NEWSLETTER

Issue 1 - April 2021

2020- 2022

The advent of the GDPR has created several challenges; among others, the need of SMEs for guidance and tools so that their compliance is facilitated, and the need for appropriately educated ICT professionals to implement Data Protection by Design.

The byDesign project is coordinated by the Hellenic Data Protection Authority and has received funding from the European Union's Rights, Equality and Citizenship Programme (REC), under grant agreement No. 101005833, and Its duration is 24 months, starting November 1, 2020.

The Partners

The byDesign consortium is compiled by three partners that represent three areas: regulatory, academic and software industry. The coordinator of the project is the Hellenic Data Protection Authority and the other two partners are the University of Piraeus Research Center and ICT Abovo PC.

HELLENIC DATA PROTECTION AUTHORITY

ICT abovo Information & Communication Technologies

UNIVERSITY OF PIRAEUS RESEARCH CENTER

Contents

1.	The Goals	4
2.	What has been achieved so far	5
2.1.	Analysis of needs	6
2.2.	Data collection through questionnaires & workshops	8
2.3.	Results	10
2.4.	Needs identified	12
2.5.	Positive reaction by the SMEs	13
2.6.	Training programme on data protection by Design	14
2.7.	Data collection through questionnaires & workshops	15
2.8.	Main results	16
2.9.	Requirements identified	18
2.10.	Positive reaction by IT professionals	19
3.	Future steps	20

byDesign
Newsletter

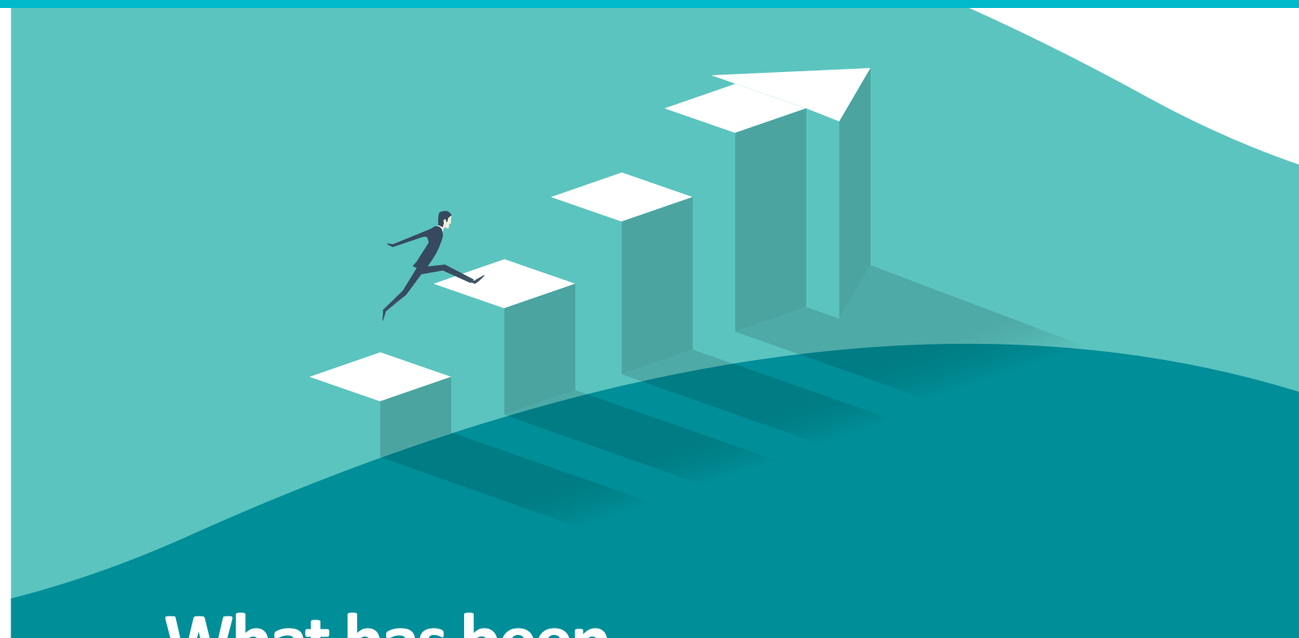
The Goals

The project has two general goals:
-to facilitate SMEs to comply with GDPR provisions and requirements
-to promote the creation of by design compliant products and services, by raising awareness of the producers of respective solutions.

