

# D2.1 Comparative Analysis of different data protection curricula

WP2. Design or improvement of a joint qualification in VET



## 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	<a href="http://www.datapro-project.eu">www.datapro-project.eu</a>

---

## PREPARED BY

• Authors	ReadLab
Date	April 2019
Version	Final
Approved by	AMC
Dissemination Level	Public

### **Disclaimer**

The European Commission support for the production of this publication does not constitute endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein

## Executive Summary

This report aims to present and analyze comparatively existing curricula addressed to current and future Data Protection Officers in the project consortium countries and beyond.

More specifically, the main objectives of the 2.1. Comparative Analysis of different data protection curricula report are to:

- Provide an understanding of the different obligations for Enterprises and Organizations emerging from the new Regulation in EU level.
- Identify emerging common themes, trends and challenges in Data Protection that skills and competences included in the curricula need to address
- Identify current in play DPO Curricula in Partners Countries - Greece, Cyprus and Germany.
- Identify current in play DPO Curricula in third countries and international level

2018 has been a monumental year of changes in the data protection landscape, across the globe. GDPR, enacted by the EU, could be characterized as the strictest and most complex data privacy law to date, which imposes tough obligations to organizations and businesses and prescribes costly fines for non-compliance.

The role of the “Data Protection Officer” is formally recognized by the GDPR as a useful and necessary component of an effective data privacy and protection accountability and compliance framework. More specifically, the key issues of the designation and the position of the DPO, as well as their responsibilities and tasks are foreseen in Articles 37-39.

The enforcement of GDPR created a new competitive environment, which requires entities, both institutions and companies, to adopt. This new environment asks for DPOs to have “expert knowledge of data protection law and practices”, accompanied by a diverse skill set that includes:

- Interpersonal and communication skills
- Organisational and privacy program management skills
- Leadership skills
- Data privacy strategy skills
- Business skills
- Operational and digital skills - Technology skills
- External engagement skills

On the supply side, the analysis of the curricula collected in Greece, Cyprus, Germany and beyond, shows that the main focus is on the upskill/reskill of the current and future data protection officers in operational, legal and IT skills from a more organization-centered approach.

Despite the absence of a common Occupational Profile, there is an unanimity towards certain learning objectives, including knowledge of data protection regulations, of the obligations

emanating from the latter, and of the methods to follow to fulfill those obligations, thus achieving compliance.

It is observed that the supply side currently offers curricula entailing Introductory, Operational, Legal and IT modules. It is also observed that there is a total absence of **soft and/or transversal skills training**.

Moreover, target groups are the widest possible and none of the identified courses are able to offer specialized skills and especially digital skills in specific market sector and areas. **Elective courses** and **adaptability** are missing from all the identified courses.

Adaptability could undoubtedly more easily be achieved through online delivery of the training, which currently holds less prevalence than the in-classroom method.

Also, the **lack of WBL and/or Apprenticeships component** in the curricula identified and analyzed highlights the missing element of “on-hands” learning.

Finally, the absence of formal recognition of the certifications of DPO training currently available is also noted.

Although GDPR is quite vague to the DPO knowledge, skills and attitudes requirements, it is obvious that the role emerges as multi-faceted, multidimensional requiring solid knowledge base combined with diverse skills palette including a wide range of soft skills, as well as certain attitudes and abilities.

Drawing on the conclusions of the comparative analysis, this report recommends that the DataPRO curricula should follow a modular approach focusing on the needed balance between hard and soft skills, while e-learning delivery is also recommended, allowing for flexibility and adaptability.

Recommendations include the inclusion of a WBL/Apprenticeships component, and the achievement of accreditation and/or recognition, beyond certification.

## Contents

1.	The DataPRO project.....	5
2.	Purpose and Scope of this Report.....	6
3.	Methodology .....	7
4.	Background – The GDPR effect in the European and international data protection landscape.....	8
5.	Obligations for Enterprises and Organizations emerging from the new Regulation.....	10
6.	The DPO Role in the spotlight .....	14
7.	The DPO Role under the GDPR .....	16
7.1.	Designation .....	16
7.2.	DPO’s Tasks.....	16
7.3.	DPO Knowledge Requirements, Professional Qualities and Abilities .....	17
8.	Trends and challenges in Data Protection posed by GDPR .....	20
9.	Established and applied curricula in Greece .....	22
10.	Established and applied Curricula in Germany .....	24
11.	Established and applied Curricula in Cyprus .....	26
12.	Established and applied Curricula in other EU countries beyond the consortium and in international level.....	28
13.	Comparative Analysis.....	30
13.1.	Learning objectives .....	30
13.2.	Target groups.....	31
13.3.	Training Delivery Methods.....	33
13.4.	Module Types .....	36
13.5.	Methods of Certification .....	38
14.	Conclusions.....	41
15.	Recommendations for the design and delivery of the DataPRO Curricula.....	42
16.	References .....	<b>Error! Bookmark not defined.</b>
17.	Annexes .....	44
•	Annex I. Established and applied curricula in Greece .....	44
•	.....	50
•	Annex II: Established and applied Curricula in Germany.....	50
•	Annex III: Established and applied Curricula in Cyprus .....	59

- Annex IV: Established and applied Curricula in other EU countries and in international level  
65

## List of Figures

Figure 1 Module Types in Greece.....	23
<i>Figure 2 Module Types in Germany.....</i>	<i>25</i>
<i>Figure 3 Module Types in Cyprus.....</i>	<i>27</i>
<i>Figure 4 Module Types (International).....</i>	<i>29</i>
<i>Figure 5 Training Delivery Methods.....</i>	<i>34</i>
<i>Figure 6 Module Types.....</i>	<i>36</i>
<i>Figure 7 Module types (2).....</i>	<i>36</i>
<i>Figure 8 Soft VS Digital Skills.....</i>	<i>37</i>
<i>Figure 9 Certification Methods.....</i>	<i>40</i>

## List of Tables

<i>Table 1 Target Groups.....</i>	<i>32</i>
<i>Table 2 Training delivery methods.....</i>	<i>34</i>
<i>Table 3 Module Type Content.....</i>	<i>38</i>
<i>Table 4 Methods of Certification.....</i>	<i>39</i>

## 1. The DataPRO project

The 2.1. Comparative Analysis of different data protection curricula report is one of the key outputs of the DataPro project: Updating the EU Data Protection Sector with new Skills. It is a two-year EU-funded project working across three EU member states – Greece, Cyprus and Germany.

The DataPRO Project aims to respond to the challenges of the new European data protection regime that is being shaped by the adoption on 27 April 2016, of the General Data Protection Regulation (GDPR) 2016/679.

Since there is no common European framework on skills and competences needed in data protection Sector, business Sector is facing a rising skills mismatch between data protection employees across European countries with different occupational profile on skills and competences and most importantly, different level of legislation/integration on data protection.

The DataPRO project aims at:

1. The development of a renewed joint Occupational/Qualification Profile for Data Protection Officer (DPO) that will be the result of a targeted Training Needs Analysis
2. The development of two interconnected joint Curricula accompanied by advanced WBL schemes that will empower learners and employees with renewed skills and competences

## 2. Purpose and Scope of this Report

In the broader context of assessing the state of play in the Data Protection sector, this report aims to present and analyze comparatively existing curricula addressed to current and future Data Protection Officers in the project consortium countries and beyond.

More specifically, the main objectives of the 2.1. Comparative Analysis of different data protection curricula report are to:

- Provide an understanding of the different obligations for Enterprises and Organizations emerging from the new Regulation in EU level.
- Identify emerging common themes, trends and challenges in Data Protection that skills and competences included in the curricula need to address
- Identify current in play DPO Curricula in Partners Countries - Greece, Cyprus and Germany.
- Identify current in play DPO Curricula in third countries and international level

The structure of the report follows with an overview of the impact of GDPR enforcement in the European and international data protection landscape. In that context, it outlines key features of the Regulation, and then proceeds to presenting the obligations emanating from its enforcement for legal entities - both organisations and companies.

The next section outlines the DPO role under the GDPR, with reference to the DPO designation, the DPO's tasks and responsibilities, as well as knowledge and skills requirements. In the same section, key challenges posed by GDPR and affecting the evolution of the DPO role are also discussed.

Having an overview of the demand side, as it is shaped by the Regulation, the report proceeds to examining the existing supply side. Currently offered training opportunities for DPOs in the consortium countries, in other EU member states beyond the partnership and in international level, are being analyzed and comparatively assessed.

With these contextual foundations in place, the report issues recommendations for the design and development of the DataPro curricula, aiming to feed in forthcoming project deliverables.



### 3. Methodology

This report is a quantitative and qualitative research based on secondary data retrieved from open sources.

The collected data have been identified, combined and finally compared in order to reveal the situation of the existing training options in the data protection sector- not only in the partner countries but also in EU member states beyond partnership as well as in third countries- and proceed to recommendations about the efficient structure of the DaraPRO curricula.

In terms of data collection methodology, a common Course Record template was developed by the Assigned Task Leader (P10-ReadLab) to be used by partners in Greece, Germany and Cyprus. All partners contributed to the validation of the criteria to be used for the assessment of the curricula to be identified, through dedicated online discussions (skype meetings). Thus, the set of criteria that guided the research and analysis includes:

- Content and structure of the curricula
- Existing Target Groups and their specific characteristics;
- Training methods and techniques used;
- Activities undertaken within those Curricula and results;
- Impact and Results
- WBL and Apprenticeship Programs

The template used, along with the input gathered, is presented in the Annexes, at the end of this document.

In terms of comparing and analyzing the data collected, the method followed entails outlining the demand landscape on the one hand and the current state of supply on the other. More specifically, the research and analysis of the present study:

- Presents a state-of-the-art analysis regarding the latest GDPR compliance trends, gaps and needs in the Data Protection market. This analysis was conducted through an extensive desktop research. In this way, skills and knowledge needed in the Data Protection sector are identified. This section provides an overview of the **demand side**.
- Outlines the **supply side**, through collecting and comparatively analysing several currently offered Training Curricula not only from partner countries (Greece, Germany, Cyprus) but also from EU member states beyond partnership (Spain, Luxembourg), as well as third countries (USA and Singapore) and international professional bodies (iapp). The aim is to track currently offered learning opportunities, identify potential similarities and gaps through comparative analysis and with reference to the demand side.

## 4. Background – The GDPR effect in the European and international data protection landscape

Digital transformation<sup>1</sup> admittedly altered the way humans interact. In today's occasion of digital services, social media networking and the so-called fourth industrial revolution, the amount of data created, collected, stored, processed and, thus, needs to be protected, continues to grow at unprecedented rates.

In the EU, the privacy concerns and security risks emanating from such a data-driven society, also throwing a spanner in the works of a secure and competitive digital single market, led to the reform of the legislative and policy framework regarding data protection.

Almost a year ago, on May 25th, 2018, the General Data Protection Regulation (GDPR)<sup>2</sup> entered into force, repealing the existing Directive 46/95/EC. The choice of legal instrument denounces the massive scale of the change. As a Regulation, the GDPR, had binding legal force throughout every Member State starting from the set date above, whereas a Directive, including the one replaced, lays down certain results that must be achieved but each Member State is free to decide how to interpret directives into national laws. Consequently, the GDPR aimed at achieving a higher level of harmonization, leaving no room for national ratification processes and allowing for greater legal certainty across the EU<sup>3</sup>.

However, GDPR has an “extra-territorial effect”. Its provisions expand the scope of data protection so that it applies to anyone or any organization that collects and processes information related to EU citizens, no matter where they are based or where the data is stored<sup>4</sup>. Article 3 foresees that the Regulation applies to personal data processing by institutions (a) established in the EU, irrespective of where the processing activity takes place, or (b) process personal data of European citizens, irrespective of their place of establishment<sup>5</sup>. Therefore, even though the GDPR only protects EU citizens, its impact is bound to be global in

---

<sup>1</sup> European Commission (2018), Digital Transformation Scoreboard 2018: EU businesses go digital: Opportunities, outcomes and uptake, Luxembourg: Publications Office of the European Union, [https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/Digital%20Transformation%20Scoreboard%202018\\_0.pdf](https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/Digital%20Transformation%20Scoreboard%202018_0.pdf)

<sup>2</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

<sup>3</sup> De Hert, P., & Czerniawski, M. (2016). Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context. *International Data Privacy Law*, 6(3), 230-243.

<sup>4</sup> Tankard, C. (2016). What the GDPR means for businesses. *Network Security*, 2016(6), 5-8.

<sup>5</sup> De Hert, P., & Czerniawski, M. (2016). Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context. *International Data Privacy Law*, 6(3), 230-243.

nature, affecting any organization that targets the European market or provides services and hold personally identifiable information on EU residents<sup>6</sup>.

Besides its “extra-territorial” scope, another crucial dimension of the GDPR is its technology neutrality. Recital 15 foresees that “the protection of natural persons should be technologically neutral and should not depend on the techniques used. The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing”. Technological neutrality ensures the Regulation’s enduring application despite potential technological advancements, thus maximizing its impact.

Finally, a third element of GDPR largely affecting its wide impact and endurance is that it imposes “data protection by design and by default” to organizations and businesses.<sup>7</sup> Privacy by design means that entities are obliged to consider privacy at the initial design stages as well as throughout the complete development process of new products, processes or services that involve personal data processing. Privacy by default holds that when a system or service includes choices for the individual/data subject on how much personal data they share with others, the default settings should be the most privacy-friendly ones.

Based on the aforementioned, it is clearly demonstrated that GDPR carries distinctive features profoundly affecting the data protection landscape in both European and international level, as it imposes inescapable legally binding obligations to all entities, both organizations and businesses, providing products or services, which involve data processing.

---

<sup>6</sup> He Li, Lu Yu & Wu He (2019) The Impact of GDPR on Global Technology Development, *Journal of Global Information Technology Management*, 22:1, 1-6

<sup>7</sup> GDPR, Article 25 and Recital 78

## 5. Obligations for Enterprises and Organizations emerging from the new Regulation

Generally, the GDPR places direct legally binding obligations on enterprises and organizations (both public bodies and private organizations) processing data of EU citizens, thus acting in the role of data controllers<sup>8</sup> and data processors<sup>9</sup>.

“Processing” is defined in Article 4(2) of the GDPR as “any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction”<sup>10</sup>. Obviously, “processing” is being used with a scope beyond the word’s own meaning to include everything one can do with personal data.

In order to be accountable, entities processing personal data must fulfil a set of compliance criteria. Key compliance obligations for enterprises and organizations can be grouped under two subheadings – obligations that protect the rights of the individuals / data subjects and obligations based on risk<sup>11</sup>.

As regards the rights of the individuals / data subjects, GDPR aims to reinstitute the control of European citizens over their own personal data<sup>12</sup>, thus it has extended the scope of their rights towards data controllers<sup>13</sup>, introducing new ones as well, eventually aiming to safeguard their fundamental right to data protection<sup>14</sup>.

---

<sup>8</sup> The controller is defined by GDPR Article 4(7) as the person or body, which determines the purposes and means of the processing

<sup>9</sup> The processor is defined by GDPR Article 4(8) as the person or body, which processes data on behalf of the controller.

<sup>10</sup> GDPR, Article 4(2)

<sup>11</sup> European Commission (2018), The GDPR: new opportunities, new obligations, Luxembourg: Publications Office of the European Union, [https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-sme-obligations\\_en.pdf](https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-sme-obligations_en.pdf)

<sup>12</sup> European Commission (2018), It’s your data – take control: Data Protection in the EU, Luxembourg: Publications Office of the European Union, [https://ec.europa.eu/commission/sites/beta-political/files/data-protection-overview-citizens\\_en.pdf](https://ec.europa.eu/commission/sites/beta-political/files/data-protection-overview-citizens_en.pdf)

<sup>13</sup> Jef Ausloos & Pierre Dewitte (2018), Shattering One-Way Mirrors. Data Subject Access Rights in Practice, KU Leuven Centre for IT & IP Law, International Data Privacy Law (2018) 8(1), pp.4-28

<sup>14</sup> Article 8, Charter of Fundamental Rights of the European Union, [https://www.europarl.europa.eu/charter/pdf/text\\_en.pdf](https://www.europarl.europa.eu/charter/pdf/text_en.pdf)

More specifically, the obligations that protect individual rights<sup>15</sup> are:

- providing transparent information. Companies must provide individuals with information on who is processing what and why.
- respecting the individual's right to access their data. Individuals have the right to request access to their personal data, free of charge and in an accessible format.
- their right to data portability. When the processing is based on consent or a contract, the individual can ask for their personal data to be returned or transmitted to another company.
- their right to erasure (right to be forgotten). In some circumstances, an individual can request that the data controller erase their personal data, such as when the data is no longer needed to fulfil the processing purpose.
- their right to correct and right to object. If an individual believes that their personal data is incorrect, incomplete or inaccurate, he or she has the right to have it rectified or completed without undue delay. An individual may also object at any time to the processing of their personal data for a particular use.

