Common Curriculum

e-OpenSpace Project

Erasmus+ programme

Intellectual Output 3

Version 2.A, 05-03-2019

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

VERSION HISTORY

Version #	Implemented By	Revision Date	Approved By	Approval Date	Reason
1.0	*Hristo Alaminov*	*09/30/18*		*<mm/dd/yy>*	*First draft*
1.1	*Marko Sijan*	*02/02/19*			*Revision*
1.2	*Anna Dudkowska*				*Revision*
1.3	*Przemyslaw Tacik*				*Revision*
1.4	*Carmine Falanga*				*Revision*
1.5	*Nikolay Yanev*	*02/07/19*			*Revision*
2.0	*Hristo Alaminov*	*03/05/19*			*Revision*

Content

Introduction

The e-OpenSpace project aims at the establishment of a sustainable and long-term Strategic Partnership between national supervisory authorities, academia and civil society organisations for the delivery of knowledge and the development of skills related to privacy and personal data protection. In order to achieve higher impact and to avoid overlap with other activities in this domain, such as digital and privacy education for children, the project outputs are focused on promotion of non-formal digital learning and awareness on privacy and personal data protection for adults, civil servants and practitioners. The contemporary digital environment necessitates new approaches for communication between data protection authorities, academia and society. Furthermore, non-formal education and trainings have already proven themselves as efficient tools with a potential for multiplication of the acquired knowledge.

The project aims to provide an innovative way of conducting non-formal digital learning based on synergy between DPAs, which as a rule have the most comprehensive information about data protection, and universities with their extensive experience in providing education for adults.

Implementing the project activities, the project consortium creates opportunities for additional type of education in the field of personal data and privacy protection – short non-formal digital learning. The e-learning curriculum is with more focused content, covering the various aspects of the privacy and personal data protection and accessible from everywhere. Meanwhile, already prepared and experienced DPAs trainers will enrich their abilities with new skills for providing e-learning content, including in multinational cross-border environment.

Common Curriculum for non-formal digital learning in privacy and personal data protection is an essential element of the "Big Picture" of the project. It is a linkage between the processes by providing the content of the learning. Even more, Common Curriculum ensures quality of the providing non-formal digital learning for adults, civil servants and practitioners. It can be considered as a standard in the learning content applicable to all EU Member States.

Common Curriculum is the first unified learning content of its kind. Hence, its transferability potential is with European dimensions.

Modules

There are 10 modules of the Common Curriculum:

- Module 1: Legal framework for privacy and personal data protection, Definitions in the field of personal data protection, Principles for the processing of personal data;
- Module 2: Conditions for the lawful processing of personal data;
- Module 3: Rights of the data subjects;
- Module 4: Controller and processors – obligations;
- Module 5: Data Protection Officer – requirements and tasks, conditions for mandatory designation;
- Module 6: Codes of conduct and certification mechanisms;
- Module 7: Transfers of personal data to third countries or international organisations;
- Module 8: European Data Protection Board and national supervisory authorities, cooperation and consistency mechanism;
- Module 9: Remedies, liability and administrative sanctions;
- Module 10: International privacy organisations and initiatives and academia (incl. Good Practices);

Module 1: Legal framework for privacy and personal data protection; Definitions in the field of personal data protection; Principles for the processing of personal data

The module is of general and introductory character. It aims to present how the law (and particularly EU law) approaches personal data protection and which legal instruments are applicable to protecting data in Europe. Moreover, it outlines some basic concepts whose understanding is a key to proper dealing with personal data. Devoting attention to this module should allow the participant to properly identify what the GDPR actually is and what its scope of application is in general. After completion participant should be able to differentiate situations in which she or he might be either a subject of rights or a bearer of a GDPR-related obligation.

The knowledge in this module is particularly important for understanding the GDPR. It enables on whether the participant can properly assess if the GDPR is at all applicable or if it is not. It is of great importance for so-called "border cases" that might not intuitively link with data protection at first glance.

References

1. 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 (General Data Protection Regulation)

Keywords

personal data, processing, data subject, consent, lawful processing, conditions, principles, fragile data.

Module 2: Conditions for the lawful processing of personal data

The lawfulness of data processing is very important in the everyday fast growing digital era that surrounds us. Companies (data controllers) around the world depend on a large number of customers/ users (data subjects) and possibility to have access to their personal data. Also, the amount of personal data being processed grows each day in social networks and "Internet of things" makes that processing even more complex to recognize as lawful. It is necessary to emphasize that this acknowledgment lead us to conclusion that we all should pay more attention on protection of personal data.

