Upgrading the EU Data Protection Sector with new skills

Co-funded by the
Erasmus+ Programme
of the European Union

# D2.3 State of the art comparative analysis

WP2. Design or improvement of a joint qualification in VET

Project No: 597857-EEP-1-2018-1-EL-E 597857-EEP-1-2018-1-EL-EPPKA3-VET-JQ

Co-funded by the Erasmus+ Programme of the European Union

## PROJECT INFORMATION

| | |
|---|---|
| Project Acronym | DataPRO |
| Project title | Upgrading the EU Data Protection Sector with new Skills |
| Agreement number | 2018-1737 / 001-001 |
| EU programme | ERASMUS+ KA3 Support for Policy Reform |
| Project website | www.datapro-project.eu |

**PREPARED BY**



| | |
|---|---|
| • Authors | ReadLab |
| Date | August 2019 |
| Approved by | AMC |
| Version | Final |
| Dissemination Level | Public |

# Executive summary

This report refers to the training needs analysis for Data Protection Officers (DPOs). In this context a field research was conducted in Cyprus, Germany and Greece consisting of:

- An online survey targeting DPOs and experts as well as employees involved in data protection processes in their organisation.
- Focus Groups targeting different sectors including Banking and Health sector
- Interviews with experts, DPOs, and trainers.

The research findings are presented in this report with a view to:

- Understand how the data protection and privacy environment is being shaped investigating needs and challenges of public and private organizations.
- Focus on skills gaps and mismatches between Data Protection Officers (DPOs). Examining the views of experts regarding missing skills, importance of specific or what skills are currently needed the most, is a necessary step towards designing an innovative DPO Curricula.
- Acquire a deeper knowledge regarding existing training courses, identify best practices and areas of improvements.

The EU GDPR is a tough privacy and security law in international level. It is large, far-reaching and fairly light on specifics making it hard to be put in effect especially for small and medium-sized enterprises (SMEs).

GDPR continues to be interpreted and this results in **uncertainties on reaching the desired level of implementation**. Measures are taken and business and reporting processes are restructured but the prevailing impression it that this is not enough.

A lot of participants identified the need of not only adjust current processes but also introduce new ones with a different mindset: **Data protection by design** i.e. considering personal data protection issues **upfront in every activity**.

Based on the collected information, it seems that the topic is more mature in Germany compared to Cyprus and Greece. Greece and Cyprus are in initial stage and the focus is on the appropriate interpretation of GDPR rules and obligations.

In a nutshell, data protection is in its early stages in the private and public sector. Especially, for private companies and SMEs, data protection and privacy teams are understaffed or underfunded. In other words, data protection is not highly prioritized in the TODO list and it seems that they just beginning to grapple with GDPR compliance.

Concerning skills demand and skills gaps, the timely implementation of the DataPRO initiative and the innovative topic steered the discussions and shed light to different areas.

Although the main finding, as anticipated, was that **both a legal and IT background** is needed it was explicitly stated by the majority of participants that this is not enough. The main takeaway of this research is the **multidisciplinary perspective** of the DPO role.

Soft skills including **communication and analytical or problem-solving skills** were identified as must-have for a person with DPO role. Experts and DPOs went a step beyond and accentuated the **project management abilities** an efficient and productive DPO should demonstrate. Being able to request, marshal and lead the involved persons in order to carry out their tasks and duties are considered the most important competences. The major missing skill is the lack of practical knowledge.

The most substantial finding regarding training needs and provisions is that more practical and/or "hands-on" trainings are needed by the market. Considering the huge variety of jobs and tasks that fall under the privacy rubric, it's impossible to deliver the necessary trainings in a one stop manner. The wide scope affects both the scope of the training material and delivery methods from a curriculum design perspective.

The most important point that emerged for a DPO training curricula is the need to embed practical trainings with the use of test cases, real-life scenarios, team assignments, etc. It seems that the first cycle of getting familiarized with the topic is ending. More hands-on approach is needed in favor of handbooks or static presentations. In addition, delivery methods including Work-based learning should be encouraged. Internships or mentorships along with effective evaluation strategies can offer the so much needed "inside look".

Finally, the structure of related training courses should be **hierarchically designed** consisting of relatively **small and potentially independent modules** or entities of knowledge in terms of hours of effort needed offering more flexibility when a call for update is needed or decided by the training authority. While this is a challenging requirement during the curriculum design process, it will certainly facilitate the foreseen training content and material updates.

# Contents



# List of figures

# List of tables

# 1 Introduction

The following report is developed based on a detailed Quantitative and Qualitative field research which was conducted by the members of the DataPRO consortium. The analysis is based on the guidelines and project description of the DataPRO project application. The main goal is to acquire a deeper knowledge on the sector by analyzing the views of data protection experts, Data Protection Officers, employers and employees who are involved in collecting, storing and processing personal data.

The retrieved information and results are analyzed in detail in order to draw conclusions based on the opinions and views of the DataPRO research participants. The methodology adopted, is described on the **D2.2 Terms of Reference** and its main tools are questionnaires, Focus Groups and interviews.

The areas of interest, as they have already been identified in the project's detailed description, are:

- Analyze the data protection and security area in terms of **needs, challenges and changes** raised from the General Data Protection Regulation (GDPR). Since the regulation was put into effect on May 25, 2018 and it imposes obligations onto organizations targeting or collecting data related to people, it is important to identify how the overall environment and sector dynamics are is being shaped.
- Focus on **Data Protection Officer skills**. The objective here is to analyze potential skills gap and conclude on the needed and missing skills.
- Examine the opinions of participants regarding current professional trainings and analyze their views regarding what is missing, how training should be delivered and what are the training areas that should be prioritized.

This analysis is structured on a country level followed by a final summary and synthesis subsection where the key conclusions and key points are described.

# 2 Methodology

The quantitative analysis has been implemented in Cyprus, Germany and Greece. The target group included a diverse range of professional working in data protection elated professions or roles.

The survey questionnaire was implemented online through the eusurvey tool [1]. The consortium disseminated the survey through their well-established network and communication channels and the result was approximately 300 participants. The online version of the questionnaire can be found here: **https://ec.europa.eu/eusurvey/runner/DataPROSurvey2019.**

The structure of the survey was mainly based on closed-ended questions having as available options Yes/No or scores within a scale from 1 to 5. The aim was twofold: First, be able to acquire a significant amount of information in a relative quick and efficient manner and second, be able to conduct comparisons on a numerical scale and identify possible differences in responses, potential common trends and underlying patterns.

The quantitative results are then compared to the results of the qualitative research towards a more representative study with a view to identify common skills and competences for Data Protection Officers and understand what is needed in terms training curricula.

The analysis of the online survey is structured around the following key areas:

- Participant's demographics and profile
- Impact of GDPR and level of preparedness in individual and organizational level
- Skill gaps and needs for the DPO role
- Training needs

In the DataPRO qualitative research, focus groups and interviews were used as the main data collection methods in Germany, Greece and Cyprus. Focus groups and interviews were semi-structured e.g. they consist of several key questions defining the same area of interest as in the online survey. This format provided the participants with some guidance on what to talk while allowed both the moderator and participants to diverge in order to pursue or follow up an idea or view in more detail.

[1] https://ec.europa.eu/eusurvey/home/welcome

# 3 Quantitative research – Findings from the cross-national survey

## 3.1 Participant's Demographics and Profile

Characteristics of the responders are used as a basis for conducting basic comparison analysis and understand the different views due to different profiles e.g. how their field of expertise affect their answers. The related screening questions include:

- Age Group
- Category that best describes the current professional level
- Gender
- Country
- Working as Data Protection Officer

The analysis by default presents the findings per Country. When a hint or an abnormal pattern/outlier is found, the analysis goes to a deeper level comparing results between DPOs and persons that occasionally or partially are involved in data protection tasks during their everyday tasks i.e. the Non-DPOs.

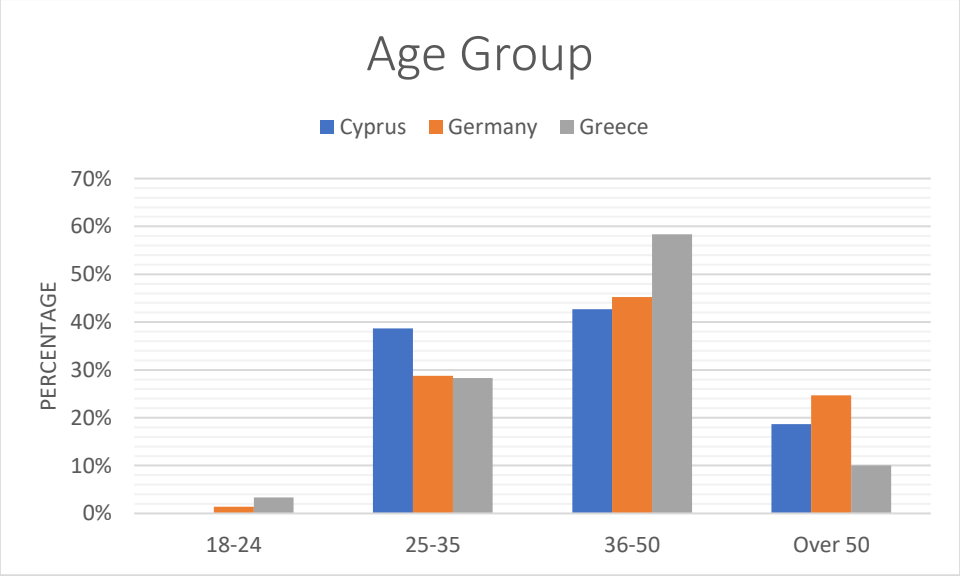


*Figure 1 Age profile of the participants*

Most of the responders fall into the 36-50 age group; a common observation in the three respective countries. The main key points regarding the age group distribution of the responders are:

- The Over 50 age group reaches a top figure of 24,66% in Germany while in the other two countries is significantly lower (18,67% for Cyprus and only 10% for Greece)
- The 18-24 age group is not represented at all in Cyprus.
- The 36-50 is the dominating category for all three countries.

In general, the survey answers do not represent the view of students or young people who are at the beginning of their career.

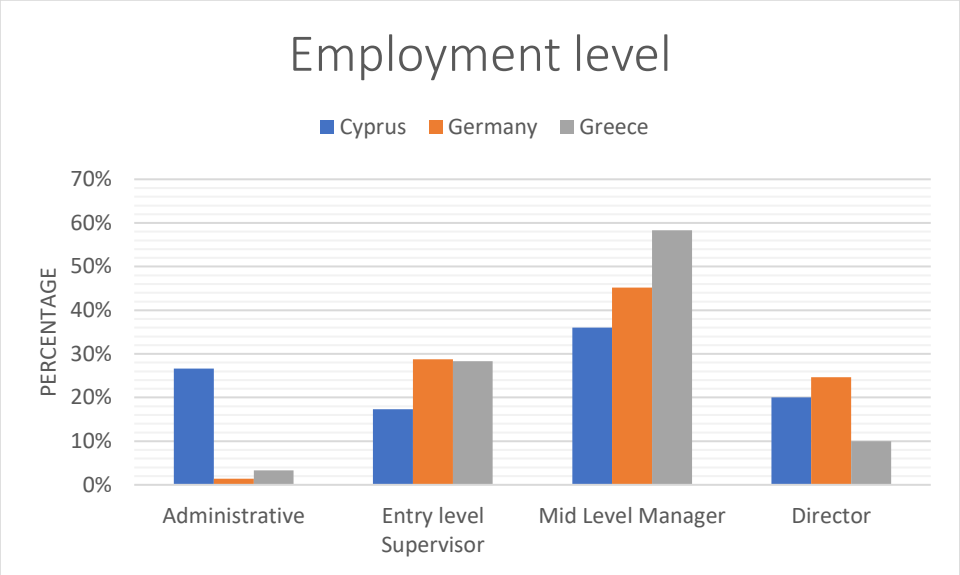


*Figure 2 Employment level of the responders*

Regarding the employment level, there is a dominant pattern: Most of the responders are mid-level managers, then entry-level supervisors, directors and finally the smallest share goes to administrative staff. The outlier found here was in Cyprus, where there is a spike in the responders that stated that they work as administrative staff (27%). Therefore, the audience from Cyprus is slightly different and more equally distributed compared to Germany and Greece where Mid-Level Managers hold the largest share (46% and 58% respectively).