GDPR Article	Individuals' Right	Brief description
12, 13 and 14	Right to Information	Aiming at improved transparency of data processing, individuals have the right to request (free of charge) for what purposes and by whom exactly (third parties included) their data are processed.
15	Right to Access	The request may also pertain a copy of such data that must be provided electronically, in an easily readable format and without undue delay
16	Right to Correct	If personal data is inaccurate or incomplete, the individual has the right to ask for them to be rectified.
17	Right to Erasure (Right to "be forgotten")	Individuals have the right (under qualified circumstances) for their data to be erased from the controllers' dataset
18	Right to Restriction of Processing	Controllers are bound by the right of the individuals to ask for their personal information to be suspended from the processing.

<sup>15</sup> GDPR, Articles 15 to 22. Also see, European Commission (2018), The GDPR: new opportunities, new obligations, Luxembourg: Publications Office of the European Union, [https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-sme-obligations\\_en.pdf](https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-sme-obligations_en.pdf)

20	Right to Data Portability	Individuals have the right for their data to be transferred from one controller to another (or directly to the data subjects themselves) in an automatic and easily readable format.
21	Right to Object	Right to contest the processing of personal data by controllers.
22	Right not to be Subject to Automated Decisions	Individuals have the right not to be subject to decisions based on solely automated means (including profiling), which leads to legal effects for the individuals.

Obligations based on risk - Actions to implement or integrate data protection and to demonstrate compliance include<sup>16</sup>:

- appointment of a Data Protection Officer (DPO) to monitor, implement and advise on compliance with the GDPR<sup>17</sup>;
- undertaking Data Protection Impact Assessment (DPIA) to identify and manage data protection risks<sup>18</sup>;
- undertaking Data Protection by Design and by Default to give effect to the data protection principles at the time of determining the means of processing and to integrate the necessary safeguards<sup>19</sup>;
- providing proper notification in the case of a data breach<sup>20</sup>;
- responding to requests by individuals wishing to exercise their rights<sup>21</sup>;
- keeping records of processing activities<sup>22</sup>; and
- drawing up data processing or handling policies or practices to demonstrate compliance and accountability<sup>23</sup>

---

<sup>16</sup> Ibid.

<sup>17</sup> GDPR, Article 37

<sup>18</sup> GDPR, Article 35

<sup>19</sup> GDPR, Article 25(1)

<sup>20</sup> GDPR, Articles 33-34

<sup>21</sup> GDPR, Article 12(3)

<sup>22</sup> GDPR, Article 30

<sup>23</sup> GDPR, Article 24(2)

GDPR imposes harsh fines and penalties for non-compliance. They are designed to make non-compliance extremely costly for entities, especially businesses, regardless of their size. Article 83 prescribes administrative fines for infringements, which could be as high as 4% of an organization's total global turnover, depending on the severity of the violation<sup>24</sup>.

Thus, compliance with its provisions became imperative for all kinds of organisations, including businesses, putting the DPO role in the spotlight.

---

<sup>24</sup> GDPR, Article 83

## 6. The DPO Role in the spotlight

GDPR was not the first to introduce the DPO role. Appointing a DPO was also included in the Directive 95/46/EC<sup>3</sup>, though not as an obligatory action if certain criteria were fulfilled. However, the concept around the role evolved over the years in quite a few EU member states.

The concept of DPO is not new. Although Directive 95/46/EC did not require any organization to appoint a DPO, the practice of appointing a DPO has nevertheless developed in several Member States over the years. In the event of non-compliance, the DPO is not being considered personally responsible under the GDPR. The Regulation explicitly foresees that it is the controller or the processor who is required to ensure and to be able to demonstrate that the processing is performed in accordance with its provisions

Before GDPR was adopted and put into force, the Working Party set up under Article 29 of Directive 95/46/EC (WP29)<sup>25</sup>, suggested that the DPO represents the key element of accountability and can DPO appointment can turn out to be a business' comparative advantage besides promoting compliance<sup>26</sup>.

Further to implementing compliance-oriented tasks, the DPO also has a mediator role among the parties involved, meaning the relevant authorities, the individuals/data subjects, and the different units within the business.

According to IAPP (International Association of Privacy Professionals), before the GDPR take effect, at least 28.000 DPOs were estimated to be needed in Europe and the United States alone and another 75.000 DPO positions would be created around the globe.<sup>27</sup>

---

<sup>25</sup> This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. Website: [http://ec.europa.eu/justice/data-protection/index\\_en.htm](http://ec.europa.eu/justice/data-protection/index_en.htm)

<sup>26</sup> WP29, Guidelines on Data Protection Officers ('DPOs'), Revised and Adopted on 5 April 2017, [http://ec.europa.eu/information\\_society/newsroom/image/document/2016-51/wp243\\_en\\_40855.pdf?wb48617274=CD63BD9A](http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A)

<sup>27</sup> Rita Heimer & Sam Pfeifle, GDPR's global reach to require at least 75,000 DPOs worldwide, The Privacy Advisor, IAPP, 9 November 2016, <https://iapp.org/news/a/study-gdprs-global-reach-to-require-at-least-75000-dpos-worldwide/>



Indicatively, it has been referred that DPO job listings in Britain on the Indeed job search site have increased by more than 700 percent over the past months, from 12.7 listings per every 1 million in April 2016 to 102.7 listings per 1 million in December<sup>28</sup>.

According to Deloitte's General Data Protection Regulation ("GDPR") survey<sup>29</sup>, conducted in the UK, Spain, Italy, Netherlands, France, Germany, Sweden, USA, Canada, India, and Australia, six months after GDPR enforcement, 99% of Indian businesses have appointed a DPO, followed by Spain (96%), and Italy (93%). In contrast, only 76% of businesses in France and 74% of businesses in Australia have assigned a DPO for their organisation<sup>30</sup>.

Demand for DPOs figured in various media under descriptive headings such as "a new job position"<sup>31</sup>. Though not entirely new, the position inevitably generated a new debate on the knowledge, skills and competences required to successfully perform its tasks and responsibilities.

---

<sup>28</sup> Rodriguez S., Rise of the data protection officer, the hottest tech ticket in town, Reuters, 14 February 2018, <https://www.reuters.com/article/us-cyber-gdpr-dpo/rise-of-the-data-protection-officer-the-hottest-tech-ticket-in-town-idUSKCN1FY1MY>

<sup>29</sup>Deloitte. A new era for privacy – GDPR six months on, <https://www2.deloitte.com/uk/en/pages/risk/articles/gdpr-six-months-on.html>

Deloitte's General Data Protection Regulation ("GDPR") survey was based on 1,100 responses from individuals with involvement in GDPR within their organisations and 1,650 responses from consumers. The survey was conducted across 11 countries to get a view on consumer perceptions and organisations' responses to GDPR inside and outside the EU. The countries surveyed were the UK, Spain, Italy, Netherlands, France, Germany, Sweden, USA, Canada, India, and Australia.

<sup>30</sup> Ibid.

<sup>31</sup> Robin Kurzer, GDPR introduces a new job position: The data protection officer, Martech Today, 16 February 2018, <https://martechtoday.com/gdpr-introduces-new-job-position-data-protection-officer-211269>

## 7. The DPO Role under the GDPR

The role of the “Data Protection Officer” is formally recognized by the GDPR as a useful and necessary component of an effective data privacy and protection accountability and compliance framework. More specifically, the key issues of the designation and the position of the DPO, as well as their responsibilities and tasks are foreseen in Articles 37-39.

### 7.1. Designation

Under the GDPR, appointing a DPO is mandatory under three circumstances:

1. The organisation is a **public authority or body**.
2. The organisation’s core activities consist of data processing operations that require regular and systematic **monitoring of data subjects on a large scale**.
3. The organisation’s core activities consist of large-scale processing of **special categories of data** (sensitive data such as personal information on health, religion, race or sexual orientation) and/or personal data relating to criminal convictions and offences.

SMEs (small and medium-sized enterprises) are not exempt from the DPO requirements, should any or all of the above apply to them.

### 7.2. DPO’s Tasks

Article 39 outlines the following tasks for the DPO:<sup>32</sup>

**Information:** One of the tasks of a DPO is to raise data protection awareness, meaning to inform their institutions on their obligations, emanating both from GDPR as well as any other relevant legal framework in national or EU level. Awareness raising involves providing information regarding GDPR compliance obligations internally as well as externally (institution leadership, staff, customers etc.). It also includes capacity-building training for employees involved with data processing.

**Advice:** The DPO should also provide advice with reference to data protection compliance with any relevant legal framework in national or EU level, including GDPR. The task of providing advice has many aspects and is heavily dependent on the organisation’s processing operations. The GDPR specifies that DPOs have to provide advice on data protection impact assessments (DPIA).

---

<sup>32</sup> GDPR, Article 39

**Monitoring:** DPOs have the duty of monitoring the compliance of the organisation with the GDPR, relevant national laws and its own internal and external data protection and security policies. Article 39(1)(b) provides the following non-exhaustive list of matters which DPOs should monitor, namely, assignment of data protection responsibilities, data protection awareness initiatives and training sessions of the staff involved in personal data processing and related audits. DPOs also have the obligation to monitor how DPIAs are performed.

**Cooperation with DPAs:** DPOs are obliged to co-operate with the EU DPAs. This is a significant task of the DPO, especially in the context of multinational companies and their relationship with the lead DPA. The GDPR envisages that DPOs will act as intermediaries between their organisations and EU DPAs in several contexts, including investigations, complaint handling and prior consultation, but also more generally in the context of demonstrating organisational accountability on request by DPAs. DPOs are expected to have detailed knowledge of their organisation's processing operations and business drivers and be able to communicate those to DPAs on request and as appropriate.

**Contact Point for EU DPAs:** DPOs have the obligation to act as the point of contact for EU DPAs on personal data processing issues including prior consultation.

**Contact Point for Individuals/Data Subjects:** Individuals/Data subjects may choose to contact the DPO on all issues related to the processing of their personal data. They may also exercise their GDPR rights, such as access, rectification, erasure, objection and portability, by contacting the DPO.

Finally, as a **horizontal obligation** in the performance of their tasks, DPOs must consider the "risk" of processing operations, taking into account the nature, scope, context and purposes of processing when exercising their tasks.

### 7.3. DPO Knowledge Requirements, Professional Qualities and Abilities

The GDPR foresees in Article 37(5) that "the data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39"<sup>33</sup>.

However, it does not explicitly describe the required "**professional qualities**" and the "**expert knowledge of data protection law and practices**" and the abilities which DPOs should possess in order to carry out their GDPR tasks.

The GDPR knowledge requirement for DPOs raises the following issues:

---

<sup>33</sup> GDPR, Article 37(5)

The first regards that it prescribes that the DPO should possess “expert knowledge of data protection law”. However, it does not specify whether this notion refers to “expert” knowledge of the data protection laws of all the countries in which an organisation operates.

Secondly, the GDPR does not specify whether DPOs should possess knowledge of related fields, such as information security standards.

Existing research and opinions from EU DPO associations and the European Data Protection Supervisor seem to be quite contradictory regarding the knowledge requirement. For example, a study conducted by the German Association for Data Protection and Security concluded that DPOs should also have sound knowledge of information security standards in order to discharge their DPO duties effectively.<sup>34</sup> The European Data Protection Supervisor considers that DPOs should have detailed knowledge of their organisations as well as “good working knowledge” of the relevant data protection laws in order to undertake their tasks effectively.<sup>35</sup>

With reference to “professional qualities” and abilities required DPOs to have to perform their tasks, the GDPR is also vague, as it does not specify them.

However, relevant research reveals recommendations on the required DPO skillset, provided by relevant professional associations:<sup>36</sup>

**Interpersonal and communication skills:** A DPO has to be able to communicate, negotiate, resolve conflicts and build relationships with various external and internal stakeholders (e.g. EU DPAs, individuals, management of the entity, the different entity units, civil society and advocacy groups).

**Organisational and privacy program management skills:** A DPO should possess advanced organisational skills so that they can carry out all their tasks and be able to build, implement and oversee the privacy programs of their organisations effectively.

**Leadership skills:** The DPO is required to have advanced leadership skills so that they can drive data privacy compliance within their organisations and manage a team of data protection lawyers, privacy professionals and other advisors. DPOs who operate within a team should be capable of delegating tasks as well as guiding, instructing and overseeing their team.

---

<sup>34</sup> CIPL GDPR Project DPO Paper, Ensuring the Effectiveness and Strategic Role of the Data Protection Officer under the General Data Protection Regulation, 17 November 2016, [https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/final\\_cipl\\_gdpr\\_dpo\\_paper\\_17\\_november\\_2016.pdf](https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/final_cipl_gdpr_dpo_paper_17_november_2016.pdf)

<sup>35</sup> EDPS (2005), Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001, p 9., [https://edps.europa.eu/sites/edp/files/publication/05-11-28\\_dpo\\_paper\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/05-11-28_dpo_paper_en.pdf)

<sup>36</sup> CIPL GDPR Project DPO Paper, Ensuring the Effectiveness and Strategic Role of the Data Protection Officer under the General Data Protection Regulation, 17 November 2016, [https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/final\\_cipl\\_gdpr\\_dpo\\_paper\\_17\\_november\\_2016.pdf](https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/final_cipl_gdpr_dpo_paper_17_november_2016.pdf)

**Data privacy strategy skills:** DPOs are more than just compliance “box-tick” officers. The role includes setting up the data privacy strategy for their organisations and linking that strategy to business drives and strategy as well as organisational culture.

**Business skills:** The DPO may also perform the role of a chief data strategist and be a business enabler for data-driven innovation, while protecting the fundamental rights and freedoms of individuals/data subjects. As such, the DPO must have a firm understanding of the institutional data strategy and the relevance of data privacy compliance for data and business strategy. The DPO will be required to work closely and ensure a more joined-up relationship with other executives, especially the Chief Information Security Officer, the Chief Information Officer, the Chief Data Officer, the Chief Marketing Officer etc.

**Technology skills:** DPOs should possess a sufficient understanding of the technologies involved in the data processing operations they oversee, as well as of the operations themselves (with the ability to rely on relevant experts).

**External engagement skills:** DPOs will have to be able to represent the company and interact with DPAs in the context of consultations, investigations or enforcement; with individuals, when they exercise their rights under the GDPR; and with organization/business partners, media, industry associations and other third parties.

The DPO role demands a diverse skill set including technical and legal knowledge, commercial awareness, a deep understanding of the business, and strong communication skills. To some extent, the DPO needs to be attentive to detail, understand the technical aspects of data processing activities, as well as how the relevant legislative framework and IT security apply. Simultaneously, the DPO needs to be a big picture thinker, having the ability to view privacy issues within the wider commercial context, thereby helping the business to meet its objectives in a compliant manner.<sup>37</sup>

Although GDPR is quite vague to the DPO knowledge, skills and attitudes requirements, it is obvious that the role emerges as multi-faceted, multidimensional requiring solid knowledge base combined with diverse skills palette including a wide range of soft skills, as well as certain attitudes and abilities.

---

<sup>37</sup> CIPL Discussion Paper (2014), the Role and Function of a Data Protection Officer in Practice and in the European Commission’s Proposed General Data Protection Regulation - Report on DPO Survey Results, [https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/role\\_and\\_function\\_of\\_a\\_dpo\\_in\\_practice\\_report\\_on\\_survey\\_results.pdf](https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/role_and_function_of_a_dpo_in_practice_report_on_survey_results.pdf)

## 8. Trends and challenges in Data Protection posed by GDPR

2018 has been a monumental year of changes in the data protection landscape, across the globe. GDPR, enacted by the EU, could be characterized as the strictest and most complex data privacy law to date, which imposes tough obligations to organizations and businesses and prescribes costly fines for non-compliance.

