DELIVERABLE

Project Acronym: SMEDATA

Grant Agreement number: 814763

Project Title: Ensuring the Highest Degree of Privacy and Personal Data Protection through Innovative Tools for SMEs and Citizens

D3.1 Report on the survey analysis of SMEs as data controllers in light of GDPR
Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Author</th>
<th>Organisation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>19/04/2019</td>
<td>Kamelia Angelova</td>
<td>EWLA-BG</td>
<td>First draft</td>
</tr>
<tr>
<td>1.2</td>
<td>23/04/2019</td>
<td>Hristo Alaminov</td>
<td>CPDP</td>
<td>Review</td>
</tr>
<tr>
<td>1.3</td>
<td>25/04/2019</td>
<td>Kamelia Angelova</td>
<td>EWLA-BG</td>
<td>Review</td>
</tr>
<tr>
<td>2.0</td>
<td>30/04/2019</td>
<td>Hristo Alaminov</td>
<td>CPDP</td>
<td>Review</td>
</tr>
</tbody>
</table>

Date of delivery

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>final ■ /draft □</td>
</tr>
</tbody>
</table>

Abstract

Report on the survey analysis of SMEs as data controllers in light of GDPR aims to present and analyse the results of the conducted survey among SMEs and associations of SMEs for the purposes of WP3. The report outlines the main identified challenges met by SMEs in the implementation of the GDPR, the respective main areas for intervention in order to ensure GDPR compliance as well as the most relevant mechanisms for raising awareness on data protection issues among SMEs.

Keywords

Survey, results, challenges, areas of intervention, raising-awareness mechanism, self-assessment tool.
# Table of Contents

Introduction to the Report ................................................................. 5

Methodology .................................................................................. 6
  I. SURVEY OBJECTIVES AND DESIGN ........................................... 6
  II. PROCEDURES USED FOR CONDUCTING THE SURVEY .......... 8
  III. SURVEY PARTICIPANTS .......................................................... 9
  IV. DATA PROCESSING IN CONDUCTING THE SURVEY ............... 10

Analysis of the survey results .......................................................... 11
  I. CURRENT ISSUES AND CHALLENGES FOR SMES AND COMMON DATA PROTECTION AREAS OF INTERVENTION .............................. 11
  II. RAISING-AWARENESS MECHANISMS ..................................... 27
  III. SELF-ASSESSMENT TOOL ......................................................... 32

Conclusions .................................................................................... 36

Appendix A Survey Questionnaire Text in English ............................... 38
Appendix B Survey Questionnaire Text in Bulgarian ............................. 46
Appendix C Survey Questionnaire Text in Italian ................................. 54
Appendix D Interview Form .............................................................. 62

---

## Disclaimer

The content of current Report on the survey analysis of SMEs as data controllers in light of GDPR represents the views of the author only and is their sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
## List of abbreviation

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPDP</td>
<td>Commission for Personal Data Protection</td>
</tr>
<tr>
<td></td>
<td>(Комисия за защита на личните данни)</td>
</tr>
<tr>
<td>APIS</td>
<td>APIS Europa</td>
</tr>
<tr>
<td>SAJUZ</td>
<td>The Union of Bulgarian Jurists</td>
</tr>
<tr>
<td></td>
<td>(Съюз на юристите в България)</td>
</tr>
<tr>
<td>EY</td>
<td>Ernst &amp; Young Law Partnership</td>
</tr>
<tr>
<td></td>
<td>(Адвокатско съдружие Ърнст и Янг)</td>
</tr>
<tr>
<td>EWLA - BG</td>
<td>European Women Lawyers Association - Bulgaria</td>
</tr>
<tr>
<td>GPDPIT</td>
<td>Garante per la Protezione dei Dati Personali</td>
</tr>
<tr>
<td>UNIROMA3</td>
<td>Università degli Studi Roma Tre</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>EC</td>
<td>European Commission</td>
</tr>
<tr>
<td>REC</td>
<td>‘Rights, Equality, Citizenship’ programme</td>
</tr>
<tr>
<td>WP</td>
<td>Work Package(s)</td>
</tr>
<tr>
<td>SME</td>
<td>Small and medium-sized enterprises</td>
</tr>
</tbody>
</table>
Introduction to the Report

The SMEDATA project was developed by the Consortium members (CPDP, APIS, SAJUZ, EY, EWLA – BG, GPDPIT and UNIROMA3). The project will promote the preparation for the effective application of the General Data Protection Regulation (GDPR) through awareness, multiplying training and sustainable capacity building for SMEs and their associations, including their legal advisors. The project aims at ensuring sector specific and sustainable knowledge and implementation of the GDPR through self-assessment and awareness tool and assisting the understanding and compliance with the GDPR.

This Report on the survey analysis of SMEs as data controllers in light of GDPR (‘the Report’) is a deliverable of WP3 “Self-assessment tool for sustainable awareness based on SMEs’ specific needs and processes from the prospective of personal data protection” of the SMEDATA project. The objectives of this WP are:

► To promote affordable and tailor-made solution to the SMEs to assess the compliance of their processes with the GDPR and to ensure continuous process of SMEs self-improvement.
► To build sustainable awareness and understanding of the data privacy rules and standards to achieve compliance with the GDPR while reflecting the SMEs’ specific needs and processes which entail personal data processing.
► To prepare SMEs, as well as their associations to comply with their obligations under the GDPR taking into account the specifics of their sectors.

The Report aims to summarize main areas for intervention in order to ensure GDPR compliance of the SMEs as well as possible ways for raising awareness on the GDPR among SMEs entities and SMEs staff and clients. The report represents the main findings of the Survey based on elaboration and dissemination of specially tailored questionnaires among more than 100 stakeholders in Bulgaria, Italy and other EU Member States (the questionnaire is included as an attachment to the Report).

The Report was prepared by a team of representatives (working group) of the Consortium members (CPDP, APIS, SAJUZ, EY, EWLA – BG, GPDPIT and UNIROMA3).
Methodology

The Report was made with a comprehensive methodology to obtain deeper insights among SMEs and their associations regarding the problems which SMEs most often meet in reaching compliance with the GDPR requirements as well as for identification and establishing what type of tools and mechanisms could facilitate SMEs’ performance of on data protection issues.

In terms of methodological approach, this task was implemented through a sequence of inter-related activities, namely:

1. SURVEY OBJECTIVES AND DESIGN

1. Survey Objectives

The survey questionnaire was designed to address the following main objectives:

- To collect information on challenges, issues or concerns which the businesses, in particular, micro, small and medium-sized enterprises (SMEs) and associations of SMEs, face in connection to the implementation of the requirements of EU Regulation 2016/679 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data (“GDPR”);
- To provide an overview of on the most appropriate raising awareness tools and mechanism for SMEs;
- To provide key insights on the most relevant for SMEs structure and content of a self-assessment and awareness tool providing the necessary resources to SMEs to achieve compliance with the effective data protection regulations of their activities, processes, controls as well as organizational and business practices.

2. Survey Design and Structure

The initial step in preparation of the survey constituted of design and drafting of a questionnaire to entail the established set of objectives for the survey. The questionnaire was prepared by a team of representatives (working group) of the Consortium members.

The working group worked simultaneously on the questionnaires for the surveys under WP 2 and WP3 so that it was possible to launch both surveys simultaneously to receive a broader response by the target survey participants. The accent in the preparation of the WP3 survey questionnaire was to include questions that reflect the objectives of the survey.
The survey was kept broad and short to increase the likelihood of participation. Qualitative analysis was performed on the nuances of the GDPR to ascertain the exact type of potential challenges met by SMEs which to be included as possible response options in the survey. An important aspect of the survey questions was to reflect the views of SMEs so that their needs can be covered by the self-assessment tool to be prepared in the framework of WP3.

The survey questionnaire comprised the following sections:

i. **Information about respondents**: this section collects information about the type of organization in which respondents are engaged (SME, Association of SME or other body representing data controllers); the sector of activity and whether the activity of the organization is regional, national, European or international.

ii. **Survey questions**: The questions included in the questionnaire can be broadly divided in three sub-sections:

   - **Common challenges and areas of intervention**: The first two questions aimed at gathering feedback from respondents on the main challenges encountered by SMEs in achieving GDPR compliance. In essence, the questions allow collecting information for the purposes of establishing the main areas of intervention regarding GDPR compliance of SMEs.

   - **Raising-awareness mechanisms**: The question asked about the most appropriate for the needs of SMEs raising-awareness mechanisms applicable in different economic sector with respect to GDPR issues.

   - **Self-Assessment Tool**: The remaining questions were devoted to collect opinions of SMEs and their associations on the most appropriate and useful form, contents and structure of a self-assessment and awareness tool to serve SMEs in their implementation of the GDPR. These questions are closely related to the working hypothesis on the structure and content of the proposed self-assessment and awareness tool.

iii. **Glossary for the Survey**: An explanation of terminology to assist survey participants – was also provided.

The electronic format survey questionnaire was prepared and launched in three languages: English, Bulgarian and Italian.