More particularly, it aims to

- 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. In this way, byDesign expects to provide practical assistance and guidance to the large community of SMEs in Greece towards facilitating GDPR compliance.
- 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.
- maximise its **impact**, through awareness raising, dissemination, networking and sustainability of project results.

All in all, byDesign aims at being a project of high impact in the Greek society, with a European dimension.



What has been achieved so far...

Analysis of needs

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 ideally geographically dispersed around Greece. To this end, surveys were considered as the most appropriate tool, since they offer the advantage of gathering information anonymously. "EUSurvey", a secure platform for designing and conducting online surveys, was used.

Four different sets of questionnaires were prepared to address the different groups of stakeholders. The questions were carefully selected, on the basis of the experience of the HDPA over the years, so as to be appropriate for each group.

Although the four groups of stakeholders were different, the structure of the questionnaires was similar. Questions were formulated into four main areas and specific points of interest were elaborated within each area:

- Lawfulness and transparency
- Accountability
- Business activities entailing data processing
- Guidance needs and wishes

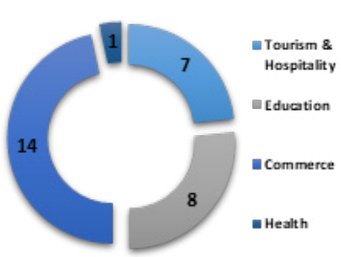
As the HDPA also observed that SMEs of different sectors have different needs for guidance in terms of GDPR compliance, it was decided to focus on six sectors of the Greek economy. The sectors selected were the following:

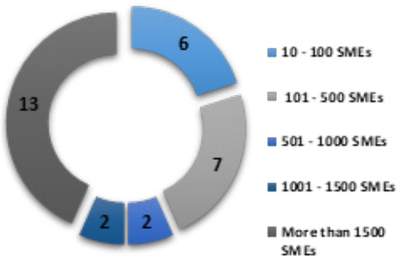
- Commerce, focused (but not exclusively) on retail
- Tourism and Hospitality
- Education
- Health
- Catering and restaurants
- Sports and exercise

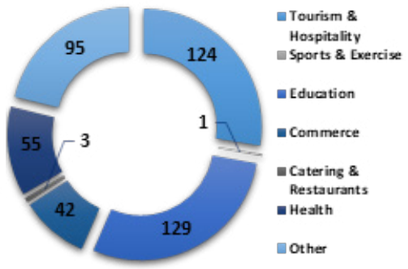
The results of the questionnaires were analysed and a set of initial conclusions and open issues were identified. Subsequently, two workshops took place, on 18/2/2021 and 19/2/2021, in which the attendees consisted of representatives of the stakeholders participating in the aforementioned surveys. During these online workshops, the initial conclusions and open issues were discussed, whereas the stakeholders were asked specific questions in order to clarify accurately their needs and expectations.

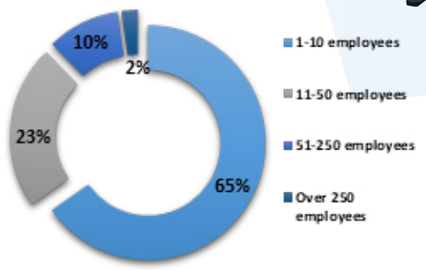
byDesign
Newsletter

Data collection through questionnaires & workshops









The sectors of Commerce, Tourism & Hospitality and Education were very well represented. For the Health sector, only one association replied, which represents small private hospitals.

The questionnaires were answered by large associations that represent hundreds of thousands of businesses. More than 1000 SMEs (which was the initial goal) were well represented.

The questionnaire addressed to individual SMEs received an equally positive response. The sectors of Education, Tourism & Hospitality, Health, and Commerce were very well represented through an adequate sample of answers. The sectors of Catering & Restaurants and Sports & Exercise were not well-represented due to the effects of the pandemic.