This data privacy trend dramatically changes the way private entities collect and process individuals' data. Whereas previously penalties on data mishandling were practically non-existent, the GDPR, as well as other international legal frameworks, constitute non-compliance not affordable. New legislation has also expanded the definition of personal data to include identifiable information that is collected automatically, such as online identifiers (i.e. cookies), whereas before this type of data was not considered to be personal data.

Obviously, any entity providing goods or services involving data processing, cannot risk non-compliance. Moreover, organizations and companies must also be continuously informed on new legislation as tougher laws on data privacy emerge in countries aiming to converge with data privacy standards.

With the regulatory framework evolving so quickly, it's hard to stay on top of the latest developments. Faced with increased scrutiny from both regulatory authorities and individuals/data subjects, organizations of all sizes must reassess their practices and take greater responsibility for their actions — or inaction.

Key trends and challenges posed by GDPR, and currently shaping the data protection landscape, within which DPOs are being called to perform are:

- **It is expected that data privacy will prioritize both data subjects and the organization:** while in the last years, data protection aimed primarily at protecting the organization, GDPR has brought about a change in the data privacy concept with protection focus shifting towards the individuals/data subjects. This trend highlights the necessity of cultural change in the world of business which can be achieved by a more intensive legal and operational nature training. In this way, the trainees and future DPOs will be able to understand the new GDPR culture and environment and adjust their business culture and way of operating accordingly.
- **GDPR will remain open to interpretation:** GDPR remains ambiguous, open to interpretation variations. Almost a year after the regulation went into effect, entities are still confused about its practical application, attestation practices and whether they're compliant. This confusion will most probably continue to exist and differentiated interpretations also.

The ever-increasing conversations about GDPR compliance inside and outside organizations — and the ever-increasing number of companies that reaches out vendors in order to make

compliance easier on them, indicates the increasing necessity for DPOs to get equipped with solid knowledge and adaptive skill set.

As GDPR interpretation, implementation and operation evolves, the DPO role will also be evolving, thus requiring flexibility and adaptability. Aiming to address these challenges, the DPO role seems to be increasingly going beyond the traditional mid-level compliance manager function and typically including being a strategic advisor on the responsible and innovative use of personal data.

Therefore, the DPO emerges as a strategic leader, business enabler and data strategist. Given this role, a wide range of skills and expertise are required for effective performance.

## 9. Established and applied curricula in Greece

As it concerns the established curricula in Greece, the consortium collected 5 available courses. In detail, the courses are:

1. **Certificate of Knowledge and Skills for the Protection of Personal Data** provided by “Veritas- Vocational training and studies” organization<sup>38</sup>
2. **DPO Certification Master Class** provided by the “Priority Quality Consultants” Vocational training organization<sup>39</sup>
3. **DPO EXECUTIVE** provided by “TUV Austria” certification body<sup>40</sup>
4. **DATA PROTECTION OFFICER (DPO)** (provided by “Legal Library”<sup>41</sup>
5. **Data Protection Training & Certification** provided by “DPO Training” Vocational training organization<sup>42</sup>.

From the selected sample, we can see that even though all the courses are provided by Vocational Training Organizations there is not a clear common practice in terms of structure and training method. The only common trend that is identified is the number of training hours which seem to range from 32hrs to 40hrs and the total absence of WBL programs. This heterogeneity in the Greek GDPR/ DPO training market depicts the ambiguity that exists in the market regarding the DPO role and the GDPR in general. More specifically, the Greek market seems to slightly trust more the “e-learning” training method than the “in-presence” one, with 3 out of the 5 available courses to be offered on-line. As it concerns the certification methods, the market is looking forward to providing a certificate by a nationally recognized certification body (ELKEDIM, TUV, ACTA etc), only after a successful exam. Only one of the documented courses provide just a course completion certificate by SEKASE.

With reference to the prevalent module types in Greece, the picture is quite balanced. The operational modules along with the legal ones, seem to gather the highest percentages with 31% & 30% respectively. The introductory modules follow with 20% and the IT modules with 19%. As the chart below shows, the courses in the Greek market are well structured with no big differentiations as it concerns the nature of the offered modules.

---

<sup>38</sup> Certificate of Knowledge and Skills for the Protection of Personal Data provided by “Veritas-Vocational training and studies” organization, <https://veritas.edu.gr/pistopoiitiko-gnoseon-gdpr/>

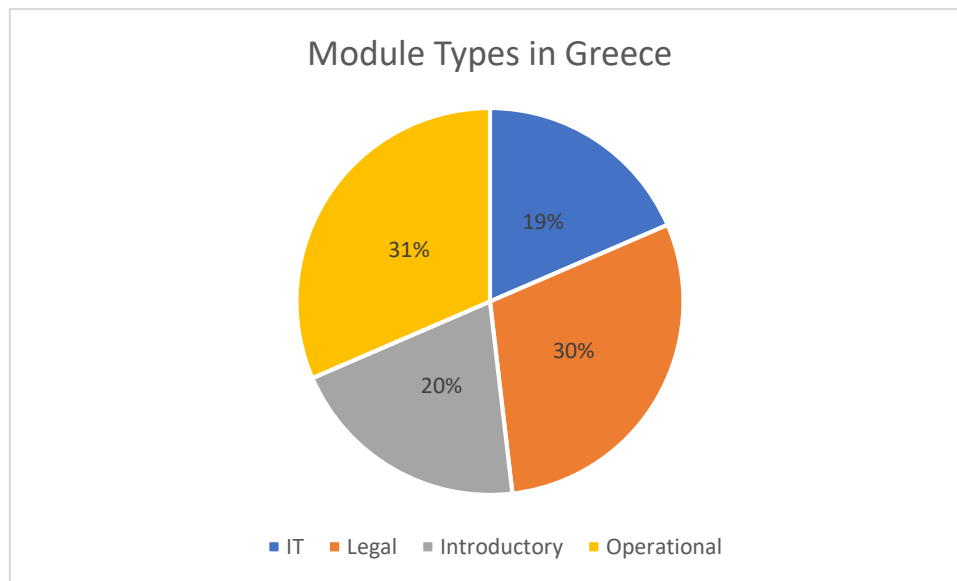
<sup>39</sup> DPO Certification Master Class provided by the “Priority Quality Consultants” Vocational training organization, <https://www.priority.com.gr/page/gdpr-dpo-training>

<sup>40</sup> DPO EXECUTIVE provided by “TUV Austria” certification body, [https://www.tuvaustria.academy/category\\_id=42%26service\\_id=138](https://www.tuvaustria.academy/category_id=42%26service_id=138)

<sup>41</sup> DATA PROTECTION OFFICER (DPO) (provided by “Legal Library”, <https://www.nb.org/greek/catalog/product/view/id/16758/s/data-protection-officer-accredited-course-v15/category/224/>)

<sup>42</sup> Data Protection Training & Certification provided by “DPO Training” Vocational training organization <http://www.dpotraining.gr/online6.html>





*Figure 1 Module Types in Greece*

Despite the lack of common trends in the training methods and course structure in Greece, our data depicts a stability as it concerns the certification methods and the modules mix.

## 10. Established and applied Curricula in Germany

Regarding the applied curricula in Germany, the consortium collected the following five courses:

1. **DPO** provided by “Institut für Managementberatung (IFM)” vocational training organization<sup>43</sup>
2. **Introduction to duties of a company DPO** provided by “Forum für Datenschutz (FFD)” vocational training organization<sup>44</sup>
3. **Training for a DPO (GDPR, BDSG)** provided by “Deutsche Gesellschaft für Informationssicherheit AG” vocational training organization<sup>45</sup>
4. **Certified EU General Data Protection Regulation (EU GDPR)** provided by “The Knowledge Academy” vocational training organization<sup>46</sup>
5. **Certified Data Protection Officer** provided by provided by “The Knowledge Academy” vocational training organization<sup>47</sup>

As it concerns the structure of the available courses, our sample shows a substantial differentiation from the Greek courses. The training duration is significantly more extended as it ranges from 1 day to 20 days. Also, we can observe a high balance between the four module types (see figure 1). However, the overall picture remains the same, with the operational and legal type modules to keep the first two places holding the highest percentages and the IT modules to have the smallest percentage among the four module types.

---

<sup>43</sup> DPO provided by “Institut für Managementberatung (IFM)” vocational training organization, <https://ifm-business.de/privatpersonen/geofoerderte-weiterbildung/management/datenschutzbeauftragter/>

<sup>44</sup> Introduction to duties of a company DPO provided by “Forum für Datenschutz (FFD)” vocational training organization <https://www.ffd-seminare.de/veranstaltungen/seminare/seminar/einfuehrung-in-die-aufgaben-des-betrieblichen-datenschutzbeauftragten.html>

<sup>45</sup> Training for a DPO (GDPR, BDSG) provided by “Deutsche Gesellschaft für Informationssicherheit AG” vocational training organization, <https://akademie.dgi-ag.de/ausbildungen-und-seminare/datenschutz/dsb>

<sup>46</sup> Certified EU General Data Protection Regulation (EU GDPR) provided by “The Knowledge Academy” vocational training organization, <https://www.theknowledgeacademy.com/de/courses/gdpr-training/certified-eu-general-data-protection-regulation-gdpr/>

<sup>47</sup> Certified Data Protection Officer provided by provided by “The Knowledge Academy” vocational training organization, <https://www.theknowledgeacademy.com/de/courses/gdpr-training/certified-data-protection-officer-cdpo/>

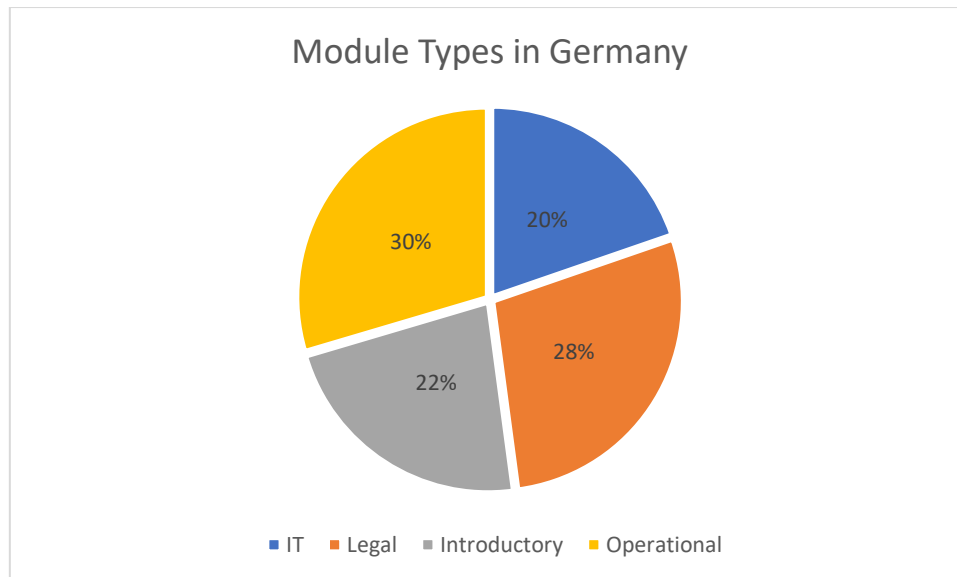


Figure 2 Module Types in Germany

In addition, concerning the certification methods, a preference towards simple Course Completion Certificates instead of certifications by a recognized certification body is noticed. Only 2 out of the 5 documented courses provide a certification by exam. This event highlights the results of the absence of an officially recognized GDPR certification body and the ambiguity of the market.

Finally, the absolute prevalence of the “in-presence” teaching method against the “e-learning” method needs to be highlighted. Only 1 out of the 5 recorded courses has “e-learning” as option. This trend can easily be linked with the long duration of the courses, since the e-learning ones tend to be shorter. Also, it is important to highlight the WBL and/or apprenticeships programs are also absent from all the recorded courses.

## 11. Established and applied Curricula in Cyprus

As it concerns the available curricula in Cyprus, the consortium documented the below four courses:

1. **Privacy & Data Protection Foundation**, provided by European Institute of Management and Finance (EIMF)<sup>48</sup>
2. **Privacy & Data Protection Practitioner**, provided by European Institute of Management and Finance (EIMF)<sup>49</sup>
3. **Certified Data Protection Officer (CDPO)**, provided by “The Knowledge Academy” vocational training organization<sup>50</sup>
4. **ROLE AND TASKS OF THE DATA PROTECTION OFFICER (DPO) BASED ON THE NEW GENERAL REGULATION ON PROTECTION OF PERSONAL DATA**, provided by Cyprus Chamber of Commerce and Industry (CCCI)<sup>51</sup>

Regarding the course structure, the training duration of the recorded courses varies from 1 to 3 days. Also, we can see again the same picture as it concerns the module types of the courses. Once again, the operational and legal modules hold a significant percentage and the first two places of the pie. The IT modules comes once again last in the module mix of the courses with 18% (see figure 3). Until now, the IT knowledge deficit is prevalence in all three partner countries.

---

<sup>48</sup> Privacy & Data Protection Foundation, provided by European Institute of Management and Finance (EIMF), <https://eimf.eu/courses/exin-privacy-data-protection-foundation-certificate-in-general-data-protection-regulation-2/>

<sup>49</sup> Privacy & Data Protection Practitioner, provided by European Institute of Management and Finance (EIMF), <https://eimf.eu/exin-general-data-protection-practitioner-certificate/>

<sup>50</sup> Certified Data Protection Officer (CDPO), provided by “The Knowledge Academy” vocational training organization, <https://www.theknowledgeacademy.com/cy/courses/gdpr-training/certified-data-protection-officer-cdpo/>

<sup>51</sup> ROLE AND TASKS OF THE DATA PROTECTION OFFICER (DPO) BASED ON THE NEW GENERAL REGULATION ON PROTECTION OF PERSONAL DATA, provided by Cyprus Chamber of Commerce and Industry (CCCI), <http://www.ccci.org.cy/seminar-for-data-protection-officer-dpo/>

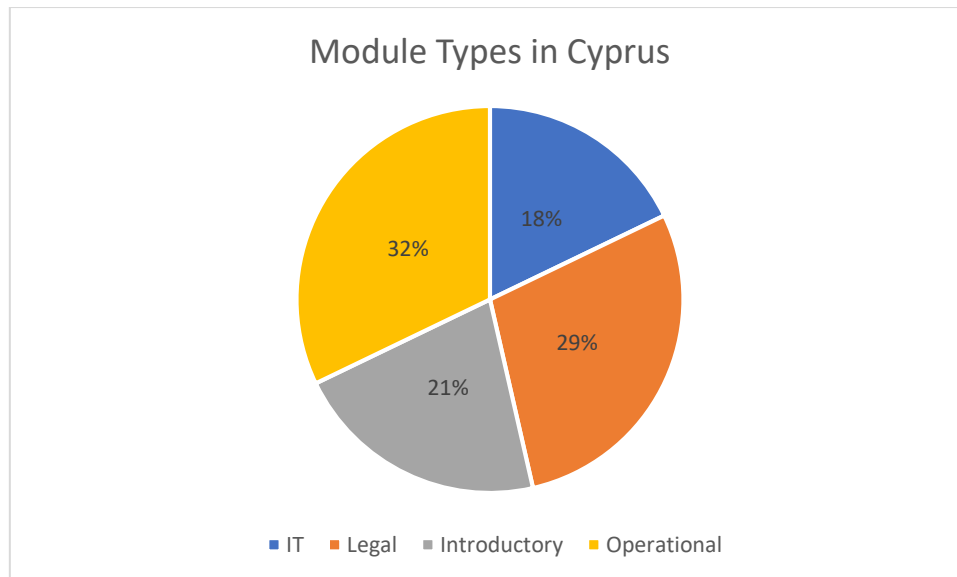


Figure 3 Module Types in Cyprus

Additionally, regarding the teaching methods, the absolute prevalence of the “In-presence” method, just like in the German market, is identified. Only 1 out of the 4 recorded courses provides “e-learning” as an option. However, the Cypriot market does not follow the logic of the German one regarding the long duration of training. The Cypriot market stands in the middle with short “in-presence” courses.