For the legal basis of processing personal information there are defined six different conditions that justify the processing of data. Those are consent, contractual necessity, and compliance with legal obligations, vital interests, public interest, and legitimate interests. A lawful basis for processing personal data consists of at least one of those legal grounds and can vary per personal data processing activity and purpose.

This module aims to explain lawfulness of processing of personal data and interpret conditions that justify it.

References

1. Guidelines on the processing of personal data in the context of public procurement, grants as well as selection and use of external experts
2. Guidelines on the processing of personal data with regard to the management of conflicts of interest in EU institutions and bodies

Key words

personal data, processing, data subject, data controller, consent, lawful processing, conditions

Module 3: Rights of the data subjects

One of the basic goals of General Data Protection Regulation was the necessity to strengthen rights on personal data protection of individuals in increasingly developed digital society. To help data subjects in assuring protection of their privacy, GDPR empowers data subjects with certain rights. The aforementioned legislative framework guarantees to all European citizens the equal rights to the protection of personal data.

GDPR requires companies (data controllers) that gather personal data to provide natural person (data subject) with clear and convenient explanations of how their personal data is collected, stored, shared, protected and similar.

Under the GDPR, data subjects get more rights and in this regard, it is important that every individual know his rights to ensure the privacy and protection of his/hers personal data.

This module aims to explain rights of data subjects and how to exercise them.

References

1. Guidelines on the right to data portability
2. Guidelines on the right to be forgotten

Key words

data subject, data controllers, right, forgotten, data portability, erasure, object, informed, rectification, decision-making

Module 4: Controller and processors – obligations

Responsibilities and obligations of the controller and processor correspond to the level of risk of their data processing activities. This is connected with the risk-based approach on which the GDPR is based on.

The Controller is obliged to take the steps in order to identify the relatable risks and in response implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with GDPR including the effectiveness of the measures. The principle of accountability is a cornerstone of the GDPR.

This module aims to explain the obligations of the controller and processors and how to exercise them.

References

1. Article 29 Working Party Guidelines on Personal data breach notification under Regulation 2016/679, 3 October 2017 (WP 250)
2. Article 29 Working Party Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation (EU) 2016/679, 4 April 2017
3. Article 29 Working Party Guidelines on the Data Protection Officers, 5 April 2017 (WP 243)

Key words

Controller, processor, data protection authority, risk-based approach, accountability principle, data protection officer, data protection impact assessment, data breach notification, record of processing activities, code of conduct, certification

Module 5: Data Protection Officer – requirements and tasks, conditions for mandatory designation

There are few important questions that you will face after the completion of this module:

- Have you been designated as a data protection officer (DPO)?
- Would you like to know what is associated DPO with?
- You are processing data and you want to know if you are obliged to designate DPO?

Depending on the structure and operations carried out by the controller GDPR envisages an evaluation to be carried out on whether a designation of a DPO is necessary or not. The data protection officer plays a key role in ensuring the lawful processing of personal data in the controllers structure and help demonstrate compliance. The data protection officer must have the ability to perform his/her duties in an independent manner. In this regard to fall into the scope of those requirements the DPO must have professional qualities, expertise in the field of data protection and have access to the management in his/her organization.

In this module you will find basic information concerning requirements and tasks, conditions for mandatory designation DPO

References

1. Article 29 Working Party Guidelines on the Data Protection Officers, 5 April 2017 (WP 243)

Key words

data protection officer, controller, processor, personal data, processing operations

Module 6: Codes of conduct and certification mechanisms

The General Data Protection Regulation aims at unified approach for protecting of personal data across the European Union and the European citizens all over the world. Trusting the ability of data controllers to apply appropriate technical and organisational measure, all national registration mechanisms were sent into history. Such fundamental change can be considered as very challenging especially for those data controllers that rely on rigorous registration systems of the national data protection authorities. In order to support such controllers, the GDPR foresees several options for demonstration of compliance with the EU data protection legal framework, applicable not only for a single data controller but for group of similar or unlimited number of data controllers inside or outside the European Union. Aforementioned types of demonstrating compliance with the GDPR also help data subjects to identify easier those data controllers that can be trusted in the light of data security, integrity, confidentiality and availability.

