult to cover all aspect and you risk to be too basic, so my recommendation is to focus and building a generic common sense ands a common language,
* create a methodological franework on how to conduct a DPIA and so on
* easy and multichannel
* real case studies,
* Q&As,
* practical FAQs on real issues such as data deletion and on misleading situation such as multinational companies
* slides is first, textbook is optional. The problem with slides is that trainers are different but you have to provide a good level of background information in addition to the slides because otherwise trainers may be in difficulty. Like comments to the slides in the notes and so on.
* have to clearly split the topics and do not do a mix
* language, examples, diagrams and examples,
* try to tailor also big companies in the examples, not only flower shops, but also the big things.
* Keep the legal to the minimum
* It would be really useful to have some best practises and examples in the training material.
* keep in mind, above all, the practical feasibility of the training materials.
* welcome materials providing guidance as to the unified application of GDPR
* some resources where professionals may find widely accepted and EU-wide applicable opinions, guidelines, land-mark authority and/or court decisions, template notices, and sample registers etc.
* New things coming with the GDPR are necessary and maybe its effects for certain organizations.
* Examples from practise would especially good, e.g. about the accountability principle.
* emphasizing the important parts could be good, e.g. data breach which is only a few articles in the GDPR, but very important.
* to not only put it on English but translate it also to other EU languages. Own language would be much easier.
* Include "fake cases" – e.g. a data breach, international cases, a decision about if a DPIA is necessary or not.

Q12. Would you be willing to test the training materials in actual training sessions (in later stages of the project)?

Universally yes (although some noted that it would have to be in their language)

Q16. As I mentioned at the beginning, the EU is funding the STAR project the aim of which is to develop training materials that DPAs and DPOs can use in providing training to their stakeholders. To what extent would DPAs need or could benefit from harmonised training materials?

Benefits

* Broad support for the concept – useful, added value, given the "point" of the GDPR to harmonise – contribute to uniform application, increase unified understanding of the GDPR.
* Several DPAs not able to develop training materials or procedures. Harmonise training lowers risk to DPAS
* Could help to fill gaps in codes of conduct and procedures
* DPOs sometimes have difficulty finding material.
* Should be adaptable to needs of trainers/trainees

Issues

* National law cannot be neglected
  + This may be particularly significant for specialised knowledge
  + Perhaps better as awareness tools (general knowledge) and Include disclaimer about not taking into account national specificities.
* Language barrier too big if the slides are only in English
  + (Even in countries like Sweden where English proficiency is high).
  + Demand for drafting in all EU languages
  + Reduced number of languages may be ok, but the more the better (check biggest market and degree of internationalisation).
* For face-to-face training the capacity, cultural background of the trainer will be very important and influence how the training is delivered.
* Tailor to particular sectors in order to be effective. (but attendees should have a grasp of general concepts and why the GDPR exists).