Finally, concerning the certification methods there is a balance between “Certificate by exam” and “Course Completion Certificate”, with 2 out of 4 modules to offer just the Course Completion Certificate. Once again, the WBL/apprenticeships component is also absent from all the recorded courses.

## 12. Established and applied Curricula in other EU countries beyond the consortium and in international level

For the desktop research to have a more complete view of the global GDPR training market, the consortium gathered three courses from EU countries and beyond the consortium, one from the USA and one from Singapore. Also, the sample was enriched with another two courses offered by IAPP as a Global Standard respectively.

More specifically, the recorded courses are:

### EU Countries beyond the consortium

1. **Data Protection: Refresher and Advanced Course for DPOs and Data Protection Experts**, Luxemburg, provided by EIPA<sup>52</sup>
2. **Advanced Data Protection Officer (DPO) program**, Spain, provided by Institute of Advanced Management<sup>53</sup>
3. **European Data Protection Regulation**, Spain, provided by AENOR<sup>54</sup>

### International Level

1. **Certified GDPR Foundation and Practitioner Online Combination Training Course**, USA, provide by "IT Governance"<sup>55</sup>
2. **General Data Protection Regulation (GDPR) & application on Asia**, Singapore, provided by "DPEX"<sup>56</sup>
3. **European Data Protection Online Training**, provided by IAPP<sup>57</sup>
4. **Privacy Program Management**, provided by IAPP<sup>58</sup>

As it concerns the structure of the recorded courses, the training duration varies from 2 days to 5 days and from 3 hours to 180 hours. Also, a high balance between the four module types (see figure 4) is observed.

---

<sup>52</sup> Data Protection: Refresher and Advanced Course for DPOs and Data Protection Experts, Luxemburg, provided by EIPA, <https://www.eipa.eu/product/data-protection-refresher/>

<sup>53</sup> Advanced Data Protection Officer (DPO) program, Spain, provided by Institute of Advanced Management, <https://www.ceuiam.com/en/business-school/officer-data-protection--course>

<sup>54</sup> European Data Protection Regulation, Spain, provided by AENOR, <https://www.en.aenor.com/formacion/encuentre-su-curso/detalle?c=8c8bc300-1273-e911-a84f-000d3a45a2ae>

<sup>55</sup> Certified GDPR Foundation and Practitioner Online Combination Training Course, USA, provide by "IT Governance", <https://www.itgovernanceusa.com/shop/product/certified-gdpr-foundation-and-practitioner-online-combination-training-course>

<sup>56</sup> General Data Protection Regulation (GDPR) & application on Asia, Singapore, provided by "DPEX", [https://www.dpexcentre.com/courses/exin-gdpr/gdpr\\_sg/#tab-id-1](https://www.dpexcentre.com/courses/exin-gdpr/gdpr_sg/#tab-id-1)

<sup>57</sup> European Data Protection Online Training, provided by IAPP, <https://iapp.org/store/trainings/a191a00000zezzAAA/>

<sup>58</sup> Privacy Program Management, provided by IAPP, <https://iapp.org/store/trainings/a191a000001KfwUAAS/>

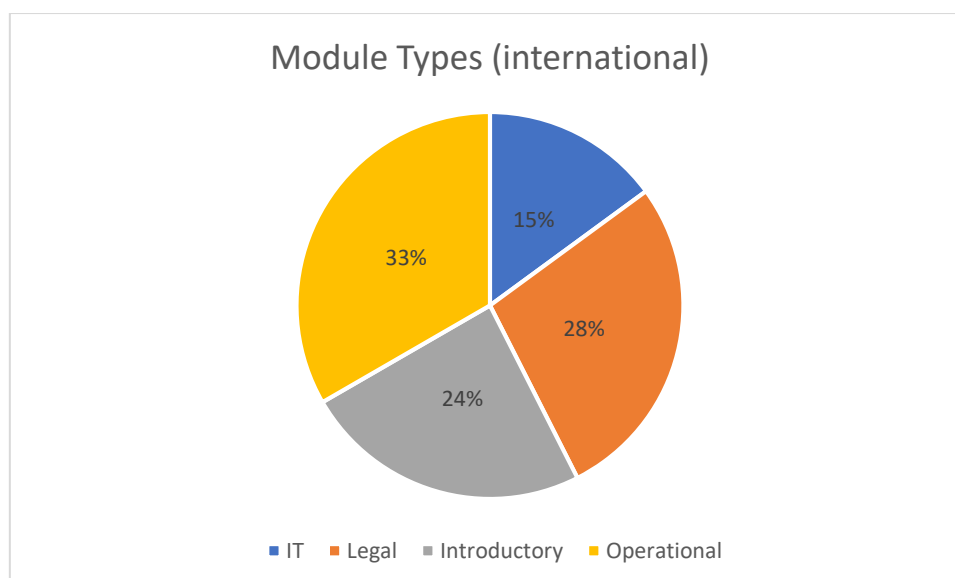


Figure 4 Module Types (International)

However, the overall picture remains the same, with the operational & legal type modules to keep the first two places holding the highest percentages and the IT modules to have the lowest percentage among the four module types. The IT knowledge deficit seems to be an international trend that calls for immediate action in the light of the digital transformation of the data protection sector.

In addition, concerning the certification methods, there is a preference towards a simple Course Completion Certificate instead of certifications by a recognized certification body. 3 out of the 7 documented courses provide a certification by exam, though this exam is optional. This event not only highlights but reassures the impact of the absence of an officially recognized GDPR certification and the ambiguity of the market regarding the business needs and the nature of the GDPR.

Finally, the balance between the “in-presence” teaching method and the “e-learning” method in the international sample needs to be highlighted. 4 out of the 7 recorded courses offer “e-learning” training while the remaining 3 are “in-presence” courses. Also, it is important to observe once more, the absence of WBL and/or apprenticeships programs and the necessity that derives from this clue.

## 13. Comparative Analysis

The partnership recorded several VET courses addressed to DPOs in consortium countries (Greece, Germany, Cyprus), EU member states beyond the partnership such as Spain and Luxemburg, and third countries such as USA & Singapore. The available VET courses were collected through a common template to compare teaching modules offered, training methods and types of certification.

Some characteristics are horizontal across the majority of the offered training curricula. The methodology is based on the predefined elements that characterizes each course and the main areas are described below:

### 13.1. Learning objectives

The learning objectives of all the collected courses are:

- Present an overview of the European Data Protection regulations, highlighting the practical aspects that affect the entities responsible for the treatments and their service providers
- Know the basic principles of the new Data Protection regulations
- Offer a detailed analysis of the obligations that affect those public and private entities that process personal data
- Learn to manage the rights of those affected
- Know the new sanctioning regime, as well as the functions assumed by national authorities and community institutions in the control of Compliance with Data Protection regulations
- Expose the new security obligations and methodologies for their implementation
- Analyze the functions that will be carried out by the Data Protection Officer (DPO), obtaining the knowledge of the regulations required to carry them out

At the end of the courses/ seminars, the trainees would be able to inform and advise clients and their businesses responsibly to fully comply with GDPR requirements, providing specialized advice and services to avoid errors and penalties.

Despite the absence of a common Occupational Profile, there is an unanimity towards certain learning objectives. This fact depicts a clear need of the labor market and serves as a roadmap for the future courses to come.

The same unanimity is noticed regarding the target groups too.



## 13.2. Target groups

Most of the documented courses have a very broad target group with no special prerequisites required to take the course. This can be explained not only by the absence of a European DPO Occupational profile but also from the broad range of supportive positions that job openings demand instead of a standalone DPO position (see figure 1).

The following table summarizes the target groups per course collected:

Country	Title	Target groups
Greece	DPO Certification Master Class	DPOs and executives, regardless of their background
Greece	DPO Executive	DPO executives; future DPO professionals; senior executives; professional groups involved in the collection, processing and use of data; non-privacy professionals who have privacy as part of their responsibilities
Greece	Data Protection Officer (DPO)	Managers (CEO, COO, DG, Marketing, Production, etc.); compliance officers; IT& communication executives; lawyers; law firms; insurance companies; banks; telecommunications providers; local government; hotels; transport companies; hospitals& diagnostic centers; web services & e-shops; public services; energy sector; private companies
Greece	Data Protection Training & Certification	Lawyers; executives; IT& communication executives
Germany	DPO	Data protection Officers; beginner-level DPOs with no prior knowledge of EU GDPR.
Germany	Introduction to duties of a company DPO	DPOs; HR managers; executives on data processing, general organization, law and controlling; IT consultants; head& employees of legal departments
Germany	Training for a DPO (GDPR, BDSG)	DPOs; IT security officers; information security managers; risk managers; compliance responsibilities; executives; business consultant; auditors
Germany	Certified EU General Data Protection Regulation (EU GDPR) Foundation and Practitioner	Information security professionals; compliance officers; DPOs; risk managers; privacy managers; IT security professionals
Germany	Certified Data Protection Officer (CDPO)	DPOs; data protection professionals and personnel; information officers; compliance officers; HR managers
Cyprus	Privacy & Data Protection Foundation	DPOs with no prior GDPR knowledge
Cyprus	Privacy & Data Protection Practitioner	DPOs with no prior GDPR knowledge

Cyprus	Certified Data Protection Officer	Management executives; marketing executives; financial managers; HR managers; compliance managers; information security officers; IT Managers
Cyprus	Role and tasks of the Data Protection Officer based on the new general regulation on protection of personal data	Senior executives; DPOs
Luxembourg	Data Protection: Refresher and Advanced Course for DPOs and Data Protection Experts	DPOs; data protection experts& advisors; anyone from public and private sector responsible for GDPR compliance
Spain	Advanced Data Protection Officer (DPO) program	Experienced DPOs; legal postgraduates
Spain	European Data Protection Regulation	Internal& external auditors; consultants; lawyers; data protection services professionals; security personnel; regulatory compliance offices
USA	Certified GDPR Foundation and Practitioner Online Combination Training Course	Business directors/ managers; GDPR compliance managers; individuals with basic knowledge
Singapore	General data protection regulation & application on Asia	DPOs; privacy officers; legal officers; compliance officers; security officers; business continuity managers
iapp/ International	European Data Protection Online Training	Professional who plan to be certified; individuals who want to deepen their GDPR knowledge
iapp/ International	Privacy Program Management	Professional who plan to be certified; individuals who want to deepen their GDPR knowledge

Table 1 Target Groups

From the table data, it can be summarized that the main target groups are:

- Managers
- Compliance Officers
- IT & Communication executives
- Lawyers and Law Firms
- DPO's
- HR managers
- Anyone in the public or private sector who is responsible for their organization's compliance with the GDPR

This broad target group base indicates the general nature of the courses, which can also be noticed by the module structures. This characteristic can be justified by the need of the offered courses to have a general application and address to a larger audience as an answer

to the deficiencies of the data protection sector. However, the ability of specialization of the courses through elective teaching modules can enhance their quality and the adaptability of the where it is needed.

In the following chapters, the structure, the nature and the goals of the documented courses are being further analyzed.

### 13.3. Training Delivery Methods

In general, the types of training delivery fall into two basic categories: In- presence (classroom-based) courses and e-learning courses. As it concerns the sample, there is a clear prevalence of the in-presence training delivery method (58%) against the e-learning method (32%). There is also a small percentage of courses which are available in both ways (10%).

The below table summarizes the training delivery methods per course collected:

Country	Title	Training delivery method
Greece	Certificate of Knowledge and Skills for the Protection of Personal Data	E-learning
Greece	DPO Certification Master Class	E-learning
Greece	DPO Executive	In-presence
Greece	Data Protection Officer (DPO)	In-presence, video (live streaming)
Greece	Data Protection Training & Certification	E-learning
Germany	DPO	In-presence
Germany	Introduction to duties of a company DPO	In-presence
Germany	Training for a DPO (GDPR, BDSG)	In-presence
Germany	Certified EU General Data Protection Regulation (EU GDPR) Foundation and Practitioner	In-presence; live Virtual; e-learning
Germany	Certified Data Protection Officer (CDPO)	In-presence
Cyprus	Privacy & Data Protection Foundation	In-presence
Cyprus	Privacy & Data Protection Practitioner	In-presence
Cyprus	Certified Data Protection Officer	In-presence; e-Learning
Cyprus	Role and tasks of the Data Protection Officer based on the new general regulation on protection of personal data	In- presence
Luxembourg	Data Protection: Refresher and Advanced Course for DPOs and Data Protection Experts	In- presence
Spain	Advanced Data Protection Officer (DPO) program	E-learning

Spain	European Data Protection Regulation	In- presence
USA	Certified GDPR Foundation and Practitioner Online Combination Training Course	E-learning
Singapore	General data protection regulation & application on Asia	In- presence
iapp/ International	European Data Protection Online Training	E-learning
iapp/ International	Privacy Program Management	E-learning

Table 2 Training delivery methods

Between these two categories, significant differences regarding their teaching techniques can be traced. The in-presence courses mostly include a mix of lectures and assignments based on case studies at the end of each module.

On the other hand, the e-learning courses are based mostly on video lectures- on- demand or scheduled by the course provider-, virtual lectures and on-line assignments. However, the prevalence of the offline teaching technique cannot be justified only by the structure of the course.

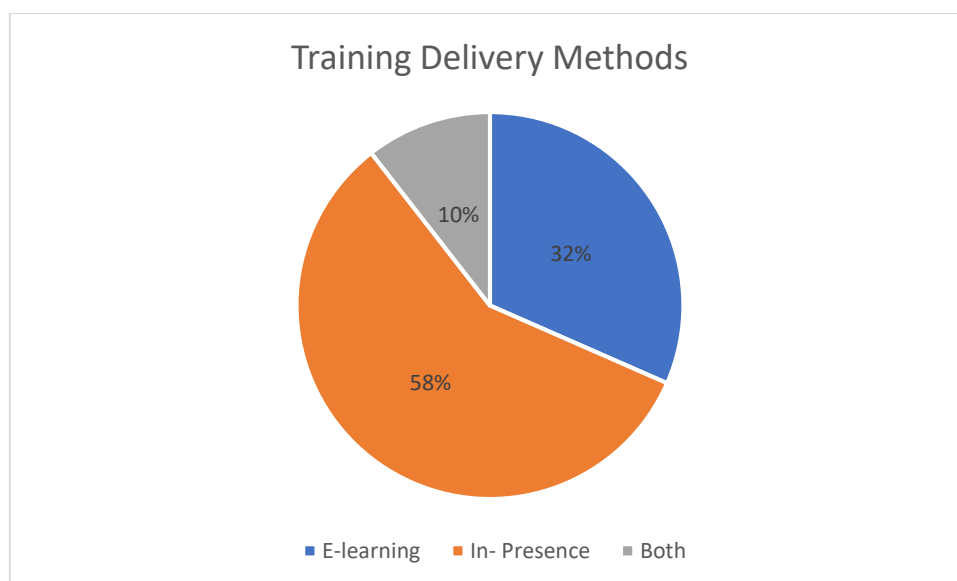


Figure 5 Training Delivery Methods

It is commonly known that the on-line courses tend to be more popular than the offline ones nowadays. Recent research of Bersin by Deloitte,<sup>59</sup> Fosway and many more revealed the

<sup>59</sup> Bersin by Deloitte, Leading in Learning Building capabilities to deliver on your business strategy, <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/HumanCapital/gx-cons-hc-learning-solutions-placemat.pdf>

learning habits of modern professionals in 2018.<sup>60</sup> The results paint a picture of employees adapting to cope with the fast pace of modern working life. They are often busy and overwhelmed but still keen to learn; they value high quality content that's personalized and relevant to their needs; and they are getting increasingly impatient and turned off by content and experiences that isn't high value, relevant, and available when they want it.

Both employees and employers struggle to justify the time spent in classrooms. The benefits of digital learning for business are as powerful as the ones for learners. From an efficiency perspective, not only is it more cost effective to design and deliver learning digitally rather than flying facilitators around the world, but online learning also reduces 'seat time' for learners, so your people can spend less time in the classroom and more time contributing to the success of their business.