In terms of SME size most respondents fall in the micro business category and 88% of the responses originate from up-to-medium sized enterprises. This was to be expected, as it resembles the structure of Greek economy.

One union filled the questionnaire. Although this union represents more than 25.000 employees, it is noted that it cannot accurately reflect the views of Greek employees.

Five consumer associations filled the questionnaires. Since that particular questionnaire was sent to 8 Pan-Hellenic associations, this response was considered very positive.

Finally, more than 112 persons (out of 134 initially invited) participated at the two online workshops, held on 18/02/2021 and 19/02/2021.

Results

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. During the online workshops the stakeholders' needs and expectations were discussed.
Some of the results of the questionnaires are presented below:

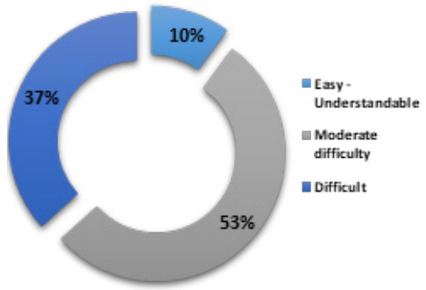


Figure 1: How SMEs assess the requirements of the GDPR on informing the data subjects

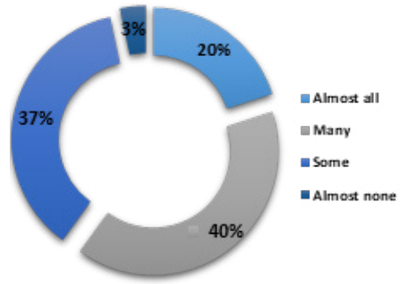


Figure 2: Do SMEs provide information on the legal basis of any processing activity?

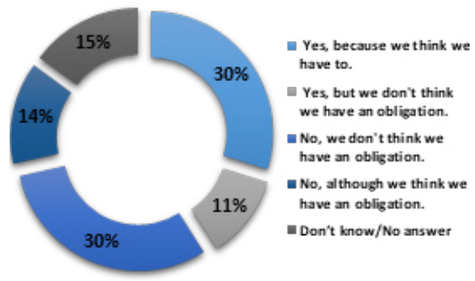


Figure 3: Do you have a Data Protection Officer?

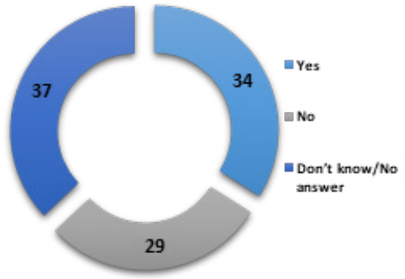


Figure 4: Do you have a records of processing activities?

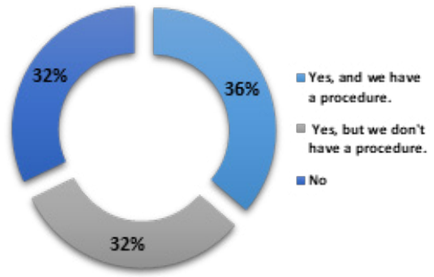


Figure 5: Are you aware of the obligation to handle personal data breach incidents?