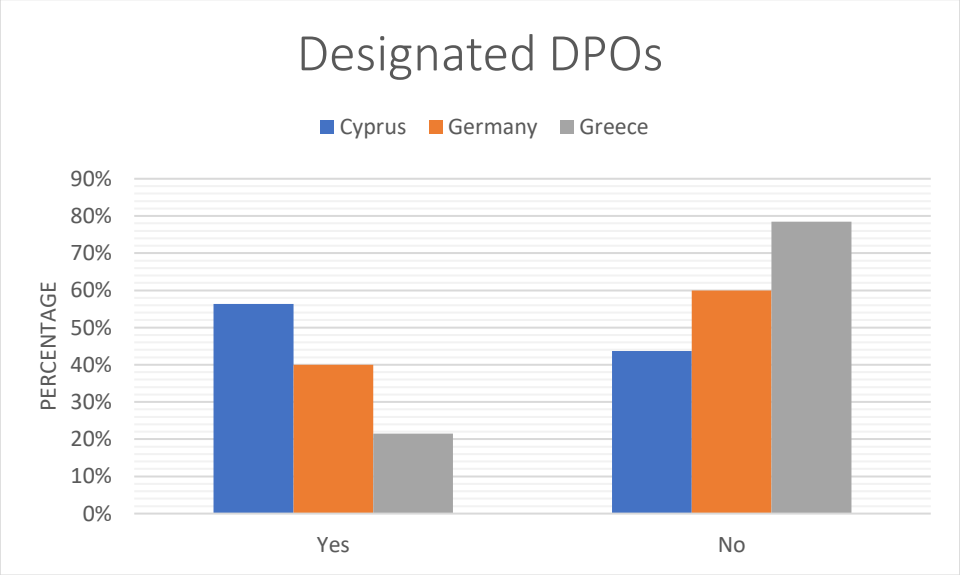


*Figure 3 Percentage of responders having the DPO role in their companies/organisations*

In Cyprus, the majority of the responders stated that they are the designated DPOs in their organization (56,34%) while the trend is different in the other two countries: in Germany 40% and in Greece only 21,51% stated answered as official DPOs.

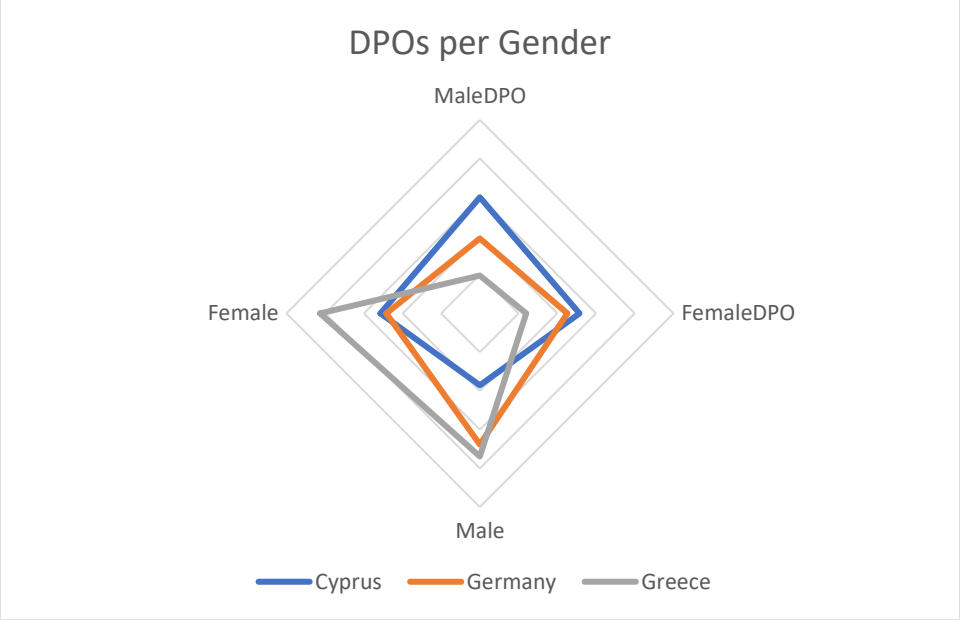


*Figure 4 DPOs per Gender*

The survey participants are equally distributed regarding their gender (49.4% are male).

- In Cyprus, most responders were male DPOs (30%) while the minimum share was that of male responders that are not the designated DPOs in their organization (18.57%)
- In Germany, the sample is quite balanced (maximum share for non-DPO males at 33.87%, minimum share for male DPOs at 19.35%)
- In Greece male and female percentages follow a balanced pattern and no outlier is found.

In general, men and women DPOs follow a balanced distribution among the three countries (Cyprus: 30% male DPOs vs 25,71% female DPOs, Germany 19,35% vs 22,58%, Greece 9,78% vs 11,96%).

The survey targeted officially assigned Data Protection Officers or people who perform data protection related tasks in their work environment i.e. Non-DPOs. Thus, the responses and their analysis are based on real-world observations incorporating empirical data.

In general, the audience is quite representative in terms of age and gender with one exception: Age group 18-24 is underrepresented. On the other hand, participation of experts and DPOs is adequate and the respective variable can be used for parametric analysis. The validity of results is also supported by the fact that the questionnaires collected were fully completed. Since the questions were optional, this was a good indicator that the structure and the content of the questionnaire was easy to interpret and complete.

## 3.2 GDPR: Impact of change and levels of preparedness

The first set of questions in the survey aimed at discerning the big picture. More specifically, the participants were asked to express their opinion regarding their level of preparedness and to assess how much they have been affected in their everyday duties by GDPR enforcement. Finally, they expressed their opinion regarding the effect in organization level coming from the application of GDPR.

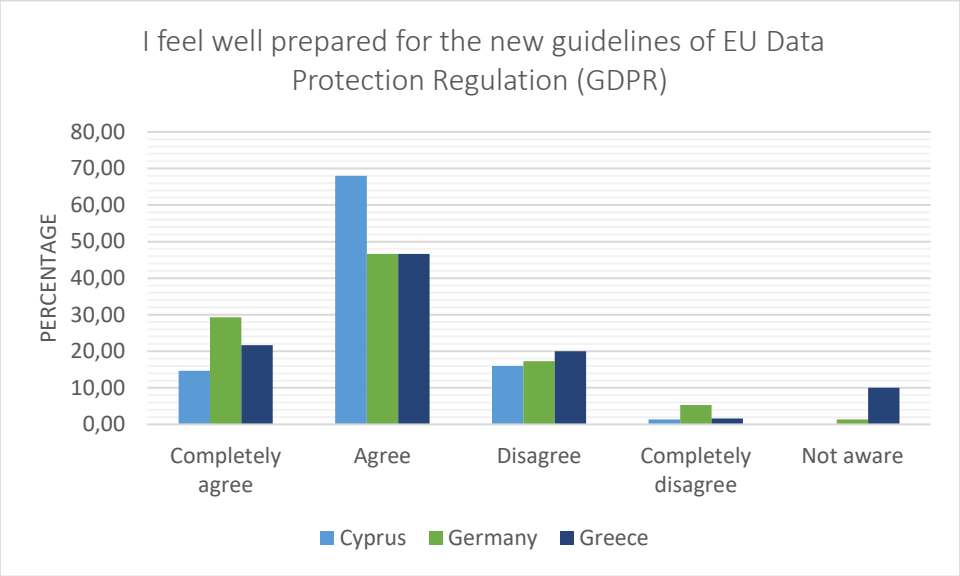


*Figure 5 Opinion question on the Preparedness level for the new GDPR guidelines*

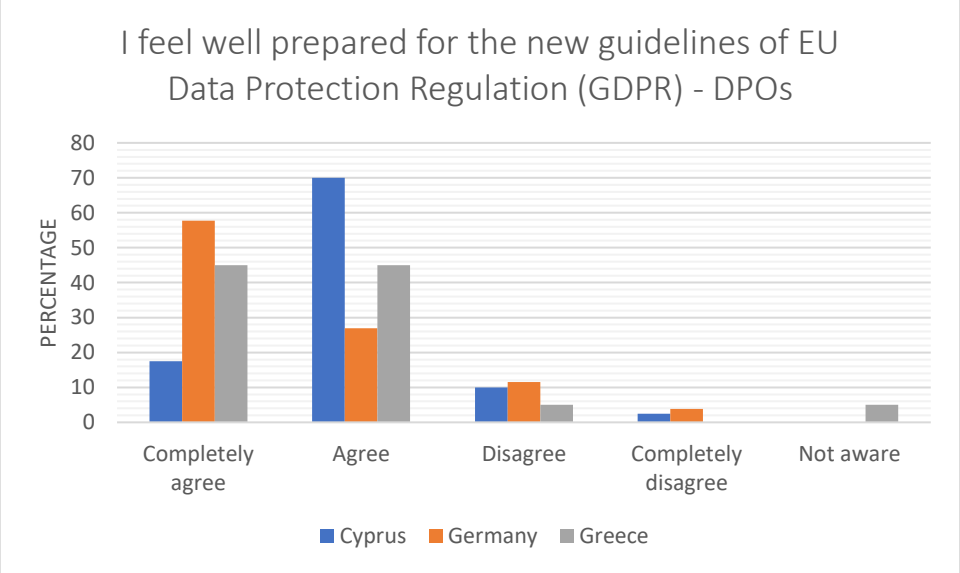


*Figure 6 Opinion question on the Preparedness level for the new GDPR guidelines – answers from DPOs*

Concerning preparedness level, the dominant trend is that positive opinions received the largest share (Cyprus 83%, Germany 76% and Greece 68%). Looking into answers coming only from DPOs, the trend is the same with percentages being larger as expected. Greek DPOs responded with the impressive 90% which is the biggest number compared to the other two

countries. It seems that German and Greek DPOs feel quite confident about their level of preparedness since the *Completely Agree* option outperforms the *Agree* (58% vs 27% for Germany and 46% vs 44% for Greece.

Participants are optimistic and feel well prepared.

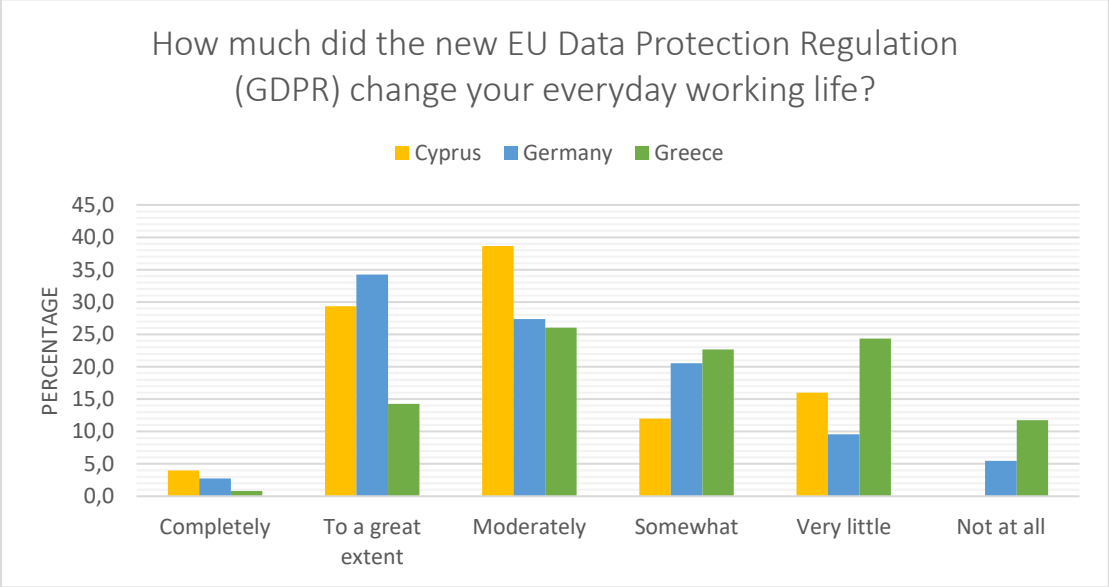


*Figure 7 Changes in duties and tasks in everyday work*

The working life of the responders has been affected in terms of tasks and duties but there are deviations per Country. Positive values (*Completely*, *To a great extent*) from Germany reached 37% and from Cyprus 33%. Greece on the other hand, seems to follow another pattern: Only 15% were positive answers. This is possibly due to the lack of implemented measures and the implementation of rules and processes at technical or operational level. The almost 12% percentage of the *Not at all* option, is a strong indication that the conversation related to GDPR realization is basically in theoretical level compared to Cyprus and Germany.

