September 2021

THE PROJECT “byDesign” Brochure

ABOUT THE PROJECT

The byDesign project (https://bydesign-project.eu/) is coordinated by the Hellenic Data Protection Authority (HDPA); the other two partners are the University of Piraeus Research Center and ICT Abovo PC.

Its duration is 24 months, starting November 1, 2020.

HELLENIC DATA PROTECTION AUTHORITY

ICT abovo Information & Communication Technologies

UNIVERSITY OF PIRAEUS RESEARCH CENTER

This brochure has received funding from the European Union’s Rights, Equality and Citizenship Programme (REC) 2014-2020.

THE GOALS

The project aims to:

1

offer an online toolkit,

particularly tailored to SMEs, which will assist them to perform the necessary actions in order to achieve compliance, along with a set of context-aware templates of essential documents.

2

develop a comprehensive training programme on Data Protection by Design,

targeting developers and other stakeholders of the ICT products and services creation chain. On the basis of this programme, byDesign aims at training a critical mass of professionals, as well as university students, thereby introducing a data protection culture to the ICT community in Greece.

3

maximise its impact,

through awareness-raising, dissemination, networking and sustainability of project results.

WHAT HAS BEEN ACHIEVED SO FAR

COMPLIANCE TOOLKIT FOR SMEs

Need analysis

The goal of **the first task** of the project was to obtain the views from a large number of stakeholders, i.e., SME representatives, consumers and employees, who are geographically dispersed around Greece. To this end, surveys were considered as the most appropriate tool, since they offer the advantage of gathering information anonymously.

Four different sets of questionnaires were prepared to address the different groups of stakeholders. Given that SMEs of different sectors have different needs for guidance in terms of GDPR compliance, it was decided to focus on six sectors of the Greek economy: a) commerce (focused on retail), b) tourism and hospitality, c) education, d) health, e) catering and restaurants, f) sports and exercise.
The results of the questionnaires were analysed and a set of initial conclusions and open issues was identified. Two online workshops took place, afterwards, on 18/2/2021 and 19/2/2021, in which the attendees were representatives of the stakeholders participating in the aforementioned surveys. During these workshops, the initial conclusions and open issues were discussed, while the stakeholders were asked specific questions in order to clarify accurately their needs and expectations.

Results and needs identified

The HDPA processed the results of the questionnaires in order to identify in which areas guidance is needed and which would be the appropriate form for this guidance. The analysis of the information collected from the questionnaires and the workshops led to the identification of the following needs:

-Firstly, a compliance toolkit shall be created in the form of an online wizard, where the user (SME) selects its typical activities from a list of predefined activities and the tool proposes specific sub-tools and texts.

-Secondly, material with simplified information (with FAQs, examples, templates, etc.) covering the following aspects will be drawn up:

- **Lawfulness and transparency** (providing information to data subjects, legal bases and consent, data protection rights and data subject request handling procedures, destruction of personal data).
- **Accountability** (records of processing activities, security measures for personal data processing, data breach handling, engaging subcontractors – data processors).
- **Business activities entailing data processing** (business website, cookies and tracking, direct marketing through electronic means, videosurveillance for security purposes, processing of employee data).

WHAT HAS BEEN ACHIEVED SO FAR

TRAINING PROGRAMME ON DATA PROTECTION BY DESIGN

The **second goal of the first task of the project** was to develop a training programme on data protection by design, focusing on developers and other stakeholders of ICT products and services, such as software engineers and architects, developers, ICT product/project managers and related specialities. To this end, it was essential to identify the main gaps and needs in terms of practical application of data protection by design in ICT products and services.

The methodology used to identify the requirements of the training programme was based a) on analysing the input obtained from replies of the different stakeholders to questionnaires, as well as b) on analysing the input obtained via online workshops.

Four different questionnaires were set up, one for each category of stakeholders (i.e. those holding business roles, analysts, coders, students).

Data collection through questionnaires and workshops

The participants, according to their role in the ICT, field fall into the following categories:

- Business role (e.g., department or unit managers, sales and marketing managers, customer relations managers, etc.)
- Requirements analysis, solution design (e.g., system analysts, system engineers, etc.)
- Software development, programming (e.g., software application developer, chief operating officer, technical support engineer)
- Bachelor, Master and Ph.D. Students, with software development experience.

Main results

The results of the surveys were analysed and a set of initial conclusions and questions were identified. Then, four online workshops were held, 22-23 February 2021, in which the attendees were representatives of the participants in the surveys. The goal of these workshops was to present and discuss the results from the analysis of the questionnaires. More particularly, the stakeholders were asked specific questions so that their needs and expectations were made clear. In that way, it was possible to reach a set of requirements for the training activities.

Requirements identified

The main requirements for the training, resulting from the findings of the questionnaires and workshops, have been identified as follows:

Training is needed on

- data protection/privacy and security risks through DPIA and security risk assessment practical cases/ examples
- organizational GDPR roles through practical cases and examples
- data retention periods with industry-specific cases
- Data Protection/Privacy by Design requirements in existing ICT services, products, applications
- data protection/privacy-friendly default configurations for mobile applications
- the adjustment of older systems/applications to become privacy friendly
- the implementation of software tools to preserve personal data protection and to satisfy legitimacy principles
- mechanisms on data breaches avoidance, monitoring and data breaches handling
- guidelines on privacy by design self-assessment.

LATEST DEVELOPMENTS AND FUTURE STEPS

On the basis of the work already accomplished, the next task began by defining the topics addressed by the online tool, i.e. the concrete types of guidance to be offered, such as data protection policies, data subjects' rights exercise templates, website related policies, terms of use, model clauses for subcontractors, sample texts for satisfying the transparency of the data processing, model records of processing activities, etc. This task, which is already underway, continues with assembling the material reflecting broadly identified good practices in these topics.

This work is following two directions:

1

creation of the content tiles

i.e. fundamental parts for each type of the documents mentioned above, that will be used to populate the actual instances of the documents based on the specific characteristics of an SME data controller;

2

the methodological framework for the generation of concrete document instances

based on the contextual information on the particular data controller, such as the domains/ sectors to which the controller belongs (healthcare, telecom, e-government, e-commerce, etc.), the data types collected, the processing operations it performs, the underlying purpose, complementary legal obligations etc.

Based on these two directions, byDesign will result in a contextual framework providing SMEs with suitable sample documents based on their characteristics, thus significantly facilitating their compliance process.

The actual development of the online toolkit will take place afterwards. The tool will be offered as a web application and it will be using state-of-the-art web technologies and software. The aim is to be able to present in a meaningful and user-friendly way the different kinds of material accumulated throughout the previous task, along with the realisation of the mechanism for the context-aware generation of customised instances of this material, on the basis of particular features of an SME data controller.