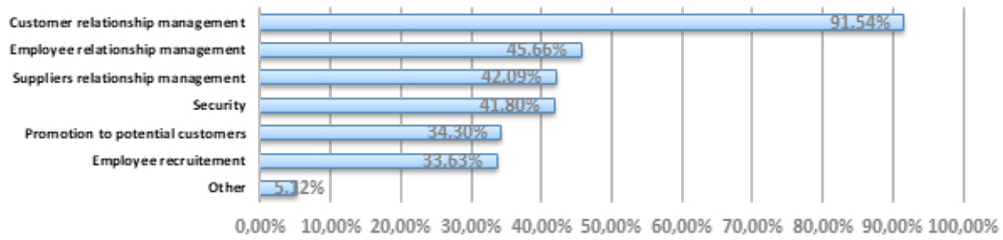


Figure 6: SMEs data processing activities

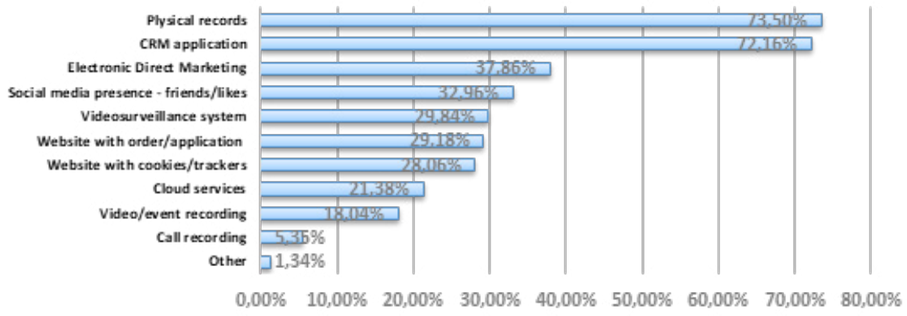


Figure 7: SMEs means of data processing activities

Needs identified

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 on-line 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).

Positive reaction by the SMEs

The project received very positive comments from SME associations and individual SMEs but also from data protection practitioners all over Greece. SME representatives already expressed a high interest in this form of guidance. It is expected that, in the future, more business sectors will benefit from the toolkit as soon as it becomes available.

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 received by the replies of the different stakeholders to questionnaires; also b) on analysing the input obtained by online workshops, in which the initial results were further discussed in order to obtain a more specific feedback through open discussion.

It is noted that four different questionnaires were set up, one for each category of stakeholders (i.e. those holding business roles, analysts, coders, students).
For the needs of the survey, and taking into account the need to ensure reliability, anonymity and data protection, “EUSurvey” was selected as the most appropriate platform.

Data collection through questionnaires & workshops

In total, 191 completed questionnaires were submitted; 168 by IT professionals and 23 by students. 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, on 22 and 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.
The main results of the questionnaires are presented in the graphs below:

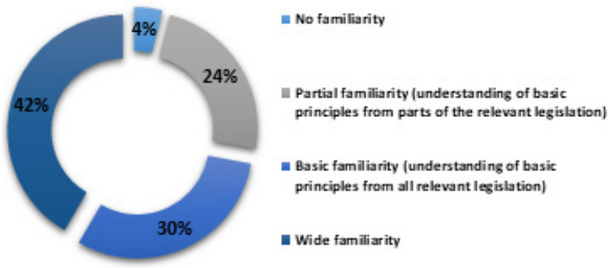


Figure 1: Familiarity with laws/regulations on personal data protection

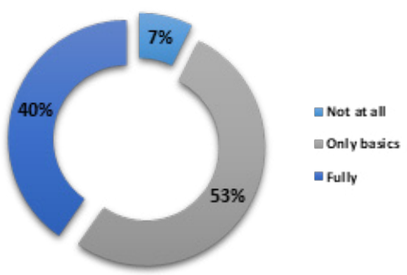


Figure 2: Understanding of the rules/ guidelines prescribed by the Data Protection by Design