The findings are identical with the ones mentioned above when looking into answers from DPOs.

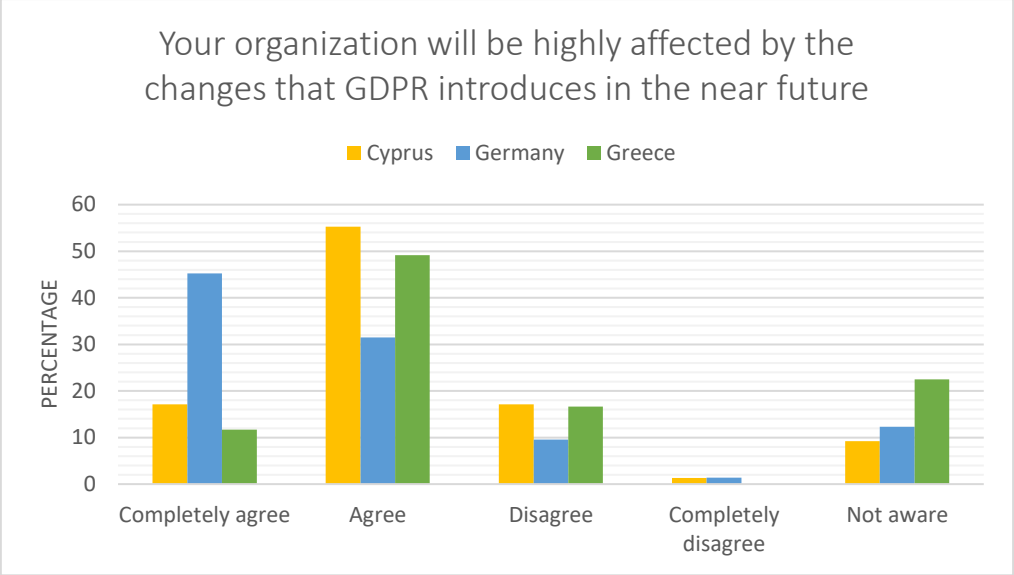


*Figure 8 Changes introduced by the GDPR adoption on organizational level*

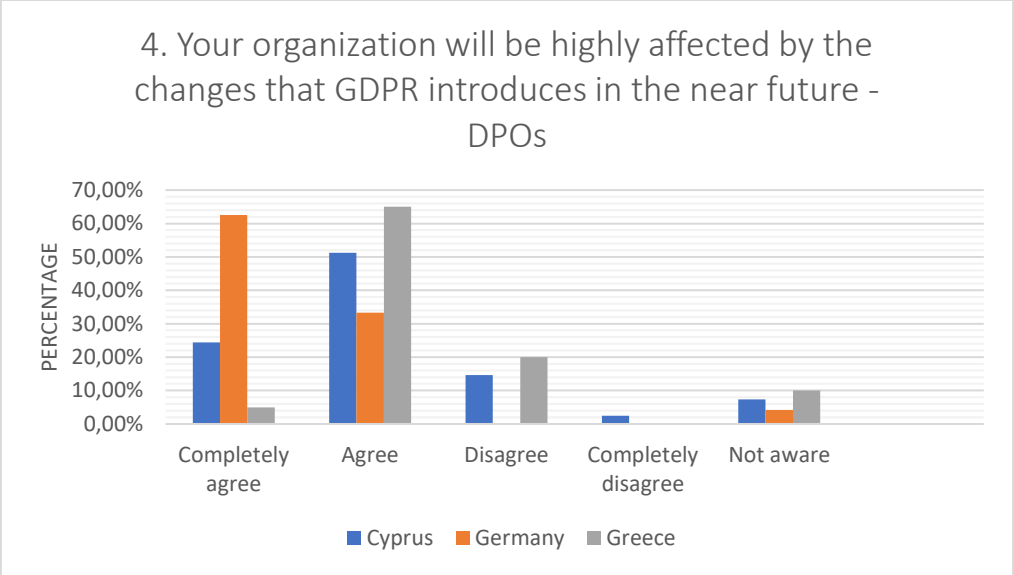


*Figure 9 Changes introduced by the GDPR adoption on organizational level – Answers from DPOs*

The survey subsection ends with an opinion question on organization level. Again, Cyprus and Germany are in the same page compared to Greece: 78% and 72% positive answers for Cyprus and Germany respectively, while Greece reached a 61% percentage. At the same time the *Not aware* option received an impressive 23% in Greece.

This is in line with the findings from the previous questions from a country point of view: Although the common identified trend is that organizations will be highly affected in all three Countries, in Greece this statement was expressed with substantially less positive values implying that the topic of GDPR compliance is less mature.

This finding is also demonstrated when taking a closer look in responses from DPOs. The responses are more aligned here and the positive values exceed 70% per country: Greek DPOs have an important differentiation on this issue from Greek non-DPOs.

Germany reaches 96% in positive values, with the 63% choosing *Completely agree*. This strong statement by the German DPOs shows their practical involvement in implementing related measures and rules compared to the other two countries. In a nutshell, DPOs feel well prepared and they are quite certain about impact and effects rising from the GDPR implementation, which was an anticipated result.

The general picture regarding the impact of the GPDR compliance and the preparedness level is that German participants feel more certain regarding their level of preparedness or the fact that changes are needed. This is also in line with the findings of the qualitative research where Germany seems to be more mature and having entered an "optimisation" stage. Cyprus and Greece are more on a theoretical perspective: people understand that changes will have to take place, but they are uncertain on what, how or when this is going to happen.

## 3.3 Skill gaps and needs for the DPO role

The next set of questions aimed at exploring the views of the respondents on the skills that are necessary for Data Protection Officers and to identify the skills that are lacking. More specifically this section aims at assessing:

- The importance of soft skills for the DPOs
- The Importance of specific skills tailored to the DPO tasks
- The importance of specific must-have competences including credibility, data processing awareness, and ability of performing Data Protection Impact Assessments (DPIAs).

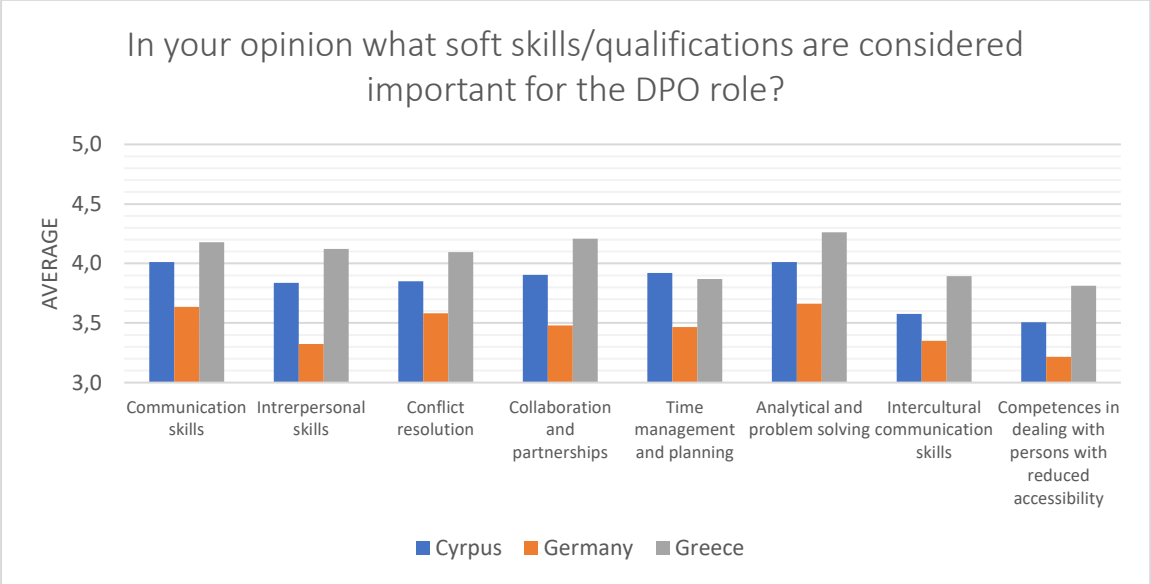


*Figure 10 Importance of soft skills of a DPO*

Responders were asked to assess a set of predefined soft skills in a range from 1 – not important to 5 – very important. According to responses the key findings are:

- Cyprus favors as top soft skills *Communication skills* and *analytical & problem-solving skills* while the lowest scores go to *Competences in dealing with persons with reduced accessibility* and *intercultural communication skills*.
- Germany favors as top soft skills *analytical and problem-solving skills* along with *Communication skills* and *Conflict resolution* while *interpersonal and intercultural Communication* skills get the lowest scores.
- Greece, like Cyprus, prioritizes the same soft skills while *time management and planning* are last in the list.

Therefore, communication and analytical or problem-solving skills can be characterized as "must have". These findings are based on mean values of the survey population. The following table displays the standard deviation values per country for each response.

| Soft Skills | STD Cyrpus | STD Germany | STD Greece |
|---|---|---|---|
| Communication skills | 1,09 | 1,48 | 0,97 |
| Intrerpersonal skills | 1,14 | 1,32 | 0,94 |
| Conflict resolution | 1,18 | 1,38 | 1,00 |
| Collaboration and partnerships | 1,15 | 1,17 | 0,86 |
| Time management and planning | 1,10 | 1,24 | 0,96 |
| Analytical and problem solving | 1,14 | 1,31 | 0,91 |
| Intercultural communication skills | 1,11 | 1,20 | 0,98 |
| Competences in dealing with persons with reduced accessibility | 1,09 | 1,48 | 0,97 |

*Table 1 Standard deviation values on soft skills question*

The standard deviation is the square root of the variance and expresses the variance in the responses. The larger the standard deviation for any dataset, the more the data are spread out from the mean. The smaller the standard deviation, the more tightly are the individual data points clustered around the mean.

A comparison on a country level reveals that Greece has the lower standard deviation values, Germany the largest ones while Cyprus lies in-between. This implies that the scores of Greek responders are more robust, or the majority of the population voted the same way. In Germany this is probably due to the wide nature of the named skills, e.g. Communication skills is a very broad term and may be mistreated.

Selecting answers coming only from DPOs, the picture is slightly altered. *Time management and planning* in Cyprus, *collaboration and partnerships* in Germany and *Conflict resolution* in Greece are entering the top list. This finding based only on the experts' opinions, highlights the strong project management perspective that each DPO should have.