Opportunities such as Codes of conduct as well as certification mechanisms can be considered as worthy options in paying less for adopting internal controllers' rules to the GDPR.

References

1. 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 (General Data Protection Regulation)
2. Draft Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679
3. Guidelines on the accreditation of certification bodies
4. Draft Guidelines on codes of conduct and monitoring bodies to cover the provisions in Articles 40-1 and on codes of conduct as appropriate safeguards for international transfers of personal data (Article 46(2)(e)).

Key words

personal data, code of conduct, certification, accreditation, compliance

Module 7: Transfers of personal data to third countries or international organisations

It is no doubt that technology plays a crucial part in our daily lives than ever before, due to the global economy gone digital and the increased communications across borders facilitated by the Internet. Moreover, companies around the world highly depend on innovations driven by personal data to do business with clients all around the globe. It means that the amounts of personal data being processed, as well as the processing operations themselves have increased significantly. It is no exaggeration to say that personal data has become tools of the trade for almost every company there is.

In this picture, international data transfers have had an essential and rather positive impact on the global business.

References

1. Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679
2. Working Document setting forth a co-operation Procedure for the approval of "Binding Corporate Rules" for controllers and processors under GDPR
3. Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data
4. Recommendation on the Standard Application for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data
5. Guidelines for identifying a controller or processor's lead supervisory authority

Key words

data protection, transfers, third countries, free exchange, personal data, international organisations

Module 8: European Data Protection Board and national supervisory authorities; cooperation and consistency mechanism

The European Data Protection Board is established in order to ensure the consistent application of the GDPR and assist the member states. In order to have the necessary instruments to answer the requirements of the new Regulation the Board has been given a legal personality. The European Data Protection Board (EDPB) replaces the Article 29 Working Party (WP29) under the General Data Protection Regulation (GDPR). The Article 29 Working Party or WP29 were often mentioned when it published another set of guidelines for the implementation and enforcement of the GDPR. For some people it's a bit confusing so a quick look at the European Data Protection Board and why we report on the guidelines of the WP29.

References

1. 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 (General Data Protection Regulation)

Key words

EDPB, data controllers, DPA, cooperation, Consistency Mechanism, binding decision making, guidelines, recommendations and best practices

Module 9: Remedies, liability and administrative sanctions

With less than a year to the introduction of the General Data Protection Regulation (EU) 2016/679 (the "GDPR") and given its far reaching effect on those who process personal data, it is important to consider the potential consequences for data controllers and data processors. The GDPR envisages both administrative sanctions by the relevant supervisory authority and judicial remedies which can be brought side by side. Where a data subject alleges that there has been a breach of the GDPR which has caused the data subject damage, that is either material or non-material, he or she can lodge a complaint with the relevant supervisory authority within a member state. There is also a right to seek compensation from the data controller or data processor for the damage suffered.

References

1. 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 (General Data Protection Regulation)

Key words

GDPR, data controllers, subject's rights, administrative sanctions, fines

Module 10: International privacy organisations and initiatives and academia (incl. Good Practices)

This training module is aiming to give an overall picture of the international organizations active in the field of data protection. It depicts the broader institutional and historical puzzle, where the current system of personal data protection of the EU fits.

Knowledge and competences. After the completion of the module the trainee will have broad understanding of data protection and its scope. He/she will be acquainted with the basic milestones in the development of the personal data protection concept. He/she will have a broader picture of the topic both in geographical and sectoral dimension. He/she will have basic knowledge about the most important international privacy organisations, initiatives and instruments. The trainee will understand the differences between various data protection frameworks and will be acquainted with tools providing basic information about the data protection law in specific countries.

References

1. Baker & McKenzie Handbooks
2. Burkert, H. Privacy - Data Protection, A German/European Perspective. No date. Accessible in Second Symposium of the German American Academic Council's Project "Global Networks and Local Values", Woods Hole, Massachusetts, June 3 - 5, 1999.
3. DLA Piper Data Protection Laws of the World
4. International Association of Privacy Professionals
5. OECD Privacy Guidelines
6. Privacy International
7. UNESCO instruments relevant to the areas of access, freedom of expression, privacy and ethics

Key words

historical aspects of personal data protection; privacy and security; personal protection: US, Canada, Australia; personal data protection in academia; international privacy instruments; personal data protection in IT