On the other hand, the biggest opportunity that face to face training presents is the ability to discuss, collaborate, practice and role play, all 'live' and with guidance from a facilitator on hand. Being part of a group and held accountable are powerful learning tools, and these opportunities to apply learning are a good reason to bring employees together at the same time. This is probably how the trend of the offline courses prevalence in the data protection sector can be explained.

Most of the offered courses consist of Operational (33%) and Legal (31%) modules (see figure 4). The nature of these modules and their practical application through assignments require the possibility of collaboration, discussion and role play. The close guidance from the lecturer is of paramount importance for the concrete understanding of the practical application of the module and the purpose of the assignment.

A critical element identified, is the **total absence of mandatory and elective modules**. This fact enhances the theoretical and general nature of the offered courses making them suitable for the broad nature of the desired target group. Until now, the documented courses cover a general approach of the GDPR and DPO subjects applicable to vast majority of businesses and organizations. However, there are no sufficient sector-tailored courses regarding DPO and GDPR issues (DPO training focused on specific business sectors such as healthcare sector, tourist sector etc).

On the one hand, the inclusion of **elective teaching modules could enhance the flexibility and the thematic areas covered**. It can also broaden the target groups since it could include trainees from specific business sectors who are seeking targeted knowledge. On the other hand, **this approach could take place in more IT topics and sector specific topics**.

Another critical component that is entirely absent from the courses collected is the **WBL and Apprenticeship Programs**.

---

<sup>60</sup> Fosway Group, Digital Learning Realities Research 2018, <http://www.fosway.com/research/next-gen-learning/digital-learning-realities-2018/>

### 13.4. Module Types

In terms of knowledge, the documented courses offer both theoretical and practical knowledge in specific areas. Special focus is given to the Operational courses where the DPOs' are learning how to implement and manage the legal outcomes of the GDPR in their businesses and control and manage different types of crisis and problems that may occur.

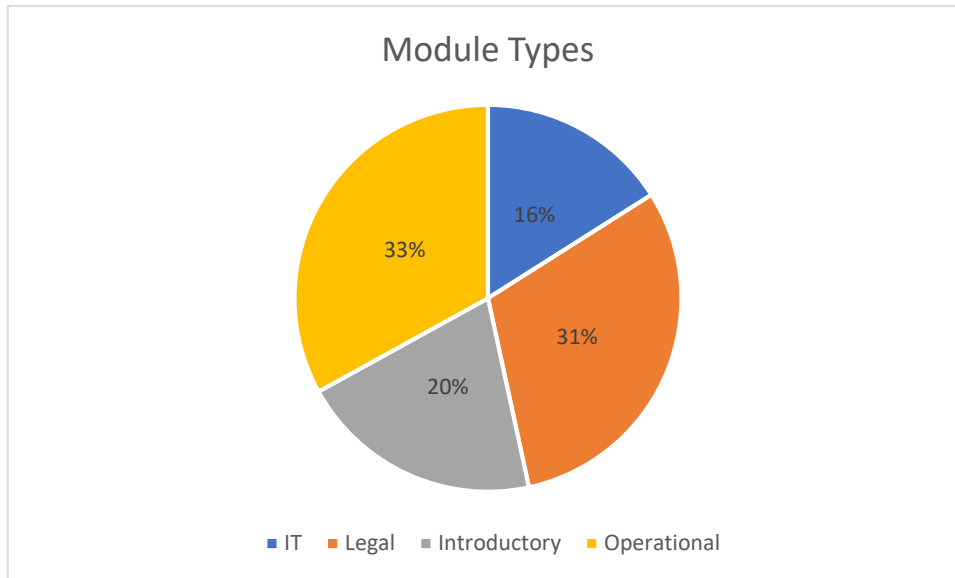


Figure 6 Module Types

The type and the number of the teaching modules of all courses were summarized in order to better understand the focus and the time dedicated to specific training areas. The graphs below depict horizontally the percentage per module type (Figure 4) and the number of modules per module type (Figure 5).

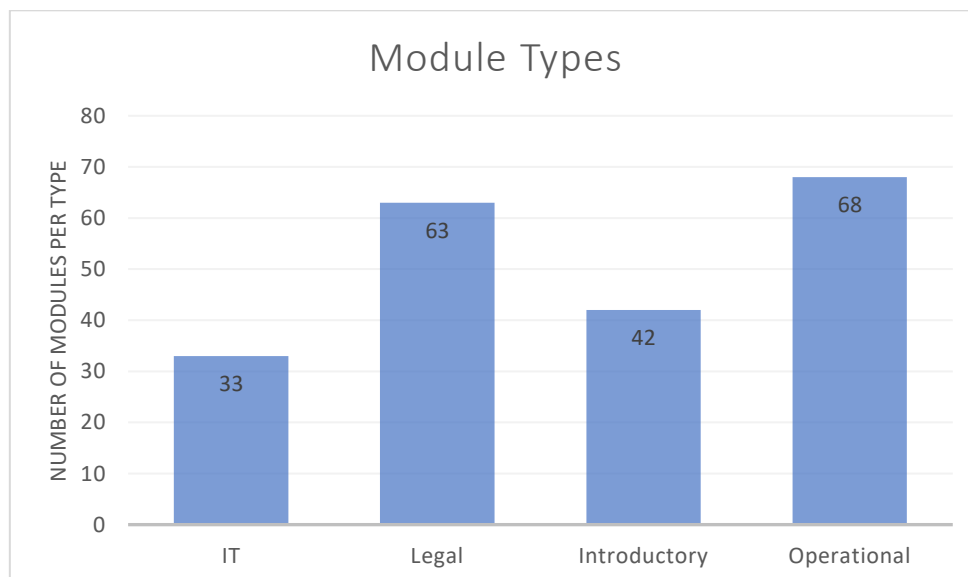


Figure 7 Module types (2)

The operational modules (33%) are the main area of interest while legal (31%) and introductory (20%) modules have also an important share. IT modules have the lowest percentage among the delivered courses (16%).

The reason of the above result lies to the goal and the nature of the courses. The existing courses are mainly fast-track courses with duration from 14hrs to 180hrs and 1 to 20 days and are addressed to a broad target group (Managers, Compliance Officers, IT & Communication executives, Lawyers and Law Firms) with no specific IT capabilities required.

As a result, the courses are mainly focused on providing soft skills and practical implementation of the legal and introductory deliverables of the course. This fact justifies the face to face training delivery method.

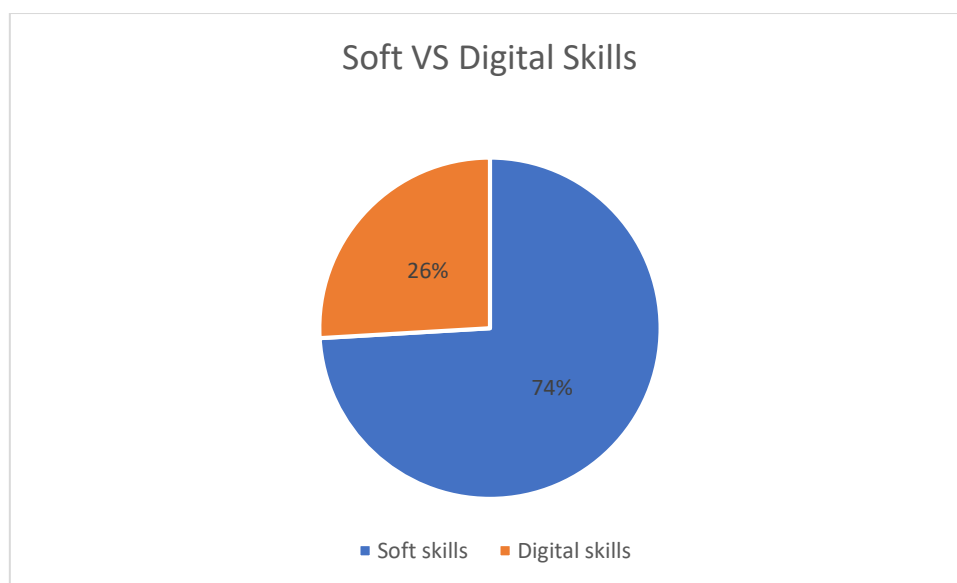


Figure 8 Soft VS Digital Skills

The table below can provide an indicative overview of the content of each module type:

Module Types	Content in terms of courses
<b>IT</b>	Data Breach Incident Response; Information security measures to protect personal data; Cyber Privacy Insurance; Data Security; Clouding Computing & Social Media; Implementation of technical security; Security by Design; Security of Processing;
<b>Legal</b>	Legal Requirements; Rights of Individuals; Consideration of Interconnected Laws; Lawful processing of personal Data; Controlling Authorities and Penalty system; The rights of Data Subjects; Data Protection Laws; Compliance; Applicable laws and Regulations;
<b>Introductory</b>	Introduction to GDPR; The Content of Personal Data; Data Protection Officer; Scope of the DPO Duties; Definitions of Data Protection; Key GDPR Terminology; Principle of the GDPR; Fundamental of Data Protection;

<b>Operational</b>	Instructions for Business Preparation; Data Breach Incident Response; Information security measures to protect personal data; Risk Management; Business Continuity; Communication; Dissemination in a Corporate Group; DP Audit; Data Protection Impact Assessment (DPIA); Incident Response Plans; Accountability; Privacy Governance;
--------------------	---

Table 3 Module Type Content

### 13.5. Methods of Certification

The assessment methods recorded, cover a range of three methods: a) **Certification by exam**, b) **Course Completion Certificate** and c) **Optional Exam**. In general, the assessment procedure should be valid and reliable, which means that more than one type of assessment should be incorporated in one course providing complementarity.

The below table summarizes the certification methods per course collected:

Country	Title	Methods of Certification
Greece	Certificate of Knowledge and Skills for the Protection of Personal Data	Optional exam
Greece	DPO Certification Master Class	Certification by exam
Greece	DPO Executive	Certification by exam
Greece	Data Protection Officer (DPO)	Course Completion Certificate
Greece	Data Protection Training & Certification	Certification by exam
Germany	DPO	Course Completion Certificate
Germany	Introduction to duties of a company DPO	Course Completion Certificate
Germany	Training for a DPO (GDPR, BDSG)	Certification by exam
Germany	Certified EU General Data Protection Regulation (EU GDPR) Foundation and Practitioner	Certification by exam
Germany	Certified Data Protection Officer (CDPO)	Certification by exam
Cyprus	Privacy & Data Protection Foundation	Certification by exam
Cyprus	Privacy & Data Protection Practitioner	Certification by exam
Cyprus	Certified Data Protection Officer	Course Completion Certificate
Cyprus	Role and tasks of the Data Protection Officer based on the new general regulation on protection of personal data	Course Completion Certificate
Luxembourg	Data Protection: Refresher and Advanced Course for DPOs and Data Protection Experts	Course Completion Certificate



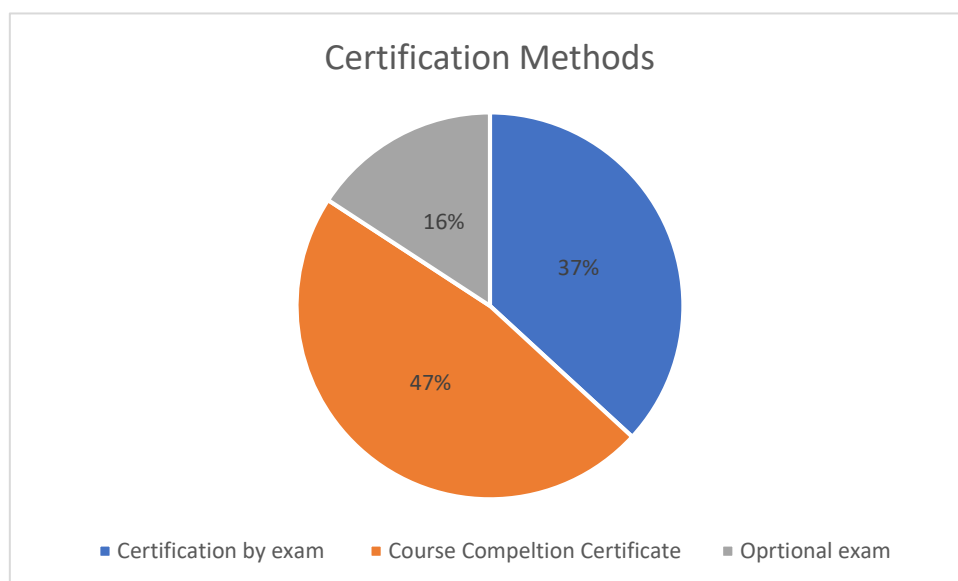
Spain	Advanced Data Protection Officer (DPO) program	Course Completion Certificate
Spain	European Data Protection Regulation	Course Completion Certificate
USA	Certified GDPR Foundation and Practitioner Online Combination Training Course	Certification by exam
Singapore	General data protection regulation & application on Asia	Course Completion Certificate
iapp/ International	European Data Protection Online Training	Optional exam
iapp/ International	Privacy Program Management	Optional exam

Table 4 Methods of Certification

The identified VET trainings have two main types of assessment: a) **Formative assessments** and b) **multiple-choice assessments**.

**Formative assessment** means that the learners are being performance-based evaluated during the teaching procedure and through assignments, exams and their total presence throughout the course. This is a common practice in VET environments and for certification of formal and informal training, since it allows for capturing more complex performance and processes than the computer based.

**Multiple-choice assessment** though written and computer-based exams, comes to complete the formative assessment in the most appropriate way. The low reliability of human rater regarding the performance-based assessment, demonstrates the need of existence of the multiple-choice computer-based performance assessment process. Well-designed multiple-choice questions provide standardised and comparable data on student performance. This is the most common case for courses offered through an online platform.



*Figure 9 Certification Methods*

A great percentage of the offered courses (37%) are following the most widely accepted practice in the labor market by providing a Certificate by a well-known accreditation body only after the successful completion of the training and the exam procedure. This method guarantees and certifies the quality of the knowledge obtained and equips the certificate holder with a strong and complete tool for their professional development in the labor market.

However, most of the courses collected and analyzed (47%) are offering only the Course Completion Certificate after the successful completion of the training course. The award of the Course Completion Certificate is based on the total presence of the learner throughout the course, their presence to the obligatory lectures and their performance in the assignments delivered. By this practice the VET provider offers only the course without the Certification and leaves the learner free to choose if they want to purchase an exam form a certification institute of their choice or stay with the Course Completion Certificate which is also a competitive attribute in the labor market.

As it has already been stated, since there is no formal recognition of any GDPR or DPO certification, this could make it difficult for both hiring companies and job seekers to target the “best” certification for a DPO position. The lack of a certain officially recognised certification leaves space to the certification market for diversification and for different practices among the VET providers.

## 14. Conclusions

The current study provided an overview of the data protection landscape after GDPR enforcement and of the needed skills and knowledge of DPOs in this context. Additionally, provided an outline and comparative analysis of researched and collected VET courses in the Data Protection Sector provided in Greece, Germany, Cyprus, Spain, Luxemburg, USA and Singapore with a view to **what** and **how** is being offered.

On the demand side, the enforcement of GDPR created a new competitive environment, which requires entities, both institutions and companies, to adopt. This new environment asks for DPOs to have “expert knowledge of data protection law and practices”, accompanied by a diverse skill set that includes:

- Interpersonal and communication skills
- Organisational and privacy program management skills
- Leadership skills
- Data privacy strategy skills
- Business skills
- Operational and digital skills - Technology skills
- External engagement skills

On the supply side, the main focus is on the upskill/reskill of the current and future data protection officers in operational, legal and IT skills from a more organizational centered approach.

Despite the absence of a common Occupational Profile, there is an unanimity towards certain learning objectives, including knowledge of data protection regulations, of the obligations emanating from the latter, and of the methods to follow to fulfill those obligations, thus achieving compliance.

It is observed that the supply side currently offers curricula entailing Introductory, Operational, Legal and IT modules. It is also observed that there is a total absence of **soft and/or transversal skills training**.

Moreover, target groups are the widest possible and none of the identified courses are able to offer specialized skills and especially digital skills in specific market sector and areas. **Elective courses** and **adaptability** are missing from all the identified courses.