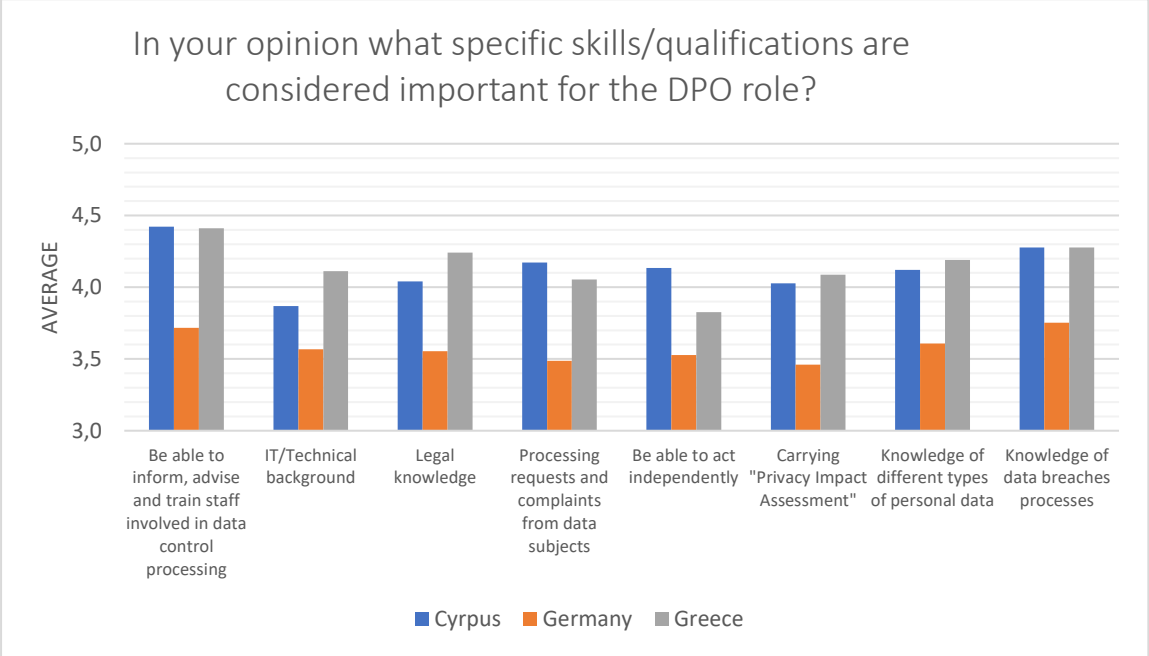


*Figure 11 opinion on importance of specific skills for DPOs*

Going a step deeper in the skillset and competences needed, the answers are totally inline between the three countries. Responders from Cyprus, Greece and Germany identified the same top two specific skills/competences:

- Be able to inform, advise and train staff involved in data control processing
- Knowledge of data breaches processes

This was actually a non-anticipated result. Promoting *being able to inform ,advise and train involved staff* against specific DPO competences like *being able to carry DPIA* or *Knowledge of different types of personal data*, highlights that all employees in an organization need to be in the same page and have basic understanding on how data protection rules, measures or processes are being implemented. In addition, this finding also implies that being GDPR compliant in organization level, is not a task for one person and this seem to be acknowledged by the survey participants.

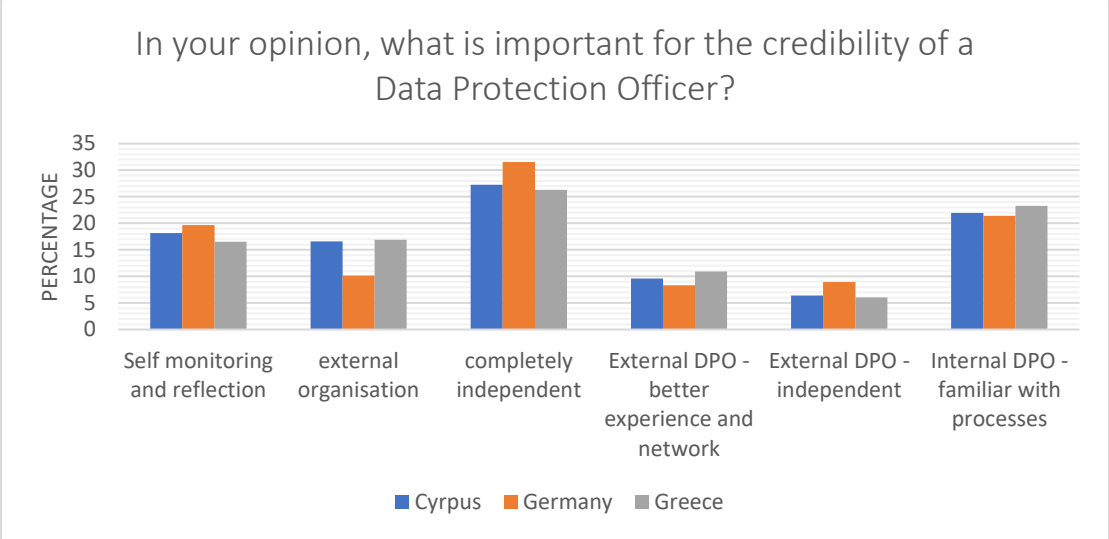


*Figure 12 Importance of parameters affecting credibility of a DPO*

Credibility of DPOs is a sensitive issue and may be affected by several parameters. The participants could select more than option in order to acquire some meaningful insights apart from the straightforward and much anticipated answer: *Completely independent*. So, it is important for the credibility of a DPO to be completely independent, but working as external or internal DPO?

The results show that the basic trend is to favor Internal DPOs rather than external ones even if the call is for credibility only. It seems that knowing internal processes is an asset that provides in credibility more than being an outsider. A possible explanation here may be the complex implementation of confidentiality rules in case of outsourcing the service.

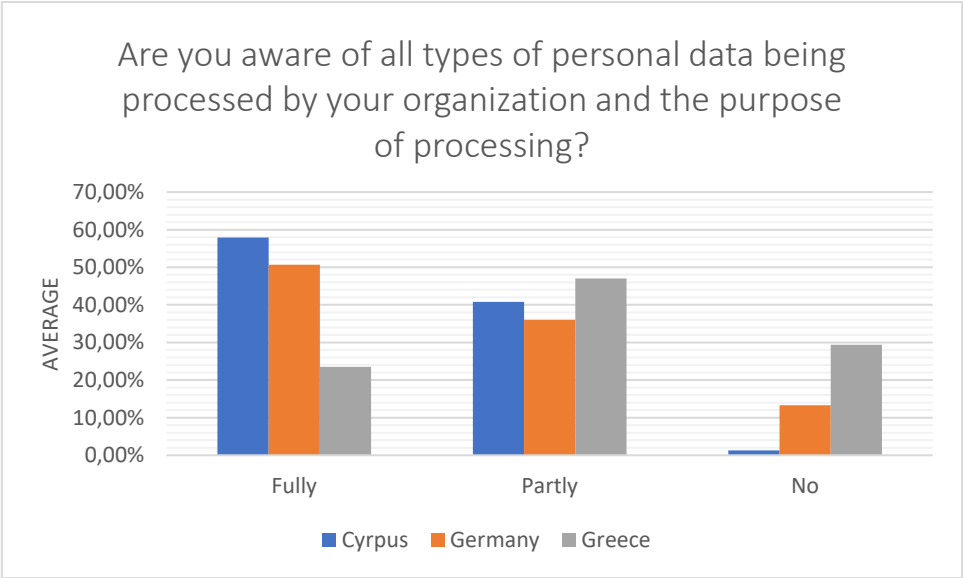


*Figure 13 Awareness on types of personal data*

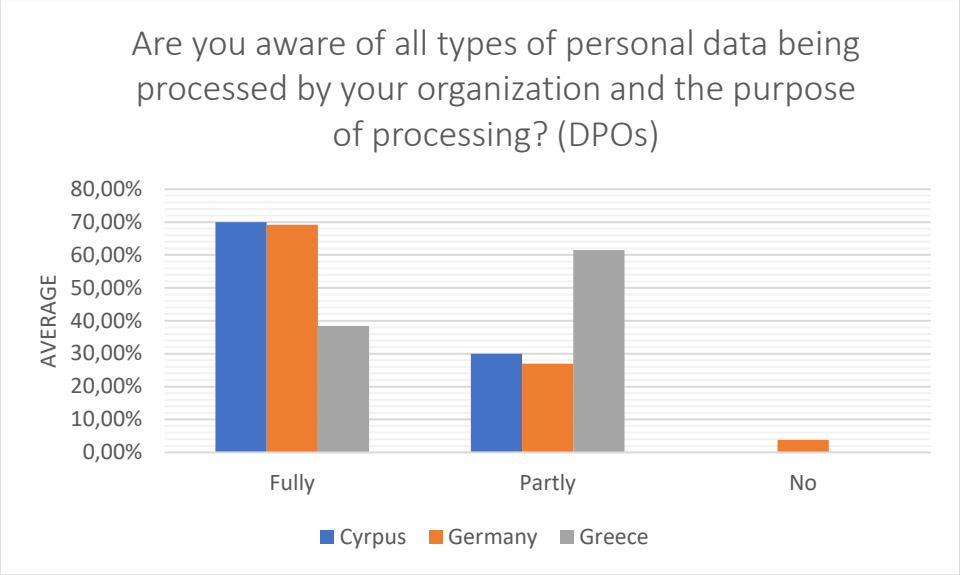


*Figure 14 Awareness on types of personal data – Answers from DPOs*

Awareness of types of personal data processed by an organization is a core knowledge towards efficient implementation of GDPR processes. Responses from Cyprus and Germany had more positive values – *Fully* - while from Greece the largest share belongs to *Partly* answers. Again, the totally negative value – *No* – gets the important 29% in Greece. This was the hint to investigate answers coming only from experts examining if this was actually a dominating trend in Greece.

Answers from DPOs were the anticipated ones as *No* answers were not given (In Germany there was a *No* answer from one DPO, but from a statistical point of view, it cannot be evaluated). Again though, Greek experts had the largest share in responding *Partly*. Given that this is a very clear and practical question, the finding implies that from a practical or operational point of view no actual measures or processes have been put in practice in Greece compared to the other two countries.

Finally, the differences in responses between DPOs and involved employees answering Fully is not so large: 70% vs 58% for Cyprus, 69% vs 51% and 65% vs 24% for Greece which is the identified outlier. The findings uncover the largest deviation of answers between Germany and Cyprus compared to Greece throughout the whole survey.