**Appendix A, B and C** contain the complete list of survey questionnaire in the three language versions.
II. PROCEDURES USED FOR CONDUCTING THE SURVEY

1. Conducting of the electronic survey

The survey was rolled out for two months from 11 March 2019 till 19 April 2019. The survey questionnaire was uploaded on the website of the SMEDATA project (http://smedata.eu). Publication of an announcement of the survey and links to the survey questionnaire were also posted on the partners’ websites. The announcement was further carried out using the following communication channels: by e-mail, public announcements via Partners’ websites and social media campaign (LinkedIn, Facebook). Available email lists were further utilized to reach a broad spectrum of potential respondents among SMEs and their associations.

The survey was conducted on an anonymous basis. It was particularly stressed to participants that the results the survey is not connected to, driven by or grounded on CPDP or GPDP supervisory functions. For the purposes of the survey it was important to clearly explain to respondents that the Survey results shall not be linked to a particular participant or used in any way to establish compliance with the applicable laws.

1. Conducting of the Interviews

Along with the survey, interviews were organized and conducted with representatives of SMEs and their associations in Bulgaria, Italy and other EU member states. The partners’ networks were utilized in order to select and organize SMEs and associations that can provide additional insight on the challenges and needs of SMEs in achieving compliance with data protection requirements.

The interviews commenced with presentation of the SMEDATA Project and provided information and clarifications to the interviewees to the effect that:

- The Survey is being undertaken by the SMEDATA project partners and is funded by the European Union’s Justice Programme (2014-2020) & Rights, Equality and Citizenship Programme (2014-2020)
- The content focuses on the respondents’ views on the application of the GDPR by SMEs.
- The invited participants will take part voluntary and may choose not to participate.
- All responses will be kept confidential and anonymous. They will only be used for statistical purposes within the framework of the project.
- The interview and the Survey are not connected to, driven by or grounded on CPDP or GPDP supervisory functions. Thus, the interview results shall not be linked to a particular participant or used in any way to establish compliance with the applicable laws.
The interviews were structured around the questions included in the survey, and in particular the following questions were raised and discussed:

- What in your experience are the main challenges met by SMEs in the process of achieving GDPR compliance?
- Are there any sector-specific problems relating to data protection requirements and security that can be indicated?
- What are the strategies that SMEs should implement to come into compliance with the GDPR?
- What types of awareness-raising mechanisms are important for SMEs in the process of GDPR implementation?
- What type of tools (self-assessment tools, guides etc.) could best suit the needs of SMEs for achieving data protection compliance?
- Could you share some additional observations relating to the needs of SMEs in connection with the entry into force of the GDPR?

Appendix D contains the prepared for the purposes of the project interview form with interview questions.

The survey questionnaires were presented to the interviewees to receive additional feedback on the survey questions. Important additional information was also obtained with respect to areas of intervention common for SMEs, most comprehensive and proved useful mechanisms for awareness raising in different economic sectors, usefulness of different communication channels for SMEs and their associations.

III. SURVEY PARTICIPANTS

The survey was aimed at two main target groups – representatives of micro, small and medium-sized enterprises (SMEs) and SMEs associations. The selection of the target groups is based on analysis and researches indicating that SMEs have neither contingency reserve, nor prepared work force for dealing with such enormous change as applying of new EU data protection rules. Concurrently, SMEs play a profound role in the economic development in all EU Member States. The greatest number of workers is employees of the SME entities.

The survey results are based on responses from more than 100 participants through the online survey questionnaire and interviews conducted with representatives of SMEs and their associations. The participants represented small to medium sized organizations established in Bulgaria, Italy as well as other EU MSs and associations of SMEs. Diverse range of sectors was covered such as:
Electricity, gas, steam and air conditioning supply
Water supply, sewerage, waste management and remediation activities
Construction
Wholesale and retail trade; repair of motor vehicles and motorcycles
Transportation and storage
Accommodation and food service activities
Information and Communication
Financial and insurance activities
Real estate activities
Professional, scientific and technical activities
Administrative and support service activities
Public administration and defence; compulsory social security
Education
Human health and social work activities
Arts, entertainment and recreation
Other service activities
Activities of extraterritorial organisations and bodies

IV. DATA PROCESSING IN CONDUCTING THE SURVEY

The data collected through the Survey will be used only for the purposes of the SMEDATA project, in particular for the Survey report under WP3. Based on the results, the Partners will complete the results under WP3 and will elaborate the self-assessment and awareness tool providing the necessary resources to SMEs to achieve compliance with the effective data protection regulations of their activities, processes, controls as well as organizational and business practices.

The participation in the electronic format of the survey and the interviews is voluntary. The name and identifying information of the respondents and interviewees will not be associated with any part of the written report of the Survey. All records will be kept confidential in the secure possession of the project team. The results shall be aggregated and shall be used only for the purpose defined above.
Analysis of the survey results

A detailed analysis of the survey responses has been made to reach important conclusions for WP3. The findings from the on-line based survey were combined with data from the conducted interviews to derive inferences with respect to additional observations made by the interviewees relating to their experience with GDPR.

The results are presented below grouped by survey topics.

1. CURRENT ISSUES AND CHALLENGES FOR SMES AND COMMON DATA PROTECTION AREAS OF INTERVENTION

The replies to the first two questions provide essential data in order to determine the current issues of SMEs as data controllers as well as to describe common data protection areas of intervention in most of the economic sectors.

1.1. Most common issues and challenges encountered by SMEs in achieving GDPR compliance

The results of the survey clearly indicate that the most common issues and challenges met by SMEs in the application of GDPR include the following:

- Assessing the data protection risks and choosing appropriate security measures for the protection of personal data;
- Performing data mapping and gap analysis and continuous monitoring of compliance;
- Provision of sufficient budget and human resources to implement GDPR.
Below we review separately each of the issues and challenges included in the survey.

(a) Getting acquainted to and understanding the new requirements of the GDPR

The survey highlighted that the majority of the respondents find that understanding of the new requirements of the GDPR is a serious challenge. This is not among the main indicated challenges for SMEs. Clearly, the time past following the entry into force of the GDPR has been used by SMEs and their representatives to get acquainted with the regulation. In the same time, better acquaintance with the new aspects of the regulation still remains a topic with a comparatively high importance for SMEs. This is particularly indicated for the case of Bulgarian SMEs, where the majority of the respondents find it to be among the most applicable issues.

(b) Performing data mapping and gap analysis/internal assessment of your organisation

The main purpose of carrying out GDPR gap analysis is to assess the current level of compliance with the GDPR of the organisation and identify and prioritise the key work areas that should be addressed. The survey shows that most of the respondents find performing data mapping and gap analysis to be a significant problem. The survey classifies it as one of the important challenges although most organizations have already gone through this process prior to or in the early months of entry into force of the GDPR.

A shared view in the interviews have been that understanding the types of personal data that are collected by the organisation, the records and systems in which it is stored, and why and how it is used, has been very important and challenging to ensuring initial compliance. However, the current challenge for SMEs is monitoring compliance. Ensuring on-going monitoring of the compliance with internal regulations, procedures and policies regulating data protection is considered the most important strategy and precondition for achieving and maintaining compliance. Thus, the focus has shifted from initial data mapping and compliance to consecutive monitoring of compliance.
(c) Assessing the data protection risks and choosing appropriate security measures for the protection of personal data

Article 32 of the GDPR defines the requirements for the security of the processing. When processing personal data, the controller and the processor must implement appropriate technical and organizational measures for protection of the personal data of natural persons to ensure a level of security appropriate to the risk and demonstrate the effectiveness of the measures taken. According to the survey results, security measures represent an area of significant concern for SMEs. 59% of the respondents find that this is a most applicable challenge.

Based on the conducted interviews, the main problematic issues that have been indicated include:

- Necessity of significant investments and financial resources for integration of risk management system and IT security measures such as data pseudonymisation, data encryption, data breach prevention and detection, identity management, etc.

- Secondly, and not less important, concern is the fact that the minimal acceptable standards for security of processing seem to remain unclear for SMEs. In this respect, Article 32(3) of the GDPR explicitly points out that organizations can adhere to an approved code of conduct from associations or other organizations to demonstrate compliance with the security requirements. Likewise, the fulfilment of the requirements of data protection by design and default (Article 25 of the GDPR) can be demonstrated by certification in accordance with Article 42 of the GDPR. Therefore, it is not surprising that there were numerous recommendations and requests by interviewees for prompt endorsement of sectoral Codes of Conduct as well as adoption of certification regime at EU or national level in order to assist companies in the implementation of appropriate security measures.
Ensuring staff awareness and training

GDPR compliance is intrinsically connected with the way employees collect, process, store, share and securely wipe personal data. For this reason, employees at most levels of an organisation including IT, marketing, customer support and data teams – need to be aware of data protection requirements and policies and how to handle information falling under the scope of the GDPR. Thus, training and awareness-raising activities for ensuring a culture and training of data protection within the organization is an important issue for SMEs.