Adaptability could undoubtedly more easily be achieved through online delivery of the training, which currently holds less prevalence than the in-classroom method.

Also, the **lack of WBL and/or Apprenticeships component** in the curricula identified and analyzed highlights the missing element of “on-hands” learning.

Finally, the absence of formal recognition of the certifications of DPO training currently available is also noted.

## 15. Recommendations for the design and delivery of the DataPRO Curricula

The rapid development of the data protection sector affects the market and the internal processes and flows of the organization. Thus, new needs and challenges will be introduced in the sector in the near future.

Although GDPR is quite vague to the DPO knowledge, skills and attitudes requirements, it is obvious that the role emerges as multi-faceted, multidimensional requiring solid knowledge base combined with diverse skills palette including a wide range of soft skills, as well as certain attitudes and abilities.

The design of the DataPRO Curricula needs to follow a modular approach focusing on the needed balance between hard and soft skills.

The delivery of the DataPRO training course could be enhanced by employing e-learning approaches. In this way DataPRO can reap the benefits of such a technology. In the context of the DataPRO project, the utilization of an e-learning platform is a necessity for several reasons:

- Accommodate different levels of experience and abilities of trainees. Given a self-paced option the trainees can learn at the pace and the depth required offering flexibility and personalised learning experience also through optional courses.
- Enable anytime, anywhere training to adapt training location and schedule to differing needs of trainees. It is expected that a large number of trainees are expected to be trained in out-of-office hours.
- Monitoring of progress through automated grading policy providing a quick and efficient overview of progress. This will allow for interventions, adjustments and improvements in the delivery of the training.
- Engage and motivate learners by providing online discussion where each learner can:
  - participate from any location,
  - participate in multiple concurrent discussions,
  - follow asynchronous discussions where participants do not need to be conversing at the same time in order to participate.

**Modular approach** is a key factor and it means that a two-phase training process will take place:

- First teach the **foundational knowledge** which underlies a specific skill. The aim here is to “bring” all students to the same level of knowledge.
- The second step is the “performance of the skill” reliably and under varying conditions. This can be realised either online (test cases, self-assessments, real work problems) or even in-person training. In any case, the critical part here is that all

students have acquired the needed knowledge in an efficient and cost-effective manner through the DataPRO online platform.

- Towards supporting flexibility, the **existence of mandatory and optional modules** is a good practice in organisational trainings, a **feature that was not present** during the VET curricula research.

Regarding the types of assessments, the research showed that even though the in-presence assessment types can capture a more complex concept, the low reliability of human rater regarding the performance-based assessment, demonstrates the need of existence of the multiple-choice computer-based performance assessment process. Well-designed multiple-choice questions provide standardised and comparable data on student performance. Computer based performance may potentially assess even more complex performances mainly by incorporating peer-reviews, case studies or open response assessment towards measuring more horizontal skills such as the capacity to develop an argument, collaborative work, etc.

Based on the WBL elements researched a critical set of elements needs to be taken into consideration during the curricula design. These elements may be adjusted on a national context taking into consideration specific institutional needs and context:

- **Location** (In and/or outside the workplace depending on institutional environment).
- **Duration** – number of hours of effort and total duration of the DataPRO course.
- **Timing** - after or during work hours – part time or full time
- **Origin of trainers** - Internal and/or external trainers

Finally, beyond certifying the Scheme for DPOs, the recognition of the DataPRO joint qualification will indeed address an unanswered need.

These conclusions and recommendations will be considered in conjunction with the insights and results of the Training Needs Analysis conducted in parallel during the Field Research of the project (deliverables D2.2 and D2.3), and synthesized in D2.4, thus providing the solid knowledge base for the development of the forthcoming project deliverables.

## 16. Annexes

- Annex I. Established and applied curricula in Greece

-1-

<b>COURSE NAME</b>	Certificate of Knowledge and Skills for the Protection of Personal Data <a href="https://veritas.edu.gr/pistopoiitiko-gnoseon-gdpr/">https://veritas.edu.gr/pistopoiitiko-gnoseon-gdpr/</a>
<b>CONTENT AND STRUCTURE</b>	32 Hours training  <b>Modules</b> <ul style="list-style-type: none"> <li>• Introduction to GDPR</li> <li>• Scope of GDPR Application</li> <li>• The Concept of Personal Data</li> <li>• Competent Authorities</li> <li>• Basic Principles, Legislation of Processing and Rights</li> <li>• Personal Data Process Manager</li> <li>• Data Protection Officer (DPO)</li> <li>• Infringement of GDPR provision</li> <li>• Indicative Instructions for Business Preparation</li> </ul>
<b>EXISTING TARGET GROUPS AND THEIR SPECIFIC CHARACTERISTICS</b>	N/A
<b>TRAINING METHODS AND TECHNIQUES</b>	E-learning
<b>ACTIVITIES UNDERTAKEN WITHIN THOSE CURRICULA</b>	Video material Acoustic material Optional exam Certification by ELKEDIM (Greek Lifelong Learning Centers)
<b>IMPACT AND RESULTS</b>	The program will present and analyze the basic principles governing the processing of personal data

	and specify the terms and conditions under which the processing of personal data is legal by the controller and perform the processing, and will also analyze the rights that the data subjects now acquire.
<b>WBL AND APPRENTICESHIP PROGRAMS</b>	N/A

-2-

<b>COURSE NAME</b>	DPO Certification Master Class  <a href="https://www.priority.com.gr/page/gdpr-dpo-training/?gclid=CjwKCAjwqZPrBRBnEiwAmNJsNiQ2pR2o-UpKqjz98UYrB7fhpSZnkcWGLKhIOSDCpT_ISiywC2ndixoCahAQAvD_BwE">https://www.priority.com.gr/page/gdpr-dpo-training/?gclid=CjwKCAjwqZPrBRBnEiwAmNJsNiQ2pR2o-UpKqjz98UYrB7fhpSZnkcWGLKhIOSDCpT_ISiywC2ndixoCahAQAvD_BwE</a>
<b>CONTENT AND STRUCTURE</b>	<p>4 days Training/ 32 hours seminar</p> <p><b>DAY 1</b></p> <ul style="list-style-type: none"> <li>• New Era</li> <li>• Data Protection Officer</li> <li>• Introduction for the Legal Requirements</li> </ul> <p><b>DAY 2</b></p> <ul style="list-style-type: none"> <li>• Legal Requirements</li> <li>• Data Flow Mapping</li> <li>• Data Privacy Impact Assessment (DPIA)</li> </ul> <p><b>DAY 3</b></p> <ul style="list-style-type: none"> <li>• Rights of Individuals</li> <li>• Disclosure of Personal Data Breach to Supervising Body</li> <li>• Transfer of Personal Data</li> </ul> <p><b>DAY 4</b></p> <ul style="list-style-type: none"> <li>• IT &amp; GDPR</li> </ul> <p>The DPO Masterclass analyzes in depth the Regulation, approaching all the perspectives and all the critical issues of GDPR. This e-learning program provides a certificate of successful tracking and can lead to certification by an internationally recognized organization.</p>

<b>EXISTING TARGET GROUPS AND THEIR SPECIFIC CHARACTERISTICS</b>	It is designed for DPOs and executives, regardless of their background, who will take the lead in their business (or their clients) so as to be complaint according to the privacy regulatory framework.
<b>TRAINING METHODS AND TECHNIQUES</b>	E-learning
<b>ACTIVITIES UNDERTAKEN WITHIN THOSE CURRICULA</b>	Online lectures Case Studies Written Exams Certification with ISO 17024 by TUV Austria Certification Body
<b>IMPACT AND RESULTS</b>	Building on the Personal Data Compliance Roadmap methodology, PDCR® analyzes in-depth from all perspectives (operational, legal, technological, process and information security) all the critical issues of GDPR and presents real-world examples of its application to large and small Greek and multinational companies.
<b>WBL AND APPRENTICESHIP PROGRAMS</b>	N/A



<b>COURSE NAME</b>	DPO EXECUTIVE (DATA PROTECTION OFFICER EXECUTIVE TRAINING PROGRAM)  <a href="https://www.tuvaustria.academy/category_id=42%26service_id=138">https://www.tuvaustria.academy/category_id=42%26service_id=138</a>
<b>CONTENT AND STRUCTURE</b>	5 days training  <ul style="list-style-type: none"> <li>• Comprehensive introduction to GDPR (including analysis and understanding of the requirements and actions stemming from GDPR).</li> <li>• GDPR Compliance plan.</li> <li>• Information security measures to protect personal data.</li> <li>• Design and implementation of privacy policies.</li> <li>• Privacy Impact Assessment (PIA).</li> <li>• Data breach Incident Response.</li> </ul>
<b>EXISTING TARGET GROUPS AND THEIR SPECIFIC CHARACTERISTICS</b>	The target audience is:  <ul style="list-style-type: none"> <li>• Executives who work as Data Protection Officers (DPO).</li> <li>• Professionals who are preparing or plan to work as DPOs.</li> <li>• Senior executives.</li> <li>• Professional groups (such as lawyers and law firms, legal advisers, IT &amp; communications executives, information security officers, etc.) involved in the collection, processing, and use of personal data.</li> <li>• Non-privacy professionals who have privacy as part of their responsibilities.</li> </ul>
<b>TRAINING METHODS AND TECHNIQUES</b>	In-presence
<b>ACTIVITIES UNDERTAKEN WITHIN THOSE CURRICULA</b>	Lectures Case Studies Written Exams Certification by TUV Austria Certification Body
<b>IMPACT AND RESULTS</b>	To prepare a specialist who would be ready to take on responsibilities of a DPO whose competences include Data Protection Management, Information Security both theoretical and practical.

<b>WBL APPRENTICESHIP PROGRAMS</b>	<b>AND</b>	N/A
--	------------	-----

-4-

<b>COURSE NAME</b>	DATA PROTECTION OFFICER (DPO)  <a href="https://www.nb.org/greek/catalog/product/view/id/16758/s/data-protection-officer-accredited-course-v15/category/224/">https://www.nb.org/greek/catalog/product/view/id/16758/s/data-protection-officer-accredited-course-v15/category/224/</a>	
<b>CONTENT STRUCTURE</b>	<b>AND</b>	40 training Hours  <b>Structure</b> <ul style="list-style-type: none"> <li>• Legal framework for the protection of personal data</li> <li>• The new national legislative framework on the protection of personal data</li> <li>• Data Protection Officer (DPO) role (DPO definition, independence and conflict of interest, relationship with supervisory authorities)</li> <li>• Information Security</li> <li>• Risk Management</li> <li>• Business Continuity</li> <li>• Data Privacy Impact Assessment (DPIA) (methodologies, standards, training)</li> <li>• Data Breach Management- Incident Response Plan</li> <li>• Cyber Privacy Insurance</li> <li>• GDP GDPR Compliance and Certification.</li> </ul>
<b>EXISTING GROUPS AND THEIR SPECIFIC CHARACTERISTICS</b>	<b>TARGET AND THEIR</b>	<b>Professional Groups</b> <ul style="list-style-type: none"> <li>• Managers (CEO, COO, DG, Marketing, Production, etc.)</li> <li>• Compliance Officers</li> <li>• IT &amp; Communications executives</li> <li>• Lawyers, Law Firms, Law Firms</li> </ul> <b>Bodies</b> <ul style="list-style-type: none"> <li>• Banks &amp; Financial Service Providers</li> <li>• Insurance companies</li> <li>• Telecommunication Providers</li> <li>• Web service providers &amp; e-shops / e-business</li> <li>• Hospitals &amp; Diagnostic Centers, pharmaceutical companies</li> <li>• Collection Agencies</li> <li>• Hotels</li> </ul>

	<ul style="list-style-type: none"> <li>• Public Services, DEKO</li> <li>• Local government</li> <li>• Energy</li> <li>• Transport Companies</li> <li>• Retail Chains &amp; Other Private Companies</li> </ul>
<b>TRAINING METHODS AND TECHNIQUES</b>	In-presence, video (live streaming)
<b>ACTIVITIES UNDERTAKEN WITHIN THOSE CURRICULA</b>	Lectures case studies Course Completion Certificate by SEKASE
<b>IMPACT AND RESULTS</b>	Offers a holistic approach to Data Protection Officers & Privacy Professionals training, specifically tailored to the requirements of the General Data Protection Regulation (GDPR), by DPO's, legal professionals, information security professionals, cyber privacy insurance professionals & Privacy Professionals.
<b>WBL AND APPRENTICESHIP PROGRAMS</b>	N/A

-5-

<b>COURSE NAME</b>	Data Protection Training & Certification <a href="http://www.dpotraining.gr/online6.html">http://www.dpotraining.gr/online6.html</a>
<b>CONTENT AND STRUCTURE</b>	40 training Hours 24/ 40 Hrs of planned online training attendance 16/ 40 Hrs of free online training attendance
<b>EXISTING TARGET GROUPS AND THEIR SPECIFIC CHARACTERISTICS</b>	Attending the seminar is an opportunity for Lawyers, executives, IT and communications executives. Seminar Structure <ul style="list-style-type: none"> <li>• Introductory- Physical Security GDPR</li> <li>• Legal- Organizational GDPR</li> <li>• Techniques- Information Security of GDPR (1)</li> </ul>

	<ul style="list-style-type: none"> <li>Techniques- Information Security of GDPR (2)</li> </ul>
<b>TRAINING METHODS AND TECHNIQUES</b>	E-learning
<b>ACTIVITIES UNDERTAKEN WITHIN THOSE CURRICULA</b>	<p>Online Lectures</p> <p>Written Exams</p> <p>Certification by ACTA</p>
<b>IMPACT AND RESULTS</b>	The seminar students will be able to inform and advise clients and their businesses responsibly to fully comply with GDPR requirements, providing specialized advice and services to avoid errors and penalties.
<b>WBL AND APPRENTICESHIP PROGRAMS</b>	N/A

- Annex II: Established and applied Curricula in Germany

-1-

<b>Course name</b>	<p><b>DPO</b> Datenschutzbeauftragter /TÜV</p> <p>IFM Institut für Managementberatung</p> <p><a href="https://ifm-business.de/privatpersonen/geoerderte-weiterbildung/management/datenschutzbeauftragter/">https://ifm-business.de/privatpersonen/geoerderte-weiterbildung/management/datenschutzbeauftragter/</a></p>
<b>Content and Structure</b>	<p>Number of modules: 4</p> <hr/> <p>Duration: 1 month (20 work days)</p> <hr/> <p>1. Data protection law/Formal requirements/Controlling bodies 1.1. Basics 1.2. Legal consents</p>

	<ul style="list-style-type: none"> <li>1.3. Core areas of data protection</li> <li>1.4. Rights of the persons concerned</li> <li>1.5. Data protection officer in companies</li> <li>1.6. Scope of the DPO duties</li>   <li>2. Data Protection management and organization <ul style="list-style-type: none"> <li>2.1. Data protection-oriented business processes</li> <li>2.2. List of standard tasks</li> <li>2.3. Risk assessment</li> <li>2.4. Assessment of consequences</li> <li>2.5. Implementation of accountability</li> <li>2.6. Required documents, design of the documentation</li> <li>2.7. Audits and certifications</li> <li>2.8. Work organization of the Data Protection Officer</li> </ul> </li>   <li>3. Information security <ul style="list-style-type: none"> <li>3.1. Terms and objects to be protected</li> <li>3.2. Threats to information security</li> <li>3.3. Technical and organizational steps and measures</li> <li>3.4. Aids / tools for a DPO</li> </ul> </li>   <li>4. Communication <ul style="list-style-type: none"> <li>4.1. Conducting effective communication with supervisors and employees</li> <li>4.2. Privacy and internal communication</li> <li>4.3. Internal and external audits</li> </ul> </li> </ul>
<b>Existing target groups and their specific characteristics</b>	Intended for Data Protection Officers to be, beginner-level, no prior knowledge of EU GDR needed.
<b>Training methods and techniques</b>	On campus (in-presence)
<b>Activities undertaken within those curricula</b>	Lectures A series (once a week) of test-project that groups is solving  Course Completion Certificate
<b>Impact and results COMPETENCES</b>	To prepare a specialist who would be ready to take on responsibilities of a DPO whose competences include Data Protection Management, Information Security both theoretical and practical.

