



Το έργο χρηματοδοτήθηκε από το  
Πρόγραμμα Δικαιώματα,  
Ισότητα και Ιθαγένεια 2014-2020  
της Ευρωπαϊκής Ένωσης

# *GDPR Compliance and the development of an online toolkit for SMEs*

## *Need Analysis*

*Kalli Karveli, M.Sc.*

*Legal Auditor*

**HDPA**



## Analysis and Identification of the requirements and needs of SMEs for GDPR compliance

- **The purpose of the project:** to assist SMEs through the development of appropriate compliance tools and training programs, in relation to addressing the challenges arising from the effective implementation of the GDPR
- **Key pillar:** the development of a "tool guide" that will facilitate SMEs in their GDPR compliance process while also offering a set of basic document templates and online tools
- To this end, **the main needs and current gaps** faced by SMEs in relation to compliance should be **assessed and identified**, so that they can then be effectively guided in this context.

# Methodology

The identification and determination of the needs of SMEs was done through

- i) **structured questionnaires** addressed to representative SMEs and the respective data subjects, adapted to the specific needs and characteristics of each group and
- ii) **the discussion of needs and impacts**, based on the results of the questionnaires, in presentations (**workshops**) organized for this purpose

# Questionnaires

- Six business sectors were selected based on their economic size **a) health, b) retail, c) catering, d) tourism, e) education and f) sports**
- More than **1000 SMEs** participated in the survey by completing the respective questionnaires from **a) representative business associations b) from the businesses themselves c) from consumer associations and d) from employee associations** of the above industries
- **Four different sets of questionnaires** were prepared to address the different groups
- **'EUSurvey'**, a secure platform for designing and conducting online surveys, was used

# Questionnaires

- Although the four groups of participants were different, the structure of the questionnaires was similar. The questions were about **four main themes** namely:
  - ✓ Lawfulness and transparency
  - ✓ Accountability
  - ✓ Business activities involving processing of personal data
  - ✓ Needs for guidance and compliance

# Questionnaires

- Responses were **anonymous**
- The response of SME associations was great **in the retail, tourism and education sectors**, but not in the health, sports and catering sectors due to the pandemic
- In SMEs, the response of the catering and sports sectors was not satisfactory, so it was decided **not to include** them in the survey
- Only one of the employee unions responded, so the participation was not considered satisfactory
- In the field of consumer associations, **the 5 largest** associations participated

# Workshops

- **2 were held:** in the first 67 participants were invited, who represented associations and individual SMEs from the trade sectors, of Tourism and Hospitality, as well as consumer associations, while in the second 67 different participants were invited, representing clubs and individual SMEs from the Health and Education sectors
- They were divided into **two sections**. In the first, the results of questionnaires and the conclusions reached while in the second, the participants were asked for their opinions, with the aim of establishing whether the identified issues arising from the processing of the questionnaires express their needs
- The suggestions and comments stemming from the workshops were taken into account in shaping the needs and requirements of SMEs, in terms of their compliance with the GDPR

## Questionnaire results

- **A) Lawfulness and transparency**

It included questions about:

- Information of subjects and legal bases
- Consent
- Rights and their exercise
- Data destruction

Both SMEs and consumer and consumer associations face problems regarding the relevant procedures

# Questionnaire results

- **B) Accountability**

It included questions about:

- Obligation to appoint a DPO
- Records of processing activities
- Security policy and measures
- Data Breaches and their handling
- Assignment to processors

The majority of SMEs had issues in these areas as well

# Questionnaire results

- **C) Business activities that include data processing**

It included questions about:

- Website
- Direct marketing by electronic means
- Video surveillance
- Employee records

## Questionnaire results

- **D) Guidance and compliance needs**
  - Both associations and individual SMEs
    - i) need **primarily** guidance **on the data subjects' rights, the website and employment contracts,**
    - ii) about **cookies, the use of electronic means and the newsletter** and
    - iii) to understand **the obligations** deriving from the Regulation, in the form of guidelines
  - The same needs emerged from the 2 WORKSHOPS

# Compliance requirements

**The requirements** that emerged from the questionnaires and workshops for the compliance toolkit are the following:

## **Lawfulness and transparency**

- ✓ **Information:** a) **material** about how to inform the data subjects b) **information templates** adaptable to different subject categories, e.g. employees, customers and in different locations (website, physical store)
- ✓ **Consent:** a) **information material** to receive a valid of consent (conditions and lawfulness of its use) b) **material** regarding cases for which consent is required (e.g. written or online application)

# Compliance requirements

## Lawfulness and transparency

- ✓ **Exercise of Rights:** procedures and templates for handling requests concerning the exercise of data rights including the concept of each right and how an SME can inform and respond to data subjects applications (customers/employees) regarding the exercise of their rights
- ✓ **Data destruction:** information material and templates for explaining to the SMEs of the conditions of data files' destruction and the relevant process

# Compliance requirements

## Accountability

- ✓ **Records of processing activities:** a) informational material for this obligation b) provision of activity file templates, citing the standard content for the typical activities of SMEs
- ✓ **Security measures:** Simple and comprehensive lists of general organizational and technical security measures, appropriate and adaptable to the typical activities of SMEs
- ✓ **Breach Incident Handling Process:** a) information about way of detecting and handling violations both internally in SMEs and to the affected data subjects, b) indicative reporting of cases of data breaches that could affect the standard operations of SMEs
- ✓ **Processor:** a) informational material, explaining issues such as who is the controller and the processor and what their roles are b) model contract between the processor and the controller

# Compliance requirements

## Business activities involving data processing

- ✓ **Business website:** requirements for the website to ensure that the IT companies that offer website services respect data protection legislation. These requirements must include transparency requirements, basic security measures and compliance with cookies
- ✓ **Promoting products and services by electronic means:** guidance on how to contact existing customers and on data retention in order to respond to complaints from message recipients. This guidance should also include marketing through social media
- ✓ **Video surveillance:** guidance with clear requirements for an SME, which can be used as a way to ensure that security companies offering video surveillance installation services follow privacy laws and GDPR.

## Compliance requirements

- ✓ **Employee files:** a) informative material, explaining the legal obligations arising from the GDPR for the processing of personal data of employees and candidate employees from SMEs, b) contract annex template which includes the basic terms regarding the processing of personal data of employees and c) template on the correct use of electronic means by employees
- ✓ Based on the needs and requirements of SMEs for their compliance with the GDPR, which resulted from the relevant analysis, the following of work, in turn, focus on identifying the issues which will be addressed by the compliance toolkit

Thank you very much for your attention