Conducting specialized external trainings and internal recurrent training of staff in relation to their specific data processing obligations has been mentioned in the interviews as one of the most important strategic approaches of SMEs.

Good planning and internal organization are crucial for achieving GDPR compliance by SMEs

A common sectoral problem is the need to ensure sufficient awareness and training to the personnel. The difficulty is usually not financial, but mainly organizational as a large part of the staff of most companies works with customer data or employee data and this requires continuous training on a different program and different issues according to the specifics of the company’s individual teams.
(e) Provision of sufficient budget and human resources to implement GDPR

GDPR compliance requires heavy financial and technical investment for SMEs - in software, technical support, legal advice. The impact on human resources, budget, and additional technical resources may be significant. It is therefore not surprising that only 6% of the respondents feel that provision of sufficient budget and human resources to implement GDPR is not a particularly applicable challenge.

Through the conducted interviews, certain sectoral specifics in regulated industries regarding budget planning were further shared. For example in certain sectors where business investments are approved years ahead of time, the budget allocation for GDPR compliance have not been taken into consideration which is a serious issue when major software adjustments for GDPR purposes are needed.
(f) Determining the appropriate legal ground for processing of personal data (consent, contract, legal obligation, legitimate interest, etc.)

According to the survey results, determining the appropriate legal ground for processing of personal data is often confusing for SMEs. Shared observations in the interview process concern unclear regulatory situation regarding legal grounds for data processing. In particular, in many cases consent forms are required without actual legal necessity.

Interestingly, general regulatory issues such as the determining the appropriate legal ground for processing of personal data are of major concern for certain sectors, while do not pose a challenge in others.

(g) Maintaining the necessary documentation in line with the principle of accountability

Maintaining the necessary documentation is undoubtedly one of the areas where most efforts have been spent by SMEs in preparation for the GDPR. According to information by the respondents procedures for the management of data protection, updating of contracts with third parties, adjustment and drafting of documentation such as information, consent forms, letters of
appointment have been an issue for most SMEs. An important challenge that has also been shared is following the ‘privacy by design’ approach which requires companies to start a project by providing, right away, the tools to protect personal data.

Following the initial phase of preparation of internal documentation and policies, respondents appear to be less concerned with the requirements for maintaining the necessary documentation in line with the principle of accountability which have expanded under the GDPR.

A suggestion made by several respondents is there are no clear guidelines on completing and maintaining the records and associated procedures for handling them (art. 30 of the GDPR), and additional guidelines in this respect would be useful.

(h) Other issues

Other issues indicated by respondents as being common challenges in achieving GDPR compliance include the following:

- Certification

An area that remains unclear for SMEs seems to be the lack of specific requirements for professional assessment of the state of GDPR readiness of an organisation, e.g. certification of privacy professionals to deliver trainings, assist with risk assessment and validate the achieved compliance of the organization. Usually SMEs assign to outside contractors an IT review of their security systems. However, as there is no licensing, certification or other type of quality standards procedures for these types of reviews, there is never certainty whether the security is appropriately achieved.
Further, with respect to security of personal data it has been suggested that certification of privacy technologists who can validate/create the way that personal data requirements are incorporated into IT products etc.

▶ **Review of compliance and training of contractors**

Respondents appear to be concerned with the level of compliance of third parties contractors. According to the survey, data protection practices of third parties often have to be observed and assisted to avoid non-compliance on the part of contractors. In certain cases events and trainings for contractors have to be organized for raising awareness on GDPR matters.

▶ **Difficulties in completing and maintaining the records of processing activities (art. 30 of the GDPR)**

It was shared by interviewees that there are no clear guidelines on completing and maintaining the records and associated procedures for handling them (art. 30 of the GDPR).

▶ **Regulatory conflicts with the anti-money laundering legislation**

A problematic regulatory issue is further the new regulation in the field of anti-money laundering which is claimed by respondents to contain contradictions with the data protection legislation. Numerous regulatory regimes create a serious challenge for SMEs, including the simultaneous application of anti-money laundering and data protection regulation.

### 1.2. Issues of particular importance with regard to GDPR requirements in the specific industry sector in which the organization operates

Depending on the sector, challenges among SMEs clearly vary. For example, in the sectors related to trade, services and utilities - technical security measures are pointed out clearly as a challenge. The opposite view is shared by the IT industry, where naturally the technical tools and solutions are easily achievable and do not raise serious concerns. On the contrary general regulatory issues such as the determining the appropriate legal ground for processing of personal data are of major concern.

Below we have reviewed in detail the survey results. Respondents prioritize the following three areas as of particular importance in the specific industry sector in which their organizations operate with regard to GDPR requirements:

▶ Implementation of appropriate technical and organisational measures to ensure security of processing of personal data (e.g. pseudonymisation, encryption, etc.)
Processing of personal data of customers, including for direct marketing;
How to respond to requests by data subjects to exercise their rights.

They are closely followed by the topics of Data Protection Impact Assessment and processing of sensitive data.

(a) Processing of personal data of employees

Processing of personal data of employees has not been pointed out in the survey as an issue of significant concern. In the data mapping and gap analysis traditional justifications for lawful processing of employee data have been revisited together with the way in which the data is collected, used and retained.
(b) Processing of personal data of customers, including for direct marketing

Customers’ data plays a critical part in business, particularly in direct marketing strategies and therefore marketers must ensure they have demonstrated clear compliance and consent. Processing of personal data of customers is a particularly sensitive issue, particularly in sectors which rely largely on direct marketing.

According to the respondents GDPR has changed the way their companies communicate with prospects and customers. Depending on the nature of a company’s data processing activities SMEs are also concerned about the GDPR’s stricter rules on consent and the impact on the organisations’ ability to use and re-use data. It has been pointed out in the survey that one of the problems has been the necessity of significant changes to websites and forms, terms and conditions, privacy policies, and other consent mechanisms.

In the next place, the GDPR conditions for consent are a major issue for SMEs in connection with direct marketing as companies must demonstrate how the data subject has consented to the processing of their personal data and that consent was knowingly and freely given, clear and specific, and should keep clear records of consent. Respectively marketing databases had to be cleansed and reviewed to ensure that the organisation can identify consent which has been granted lawfully and fairly.

(c) Need to carry out Data Protection Impact Assessment

Under art. 35 of the GDPR, companies have to conduct data protection impact assessment (DPIA) in relation to any processing that would result in high risk for individuals. The notion of high risk is not explicitly defined in the GDPR but there are three examples of high risk processing: (i) the large scale processing of sensitive personal data; (ii) automated decision taking; and (iii) systematic and large scale monitoring of publicly accessible areas.
According to the survey results, despite those examples, the assessment whether DPIA has to be carried out remains an unclear issue for SMEs. Further, it seems to be a complicated matter for SMEs what the obligatory contents and level of detail of a DPIA should be. A suggestion made by several respondents is that sample documents or good practices in carrying out DPIAs are provided to facilitate the work of SMEs.

(d) Appointment of a Data Protection Officer

The assessment whether an association needs to appoint a Data Protection Officer according to the survey results is not problematic for most companies. A specific issue that has been raised in the process of interviews is that no certification regime for trainers of DPOs exists in Bulgaria. It is considered necessary by respondents that regulation is adopted on that is entitled to train and certify DPOs at national level.

(e) How to respond to requests by data subjects to exercise their rights (e.g. right to access, right to be forgotten, right to objection, data portability right, etc.)

Respondents appear to be less confident about newer requirements and obligations, such as individuals’ rights, which have expanded under the GDPR. The survey results show that the
majority of organisations are concerned about responding to requests by data subjects to exercise their rights.

The right to be forgotten gives people the right to have out-dated or inaccurate personal data to be removed and has, according to information from the conducted interviews, forced companies in some instances to delete their whole data bases in order to comply particularly with the requirement for keeping data up-to-date and accurate. Responding to individuals’ requests raises the question of collecting additional personal data as in certain sectors only name and email are processed, while the identification in the individuals’ request contains additional extended personal data.

Concerns have also been shared relating to the need to create new software or to update available IT systems to enforce new and enhanced rights of data subjects, such as the right to be forgotten.

How to respond to requests by data subjects to exercise their rights (e.g. right to access, right to be forgotten, right to objection, data portability right, etc.)

(f) Implementation of appropriate technical and organisational measures to ensure security of processing of personal data (e.g. pseudonymisation, encryption, etc.)

Implementation of appropriate technical and organisational measures to ensure security of processing of personal data is a serious concern for the majority of the respondents. Necessity of introducing IT security measures such as data pseudonymisation, data encryption, data breach prevention and detection, identity management, etc. involve significant financial resources and technical expertise for SMEs, which is a challenge. The problem is particularly relevant where a system was not originally designed to meet data protection requirements, in compliance with the "privacy by design" principle and to a certain extent, the "privacy by default" principle.

According to the respondents it is a difficult assessment for SMEs what particular technical security measures for data protection to be used as on regulatory level there are no clear technical indicators. It is additionally shared that agreements for data processing are often concluded
without detailed description of the required technical security measures. Therefore, it is considered advisable by survey respondents that good practices on this issue are published by competent authorities to provide examples what measures would be considered sufficient as technical security.