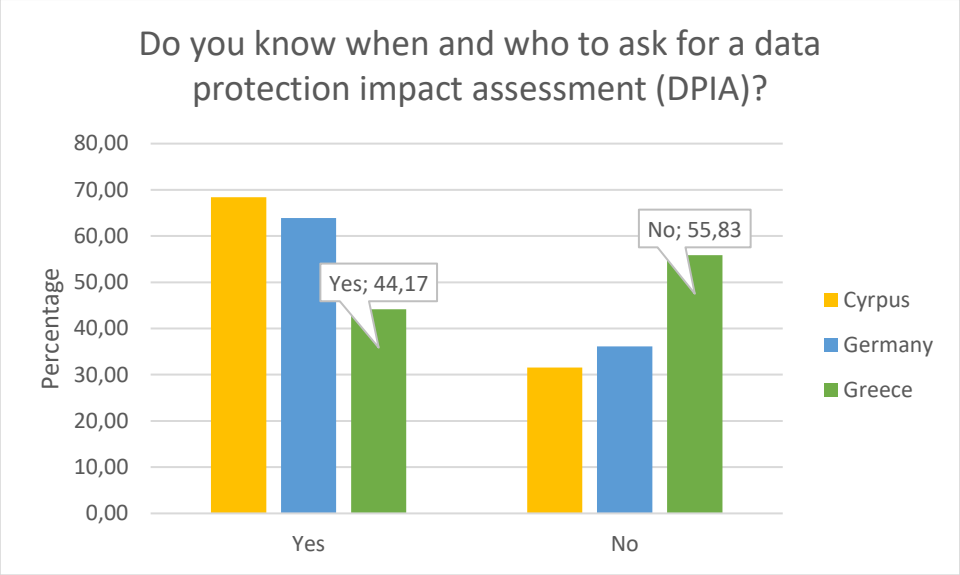


*Figure 15 Knowledge regarding DPIA*

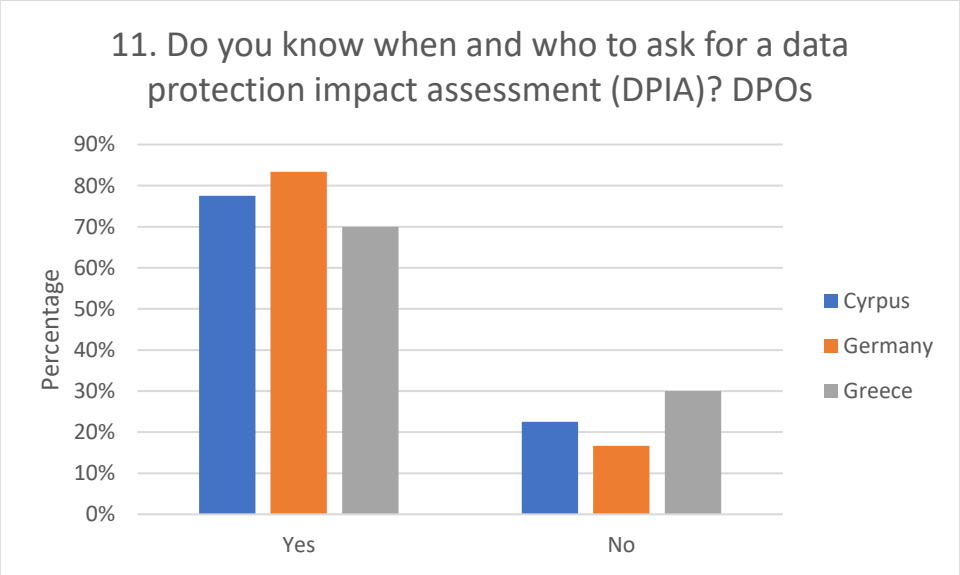


*Figure 16 Knowledge regarding DPIA – answers from DPOs*

Analyzing a more demanding and practical question than the previous one but with the same structure (Yes, No) the difference between Germany and Cyprus compared to Greece is again obvious but not so dominant. More specifically, positive values are more than the negative ones for Germany and Cyprus (68% vs 32% for Cyprus and 64% vs 36% for Germany) while for Greece the pattern is inverted (44% vs 56%).

Since this is a more specific and demanding question in terms of knowledge, the differences in responses between experts and involved employees are larger now compared to the previous, simpler question. Again though, there is an over 10% of responses from experts (30% for Greece) answering *No* in being able to conduct a Data Protection Impact Assessment. This is a statistically significant finding highlighting one more time the lack of hands-on experience.

## 3.4 Training related findings

The third and final subsection of the online survey refers to training needs and methods of delivery training content. It consists of 4 questions referring to:

- types of training that will help bridge the gap between the GDPR processes needed and the actual ones
- types of trainings related to data protection already received
- preferences of training methods/types of delivery, and finally
- a general assessment regarding currently offered training courses in the respective field of expertise.

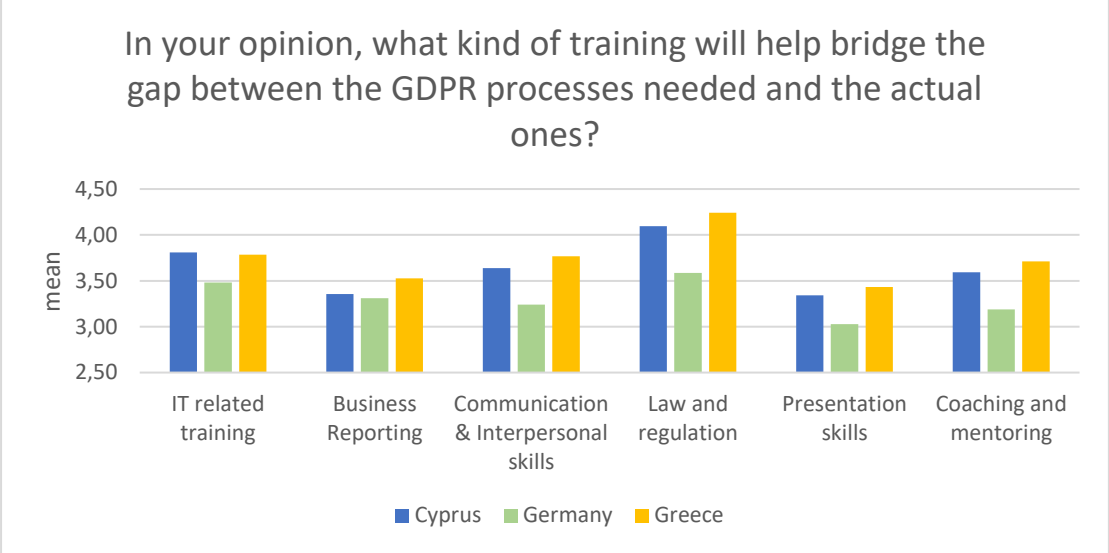


*Figure 17 Opinion question regarding training areas*

Concerning the needed types of training content, the results were the anticipated ones: *IT related training* and *Law and Regulation* are the top two options. On the other hand, focusing on *developing presentation skills* and *business reporting* received the lower score.

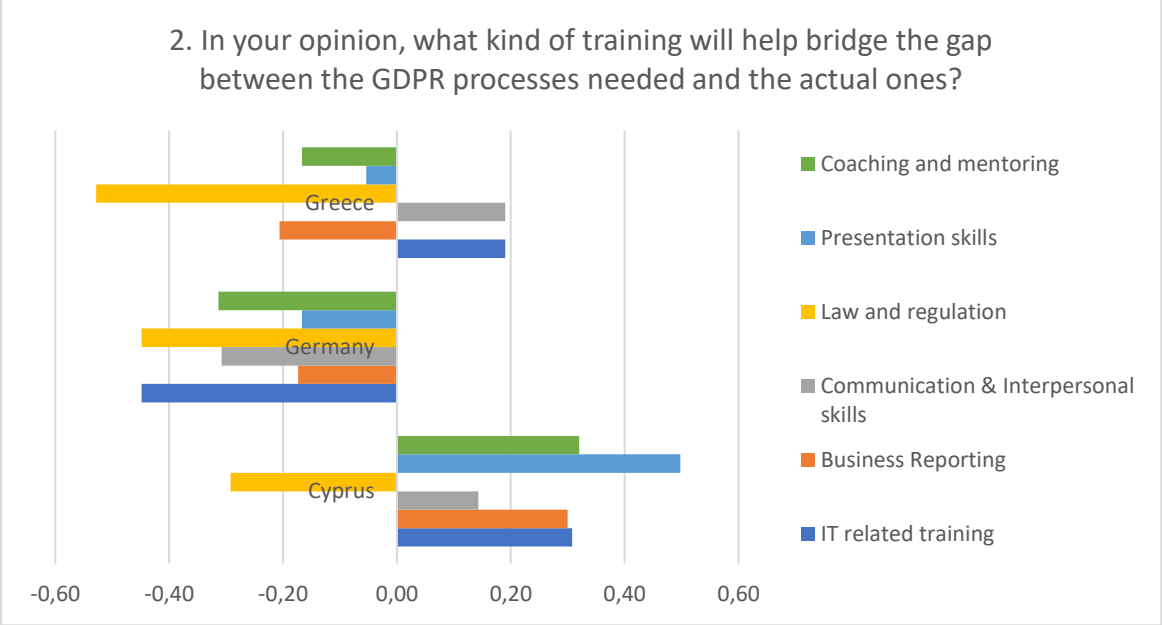


*Figure 18 Comparison between DPOs and no-DPOs answers*

The above diagram displays the score differences between DPOs or experts and non-DPOs. A positive value indicates that the respective option was rated higher from DPOs compared to non-DPOs and vice versa. The following key points were identified:

- in Cyprus DPOs outscored non-DPOS only in *Law and regulation* training areas.
- In Germany DPOs provided lower scores for all possible options. It is interesting that the top two identified training areas – IT and legal related – presented the largest difference. A possible explanation here is that non experts selected the obvious answers while persons having a more thorough view on GDPR application acknowledged the importance of other training areas as well.
- In Greece DPOs outscored in *communication & interpersonal* and *IT related trainings*.

The overall impression is that IT and legal trainings are the two most important, but they are not enough. Considering answers only from DPOs in three Countries their difference between the rest of proposed training areas is not so large and certainly do not allow for characterizing a specific training area as not needed.

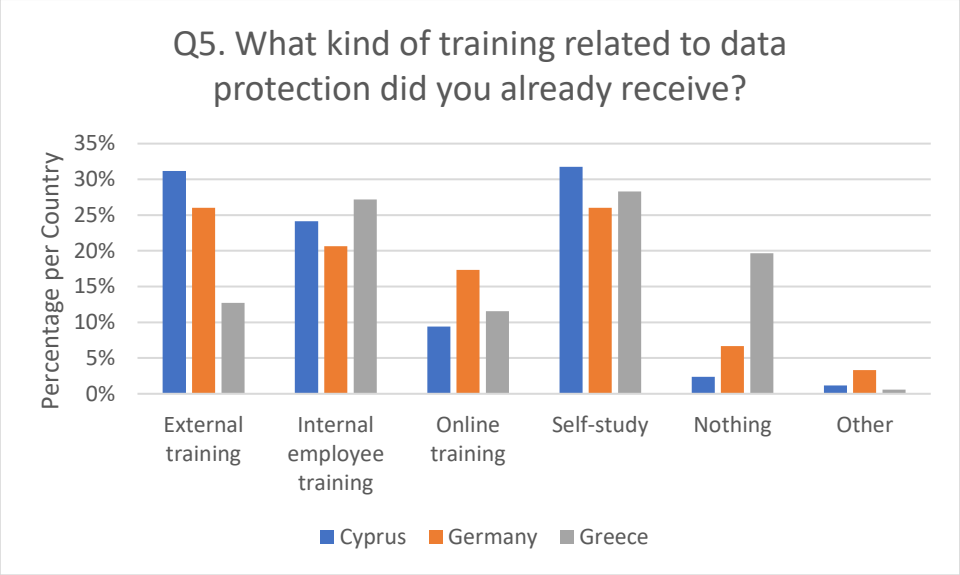


*Figure 19 Methods of trainings already received.*

Focusing on kinds of training delivery already received the findings do not present a dominant trend or an outstanding finding. Nevertheless, *Self-study* reached 32% in Cyprus, 26% in Germany and 28% in Greece and is the top option selected. The most possible explanation is that GDPR compliance is too broad a concept in terms of knowledge needed and cannot be delivered through bundled courses or trainings. This outcome is in line with views of interviewers who stated that a potentially successful DPO should be a person who is willing to learn.

The responders could provide more options – *Other* – then the predefined ones. However, no significant outcome could be drawn since only few, mainly in Germany, provided alternatives, including the terms *Seminars* and *power points*.

Comparing external and internal employee trainings, participants from Cyprus and Germany answered that they have been offered more external than internal trainings (31% vs 24% in Cyprus, 26% vs 21% in Germany) while in Greece the picture is significantly altered - 13% vs 27%. Again, Greece has the more negative opinions by far; about 20% declared that they have not been trained at all.

Online trainings were given the smallest share with Germany leading with 17%. Examining this result under the scope that Germany is much more prepared and may act as a best practice compared to the Cyprus and Greece, this is a good indicator of the future of related trainings i.e. more online trainings are expected to be implemented in Greece and Cyprus as the respective field of expertise will continue to mature.