<b>WBL Apprenticeship Programs</b>	<b>and</b> N/A
--	----------------

-2-

<b>Course name</b>	<b>Introduction to duties of a company DPO</b> Einführung in die Aufgaben des betrieblichen Datenschutzbeauftragten  FFD Forum für Datenschutz  <a href="https://www.ffd-seminare.de/veranstaltungen/seminare/seminar/einfuehrung-in-die-aufgaben-des-betrieblichen-datenschutzbeauftragten.html">https://www.ffd-seminare.de/veranstaltungen/seminare/seminar/einfuehrung-in-die-aufgaben-des-betrieblichen-datenschutzbeauftragten.html</a>
<b>Content Structure</b>	<b>and</b> Number of modules: 3  Duration: 3 days  Covered topics:  1. Data protection law

	<ul style="list-style-type: none"> <li>1.1. Introduction to the current data protection law</li> <li>1.2. Special categories of personal data</li> <li>1.3. The company data protection officer</li>   <li>2. Work-scope of the company data protection officer               <ul style="list-style-type: none"> <li>2.1. Framework conditions for the company data protection officer</li> <li>2.2. Necessary education, training and documents</li> <li>2.3. Technical and organizational security measures</li> </ul> </li>   <li>3. IT basics and basics of data security               <ul style="list-style-type: none"> <li>3.1. Foundations of Information Security</li> <li>3.2. Computers and computer networks</li> <li>3.3. Services and Applications in the Enterprise: Cloud Computing, Social Media</li> <li>3.4. Implementation of organizational and technical security</li> </ul> </li> </ul>
<b>Existing target groups and their specific characteristics</b>	<ul style="list-style-type: none"> <li>1. New company data protection officer at the beginning of her activity</li> <li>2. HR manager (responsible for appointment of DPO)</li> <li>3. DPO who want to find out about current data protection innovations and / or seek an exchange of experience</li> <li>4. Executives working in the areas of: data processing, general organization, law, controlling</li> <li>5. IT consultant</li> <li>6. Head and employees of the legal department</li> </ul>
<b>Training methods and techniques</b>	In-presence
<b>Activities undertaken within those curricula</b>	<p>Seminar</p> <p>Course Completion Certificate</p>
<b>Impact and results COMPETENCES</b>	Familiarisation with the up-to date state of the field for the personal working with the sensitive data.
<b>WBL and Apprenticeship Programs</b>	N/A

Course 3, ACQUIN	
<b>Course name</b>	<b>Training for a DPO (GDPR, BDSG)</b> Ausbildung zum Datenschutzbeauftragten gemäß DSGVO und BDSG  Deutsche Gesellschaft für Informationssicherheit AG  <a href="https://akademie.dgi-ag.de/ausbildungen-und-seminare/datenschutz/dsb">https://akademie.dgi-ag.de/ausbildungen-und-seminare/datenschutz/dsb</a>
<b>Content and Structure</b>	Number of modules: 1 (no pre-set structure)  Duration: 3 days  <ol style="list-style-type: none"> <li>1. Definitions of data protection</li> <li>2. Definitions of information security</li> <li>3. DP and informational self-determination</li> <li>4. Consideration of interconnected laws</li> <li>5. Construction and implementation of a data protection management system</li> <li>6. The default DP model</li> <li>7. Legal aspects of processing of personal data (various aspects of personal data)</li> <li>8. Process of appointment and duties of the Data Protection Officer</li> <li>9. Establishing DP management and responsibilities</li> <li>10. Rights of the data subject to access, rectification, erasure, restriction of processing, data portability and protest right</li> <li>11. Data processing on behalf - rights, obligations and consequences</li> <li>12. Data protection risk management</li> <li>13. Optical-electronic monitoring such as video recording</li> <li>14. The dissemination in the corporate group</li> <li>15. The transfer of data - principles, adequacy decision, guarantees</li> <li>16. The information, reporting and accountability obligations</li> <li>17. Certification process in the data protection auditing</li> <li>18. Technical-organizational measures such as adequacy, pseudonymisation, encryption, privacy by design and privacy by default</li> <li>19. Private and corporate Internet and e-mail use</li> <li>20. Threat situations of cyber security</li> <li>21. Information Security Management</li> <li>22. DP Audit</li> <li>23. Damages, fines and sanctions</li> </ol>



	24. Liability of the organization management and the data protection officer
<b>Existing target groups and their specific characteristics</b>	<ol style="list-style-type: none"> <li>1. New data protection officers</li> <li>2. IT Security Officer</li> <li>3. Responsible for the information security area</li> <li>4. Responsible for risk management</li> <li>5. Responsible for compliance</li> <li>6. Executives</li> <li>7. Business Consultant / Auditor</li> </ol>
<b>Training methods and techniques</b>	In-presence
<b>Activities undertaken within those curricula</b>	<p>Seminar</p> <p>Written <span style="float: right;">Exam</span></p> <p>The exam lasts 60 mins and consists of 40 questions</p> <p>Certification</p>
<b>Impact and results Competences</b>	After completion of the training the participants can plan, build, operate as well as maintain and improve Data Protection systems.
<b>WBL and Apprenticeship Programs</b>	N/A

-4-

<b>COURSE NAME</b>	<p>Certified EU General Data Protection Regulation (EU GDPR) Foundation And Practitioner – Germany</p> <p><a href="https://www.theknowledgeacademy.com/de/courses/gdpr-training/certified-eu-general-data-protection-regulation-gdpr/">https://www.theknowledgeacademy.com/de/courses/gdpr-training/certified-eu-general-data-protection-regulation-gdpr/</a></p>
<b>CONTENT AND STRUCTURE</b>	<p>2 Days GDPR Foundation training</p> <p>2 Days GDPR Practitioner training</p> <p><b>Foundation topics:</b></p> <ul style="list-style-type: none"> <li>• Introduction to the GDPR</li> <li>• Key GDPR terminology</li> </ul>

	<ul style="list-style-type: none"> <li>• An introduction to the GDPR’s structure - the legal articles and recitals</li> <li>• Main differences between the Data Protection Act and the EU GDPR</li> <li>• Principles of the GDPR</li> <li>• Key roles and features of the GDPR</li> <li>• The rights of Data subjects</li> <li>• Lawful processing of personal data</li> <li>• Subject access requests and how to deal with them</li> <li>• Complying with the EU GDPR</li> <li>• Privacy by design</li> <li>• Binding Corporate Rules</li> <li>• Data protection impact assessments (DPIA)</li> <li>• Breach reporting and responses</li> <li>• The role of the DPO</li> </ul> <p><b>Practitioner Topics</b></p> <ul style="list-style-type: none"> <li>• Demonstrating compliance with the GDPR</li> <li>• Planning for compliance - privacy compliance frameworks and gap analysis</li> <li>• Legal requirements of the GDPR</li> <li>• Lawful Processing - rights and consent</li> <li>• Data Processing for Marketing purposes</li> <li>• Subject Access Requests</li> <li>• Common data security failures, consequences, and lessons to be learnt</li> <li>• Privacy principles in the GDPR</li> <li>• Data Protection Impact Assessments</li> <li>• Personal Information Management Systems (PIMS)</li> <li>• Data Breach reporting requirements</li> <li>• Dealing with third parties and data in the Cloud</li> <li>• International transfers &amp; the EU-US Privacy Shield</li> <li>• Practical Implications of GDPR</li> <li>• Notification Obligations</li> <li>• Protecting personally identifiable information</li> <li>• Penalties for non-compliance</li> <li>• The rights of data subjects</li> <li>• Data controllers and processors - roles and responsibilities</li> </ul>
<p><b>EXISTING TARGET GROUPS AND THEIR</b></p>	<p>This GDPR Foundation and Practitioner course is intended for:</p> <ul style="list-style-type: none"> <li>• Information Security Professionals</li> <li>• Compliance Officers</li> </ul>

<b>SPECIFIC CHARACTERISTICS</b>	<ul style="list-style-type: none"> <li>• Data Protection Officers</li> <li>• Risk Managers</li> <li>• Privacy Managers</li> <li>• IT Security Professionals</li> </ul> <p>There are no pre-set formal qualifications required prior to sitting this course - it is designed for individuals looking to enhance their knowledge of GDPR and implement a compliance program within their business.</p>
<b>TRAINING METHODS AND TECHNIQUES</b>	In-presence  Live Virtual  E-learning
<b>ACTIVITIES UNDERTAKEN WITHIN THOSE CURRICULA</b>	Lectures  Online Lectures  Written Exams  Certificaton by “The Knowledge Academy”
<b>IMPACT AND RESULTS</b>	This course provides a detailed introduction to the EU GDPR, and a full overview regarding how to plan and implement a continuous compliance program. It enables delegates to fulfil the knowledge requirements of a Data Protection Officer (DPO) – a position that is now a legal requirement in EU Organisations with a central data storage and processing function.
<b>WBL AND APPRENTICESHIP PROGRAMS</b>	N/A

-5-

<b>COURSE NAME</b>	Certified Data Protection Officer (CDPO) – Germany  <a href="https://www.theknowledgeacademy.com/de/courses/gdpr-training/certified-data-protection-officer-cdpo/">https://www.theknowledgeacademy.com/de/courses/gdpr-training/certified-data-protection-officer-cdpo/</a>
<b>CONTENT AND STRUCTURE</b>	1 Day Training  This CDPO training course will explore the following areas:  <b>An Introduction</b> <ul style="list-style-type: none"> <li>• Introducing Data Protection</li> </ul>

	<ul style="list-style-type: none"> <li>• Why is Data Protection required?</li> <li>• Key Data Protection Approaches</li> <li>• Data Protection Regulations</li> </ul> <p><b>The Role of a Data Protection Officer</b></p> <ul style="list-style-type: none"> <li>• Working with Personal Data</li> <li>• Processing Personal Data</li> <li>• The Rights of the Subject</li> <li>• Encountering Challenges</li> </ul> <p><b>The Security Context</b></p> <ul style="list-style-type: none"> <li>• Data Breaches</li> <li>• Incident Response Plans</li> <li>• The Supervisory Authority</li> <li>• Recovering from Incidents</li> <li>• Recording Incidents</li> </ul> <p><b>Performing a Personal Data Audit</b></p> <ul style="list-style-type: none"> <li>• What is a Personal Data Audit?</li> <li>• The DPO’s Role</li> <li>• Collecting PII</li> <li>• Securing Personal Data</li> </ul> <p><b>Conducting a Data Protection Impact Assessment (DPIA)</b></p> <ul style="list-style-type: none"> <li>• What is a DPIA?</li> <li>• When are DPIAs required?</li> <li>• DPIAs and the DPO</li> <li>• DPIAs through the Life Cycle</li> </ul>
<p><b>EXISTING TARGET GROUPS AND THEIR SPECIFIC CHARACTERISTICS</b></p>	<p>This certification is designed for anyone involved in a role whereby the processing of personal information is performed, or anyone looking to understand the role of a Data Protection Officer.</p> <p>Therefore, those within the following positions may benefit from this CDPO training course:</p> <ul style="list-style-type: none"> <li>• Data Protection Officers (Current and Aspiring)</li> <li>• Data Protection Professionals and Personnel</li> <li>• Information Officers</li> <li>• Compliance Officers</li> <li>• Human Resources Managers</li> </ul>
<p><b>TRAINING METHODS AND TECHNIQUES</b></p>	<p>In-presence</p>

<b>ACTIVITIES UNDERTAKEN WITHIN THOSE CURRICULA</b>	Lectures Certification by “The Knowledge Academy”
<b>IMPACT AND RESULTS</b>	The seminar students will be able to inform and advise clients and their businesses responsibly to fully comply with GDPR requirements, providing specialized advice and services to avoid errors and penalties.
<b>WBL AND APPRENTICESHIP PROGRAMS</b>	N/A

- Annex III: Established and applied Curricula in Cyprus

-1-

<b>COURSE NAME</b>	<b>Privacy &amp; Data Protection Foundation</b> <a href="https://eimf.eu/courses/exin-privacy-data-protection-foundation-certificate-in-general-data-protection-regulation-2/">https://eimf.eu/courses/exin-privacy-data-protection-foundation-certificate-in-general-data-protection-regulation-2/</a>
<b>CONTENT AND STRUCTURE</b>	<p>The foundation certificate for the GDPR Specialist is also a standalone certificate that helps professionals and organizations prepare for the EU General Data Protection Regulation (GDPR) by providing the necessary knowhow. It outlines what organizations can do on the ground to improve data governance, reduce the risk of data loss and lower compliance costs.</p> <p>The content is structured in 3 basic modules:</p> <ol style="list-style-type: none"> <li>1. Privacy fundamentals &amp; regulation (45% weight)</li> <li>2. Organizing data protection (35% weight)</li> <li>3. Practice of data protection (20% weight)</li> </ol> <p>The course duration is 14hours (2 Days course)</p>

<b>EXISTING TARGET GROUPS AND THEIR SPECIFIC CHARACTERISTICS</b>	Intended for Data Protection Officers, beginner-level, no prior knowledge of EU GDR needed.
<b>TRAINING METHODS AND TECHNIQUES</b>	On-site
<b>ACTIVITIES UNDERTAKEN WITHIN THOSE CURRICULA</b>	Lectures Exams Certification by EXIN Exams can be computer based or paper based utilizing multiple-choice questions. The passing grade is 65%.
<b>IMPACT AND RESULTS</b>	
<b>WBL AND APPRENTICESHIP PROGRAMS</b>	N/A

-2-

<b>COURSE NAME</b>	<b>Privacy &amp; Data Protection Practitioner</b>  <a href="https://eimf.eu/exin-general-data-protection-practitioner-certificate/">https://eimf.eu/exin-general-data-protection-practitioner-certificate/</a>
<b>CONTENT AND STRUCTURE</b>	21 Hours Training/ 3 Days  <b>Seminar Content</b> <ul style="list-style-type: none"> <li>• Data protection policies</li> <li>• Managing and organizing data protection</li> <li>• Roles of the Controller, Processor and Data Protection Officer (DPO)</li> <li>• Data Protection Impact Assessment (DPIA)</li> <li>• Data breaches, notification and incident response</li> </ul>
<b>EXISTING TARGET GROUPS AND THEIR SPECIFIC CHARACTERISTICS</b>	Intended for Data Protection Officers, beginner-level, no prior knowledge of EU GDR needed.