(g) Obtaining the consent of the holders of parental responsibility for processing personal data of children

Obtaining the consent of the holders of parental responsibility for processing personal data of children is not an issue in most industries. More than half of the respondents find it irrelevant as a challenge in data protection compliance. According to the conducted interviews it can be an issue in the health sector and in on-line trade of specific goods.
(h) **Cookies and websites**

Pursuant to Recital 32 and art. Article 7 (3) the GDPR consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject’s agreement to the processing of personal data relating to the user. These requirements have affected the use of cookies and websites in most industries. Giving informed and unambiguous consent applies to almost all marketing, targeting, web-analytic cookies since these store user identifiers. Thus, cookie consent collection is essential to comply with the GDPR.

However, the survey does not show significant problems encountered by SMEs in connection with new requirements for cookies and websites under the GDPR. The majority of the respondents does not find this issue to be a relevant concern.

![Cookies and websites](image)

(i) **International transfers of personal data**

The GDPR requirements on international data transfers are not a challenge for the majority of the respondents. This issue affects organisations that engage in cross-border data transfers, mainly those using online IT services and cloud-based services. The main challenges shared by respondents concern the identification of all circumstances in which personal data are transferred to recipients located outside the EEA. For example, in cases of cloud services, it is not always possible to follow and establish the location of the cloud systems. Further, uncertainties exist regarding some of the data transfer mechanisms.
(j) Notification of personal data breaches

The regime of notification of personal data breaches is one of the key changes under the GDPR (art. 33 of the GDPR). A controller has to notify the DPA within 72 hours after becoming aware of any breach that presents risks to the rights and freedoms of individuals. Processors also have to notify controllers without undue delay after becoming aware of a breach. The survey results show that the majority of survey respondents are concerned with the breach notification obligations.

(k) Processing of sensitive data

The processing of ‘special categories’ of personal data (sensitive data) is generally prohibited under the GDPR (art. 9). The processing of sensitive data requires the data subject's 'explicit consent' and observance of the concrete legislative requirements. This poses significant challenges for SMEs in certain sectors such as insurance, construction, health services etc. The survey results show that nearly 2/3rd of the respondents find processing of sensitive data to be a challenge.

<table>
<thead>
<tr>
<th>Common strategy of SMEs in addressing GDPR concerns:</th>
</tr>
</thead>
<tbody>
<tr>
<td>An identified strategy to deal generally with issues related to GDPR compliance by SMEs is the following: avoiding the (excessive) collection and processing of personal data of end users of products and services.</td>
</tr>
</tbody>
</table>
(I) Other

Respondents have identified the following other sectoral issues and challenges encountered by SMEs in achieving GDPR compliance:

► **Data controller/data processor relationship**

Respondents have shared as one of the encountered problematic issues the need to conclude agreements to govern the controller/processor relationship. The changes to the contractual terms for data processing agreements require considerable efforts on the part of controllers and processors, both in respect of existing relationships and new ones. In certain sectors it is further specified that difficulties exist in making a distinction between a data controller and a data processor as well as in defining if there is a relationship as data controller/data processor or as joint controllers.

► **Lack of clear guidance per sectors and types of activities**

The lack of clear guidance per sectors and types of activities, which could assist the work of SMEs on data protection issues, is pointed out as one of the common challenges relating to sectoral specifics.
II. RAISING-AWARENESS MECHANISMS

The survey raised the question – which are the appropriate for the needs of SMEs raising-awareness mechanisms with respect to GDPR issues. The top three selected responses for most appropriate awareness raising mechanisms for SMEs with respect to GDPR issues are:

- Publication of GDPR guides and instructions for SMEs;
- Development of software tools and ready-made templates;
- Conducting specialized trainings for SMEs;

Raising awareness events (conferences, seminars, etc.) are also among the mechanisms of importance to SMEs.

Below we have presented in graphical format the results of the survey on each of the suggested raising –awareness mechanisms.

(a) Raising awareness events (conferences, seminars, etc.)
(b) Conducting specialized trainings for SMEs

Conducting specialized trainings for SMEs

- Not particularly applicable
- Slightly applicable
- Quite applicable
- Most applicable

(c) Publication of GDPR guides and instructions for SMEs

Publication of GDPR guides and instructions for SMEs

- Not particularly applicable
- Slightly applicable
- Quite applicable
- Most applicable

(d) Publication of newsletters, posters, flyers and other materials

Publication of newsletters, posters, flyers and other materials

- Not particularly applicable
- Slightly applicable
- Quite applicable
- Most applicable
(e) Conducting radio and television programmes on the topic

Among other types of awareness raising mechanisms for SMEs with respect to GDPR issues were indicated the following:

- Networking events for exchange of experience among SMEs in the same sector;
- Conducting industry-specific trainings;
- Organization of interactive trainings for employees;
- Conducting specialized external trainings and internal recurrent training of staff in relation to their specific data processing obligations;
- Conducting of working tables with representatives of the business, competent authorities and EU experts in order to

(f) Development of software tools and ready-made templates

(g) Other

General observations:

Any type of raising awareness events that provide a level of training or explanation of concepts and questions with practical orientation (incl. trainings, conferences, seminars) are important for SMEs.
solve some of the existing unclear aspects of the application of GDPR;
- Trainings that cover representatives of different sectors;
- Conferences and seminars that are not theoretically oriented but are entirely based on the Q&A principle.

The replies to the third question give a picture of the most important and comprehensive awareness raising mechanism applicable to different economic sectors. Through the interviews with representatives of SMEs and Associations of SMEs the following additional information has been identified:

It is broadly considered by the interviewees that every employee, especially those with supervising functions and those directly working with personal data, must have knowledge of the rules and restrictions with regard to handling personal and sensitive data.

Conducting of trainings for employees, but also for subcontractors, is considered an important tool to build awareness of the rules and regulations regarding data protection. GDPR guides, samples and instructions are considered an alternative way to provide information, but also raise awareness about specifics of data protection requirements.

Use of ready-made templates, particularly electronically available, has also been suggested as a raising-awareness and compliance mechanism. From the information received in the interviews and the online survey, it is clear that there are EU based appropriate sample documents, matrix and models of proven good practice.

Based on the survey results it is clear that publication of newsletters, posters and other material as well as conducting radio and television programmes is not an appropriate for GDPR compliance needs manner of raising awareness among SMEs. A clear explanation of this fact is that compliance with GDPR requires applying a complex regulation for which hands-on detailed understanding is needed. This is best achieved by means of specially-tailored trainings and publications.

Through the survey it was further established what are the internal communication channels that have been most widely used by SMEs and SME associations. Internal communication was reviewed as the organizational communication with employees through which information and instructions are exchanged and enable the organization to perform its functions efficiently. Effective internal communication channels are considered important by the respondents for fulfilling regulatory requirements, including in the field of data protection. The most often used communication channels by SMEs include:
- Electronic communication channels, incl. email;
- Printed communication channels: written letters, instructions, bulletin boards;
- Direct communication channels: personal instructions and trainings, staff meetings, seminars.
III. SELF-ASSESSMENT TOOL

1.1. Type and form of a self-assessment tool for SMEs that is considered most useful

The survey provided participants with multiple options for type and form of a self-assessment tool for SMEs that is considered most useful. The possibility to select all applicable options was provided.

The most appropriate and useful form, contents and structure of a self-assessment and awareness tool pointed out by the survey is the following:

(a) Format

The majority of the survey respondents (58%) find the most appropriate format for the self-assessment tool to be: online based tool.

![Self-assessment tool in the following format](image)

(b) Contents characteristics

The top three selected responses for most appropriate contents characteristics of a self-assessment and awareness tool are: (i) practical knowledge and advice focused tool; (ii) Q&A format guide, (iii) easy to use guide with GDPR basics.
According to the provided by interviewees information a detailed analysis of GDPR-related topics would be useful only to the extent that the themes provide specific ways for practical implementation of one or other requirement that will probably go hand in hand with a practical handbook. Developing only theoretical outcomes is not particularly beneficial in a real business environment where specific steps, investments and actions to ensure compliance are to be undertaken.

It is important to note that through discussion with representatives of SMEs in different sectors, when the discussions included legal representatives this question was viewed in a different perspective. In particular, for lawyers of SMEs working on data protection issues a detailed in-depth analysis with sector-specific information is considered most helpful for solution of serious issues met in their practice. Those observations do not undermine the general situation that SMEs as a whole need an easy to use practical tool. More detailed level of expertise from a guidance tool is however appropriate for legal professionals who have already a good professional grasp of the GDPR basics.

**Legal professionals’ insight:**

While easy-to-use tool with GDPR basics is most appropriate for the needs of SMEs, legal professionals would have a greater use of a detailed in-depth analysis with sector-specific information.
(c) Target

The survey results show that the self-assessment tool should be tailored to address **above all data protection officers**, but also legal professionals and general management of SMEs.