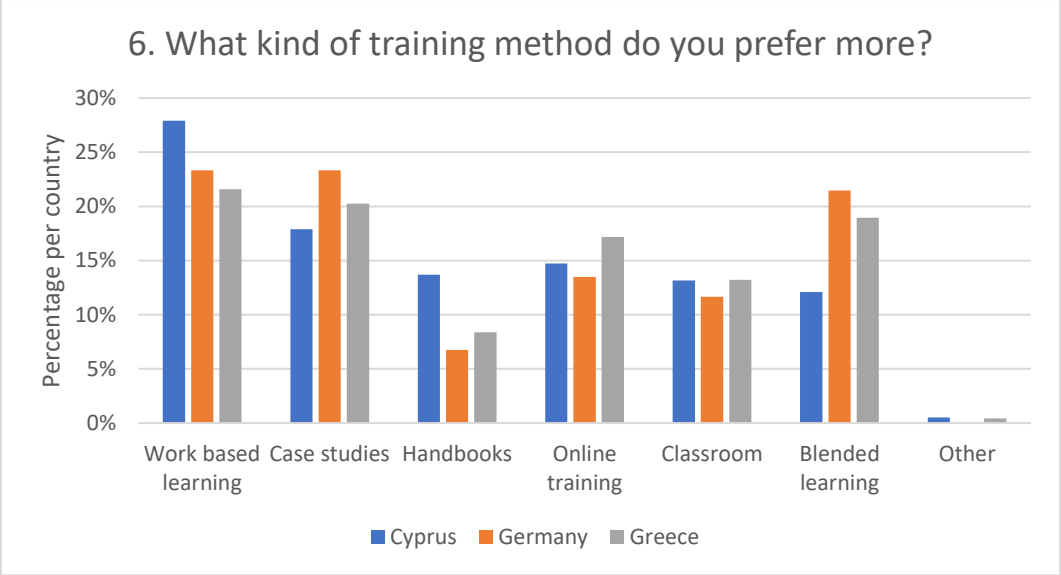


*Figure 20 Preferable training method*

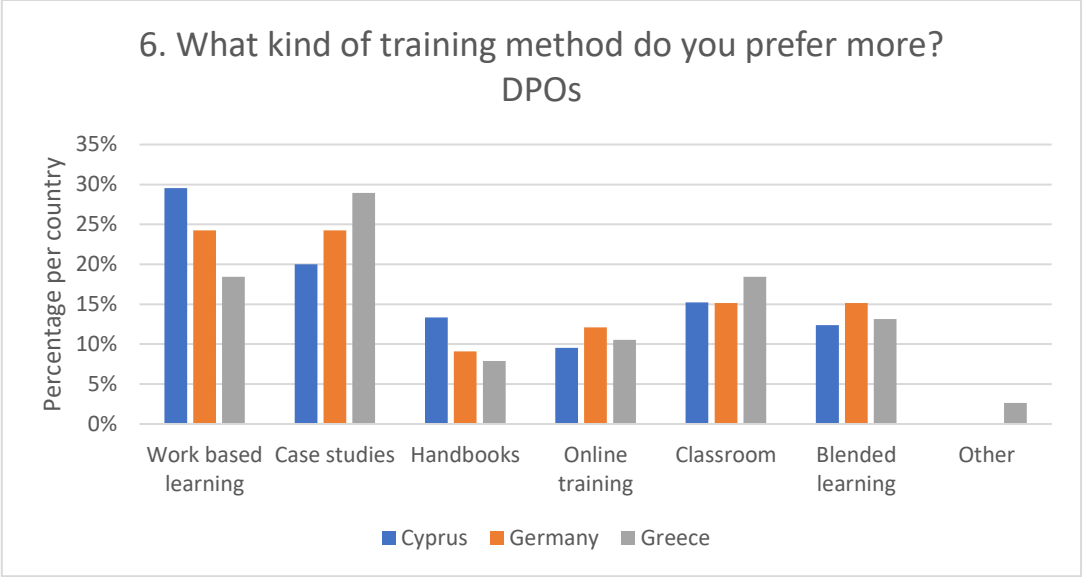


*Figure 21 Preferable training methods – answers from DPOs*

Investigating preferable training methods, the main key points were:

- In Cyprus, work based learning is by far the most preferable delivery method (28%). The rest of the options seem to be equally distributed lying from 12% (*Blended learning*) to 18% (*Case studies*).
- In Germany there is a clearer pattern. *Work-based learning* (23%), *Case studies* (23%) and *Blended learning* (21%), stand out. There is a strong outlier regarding minimum score since *Handbooks* reached only a 7%. This trend shows something that is already identified from previous questions. There is a need for more practical and/or "hands-on" training and/or delivery methods. This affects the design and sometimes the structure of the training material which should serve the practical training request.

- In Greece all options are almost equally distributed except for *Handbooks* (8%) and *Classroom* (13%). Again, the main finding is the same as in Germany; Practical training is needed.

When checking out answers coming from DPOs the picture becomes clearer. DPOs in the three countries clearly state that they prefer *Work based learning* and *case studies*.

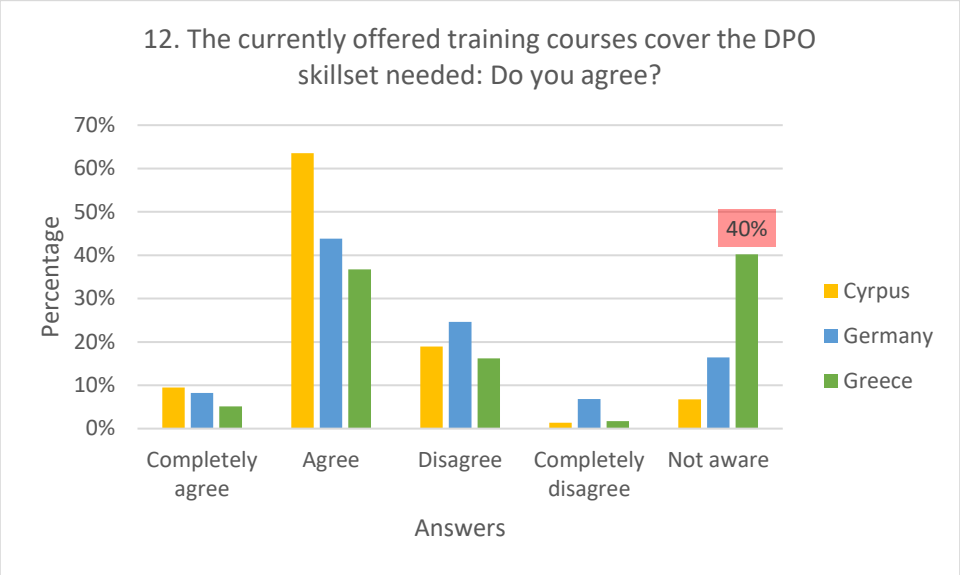


*Figure 22 Opinion on current offered training courses*

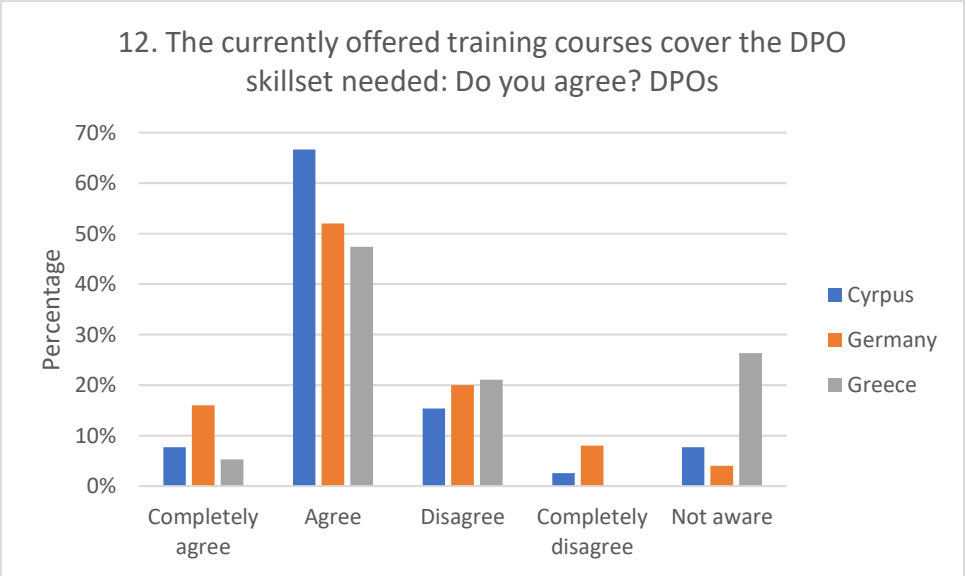


*Figure 23 Opinion on current offered training courses – answers from DPOs*

Finally, participants were asked to assess current training courses in the field. The figures per country are:

- In Cyprus the positive values are around 73% and the negative ones (*Disagree*, *Completely disagree*) reach 20%. *Not aware* option received 7%.
- In Germany positive values are 52%, negative values are 32% and neutral reach a 16%.

- In Greece, positive values reach 42%, negative values 18% and neutral values 40%.

The *Not aware* value of 40% in Greece may be characterized as an outlier compared to other countries. Being unaware of offered trainings highlight the lack of awareness raising regarding the necessity of trainings rather than that there is no need for trainings.

# 4 Qualitative analysis - findings from Focus Groups and interviews

## 4.1 Greece

### 4.1.1 Current needs and challenges in the light of the new EU Data Protection framework

The focus groups and interviews conducted in Greece included a diverse group of stakeholders and actors representing *inter alia*: ICT sector, Education and research institutions, Healthcare, Legal firms as well as independent experts and staff employed as DPO officers.

The research conducted affirms the sheer importance of the new regulatory framework as it changes not only the scope of work of Data Protection Officers but it also widens up the rights of individuals. At the same time, GDPR puts the individual at the center to actively control and have a saying on how their personal data is stored, used and shared. GDPR therefore is considered a 'paradigm change' and engenders many challenges for organisations that are called to manage change and quickly adapt to this new setting. At the same time, it is challenging for both organisations and end users, the data subjects, as they have to change the way they think about Data protection.

What was made strikingly evident in all discussions was the lack of preparedness of both public and private organisations for this new landscape drawn by GDPR. One sector that may stand as an exception to this is Healthcare, as representatives from this field stated that they were already acquiesced with the handling of large data sets of private information which render them more prepared and did not catch them completely unaware. If one is to choose one word as the most used during the discussions, this is the word 'confusion' which prevailed and really shows how employers and employees alike feel about the implementation of the new Regulation.

Disentangling the challenges, a prime worry echoed by the plurality of discussants was the **cost impact** which is generated by the need for properly qualified employees, additional trainings and specific processes for the implementation of the new regulations. Another important issue that emerged was the requirements in **infrastructure** in terms of IT and other aspects that are required to support the changes.

Finally, an interesting point raised, was that GDPR does not explicitly define the need for an officially appointed DPO inside the company. According to experts from the private sector this is more subject to the size and scope of data handling than the size of the organization. Geographic range of data processing, length of data retention, number of data subjects were identified as the main factors driving this decision.

### 4.1.2 Skills demand and current skills gaps

It is a good indication on the timely implementation of the DataPro initiative that the discussion on skills for Data Protection Officers was very welcomed by the participants as was

acknowledged as intriguing and a novel topic. Participants were prompted to reflect on the skills required by the market and the skills they perceive as important and it was obvious that addressing what is required was a theme that steered the discussion and touched many angles.

An important issue that was highlighted was the fact that it is compulsory for all public organisations to appoint a Data Protection Officer whereas in the case of private organisations it is in the discretion of the management to decide whether they need a Data Protection Officer taking into consideration the bulk and type of data they are using.