<b>TRAINING METHODS AND TECHNIQUES</b>	In-presence
<b>ACTIVITIES UNDERTAKEN WITHIN THOSE CURRICULA</b>	Lectures Exams Certification by EXIN
<b>IMPACT AND RESULTS</b>	
<b>WBL AND APPRENTICESHIP PROGRAMS</b>	N/A

-3-

<b>COURSE NAME</b>	<b>Certified Data Protection Officer (CDPO) - Cyprus</b> <a href="https://www.theknowledgeacademy.com/cy/courses/gdpr-training/certified-data-protection-officer-cdpo/">https://www.theknowledgeacademy.com/cy/courses/gdpr-training/certified-data-protection-officer-cdpo/</a>
<b>CONTENT AND STRUCTURE</b>	<p>1 Day Training</p> <p>This CDPO training course will explore the following areas:</p> <p><b>An Introduction</b></p> <ul style="list-style-type: none"> <li>• Introducing Data Protection</li> <li>• Why is Data Protection required?</li> <li>• Key Data Protection Approaches</li> <li>• Data Protection Regulations</li> </ul> <p><b>The Role of a Data Protection Officer</b></p> <ul style="list-style-type: none"> <li>• Working with Personal Data</li> <li>• Processing Personal Data</li> <li>• The Rights of the Subject</li> <li>• Encountering Challenges</li> </ul> <p><b>The Security Context</b></p> <ul style="list-style-type: none"> <li>• Data Breaches</li> <li>• Incident Response Plans</li> <li>• The Supervisory Authority</li> <li>• Recovering from Incidents</li> <li>• Recording Incidents</li> </ul> <p><b>Performing a Personal Data Audit</b></p>

	<ul style="list-style-type: none"> <li>• What is a Personal Data Audit?</li> <li>• The DPO's Role</li> <li>• Collecting PII</li> <li>• Securing Personal Data</li> </ul> <p><b>Conducting a Data Protection Impact Assessment (DPIA)</b></p> <ul style="list-style-type: none"> <li>• What is a DPIA?</li> <li>• When are DPIAs required?</li> <li>• DPIAs and the DPO</li> <li>• DPIAs through the Life Cycle</li> </ul>
<b>EXISTING TARGET GROUPS AND THEIR SPECIFIC CHARACTERISTICS</b>	Executives who are responsible for and / or processing the Personal Data, such as: Management, Marketing - Marketing, Financial Management, HR Managers, Corporate and Business Compliance Managers, Information Security Officers, IT Managers (CIOs) Managers).
<b>TRAINING METHODS AND TECHNIQUES</b>	In-presence E-Learning Course Completion Certificate by "The Knowledge Academy"
<b>ACTIVITIES UNDERTAKEN WITHIN THOSE CURRICULA</b>	Lectures
<b>IMPACT AND RESULTS</b>	The seminar students will be able to inform and advise clients and their businesses responsibly to fully comply with GDPR requirements, providing specialized advice and services to avoid errors and penalties.
<b>WBL AND APPRENTICESHIP PROGRAMS</b>	N/A

-4-

<b>COURSE NAME</b>	<b>ROLE AND TASKS OF THE DATA PROTECTION OFFICER (DPO) BASED ON THE NEW GENERAL REGULATION ON PROTECTION OF PERSONAL DATA (GDPR)</b> <a href="http://www.ccci.org.cy/seminar-for-data-protection-officer-dpo/">http://www.ccci.org.cy/seminar-for-data-protection-officer-dpo/</a>
<b>CONTENT AND STRUCTURE</b>	3 Days Training



	<p><b>SECTION 1</b></p> <p>What is the GDPR Regulation, what is its evolution? What is its scope and its main features?</p> <p><b>SECTION 2</b></p> <p>What are the main duties and obligations of the DPO and how to guarantee the independence of the DPO.</p> <p><b>SECTION 3</b></p> <p>What are the basic skills that a proper DPO should have?</p> <p><b>SECTION 4</b></p> <p>Internal DPO, or external DPO with service provision. Advantages and disadvantages of each choice.</p> <p><b>SECTION 5</b></p> <p>Design and implementation of the GDPR within the organization- 1.</p> <p><b>SECTION 6</b></p> <p>Design and implementation of the GDPR within the organization- 2.</p> <p><b>SECTION 7</b></p> <p>Design and implementation of the GDPR within the organization- 3.</p> <p><b>SECTION 8</b></p> <p>Design and implementation of the GDPR within the organization- 4</p>
<p><b>EXISTING TARGET GROUPS AND THEIR SPECIFIC CHARACTERISTICS</b></p>	<p>The program is aimed at senior executives of organizations who want to know its basic Regulation requirements on the definition of DPO, the characteristics of these executives and the role they will play within organization. It is also addressed to</p>



	Officers who intend to assume such roles, either internally executives, or as an external service provider.
<b>TRAINING METHODS AND TECHNIQUES</b>	In- presence
<b>ACTIVITIES UNDERTAKEN WITHIN THOSE CURRICULA</b>	Lectures Course Completion Certificate by the Cyprus Chamber of Commerce and Industry (CCCI)
<b>IMPACT AND RESULTS</b>	The main objective of the program is to make participants aware of the key provisions of the new Regulation and how it will affect businesses and their obligations to specialize in DPO provisions, the duties and obligations of the DPO and the knowledge and skills a DPO must possess.
<b>WBL AND APPRENTICESHIP PROGRAMS</b>	N/A

- Annex IV: Established and applied Curricula in other EU countries and in international level

### Luxemburg

-1-

<b>COURSE NAME</b>	<b>Data Protection: Refresher and Advanced Course for DPOs and Data Protection Experts</b>  <a href="https://www.eipa.eu/product/data-protection-refresher/">https://www.eipa.eu/product/data-protection-refresher/</a>
<b>CONTENT AND STRUCTURE</b>	<p>2 days training</p> <p><b>Day 1</b></p> <ul style="list-style-type: none"> <li>• GDPR basics</li> <li>• How to ensure personal data security</li> <li>• Risk Management</li> <li>• Assignment: conducting a data protection impact assessment</li> </ul> <p><b>Day 2</b></p> <ul style="list-style-type: none"> <li>• Data Protection Safeguards <ul style="list-style-type: none"> <li>a) Policies and procedures</li> <li>b) Technical safeguards for digital and physical data</li> <li>c) Guidelines for staff dealing with personal data</li> </ul> </li> <li>• Assignment: identify data protection safeguards for a particular use case</li> <li>• Data Breach Management</li> <li>• Assignment: Analyze data breach: Case studies and example</li> <li>• Respond to Data Subject's Rights: practical approaches</li> <li>• Create a Data Protection Culture within your Organisation</li> <li>• Assignment: Analyze do's and don'ts of data protection communication &amp; training plans</li> </ul>
<b>EXISTING TARGET GROUPS AND THEIR SPECIFIC CHARACTERISTICS</b>	<p>This course is for:</p> <ul style="list-style-type: none"> <li>• DPOs and managers exposed to questions related to data protection and the management of the related risks, plans and solutions</li> <li>• Data protection experts and advisors</li> <li>• Certified DPOs</li> </ul>

	<ul style="list-style-type: none"> <li>• Anyone in the public or private sector who is responsible for their organisation's compliance with the GDPR</li> </ul>
<b>TRAINING METHODS AND TECHNIQUES</b>	In-presence
<b>ACTIVITIES UNDERTAKEN WITHIN THOSE CURRICULA</b>	<p>Lectures</p> <p>Assignments</p> <p>Course Completion Certificate by EIPA</p>
<b>IMPACT AND RESULTS</b>	<p>The participants will learn:</p> <ul style="list-style-type: none"> <li>• Facilitate the development of an effective data protection strategy &amp; plan</li> <li>• Draft specific policies &amp; procedures</li> <li>• Manage data breaches</li> <li>• Ensure data-protection compliant transfers of personal data</li> <li>• Define the pragmatic approaches to ensure GDPR compliance within your organisation</li> <li>• Support your organisation in identifying gaps to be addressed in view of GDPR compliance</li> <li>• Advise your organisation how to manage personal data</li> <li>• Support a data protection communication &amp; training plan</li> <li>• Develop your professional international network in the field of data protection</li> </ul>
<b>WBL AND APPRENTICESHIP PROGRAMS</b>	N/A

## Spain

-1-

<b>COURSE NAME</b>	<p><b>Advanced Data Protection Officer (DPO) program</b></p> <p><a href="https://www.ceuiam.com/en/business-school/officer-data-protection--course">https://www.ceuiam.com/en/business-school/officer-data-protection--course</a></p>
<b>CONTENT AND STRUCTURE</b>	<p>180 hours</p> <p><b>Modules</b></p>

	<ul style="list-style-type: none"> <li>• General Data Protection Regulations</li> <li>• Active Responsibility</li> <li>• Techniques to Ensure Compliance with Data Protection Regulations</li> </ul>
<b>EXISTING TARGET GROUPS AND THEIR SPECIFIC CHARACTERISTICS</b>	<p>The Advanced Data Protection Officer Program as well as the certification is not only aimed at postgraduates with legal training. The type of training will depend exclusively on the participant's degree of experience:</p> <ul style="list-style-type: none"> <li>- For participants <b>with no professional experience</b> in projects and/or activities and tasks related to DPO functions in the field of data protection: 180 hour preparation course.</li> <li>- For participants <b>with at least 2 years' professional experience</b> in projects and/or activities and tasks related to DPO functions in the field of data protection: 100 hour preparation course.</li> <li>- For participants <b>with at least 3 years' professional experience</b> in projects and/or activities and tasks related to DPO functions in the field of data protection: 60 hour preparation course.</li> </ul>
<b>TRAINING METHODS AND TECHNIQUES</b>	<p>E-learning</p> <p>Course Completion Certificate by ANF Certification Authority ANF AC, Certifying Entity provisionally authorized for the certification of Data Protection Delegates, in accordance with the AEPD-DPD scheme</p>
<b>ACTIVITIES UNDERTAKEN WITHIN THOSE CURRICULA</b>	Recorded video lectures, articles and readings, self-assessment activities, live online sessions,
<b>IMPACT AND RESULTS</b>	210.000 Alumni, 95% employability, 25 teaching centers
<b>WBL AND APPRENTICESHIP PROGRAMS</b>	N/A

<b>COURSE NAME</b>	<b>European Data Protection Regulation</b>  <a href="https://www.en.aenor.com/formacion/encuentre-su-curso/detalle?c=8c8bc300-1273-e911-a84f-000d3a45a2ae">https://www.en.aenor.com/formacion/encuentre-su-curso/detalle?c=8c8bc300-1273-e911-a84f-000d3a45a2ae</a>
<b>CONTENT AND STRUCTURE</b>	<p>4 Days Training / 28Hours</p> <p><b>Modules</b></p> <ul style="list-style-type: none"> <li>• Fundamentals of Data Protection: Basic concepts and definitions</li> <li>• Principles of Data Protection: Differences with the previous regulation and adaptation approaches</li> <li>• Rights of the interested parties</li> <li>• Obligations of those responsible and responsible for processing</li> <li>• Security measures</li> <li>• Data Protection Delegates (DPO)</li> <li>• Control authorities and penalty system</li> </ul>
<b>EXISTING TARGET GROUPS AND THEIR SPECIFIC CHARACTERISTICS</b>	<p>The course is addressed to:</p> <ul style="list-style-type: none"> <li>• Responsible for security, organization and regulatory compliance</li> <li>• Personnel of the security, organization and / or regulatory compliance offices</li> <li>• Internal or external auditors who must evaluate compliance with the Data Protection regulations</li> <li>• Consultants, lawyers and professionals interested in providing services related to data protection regulations</li> </ul>
<b>TRAINING METHODS AND TECHNIQUES</b>	<p>In- presence</p>
<b>ACTIVITIES UNDERTAKEN WITHIN THOSE CURRICULA</b>	<p>Lectures</p>
<b>IMPACT AND RESULTS</b>	<p>The course:</p> <ul style="list-style-type: none"> <li>• Present an overview of the European Data Protection regulations, highlighting the practical aspects that affect the entities responsible for the treatments and their service providers</li> <li>• Know the basic principles of the new Data Protection regulations</li> </ul>

		<ul style="list-style-type: none"> <li>• Offer a detailed analysis of the obligations that affect those public and private entities that process personal data</li> <li>• Learn to manage the rights of those affected</li> <li>• Know the new sanctioning regime, as well as the functions assumed by national authorities and community institutions in the control of Compliance with Data Protection regulations</li> <li>• Expose the new security obligations and methodologies for their implementation</li> <li>• Analyze the functions that will be carried out by the Data Protection Officer or Delegate (DPO), obtaining the knowledge of the regulations required to carry them out</li> </ul>
<b>WBL APPRENTICESHIP PROGRAMS</b>	<b>AND</b>	N/A

### United States of America

-1-

<b>COURSE NAME</b>		<b>Certified GDPR Foundation and Practitioner Online Combination Training Course</b>  <a href="https://www.itgovernanceusa.com/shop/product/certified-gdpr-foundation-and-practitioner-online-combination-training-course">https://www.itgovernanceusa.com/shop/product/certified-gdpr-foundation-and-practitioner-online-combination-training-course</a>
<b>CONTENT STRUCTURE</b>	<b>AND</b>	5 Days Training  Foundation Modules: <ul style="list-style-type: none"> <li>• Bands of penalties and range of awards for breaches</li> <li>• Lawfulness of processing and consent</li> <li>• The six data protection principles</li> <li>• Special categories of personal data</li> <li>• The rights of data subjects, including data access requests</li> <li>• Controllers and processors</li> <li>• Data protection by design</li> <li>• Securing personal data</li> <li>• Reporting data breaches</li> <li>• How to perform a data protection impact assessment (DPIA)</li> <li>• The role of the data protection officer (DPO)</li> </ul>

	<ul style="list-style-type: none"> <li>• Transferring personal data outside the EU</li> <li>• EU-US Privacy Shield</li> <li>• Certification against GDPR</li> <li>• The powers of supervisory authorities</li> <li>• Lead supervisory authorities</li> <li>• The powers of supervisory authorities</li> </ul> <p>Practitioner Modules:</p> <ul style="list-style-type: none"> <li>• The role of the data protection officer (DPO)</li> <li>• What constitutes personal data</li> <li>• Accountability, the privacy compliance framework</li> <li>• Lessons to be learned from common data security failures</li> <li>• The six data protection principles – how to apply them and demonstrate compliance</li> <li>• The security of personal data</li> <li>• An organisational risk management framework</li> <li>• Legal requirements for a DPIA</li> <li>• How to conduct a DPIA with a DPIA tool</li> <li>• Why and how to conduct a data mapping exercise</li> <li>• The rights of data subjects</li> <li>• Giving and withdrawing consent</li> <li>• Handling data subject access requests (DSARs)</li> <li>• The roles of controllers and processors, and the relationships between them</li> <li>• Transferring personal data outside the EU and the mechanisms for compliance</li> <li>• How to become GDPR compliant using a compliance gap assessment tool</li> </ul>
<p><b>EXISTING TARGET GROUPS AND THEIR SPECIFIC CHARACTERISTICS</b></p>	<p>The course is addressed to:</p> <ul style="list-style-type: none"> <li>• Business directors or managers</li> <li>• Managers involved in or responsible for GDPR compliance</li> <li>• Individuals with a basic knowledge of data protection regulation and practices, and looking to develop their career with a professional qualification</li> </ul>
<p><b>TRAINING METHODS AND TECHNIQUES</b></p>	<p>E-learning</p>
<p><b>ACTIVITIES UNDERTAKEN WITHIN THOSE CURRICULA</b></p>	<p>Live online session</p> <p>Certification by online exam (ISO 17024)</p>



<b>IMPACT AND RESULTS</b>	A learner will gain a clear understanding of the main elements of the GDPR.
<b>WBL AND APPRENTICESHIP PROGRAMS</b>	N/A

## Singapore

-1-

<b>COURSE NAME</b>	<b>GENERAL DATA PROTECTION REGULATION (GDPR) &amp; APPLICATION ON ASIA</b>  <a href="https://www.dpexcentre.com/courses/exin-gdpr/gdpr_sg/#tab-id-1">https://www.dpexcentre.com/courses/exin-gdpr/gdpr_sg/#tab-id-1</a>
<b>CONTENT AND STRUCTURE</b>	2 Days Training  Modules: <ul style="list-style-type: none"> <li>• Privacy Fundamentals &amp; Regulation</li> <li>• Organizing data protection</li> <li>• Practice of data protection</li> </ul>
<b>EXISTING TARGET GROUPS AND THEIR SPECIFIC CHARACTERISTICS</b>	The course is addressed to: <ul style="list-style-type: none"> <li>• All employees who need an understanding of data protection and European legal requirements as defined in the GDPR</li> <li>• Data Protection Officer</li> <li>• Privacy Officer</li> <li>• Legal Officer / Compliance Officer</li> <li>• Security Officer</li> <li>• Business Continuity Manager</li> </ul>
<b>TRAINING METHODS AND TECHNIQUES</b>	In-presence
<b>ACTIVITIES UNDERTAKEN WITHIN THOSE CURRICULA</b>	Lectures Assessments Case Studies Project presentation
<b>IMPACT AND RESULTS</b>	With this course the learner will be able to: <ul style="list-style-type: none"> <li>• Understand fundamentals of Europe General Data Protection Regulation</li> </ul>

	<ul style="list-style-type: none"> <li>• Learn important definitions of privacy and organizing data protection</li> <li>• Gain insights to transfer mechanisms and practice of data protection</li> <li>• Learn Privacy by design &amp; privacy by default related to information security</li> <li>• Practice related applications of the use of data, marketing &amp; social media</li> <li>• Learn legal requirements and mechanisms for handling and transferring data across from Europe to other jurisdictions, such as Asia</li> </ul>
<p><b>WBL AND APPRENTICESHIP PROGRAMS</b></p>	<p>N/A</p>