![Target for the self-assessment tool](image)

### 1.2. Other topics or information to be included in a GDPR self-assessment tool

The survey results identify additional key issues and information that SMEs find necessary to achieve compliance. Among the main issues pointed out in the survey and in the interview process include:

- **Official guidelines issued by national data protection authorities**

According to the respondents the GDPR still leaves open a lot of questions for practical application. Further, it is considered very important that national data protection bodies provide relevant guidelines and instructions on a wide range of questions as well as appropriate good practices and models (including through cases studies and documentation) in order to meet the expectations and needs of SMEs. Guidelines by national authorities are most useful for SMEs, for instance the Spanish DPA has published guidelines for the preparation of contracts between controllers and processors. It is certainly not surprising that organisations are seeking additional guidance and clarification around the GDPR. This is the usual situation with any major change of law.

- **Codes of Conduct**

Some of the respondents note that the adoption of Codes of Conduct for different business sectors could facilitate the efforts of SMEs in achieving GDPR compliance. A quality sectoral Code of Conduct, as well as a well-trained Monitoring Body under art. 41 of the GDPR, could also adequately support companies' efforts to maintain continued compliance with the Regulation. The...
fact that adoption of sectoral Codes of Conduct is expected as a facilitating step in achieving compliances was confirmed through the interviews with representatives of business associations.

**Sample documents and examples**

The interviews with representatives of SMEs and associations of SMEs additionally show that sample documents and examples would be beneficial for SMEs, e.g. relating to the format and contents of registers of activities and other mandatory documentation under the GDPR.

It is also considered important by respondents that examples with appropriate technological measures for protection of personal data are provided as well as simplified models and matrices with the minimum mandatory requirements to be met by micro, small and medium-sized enterprises respectively.
Conclusions

The survey results provide useful knowledge of the current state of implementation of the GDPR by SMEs in Bulgaria, Italy and other EU MSs and main areas for intervention in order to ensure GDPR compliance. Based on the survey results it can be concluded that the most common issues and challenges met by SMEs in the application of the GDPR include the following:

- Assessing the data protection risks and choosing appropriate security measures for the protection of personal data;
- Provision of sufficient budget and human resources to implement GDPR;
- Performing data mapping and gap analysis and continuous monitoring of compliance.

Respondents have identified the following other sectoral issues and challenges encountered by SMEs in achieving GDPR compliance:

- Implementation of appropriate technical and organisational measures to ensure security of processing of personal data (e.g. pseudonymisation, encryption, etc.)
- Processing of personal data of customers, including for direct marketing;
- How to respond to requests by data subjects to exercise their rights

They are closely followed by the topics of Data Protection Impact Assessment and processing of sensitive data.

In the next place, the survey provided a clear picture of the most important and comprehensive awareness raising mechanism applicable to different economic sectors:

- Publication of GDPR guides and instructions for SMEs;
- Development of software tools and ready-made templates;
- Conducting specialized trainings for SMEs.

Raising awareness events (conferences, seminars, etc.) are also among the mechanisms of importance to SMEs.

Finally, the survey results confirmed the working hypothesis related to the structure and content of the proposed self-assessment and awareness tool, namely:
SMEs face similar challenges in the process of GDPR implementation;

SMEs need a wide range of awareness-raising tools for achieving GDPR compliance;

SMEs would have a greater use of a self-assessment tool that: (i) is online based (ii) easy to use Q&A format (iii) tailored for legal and data protection professionals.
Appendix A Survey Questionnaire Text in English

PERSONAL DATA PROTECTION SURVEY

Project Acronym: SMEDATA

Grant Agreement number: 814763

Project Title: Ensuring the Highest Degree of Privacy and Personal Data Protection through Innovative Tools for SMEs and Citizens

<table>
<thead>
<tr>
<th>Dissemination Level</th>
<th>PU</th>
<th>CO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public (after final adoption)</td>
<td></td>
<td>Confidential, only for members of the consortium (including the Commission Services)</td>
</tr>
</tbody>
</table>

Project co-funded by the European Commission within REC-AG-2017

Co-funded by the Rights, Equality and Citizenship (REC) Programme of the European Union
**Purpose of the Survey**

The following Personal Data Protection Survey (“the Survey”) shall be conducted as a part of the SMEDATA project coordinated by the Bulgarian Commission for Personal Data Protection (“CPDP”) in consortium with public and private partners from Bulgaria and Italy [http://smedata.eu/](http://smedata.eu/).

The purpose of the Survey is to collect information on challenges, issues or concerns which the businesses, in particular, micro, small and medium-sized enterprises (SMEs) and associations of SMEs, face in connection to the implementation of the requirements of EU Regulation 2016/679 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data (“GDPR”). The results of the Survey will be used for the elaboration of a self-assessment and awareness tool providing the necessary resources to SMEs to achieve compliance with the effective data protection regulations of their activities, processes, controls as well as organizational and business practices.

The Survey shall be conducted on an anonymous basis. The results shall be aggregated and shall be used only for the purpose defined above. The Survey is not connected to, driven by or grounded on CPDP or Garante per la protezione dei dati personali ("GPDP") supervisory functions. Thus, the Survey results shall not be linked to a particular participant or used in any way to establish compliance with the applicable laws.

Should a participant wish to access a summary of the Survey results or receive more information on the SMEDATA project, they may find more information on [www.smedata.eu](http://www.smedata.eu).

**Structure of the Survey**

The Survey is structured in several sections:

- General information: Information on the participant (no name basis)
- Questionnaire
- Glossary for the Survey: An explanation of terminology to assist survey participants will be made available by hovering over data elements underlined in black throughout the survey.

**Instructions:**

Survey Due Date — The Survey is due to be submitted by 12 April 2019.
General information

1. You are:
   - SME\(^1\)
   - Association of SMEs
   - Other body representing categories of controllers or processors

2. Your activities/ the activities of the SMEs in your association relate to (you may check more than one box):
   - Agriculture, forestry and fishing
   - Mining and quarrying
   - Manufacturing
   - Electricity, gas, steam and air conditioning supply
   - Water supply, sewerage, waste management and remediation activities
   - Construction
   - Wholesale and retail trade; repair of motor vehicles and motorcycles
   - Transportation and storage
   - Accommodation and food service activities
   - Information and Communication
   - Financial and insurance activities
   - Real estate activities
   - Professional, scientific and technical activities
   - Administrative and support service activities
   - Public administration and defence; compulsory social security
   - Education
   - Human health and social work activities
   - Arts, entertainment and recreation
   - Other service activities
   - Activities of households as employers; undifferentiated goods- and services-producing activities of households for own use
   - Activities of extraterritorial organisations and bodies

---

\(^1\) See definitions in the table below:

<table>
<thead>
<tr>
<th>Company category</th>
<th>Staff headcount</th>
<th>Turnover or Balance sheet total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medium-sized</td>
<td>&lt; 250</td>
<td>≤ € 50 m ≤ € 43 m</td>
</tr>
<tr>
<td>Small</td>
<td>&lt; 50</td>
<td>≤ € 10 m ≤ € 10 m</td>
</tr>
<tr>
<td>Micro</td>
<td>&lt; 10</td>
<td>≤ € 2 m ≤ € 2 m</td>
</tr>
</tbody>
</table>
3. Please specify the geographic coverage of your business activity/association:

- International
- European
- National
- Sub-national/local
QUESTIONNAIRE

Question No.1 Please rate which in your view are the most common issues and challenges encountered by SMEs in achieving GDPR compliance on the scale from 1 (least applicable) to 4 (most applicable)

(a) Getting acquainted to and understanding the new requirements of the GDPR
   □ 1     □ 2     □ 3     □ 4

(b) Performing data mapping and gap analysis/internal assessment of your organisation
   □ 1     □ 2     □ 3     □ 4

(c) Assessing the data protection risks and choosing appropriate security measures for the protection of personal data
   □ 1     □ 2     □ 3     □ 4

(d) Ensuring staff awareness and training
   □ 1     □ 2     □ 3     □ 4

(e) Provision of sufficient budget and human resources to implement GDPR
   □ 1     □ 2     □ 3     □ 4

(f) Determining the appropriate legal ground for processing of personal data (consent, contract, legal obligation, legitimate interest, etc.)
   □ 1     □ 2     □ 3     □ 4

(g) Maintaining the necessary documentation in line with the principle of accountability
   □ 1     □ 2     □ 3     □ 4

(h) Other (please specify) ………………………
   □ 1     □ 2     □ 3     □ 4

Question No.2 Please indicate which of the following issues are of particular importance in the specific industry sector in which your organization/association operates with regard to GDPR requirements. Please rate on the scale from 1 (least relevant) to 4 (most relevant):

(a) Processing of personal data of employees
   □ 1     □ 2     □ 3     □ 4

(b) Processing of personal data of customers, including for direct marketing
   □ 1     □ 2     □ 3     □ 4
(c) Need to carry out Data Protection Impact Assessment

☐ 1     ☐ 2     ☐ 3     ☐ 4

(d) Appointment of a Data Protection Officer

☐ 1     ☐ 2     ☐ 3     ☐ 4

(e) How to respond to requests by data subjects to exercise their rights (e.g. right to access, right to be forgotten, right to objection, data portability right, etc.)