Discussions demonstrated that if one thinks of a DPO the image that comes to mind is someone with a legal or IT background. This may be the case because when the momentum around GDPR thrust and companies had to act quickly it was either a Tech oriented person or a legal professional that was appointed. However, emanating from their experience, the participants in the interviews and focus groups concluded that having a legal or tech background is not enough for effectively performing as Data Protection Officer**.**

Soft skills were the most important skills set that the participants identified as crucial for the position of Data Protection Officer irrespectively of their qualifications and education background. Interestingly, an interviewee stressed that a DPO should primarily be a **consultant**, namely a person that has studied the operational framework of his/her organisation and can confidently apply business models that will allow the introduction and implementation of data protection systems.

Further, it was noted that the DPO profession is so multifaceted and demanding that may not be covered by one person but requires the establishment of specific departments within organisations.

The key skills identified were:

- Communication skills: The ability to effectively convey information and communicate at all levels was deemed as the most crucial skill required. It was mentioned by many participants, that key task of the data protection officer is to communicate complex legal or tech 'lingo' to staff or members of the public. Communication skills are very important in light of the new GDPR regulation and it will reinforce compliance as in many cases members of the public are reluctant when confronted with Data protection forms which purpose is not clear or it is not clearly explained to staff members how to deal with GDPR issues.
- Knowledge broker skills: In line with the communication skills but different in nature, many interviewees although did not directly used this term they pointed to the ability of DPOs to serve as intermediaries that extract or transfer knowledge within departments and who can be at ease at conversing about different aspects of data protection. At the same time, it was acknowledged that the DPO should stay alert and always update their knowledge with cases and new developments at legal and policy levels.
- Legal skills: The possession of legal skills was mentioned as a sine qua non for the Data Protection Occupation. However, what was discerned from the discussions was a

different conceptualization of what constitutes legal skills. As was stated, it is not just the knowledge of the laws and regulations but also how they relate to the organizational environment and how they will be integrated in the organisation.

- IT skills: The same stands for IT skills which also are considered necessary but not sufficient skills for the Data protection profession.
- Operational Management and business administration skills: Another skill that was highlighted corresponds to the knowledge of business processes and operational management. It was judged as necessary to be able to do change management, to introduce new processes and procedures within the organisation and to be able to monitor them.

### 4.1.3 Availability of training provision and identified training needs

The introduction of GDPR undoubtedly precipitated an increased demand for skilled DPO staff and also steered the attention towards the provision of training. However, as mentioned in the focus groups and interviews, training provision is erratic and limited to information workshops or awareness raising events.

Many participants affirmed the opinion that although at the time of GDPR introduction there was a significant movement towards organisation of workshops and info days for its application, then this momentum waned, and things return to what they were before the GDPR.

It was amply manifested from the discussions that training should not be limited to information days and they should be an ongoing process. Many participants shared that they have been invited to information workshops but this happened only once and in the first months of the GDPR and since then they haven't received any information.

Another key issue that emerged is that training is very **generic**, **not tailored** to the characteristics and needs of each specific sector and also it does not address the educational needs of staff at different levels within an organization.

It was stressed that organizations should have an approach of **continuous training** when it comes to data protection. Further, training should not put emphasis on theory but more importantly to include case studies, and real-life scenarios; in this manner DPOs, staff and aspiring DPOs can learn on the job.

### 4.1.4 Recommendations on improving the current framework

To summarize the primary research and to discern the main findings in Greece, the following points should be highlighted:

- Both public and private organizations were not prepared to fully integrate in their operations the procedures and processes as dictated by the new EU Data Protection Regulation

- There is a need for a change of mindsets and organizational culture regarding the concept of data protection and its importance
- Businesses should provide DPOs with the resources and tools to allow them to perform their duties effectively
- There is no clear Data Protection officer occupational profile and there is an evident mismatch between skills demand and supply and an overall ambiguity regarding qualifications, competences and skills required
- Soft skills should be a key component of training provision
- Training provision should not be generic, but more sector specific training should be provided.
- Training should be work based with case scenarios and work-related examples and not theoretical.
- Raising awareness of staff and the general public should be a priority regarding their rights and obligations under GDPR

## 4.2 Cyprus

### 4.2.1 Current needs and challenges in the light of the new EU Data Protection framework

The overall view in Cyprus is that the DGPR application is still at the beginning. People and organizations may be informed on the GDPR regulation; however, a few have put in practice adequate measures.

Based on the input from the Focus Groups conducted in Cyprus the section below describes the status quo – needs and challenges – in the data protection area from the view of three different sectors, namely the Banking sector, the Health sector and the Insurance and IP sector.

Regarding the **Banking sector**, it is stated that the existing business processes are highly affected. These changes are related to the end-to-end lifecycle of data processing from both an IT and legal perspective.

IT related challenges include more complex data collection schemes, time and cost intensive data processing techniques and algorithms, data storage, deletion and strict security implementations, complicated retention period rules and extended backups solutions. These new requirements result in implementing new system setups or additional resources in terms of processing power, storage and demanding uptime of services.

The main challenges related to legal aspects concern the update of the reporting procedures given that:

- GDPR does not have clear guidelines, it is too general and broad in the sense that it is helping the data subjects but not the businesses while there are no clear lines of execution.
- The rights given to the data subjects rising from the GDPR application is too costly for the banking sector, e.g. a data subject requesting his banking history demands a complicated and working flow.

The status regarding the **Health sector** is in initial phase as well despite the obvious fact that more sensitive personal data are being processed. Apart for the basic steps of establishing basic processes including consent form and protection of medical reports more support is needed especially from an IT point of view:

- More access controls need to be inserted and more complex user management schemes need to be introduced to current back-end and front-end systems,
- develop more robust data-loss protection techniques and apply encryption of data both in software and hardware subsystems.

The **Insurance and Auditing sector** in Cyprus is the most well prepared regarding DGPR compliance. Their maturity is reflected through the already established and updated procedures on workflows such as: Proof of compliance, DPIA schemes, Notification

procedures regarding data breaches, updated forms on new subject rights, integration of third-party data transfers, etc. Even so, compliance to GDPR is still a hard task and there is uncertainty of how the whole monitoring process can be fully framed.

Summarizing the key points identified in the different sectors:

- For all sectors the adoption of new technologies, the increased complexity of data flows and the growth in the number of entities involved in the personal data processing processes, have created a diverse and complex environment. The **need for increased guidance** is clearly stated with a view to a more practical approach since the interpretation of the existing EU regulation is simply not enough.
- An organization can be successfully compliant only through organizational and **cultural change. Commitment** is needed on company level and in a top-down approach: From management board to clerical level.
- **Uncertainty** regarding the level of compliance reached. Even for processes and systems already established, there is no confidence on the compliance level. The general feeling is that there is no clear guidance even in EU level regarding when the preferable level of compliance has been achieved.
- **Adjusting or creating** needed processes should be implemented in a structured way. The usage of ISOs (e.g. ISO 27001) had beneficial results in several cases.
- Some organizations are more willing to invest in persons working 100% as DPOs and not occasionally or complementary to the rest of their every-day duties. This is a quite significant trend and implies that the importance and the necessity of being GDPR compliant is getting more attention. Accepting that GDPR compliance is a must have process at organizational level, is the first step towards sorting out current uncertainties regarding roles, tasks and rules to be followed.

The insights from the conduction of interviews were in line with general status quo already identified: GDPR compliance is in initial phase and more work is need in both theoretical and technical level.

A huge challenge is cultural awareness and the unwillingness to change and adapt. The underlying feeling is that management boards do not value the importance of GDPR and believe that they are compliant by doing the minimum effort. Policies may be in place, but this is more on a theoretical level since they are not being applied in practice.

Participants possessing a legal background or coming from law firms or companies were more updated and were feeling more confident and more prepared related to what is needed.

Regarding the public sector in Cyprus it seems that the whole process is at a primary stage as well. The common practice is to subcontract data protection tasks to external law companies in order to adapt collection, storage and processing of data processes mainly due to huge lack of DPOs or of people who can administer data protection tasks.

### 4.2.2 Skills demand and current skills gaps

The dominant term referring to DPOs skills is **multitasking**. Being able to understand procedures requirements on different contexts including IT, legal and Business is not a task for one person. The mainstream term “Superman” has been mentioned more than once in many cases during the focus groups and interviews discussions from persons coming from different sectors or have different level of expertise, aiming to emphasize the multitasking dimension of the DPO role. One the other hand the prevailing view is that DPO should be able to act as the main contact point in an organization for all data protection issues that may arise. A DPO should have an excellent knowledge of the specific business processes and understand the inner dynamics and be able to act proactively, to coordinate and seek for legal and IT support appropriately. Therefore, the skill set needed tends to be based more and more on **project management skills**, especially for the officially appointed DPOs.

Project management skills seem to outperform strong IT or legal knowledge. The participants were asked if they prefer a DPO in the organization with IT or legal background and the answers were diverse. The general trend was that for public organizations a DPO with legal background might be more appropriate while in the private sector IT-background DPOs are a better fit. In any case, the need for horizontal management skills is always present.

Another skill identified by the majority of the participants was analytical skills; Be able to analyze information, adopt a problem-solve approach and make decisions are at the core of the DPO soft skills. Especially for official Data Protection Officers, acquirement of analytical skills goes a step deeper: They must be able to **map theoretical processes and workflows to tasks** and outcomes in order to ensure smooth implementation.

In general responders were hesitated to accurately define the needed skillset due to the uncertainty around DPO roles and duties. A lot of comments referred to the unclear tasks of DPOs inside the organization and the lack of a check list. The main challenges identified the DPO role and its frame of work were: 1) the difficulty in distinguishing a data processor from data controller and 2) be able to act independently but on the same time be in-line with the board/management requirements.

During follow up questions on the latter issue, the views and beliefs of the participants highlighted another set of soft skills that fall under the project management umbrella skillset. The DPO must be able to communicate efficiently and convince both upper management and individual departments regarding the specific changes or restructures needed towards compliance. Not having **leadership, communication and even negotiating skills** in some cases, the DPO is most probably unable to reach the intended results.

Finally, an interesting key point emerged regarding the DPO role was that (s)he should be able to conduct in-house soft trainings and/or briefings regarding GDPR compliance. At the end every employee working in an organization that process personal data is somehow affected by the regulation. Guidance is needed in order to ensure compliance and restriction of threats and the most appropriate person to organize and drive this knowledge transfer procedure is the Data Protection Officer.

### 4.2.3 Availability of training provision and identified training needs

The picture is clear regarding status of trainings and training needs. The most substantial finding from the qualitative research in Cyprus regarding availability of training provisions and training needs is that basic or theoretical trainings have been conducted and now it is the time to incorporate practical knowledge into new or updated training schemes.

Words or phrases like “case studies”, “hands-on”, “how-to” or “group learning”, described the fact that practical training is missing, and it must be integrated to every new or updated curriculum. On the other hand, words like “handouts” and “textbooks” received negative comments implying that practical knowledge is now more important than the theoretical one.

Along with the more practical approach, several responders expressed their desire for trainings tailored to specific sectors, especially health and bank sector. Since technological development allows for more and diverse volume of data, their processing has introduced complex control points strongly dependent on the requirements coming from the respective sector.

Regarding delivery of trainings through WBL based schemes in Cyprus, the participants explicitly stated that they were not aware of such schemes in private or public organizations.

Another important parameter is the need for **constant updating of the training material** since GDPR constantly evolves. This key point affects the structure of future DPO related training programs in the following way: in order to be able to successfully update training material and content, a structural and/or hierarchical approach is needed. Some topics are mature enough and more resilient to change, some others are in an initial phase and need to be updated. Structuring the learning material around independent and individual short modules or topics, offers flexibility when a call for update is needed.

Finally, a lot of opinions identified the gap regarding the qualifications of instructors. Speakers and trainers can cover the theoretical background and provide adequate interpretation of the GDPR rules; however, several weaknesses and shortcomings were described. Teaching content including missing real-life examples or best practices, creation and management of checklists instead of general duties and clear answers for sector specific questions e.g. personal health data were the main shortcomings.