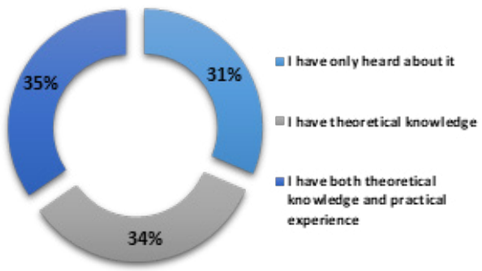


Figure 3: Familiarity with Data Protection Impact Assessment

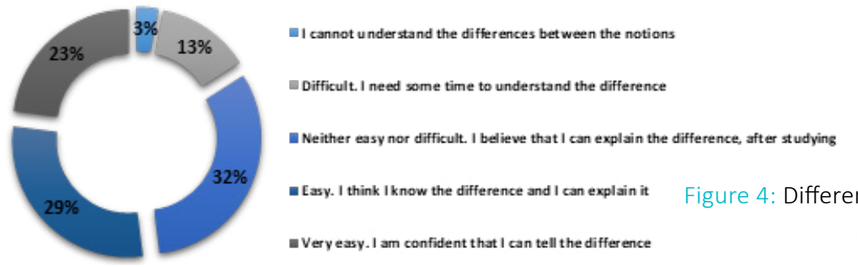


Figure 4: Difference between privacy risk and security risk

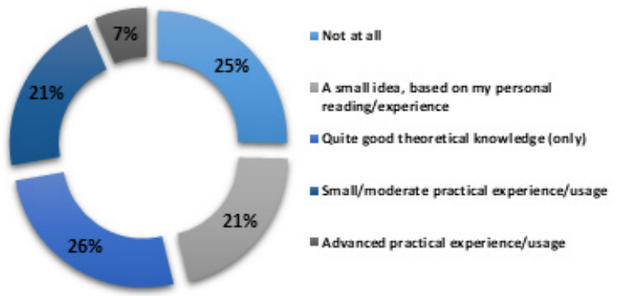


Figure 5: Familiarity with technologies to enhance user's rights

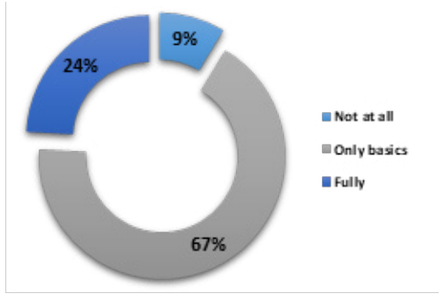


Figure 6: Knowledge and skills on Privacy By Design

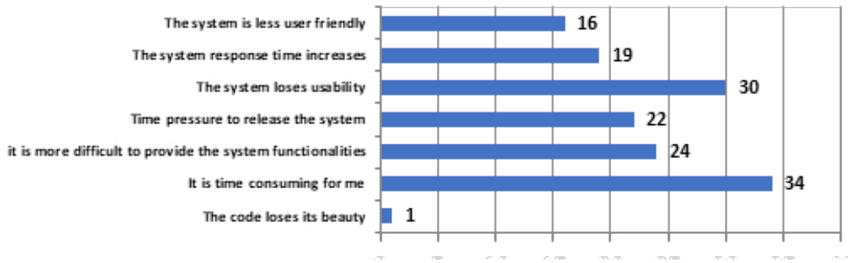


Figure 7: Advantages and disadvantages of Privacy by Design

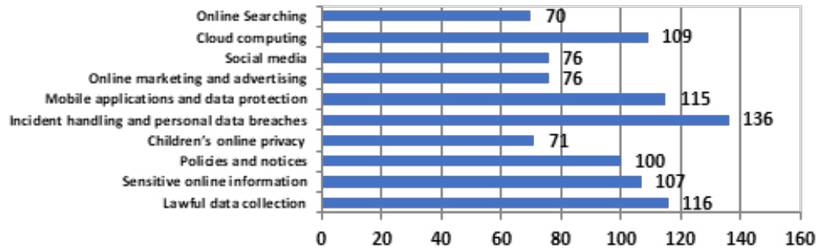


Figure 8: Domains of interest for training

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.

Positive reaction by IT professionals

The activities of the specific task resulted in positive comments from the involved IT professionals who expressed a high interest in the training material/programme that will be created.
They expressed a high interest in the training material / programmes that will be prepared. The project has already attracted interest from SME associations and individual SMEs, but also even from data protection practitioners around Greece.

Future steps

On the basis of the work already accomplished, **the next task will start 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.

Most important, this task will continue with assembling the material reflecting broadly identified good practices in these topics. This work will extend along two directions:

- **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;
- **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 (e.g. sectorial laws requiring data retention), 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.

Work in this task will roughly include four stages: **requirements elicitation, architecture design, development and testing**. Special focus will be put on the customisability and configurability of the platform to a reasonable extent, with a view to making it relatively easy to extend, even after the end of the project, as per new requirements that may arise in the course of HDPA business. **Extendibility of the tool** will primarily concern two aspects: first, as regards the document types and content; second, as regards the framework for the context-aware generation of the documents so that they fit each SME data controller's needs.

byDesign

https://bydesign-project.eu/

email: byDesign@bydesign-project.eu