☐ 1     ☐ 2     ☐ 3     ☐ 4

(f) Implementation of appropriate technical and organisational measures to ensure security of processing of personal data (e.g. pseudonymisation, encryption, etc.)

☐ 1     ☐ 2     ☐ 3     ☐ 4

(g) Obtaining the consent of the holders of parental responsibility for processing personal data of children

☐ 1     ☐ 2     ☐ 3     ☐ 4

(h) Cookies and websites

☐ 1     ☐ 2     ☐ 3     ☐ 4

(i) International transfers of personal data

☐ 1     ☐ 2     ☐ 3     ☐ 4

(j) Notification of personal data breaches

☐ 1     ☐ 2     ☐ 3     ☐ 4

(k) Processing of sensitive data

☐ 1     ☐ 2     ☐ 3     ☐ 4

(l) Other (please specify) ………………………

☐ 1     ☐ 2     ☐ 3     ☐ 4

Question No.3 Please indicate which in your view are the most appropriate awareness raising mechanisms for SMEs with respect to GDPR issues on the scale from 1 (least appropriate) to 4 (most appropriate)

(a) Raising awareness events (conferences, seminars, etc.)

☐ 1     ☐ 2     ☐ 3     ☐ 4

(b) Conducting specialized trainings for SMEs

☐ 1     ☐ 2     ☐ 3     ☐ 4
(c) Publication of GDPR guides and instructions for SMEs

☐ 1  ☐ 2  ☐ 3  ☐ 4

(d) Publication of newsletters, posters, flyers and other materials

☐ 1  ☐ 2  ☐ 3  ☐ 4

(e) Conducting radio and television programmes on the topic

☐ 1  ☐ 2  ☐ 3  ☐ 4

(f) Development of software tools and ready-made templates

☐ 1  ☐ 2  ☐ 3  ☐ 4

(g) Other (please specify) ……………………..

☐ 1  ☐ 2  ☐ 3  ☐ 4

**Question No.4 What type and form of a self-assessment tool for SMEs with the necessary information resources to achieve compliance in the field of data protection would be most useful:**

(a) Self-assessment tool in the following format *(you may check more than one box)*:

☐ Paper-based
☐ Online-based
☐ Mobile Application

(b) Self-assessment tool with the following characteristics *(you may check more than one box)*:

☐ Easy to use guide with GDPR basics
☐ Tools containing references to articles in GDPR and other legal materials
☐ In-depth analysis of complex GDPR topics
☐ Q&A format guide
☐ Practical knowledge and advice focused tool
☐ Sector-specific information tools
☐ Other (please specify) ……………………..
(c) Self-assessment tool specifically tailored for *(you may check more than one box):*

- [ ] Legal professionals within SMEs
- [ ] General management of SMEs
- [ ] Data protection officers
- [ ] Other (please specify) ......................

**Question No.5 What other topics or information should be included in a GDPR self-assessment tool?**

........................................................................................................................................................................
........................................................................................................................................................................
........................................................................................................................................................................
ПРОУЧВАНЕ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Акроним на Проекта: SMEDATA

Номер на договор за финансиране: 814763

Име на проекта: Осигуряване на най-висока степен на защита на неприкосновеността на личния живот и личните данни чрез иновативни инструменти за малки и средни предприятия и граждани

<table>
<thead>
<tr>
<th>Ниво на разпространение</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>PU (Публично)</td>
<td>X</td>
</tr>
<tr>
<td>CO (Поверително)</td>
<td></td>
</tr>
</tbody>
</table>

Проект, съфинансиран от Европейската Комисия в рамките на REC-AG-2017
Анкета относно разработването на инструмент за самооценка по прилагането на GDPR

Цел на проучването

Настоящото проучване за защита на личните данни („Проучването“) се провежда като част от проекта SMEDATA, координиран от българската Комисия за защита на личните данни („КЗЛД“) в сътрудничество с публични и частни партньори от България и Италия http://smedata.eu/index.php/bg/. Резултатите от проучването ще бъдат публикувани на тази интернет страница в края на месец април 2019 г.

Целта на настоящото Проучване е да събере информация за предизвикателствата, проблемите или притесненията, които бизнесът и по-специално микропредприятията, малките и средните предприятия (МСП) и сдруженията на МСП срещу във връзка с прилагането на изискванията на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни (“GDPR”).

Резултатите от проучването ще бъдат използвани за разработване на Ръководство за самооценка и информация, осигуряващ необходимата подкрепа на МСП за постигане на съответствие с действащите разпоредби за защита на личните данни на осъществяваната от тях дейност, процеси, контрол, както и организационни и бизнес практики.

Проучването се извършва на анонимен принцип. Резултатите ще се обобщат и ще се използват само за целта, посочена по-горе. Проучването не е свързано, продиктувано или основано на властническите функции на КЗЛД или на Органа за защита на личните данни на Италия. По този начин резултатите от Проучването няма да бъдат по никакъв начин свързани с определен участник или да бъдат използвани като средство за установяване на съответствие с приложимото законодателство.

Структура на Проучването

Проучването е структурирано в няколко раздела:

► Обща информация: информация за участника (анонимен принцип)
► Въпросник

Инструкции:

Крайна дата за попълване на Проучването – Моля, попълнете въпросника до 12 април 2019 г.
Обща информация

1. Вие сте:
   ☐ МСП
   ☐ Асоциация / сдружение на МСП
   ☐ Други организации, представляващи категории администратори или обработващи лични данни

2. Вашата дейност е свързана с (можете да посочите повече от един отговор):
   ☐ Земеделие, горско стопанство, риболов
   ☐ Минна и добивна дейност
   ☐ Производство
   ☐ Доставка на електроенергия, газ, топлоенергия и климатизация
   ☐ Водоснабдяване, канализации, управление на отпадъци и възстановителни дейности
   ☐ Строителство
   ☐ Търговия на едро и дребно; ремонт на МПС
   ☐ Транспорт и съхранение
   ☐ Хотелски и ресторантърски услуги
   ☐ Информация и комуникация
   ☐ Финансови и застрахователни дейности
   ☐ Сделки с недвижими имоти
   ☐ Професионална, научна и техническа дейност
   ☐ Административна и спомагателна дейност
   ☐ Публична администрация и отбрана; задължително социално осигуряване
   ☐ Образование
   ☐ Здравеопазване и социални дейности
   ☐ Изкуство, развлечения и отдих
   ☐ Други услуги
   ☐ Дейност на домакинства като работодатели; недиференцирани стоки и услуги – производство на домакинства за собствена употреба
   ☐ Дейности на международни организации и юридически лица

<table>
<thead>
<tr>
<th>Категория дружество</th>
<th>Брой служители</th>
<th>Оборот</th>
<th>Или</th>
<th>Общ счетоводен баланс</th>
</tr>
</thead>
<tbody>
<tr>
<td>Средно</td>
<td>&lt; 250</td>
<td>≤ € 50 м</td>
<td></td>
<td>≤ € 43 м</td>
</tr>
<tr>
<td>Малко</td>
<td>&lt; 50</td>
<td>≤ € 10 м</td>
<td></td>
<td>≤ € 10 м</td>
</tr>
<tr>
<td>Микро</td>
<td>&lt; 10</td>
<td>≤ € 2 м</td>
<td></td>
<td>≤ € 2 м</td>
</tr>
</tbody>
</table>
3. Моля, посочете географския обхват на Вашата дейност / асоциация:

☐ Международна
☐ Европейска
☐ Национална
☐ Регионална/ Местна
ВЪПРОСНИК

Въпрос № 1
Моля, посочете кои според Вас са най-важните проблеми и предизвикателства, които са поставени пред МСП в процеса на постигане на съответствие с Общия регламент за защита на данните (GDPR) по скалата от 1 (не е важно) до 4 (най-важно):

(a) Запознаване и разбиране на новите изисквания, поставени от GDPR
   □ 1     □ 2     □ 3     □ 4

(b) Идентифициране и инвентаризация на дейности, свързани с обработване на лични данни и анализ на пропуските в организацията
   □ 1     □ 2     □ 3     □ 4

(c) Оценка на риска за сигурността на личните данни и избор на подходящи мерки за защита
   □ 1     □ 2     □ 3     □ 4

(d) Осигуряване на информираност и обучение на персонала
   □ 1     □ 2     □ 3     □ 4

(e) Предоставяне на достатъчно бюджетни и човешки ресурси за изпълнение на изискванията на GDPR
   □ 1     □ 2     □ 3     □ 4

(f) Определяне на подходящо правно основание за обработване на лични данни (съгласие, договор, право задължение, законен интерес и др.)
   □ 1     □ 2     □ 3     □ 4

(g) Поддържане на необходимата документация в съответствие с принципа за отчетност и документиране на GDPR
   □ 1     □ 2     □ 3     □ 4