### 4.2.4 Recommendations on improving the current framework

Summarizing the quality research in Cyprus the following key points and recommendations have been identified:

- Public and private organizations must adequately prioritize data security and protection. This implies the adoption and establishment of a new culture and attitude or in other words **data protection by design and default**. Data protection by design is about considering personal data protection issues upfront in every activity. Therefore, integration of data protection into the processing activities and business practices from

design right through the whole lifecycle must continue since currently it is not at the desired level.

- Being GDPR compliant **is not a task for one person**. The DPO should act as the main contact point and either be the leader of a Data Protection team or efficiently collaborate and get support from the respective departments inside an organization i.e. legal department, IT department, etc.
- Trainings are in initial level. Internal or in-house trainings must be organized with a view to establish GDPR as intrinsic and "must-have" procedures. External trainings are also needed with a view to a more practical approach.
- Different industries have different requirements related to GDPR realization. This affects the training schemes and create new needs on the training content: Calls for sector-specific trainings and best practices or case studies are increasing. Constantly updated material becomes a necessity, since interpretation and application of GDPR rules evolves.

## 4.3 Germany

### 4.3.1 Current needs and challenges in the light of the new EU Data Protection framework

The status quo in Germany is different compared to Greece and Cyprus. The overall context is that the companies and public sector are more mature in embedding GDPR in existing procedures and a decent level of reorganization has been already achieved. The topic has been up to date for a long time and addressed through the Germany's Federal Data Protection Act (BDSG).

The "GDPR era" introduced new challenges though: due to its nature, being GDPR compliant is a very complex task and the reorganization stage resulted in more bureaucracy. In a nutshell:

- Administrative burden has been increased. This is a great obstacle for German SMEs where the focus is on the day-to-day business while they lack time and financial resources to implement GDPR.
- Increased number of cases where decision making is slower
- Introducing technical solutions and updated IT systems has been cost intensive. Sometimes it's better to ignore or partly implement systems with hard requirements regarding data backups, retention times, etc.
- GDPR is too broad and introduces a very wide field of actions.
- Being GDPR compliant means that you are not competitive in terms of market compared to companies from abroad.

All the above factors pose a break in the full implementation of GDPR by German companies. In addition, real control mechanisms have been put in place only recently, so the process is ongoing.

On the other hand, the public sector and especially large public bodies have almost implemented GDPR, so no real changes exist. The increased burden has affected mainly management level employees and not administrative staff.

German participants stated that the Interpretation of GDPR is a vague process. There have been cases where several conflicts have been identified while there are no strict rules defining 100% GDPR compliance; there is always room from more interpretations and more actions.

In general, application of GDPR in Germany is quite mature and a lot of organizations got over "childhood diseases". The so much needed culture and appropriate attitude regarding the necessity of a horizontal EU regulation seems to be in place. The strategy now focuses on optimizing existing procedures and decide to invest time and money on the efficient implementation of GDPR.

### 4.3.2 Skills demand and current skills gaps

According to German stakeholders, the Data Protection Officer role should mainly focus on an advisory and disclosure level. Responsibility of GDPR adoption and all relevant processes should be held at management or board level. Under this context the DPO must point out abuses, control data and overview processes. Therefore, (s)he should be able to read, understand and apply rules from a legal perspective.

Another key point raised, was that the learning curve is ongoing and it's time intensive. Given the wide context, the appointed DPO or the person with the DPO role should be able to read and combine information from different worlds e.g. IT and legal. A person not being eager or willing to learn may not reach the preferred level. Discussing the ideal background, the findings were the anticipated ones: Both IT and legal background are needed with a view to a more legal perception.

The common ground concerning DPOS skills derives from the fact that a DPO is the main contact point for managing data protection processes coming from different contexts. Thus, by design, DPO should be able to:

- Work in close collaboration and develop synergies between related departments
- Communicate efficiently and be a team player
- Establish trainings and provide advises to other employees in a periodic way.

Finally, analytical skills related to process and flow representations are needed both from theoretical and operational point of view. Mapping flows to business processes is a must have competence otherwise the whole effort stays only in theoretical level

### 4.3.3 Availability of training provision and identified training needs

In general, the market offers a lot of similar courses covering adequately the basics and/or the theoretical aspects of the EU regulation. They act as foundation trainings not acquiring previous knowledge or having strict pre-requisites. According to the views of the participants, practical training is missing since:

- Practical scenarios or cases studies are not part of the leaning process.
- Instructors are focusing on GDPR interpretation issues without complementing the teaching process with real examples.
- There is lack of methodologies on how to map GDPR rules to existing business processes e.g. flow maps, business process representation, etc.

Another interesting key point is that some best practices were listed mainly, in-house initiatives driven by certain organizations. The best example described was the training that DPOs are receiving via the Association of Hospitals in Germany (Landeskrankenhausgesellschaft). This is conducted twice a year and learning objectives are

tailored to the Health sector with practical examples on how to apply GDPR in personal health data.

### 4.3.4 Recommendations on improving the current framework

German legislators have been the first among other Member States to implement provisions covering the so-called opening clauses within the GDPR. The maturity level is higher compared to Cyprus and Greece. However, there is room for improvements and optimizations.

- More efficient and continuous monitoring of the whole process.
- During the design of data protection policies, a much broader view is needed. Apart from following the “security by design” principal, cultural differences among involved people and organizations should be taken into account.
- Using professional services is better. On the one hand the learning curve is reduced inside the company, on the other large fines imposed by data protection regulations are avoided.
- Again, one of the major issues identified was the uncertainty raised by the legal interpretation. It is highly suggested that companies that collect, process and use data, need to act proactively and identifying future issues in advance.
- DPOs should focus on resolving practical issues and be able to answer HOW questions. Questions referring to WHAT and WHEN are more or less covered by the existing theoretical background.

# 5 Summary and synthesis of results

Current needs and challenges – the big picture

GDPR is a tough privacy and security law in international level. It is large, far-reaching and vague on specifics making it hard to be put in effect especially for small and medium-sized enterprises (SMEs). DataPRO participants have described several difficulties but the prospect is not daunting. On the contrary stakeholders and especially experts feel quite confident and well prepared to tackle any potential obstacles.

A common trend highlighted by both qualitative and quantitative analysis is that being GDPR compliant is an **on-going process**. GDPR continues to be interpreted and this results in **uncertainties on reaching the desired level of implementation**. Measures are taken and business and reporting processes are restructured but the prevailing impression it that this is not enough.

In addition, the adoption of new technologies, the increased complexity of data flows and the growth in the number of entities involved in the personal data processing processes, have created a diverse and complex environment and act as a multiplier effect: more technical solutions and business flows need to be created to handle massive volumes of personal data. A lot of participants identified the need of not only to adjust current processes but also introduce new ones with a different mindset: **Data protection by design** i.e. considering personal data protection issues **upfront in every activity**.

In this context, the topic is more mature in Germany compared to Cyprus and Greece. Strategically, companies and public bodies in Germany are focusing on optimizing the whole framework with a view to tackle technical and operational issues. As many German responders stated, **monitoring and application of fines** has already started implying that basic measures have been taken. Greece and Cyprus are at initial stage and the focus is on the appropriate interpretation of GDPR rules and obligations. There are more challenges and complications in applying the commitments from the EU regulation.

In a nutshell, data protection is in its early stages in the private and public sector. Especially, for private companies and SMEs, data protection and privacy teams are understaffed or underfunded. In other words, data protection is not high prioritized in the TODO list and it seems that they just beginning to grapple with GDPR compliance.

Skills demand and skills gap: Ideal Profile of a DPO

After processing and analyzing data collected from the quantitative and qualitative report the role of a DPO is **multidisciplinary** and a combination **of both soft and hard skills** is needed. According to article 39 of the GDPR, a DPO should at least be able inform and advise the controller/processor and/or the employees, to monitor the whole compliance process and to

act as a contact point between departments inside an organization and between the organization and the involved authorities[2].

As expected, the main outcome of the field research was that both a legal and IT background are needed. Specifically:

- Legal knowledge is needed. Application of GDPR regulations call for a person to be well-versed in legal matters. The DPO should be able to read, understand, synthesize and summarize key points of legal documents.
- Basic IT knowledge is needed. The needed skills should be founded on wide-ranging experience in IT programming, infrastructure and Information System audits. Understand what kind of data are being collected and processed, what is the appropriate retention time and most important how security and privacy subsystems are working (e.g. knowledge of DFD – Data flow diagrams were the most frequent points identified by the participants. Given that privacy and security risks constantly evolve, it is extremely important for a DPO to demonstrate awareness of changes to the threat landscape and fully comprehend how emerging technologies will alter these risks.

Having a basic IT or legal background and understand GDPR regulations is not enough. Two of the most influential and characteristic quotes related to the DPO role were "**Superman**", and "**DPO should stand for Data Protection Office**" putting the multidisciplinary and multitasking dimension at the core of a DPO skillset. From this perspective, it is not strange that the discussions focused more on a wide range of missing skills.

  - **Project management skills**. The project management skillset was raised and confirmed especially from the most experienced participants and mainly include competences such as being able to request, marshal and lead the involved persons in order to carry out their tasks and duties. This is also verified by the online survey results where DPOs favored attributes like **time management and planning** in Cyprus, **collaboration and partnerships** in Germany and **conflict resolution** in Greece. This finding based only on the experts' opinions, highlights the strong project management perspective that each DPO should have.

- **Analytical and problem-solving skills** need to be empowered. Examining this skillset from a DPO point of view results in specific competences:
  - be able to map theoretical or business processes and workflows to tasks and outcomes in order to ensure smooth implementation
  - be able to analyze information and adopt a problem-solve approach
  - make decisions
- **Current DPOs lack practical knowledge**. They understand WHAT and WHEN but it seems that the answers are vague to questions starting with HOW. This seems to be the major challenge that DPOs are currently facing and it is horizontal in all three countries.

[2] https://gdpr-info.eu/art-39-gdpr/

- **Multicultural approach** was raised as a missing skill from focus groups and interviews, but this is not verified by the online survey as well, where the importance. However, it is anticipated that future DPOs will likely be dealing with controllers or processors from different countries, especially when the number and type of involved actors is increased in current online interactions (example: online orders or bookings from companies with retail presence in EU, manufacturers in China and management in US). The respective skillset is not yet fully clear in the picture, but it seems that it will be a must have asset soon.

Training provisions

The first takeaway regarding training needs and provisions is that more practical and/or "hands-on" trainings is needed.

Considering the huge variety of jobs and tasks that fall under the privacy rubric, it's impossible to deliver the necessary trainings in a one stop manner. The wide scope affects both the scope of the training material and delivery methods from a curriculum design perspective. Highlighting the most important key points a DPO training curricula:

- Trainings should definitely go beyond existing awareness raising seminars and information days. Structured courses with specific learning objectives and outcomes are needed.
- Embed practical trainings with the use of test cases, real-life scenarios, team assignments, etc. It seems that the first cycle of getting familiarized with the topic is ending. More hands-on approach is needed in favor of handbooks or static presentations.
- Delivery methods including Work-based learning should be encouraged. Internships or mentorships along with effective evaluation strategies can be offer the so much needed "inside look".
- Training of DPOs is an on-going process and needs to be appropriately updated since the GDPR interpretation constantly evolves. This affects the structure of such training courses. They should be **hierarchically designed** consisting of relatively **small and potentially independent modules** or entities of knowledge in terms of hours of effort needed. In this way the learner is given the possibility to address fast specific learning objectives and optionally in his own pace towards personalization. What is more, the structured approach offers more flexibility when a call for update is needed or decided by the training authority. While this is a challenging requirement during the curriculum design process, it will certainly facilitate the foreseen training content and material updates.
- Finally, under the practical approach umbrella, sectorial training should be taken into account. Health sector, Banking sector, Marketing Companies or companies founded around big data principles are in need for additional expertise. Training modules in the form of electives (optional lessons) incorporated in a core DPO training course are expected to dominate the market.