(h) Друго (моля, посочете) ..........................
   □ 1     □ 2     □ 3     □ 4

Въпрос № 2
Моля, посочете кои от следните въпроси, свързани с приложението на GDPR, са от особено значение в конкретния сектор, в който Вашата организация работи. Моля, оценете по скалата от 1 (не е важно) до 4 (най-важно):
(a) Обработване на лични данни на служителите
   □ 1    □ 2    □ 3    □ 4

(b) Обработване на лични данни на клиенти, включително за целите на директен маркетинг
   □ 1    □ 2    □ 3    □ 4

(c) Необходимост от извършване на оценка на въздействието върху защитата на личните данни
   □ 1    □ 2    □ 3    □ 4

(d) Назначаване на длъжностно лице по защита на данните
   □ 1    □ 2    □ 3    □ 4

(e) Как да се отговори на исканията на физически лица, упражняващи правата си (например право на достъп, право на заличаване, право на възражение, право на преносимост на данните и др.)
   □ 1    □ 2    □ 3    □ 4

(f) Прилагане на подходящи технически и организационни мерки за гарантиране на сигурността на обработката на лични данни (например псевдонимизиране, криптиране и др.)
   □ 1    □ 2    □ 3    □ 4

(g) Получаване на съгласието на носещите родителска отговорност за обработка на личните данни на деца
   □ 1    □ 2    □ 3    □ 4

(h) „Бисквитки“ (cookies) и уебсайтове
   □ 1    □ 2    □ 3    □ 4

(i) Международен трансфер на лични данни
   □ 1    □ 2    □ 3    □ 4

(j) Информиране за нарушения на сигурността на личните данни
   □ 1    □ 2    □ 3    □ 4

(k) Обработване на чувствителни данни
   □ 1    □ 2    □ 3    □ 4

(l) Други (моля, посочете) ..........................
   □ 1    □ 2    □ 3    □ 4
Въпрос № 3
Моля, посочете кои според Вас са най-подходящите механизми за повишаване на осведомеността за МСП по отношение на въпросите, свързани с GDPR по скалата от 1 (най-малко подходящи) до 4 (най-подходящи):

(a) Повишаване на осведомеността чрез организиране на събития (конференции, семинари и др.)
☐ 1    ☐ 2    ☐ 3    ☐ 4

(b) Провеждане на специализирани обучения за МСП
☐ 1    ☐ 2    ☐ 3    ☐ 4

(c) Публикуване на ръководства и указания относно GDPR за нуждите на МСП
☐ 1    ☐ 2    ☐ 3    ☐ 4

(d) Публикуване на бюлетини, информационни табла, листовки и други материали
☐ 1    ☐ 2    ☐ 3    ☐ 4

(e) Провеждане на радио и телевизионни програми свързани с темата
☐ 1    ☐ 2    ☐ 3    ☐ 4

(f) Разработване на софтуерни приложения и образци
☐ 1    ☐ 2    ☐ 3    ☐ 4

(g) Други (моля, посочете) ………………………
☐ 1    ☐ 2    ☐ 3    ☐ 4

Въпрос № 4
Според Вас какъв вид и формат на ръководство за самооценка би бил най-полезен за МСП за осигуряване на необходимите информационни ресурси за постигане на съответствие в областта на защитата на личните данни?

(a) Ръководство за самооценка в следния формат (може да посочите повече от един отговор):
☐ На хартиен носител
☐ Онлайн формат
☐ Мобилно приложение

(b) Ръководство за самооценка със следните характеристики (може да посочите повече от един отговор):
Лесен за употреба наръчник относно основите на GDPR
Ръководство, съдържащо препратки към разпоредби GDPR и други приложими нормативни актове
Подробен анализ на теми, свързани с GDPR
Ръководство под формата на въпроси и отговори
Наръчник, насочен към решаване на практически въпроси и съвети
Ръководства, свързани с особеностите на конкретни сектори
Друго (моля, посочете) ………………………

(c) Ръководство за самооценка, специално пригоден за следните категории ползватели (може да посочите повече от един отговор):

 Юристи в МСП
 Ръководни органи на МСП
 Дължностни лица по защита на данните
 Друго (моля, посочете) ………………………

Въпрос № 5
Какви други теми или информация според Вас трябва да бъдат включени в Ръководството за самооценка по приложението на GDPR?
........................................................................................................................................
........................................................................................................................................
........................................................................................................................................
........................................................................................................................................
........................................................................................................................................
........................................................................................................................................
........................................................................................................................................
........................................................................................................................................
........................................................................................................................................
........................................................................................................................................
INDAGINE SULLA PROTEZIONE DEI DATI PERSONALI

Acronimo del progetto: SMEDATA

Numero della convenzione di sovvenzione: 814763

Titolo del progetto: Garantire il Massimo Grado di Protezione della Privacy e dei Dati Personali attraverso Strumenti Innovativi per le PMI e i Cittadini.

<table>
<thead>
<tr>
<th>Livello di divulgazione</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>PU</td>
<td>Pubblico (dopo l’adozione finale)</td>
</tr>
<tr>
<td>CO</td>
<td>Confidenziale, solo per i membri del consorzio (compresi i servizi della Commissione)</td>
</tr>
</tbody>
</table>
**Scopo dell’Indagine**

La seguente indagine sulla protezione dei dati personali (“Indagine”) sarà condotta nell’ambito del progetto SMEDATA, coordinato dalla Commissione bulgara per la protezione dei dati personali (“CPDP”) in collaborazione con il Garante per la protezione dei dati personali, l’Università degli studi Roma Tre e altri partners pubblici e privati [www.smedata.eu](http://www.smedata.eu).

Lo scopo dell’Indagine è quello di raccogliere informazioni sulle sfide, sulle problematiche o sulle preoccupazioni che le imprese, in particolare le micro, piccole e medie imprese (PMI) ed associazioni di PMI, devono affrontare in relazione all’attuazione dei requisiti del Regolamento UE 2016/679 sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali ed alla libera circolazione dei dati (“GDPR”). I risultati dell’Indagine saranno utilizzati per l’elaborazione di uno strumento di autovalutazione e sensibilizzazione che fornirà alle PMI le risorse necessarie per ottenere il rispetto della vigente normativa in materia di protezione dei dati nell’ambito delle loro attività, processi, controlli, pratiche organizzative e commerciali.

L’Indagine sarà condotta in forma anonima. I risultati saranno aggregati e saranno utilizzati solo per lo scopo sopra definito. L’Indagine non è collegata, guidata o fondata sulle funzioni di vigilanza del CPDP o del Garante per la protezione dei dati personali (“GPDP”). Pertanto, i risultati dell’Indagine non saranno collegati ad uno specifico partecipante e non saranno utilizzati in alcun modo per stabilire la conformità alla normativa applicabile.

Se un partecipante desidera accedere ad una sintesi dei risultati dell’Indagine o ricevere maggiori informazioni sul progetto SMEDATA, può trovare tali informazioni su [www.smedata.eu](http://www.smedata.eu).

**Struttura dell’Indagine**

L’Indagine è strutturata in diverse sezioni:

- Informazioni generali: informazioni sul partecipante (senza nome)
- Questionario
- Glossario per l’Indagine: per aiutare i partecipanti al sondaggio, una spiegazione della terminologia sarà resa disponibile durante l’Indagine passando con il mouse sui dati evidenziati in nero.

**Istruzioni:**

Informazioni Generali

4. Sei:

☐ PMI
☐ Associazioni di piccole e medie imprese
☐ Altri soggetti rappresentanti le categorie di titolari del trattamento o responsabili del trattamento

5. Le tue attività / le attività delle piccole e medie imprese di cui si compone la tua associazione rientrano in tali ambiti (è possibile selezionare più di una scelta):

☐ Agricoltura, silvicoltura e pesca
☐ Estrazione di minerali;
☐ Attività manifatturiera;
☐ Fornitura di energia elettrica, gas, vapore e aria condizionata;
☐ Fornitura di acqua, reti fognarie, attività di trattamento di rifiuti e decontaminazione;
☐ Costruzioni;
☐ Commercio all’ingrosso ed al dettaglio; riparazione di autoveicoli e motocicli;
☐ Trasporto e magazzinaggio;
☐ Attività alberghiera e di ristorazione;
☐ Informazione e comunicazione;
☐ Attività finanziaria ed assicurativa;
☐ Attività immobiliare;
☐ Attività professionale, scientifica e tecnica;
☐ Attività amministrative e servizi di supporto;
☐ Pubblica amministrazione e difesa; assicurazione sociale obbligatoria;
☐ Istruzione;
☐ Sanità ed assistenza sociale;
☐ Arte, spettacolo e tempo libero;
☐ Altre attività di servizi;
☐ Attività esercitata a favore di famiglie come datori di lavoro; produzione di beni e servizi indifferenziati per uso proprio delle famiglie;
☐ Attività di organizzazioni e organismi extraterritoriali;

<table>
<thead>
<tr>
<th>Categoria di impresa</th>
<th>Numero di dipendenti</th>
<th>Fatturato</th>
<th>o</th>
<th>Totale di bilancio</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media</td>
<td>&lt; 250</td>
<td>≤ € 50 m</td>
<td>≤</td>
<td>€ 43 m</td>
</tr>
<tr>
<td>Piccola</td>
<td>&lt; 50</td>
<td>≤ € 10 m</td>
<td>≤</td>
<td>€ 10 m</td>
</tr>
<tr>
<td>Micro</td>
<td>&lt; 10</td>
<td>≤ € 2 m</td>
<td>≤</td>
<td>€ 2 m</td>
</tr>
</tbody>
</table>
6. Specifica la dimensione geografica della tua attività imprenditoriale/associazione:
   - Internazionale
   - Europea
   - Nazionale
   - Subnazionale/locale
QUESTIONARIO

Domanda n.1 Valuta quali sono, secondo te, le problematiche più comuni e le sfide incontrate dalle PMI nell’assicurare la compliance al GDPR in una scala da 1 (poco rilevante) a 4 (molto rilevante)

(a) Conoscenza e comprensione delle nuove prescrizioni del GDPR □ 1 □ 2 □ 3 □ 4
(b) Svolgimento di data mapping e gap analysis/internal assessment della tua organizzazione □ 1 □ 2 □ 3 □ 4
(c) Valutazione dei rischi per la protezione dei dati e scelta delle misure di sicurezza appropriate per la protezione dei dati personali □ 1 □ 2 □ 3 □ 4
(d) Garantire la consapevolezza e la formazione dello staff □ 1 □ 2 □ 3 □ 4
(e) Prevedere sufficienti risorse economiche e umane per implementare il GDPR □ 1 □ 2 □ 3 □ 4
(f) Determinare le appropriate basi legali per il trattamento dei dati personali (consenso, contratto, obbligo di legge, interesse legittimo ecc.) □ 1 □ 2 □ 3 □ 4
(g) Mantenere la documentazione necessaria in linea con i principi dell’accountability □ 1 □ 2 □ 3 □ 4
(h) Altro (specificare) ………………………… □ 1 □ 2 □ 3 □ 4

Domanda n.2: Indica quali dei seguenti temi sono di particolare importanza nello specifico settore industriale nel quale opera la tua organizzazione/associazione con riferimento alle prescrizioni del GDPR. Valuta su una scala da 1 (poco rilevante) a 4 (molto rilevante):

(a) Trattamento dei dati personali dei lavoratori □ 1 □ 2 □ 3 □ 4
(b) Trattamento dei dati personali dei consumatori, incluso il direct marketing □ 1 □ 2 □ 3 □ 4
Necessità di svolgere una Valutazione di impatto sulla protezione dei dati (DPIA)

<table>
<thead>
<tr>
<th>□ 1</th>
<th>□ 2</th>
<th>□ 3</th>
<th>□ 4</th>
</tr>
</thead>
</table>

Nomina di un Responsabile della protezione dei dati (DPO)

<table>
<thead>
<tr>
<th>□ 1</th>
<th>□ 2</th>
<th>□ 3</th>
<th>□ 4</th>
</tr>
</thead>
</table>

Come rispondere alle richieste di esercizio dei propri diritti da parte degli interessati del trattamento (es. diritto di accesso, diritto all’oblio, diritto di opposizione, diritto alla portabilità dei dati, ecc.)

<table>
<thead>
<tr>
<th>□ 1</th>
<th>□ 2</th>
<th>□ 3</th>
<th>□ 4</th>
</tr>
</thead>
</table>

Implementazione di appropriate misure tecniche e organizzative per assicurare la sicurezza dei trattamenti di dati personali (es. pseudonimizzazione, cifratura ecc.)

<table>
<thead>
<tr>
<th>□ 1</th>
<th>□ 2</th>
<th>□ 3</th>
<th>□ 4</th>
</tr>
</thead>
</table>

Ottenere il consenso dei titolari della responsabilità genitoriale per il trattamento dei dati dei minori

<table>
<thead>
<tr>
<th>□ 1</th>
<th>□ 2</th>
<th>□ 3</th>
<th>□ 4</th>
</tr>
</thead>
</table>

Cookies e siti web

<table>
<thead>
<tr>
<th>□ 1</th>
<th>□ 2</th>
<th>□ 3</th>
<th>□ 4</th>
</tr>
</thead>
</table>

Trasferimenti internazionali di dati personali

<table>
<thead>
<tr>
<th>□ 1</th>
<th>□ 2</th>
<th>□ 3</th>
<th>□ 4</th>
</tr>
</thead>
</table>

Notifica di violazioni dei dati personali

<table>
<thead>
<tr>
<th>□ 1</th>
<th>□ 2</th>
<th>□ 3</th>
<th>□ 4</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>□ 1</th>
<th>□ 2</th>
<th>□ 3</th>
<th>□ 4</th>
</tr>
</thead>
</table>

Domanda n.3: Indica quali sono, secondo te, i meccanismi più appropriati di sensibilizzazione delle PMI al rispetto delle norme del GDPR in una scala da 1 (poco appropriato) a 4 (molto appropriato)

(a) Eventi di sensibilizzazione (conferenze, seminari ecc.)

<table>
<thead>
<tr>
<th>□ 1</th>
<th>□ 2</th>
<th>□ 3</th>
<th>□ 4</th>
</tr>
</thead>
</table>

(b) Organizzare corsi di formazione specializzati per le PMI

<table>
<thead>
<tr>
<th>□ 1</th>
<th>□ 2</th>
<th>□ 3</th>
<th>□ 4</th>
</tr>
</thead>
</table>

(c) Pubblicazione di guide e istruzioni sul GDPR per le PMI

<table>
<thead>
<tr>
<th>□ 1</th>
<th>□ 2</th>
<th>□ 3</th>
<th>□ 4</th>
</tr>
</thead>
</table>
(d) Pubblicazione di newsletters, locandine, flyers e altri materiali

☐ 1     ☐ 2     ☐ 3     ☐ 4

(e) Realizzazione di programmi radio e TV sull’argomento

☐ 1     ☐ 2     ☐ 3     ☐ 4

(f) Sviluppo di strumenti software e modelli precompilati

☐ 1     ☐ 2     ☐ 3     ☐ 4

(g) Altro (specificare) …………………….

☐ 1     ☐ 2     ☐ 3     ☐ 4

Domanda n.4 Quale tipo e quale forma di strumento di autovalutazione contenente le risorse informative necessarie per ottenere conformità nel campo della protezione dei dati sarebbe più utile per le PMI?

(a) Strumento di autovalutazione nel seguente formato (è possibile selezionare più di una casella):

☐ Test cartaceo
☐ Test online
☐ Applicazione su smartphone

(b) Strumento di autovalutazione con le seguenti caratteristiche (è possibile selezionare più di una casella):

☐ Guida facile da usare contenente le basi del GDPR
☐ Strumenti contenenti riferimenti a articoli del GDPR e altri materiali legali
☐ Analisi approfondita di argomenti complessi del GDPR
☐ Guida in formato “domanda e risposta”
☐ Strumento incentrato sulla conoscenza pratica e sulla consulenza
☐ Strumenti di informazione specifici per settore
☐ Altro (specificare) …………………….

(c) Strumento di autovalutazione personalizzato per (è possibile selezionare più di una casella):
Professionisti legali all'interno delle PMI
- Direzione generale delle PMI
- Responsabile della Protezione dei Dati
- Altro (specificare) ………………………

Domanda n.5 Quali altri argomenti o informazioni dovrebbero essere inclusi in uno strumento di autovalutazione del GDPR?

……………………………………………………………………………………………………………………………………………………………………………

……………………………………………………………………………………………………………………………………………………………………………

……………………………………………………………………………………………………………………………………………………………………………
Appendix D Interview Form

INTERVIEW FORM

under

SMEDATA: Ensuring the Highest Degree of Privacy and Personal Data Protection through Innovative Tools for SMEs and Citizens

Work Package 3: Self-assessment tool for sustainable awareness based on SMEs’ specific needs and processes from the prospective of personal data protection

Interviewer:

.................................................................

SMEDATA Partner:

Date: ........................................

Interview:

Name of the organisation:

.................................................................

Contact information of the organisation:

  a.  Address:

      .................................................................

  b.  Phone:

      .................................................................

      Web site:

      .................................................................

Type of the organisation (please choose):

  a.  SME

  b.  Association of SMEs

  c.  Other body representing categories of controllers or processors
Summary (at least half a page):

Each interview should cover at least these questions:

1. What in your experience are the main challenges met by SMEs in the process of achieving GDPR compliance?

2. Are there any sector-specific problems relating to data protection requirements and security that can be indicated?

3. What are the strategies that SMEs should implement to come into compliance with the GDPR?

4. What type of awareness-raising mechanisms is important for SMEs in the process of GDPR implementation?

5. What type of tools (self-assessment tools, guides etc.) could best suit the needs of SMEs for achieving data protection compliance?

6. Could you share some additional observations relating to the needs of SMEs in connection with the entry into force of the GDPR?