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**

Work Package: **3**

D3.2 – Expert Workshops (a.k.a. Draft common criteria to cover different economic sectors for a multi-sector self-assessment and awareness tool)

Project co-funded by the European Commission within **REC-AG-2017**		
Dissemination Level		
PU	Public (after final adoption)	
CO	Confidential, only for members of the consortium (including the Commission Services)	X

Disclaimer: The content of the current document represents the views of the authors 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.

Table of Contents

The SMEDATA Project is funded by the European Union's Rights,
Equality and Citizenship Programme (2014-2020)

I. Introduction

The sets of criteria for common Self-assessment and awareness tool were planned to be precisely examined by organising and conduct of 4 plenaries of expert workshop in Sofia (2) and Rome (2) with 20 participants each. Some participants attended to the meetings; other digitally expressed their opinions via Skype. The experts were representatives of SMEs, academia for business and SMEs associations all over Europe. The objective was to elaborate common set of criteria applicable for all business sectors.

Current document summarizes the main outcomes of the expert workshops conducted so far. As a rule, organisation, conduct and reporting of the workshops can be considered as a tool for facilitating expert judgment. Term definition is ‘a meeting at which a group of people engage in intensive discussion and activity on a particular subject or project’. Thus, the scope of the reporting document is the results – **common criteria to cover different economic sectors for a multi-sector self-assessment and awareness tool**.

The report consists of 3 main chapters – Summary, Criteria model as well as Tables of processing procedures according to SME Business Category. The activities under Work Package 3 can be determined by their ultimate results. Following the different nature of the different actions, there are two main areas of interaction – the content-oriented activities as well as process-oriented activities. The implementation of both types of activities under WP 3 will result in complete Self-assessment and awareness tool (SMEDATA Deliverable 3.4). The current document covers the content-oriented activities of definition of common criteria for Self-assessment and awareness tool.

The SMEDATA Project is funded by the European Union’s Rights,
Equality and Citizenship Programme (2014-2020)

II. Summary

1. Purpose of the document and description of Activity 2 – Work Package 3

The SMEDATA project (https://smedata.eu) co-funded by the European Union's Rights, Equality and Citizenship Programme (2014–2020) is implemented by Bulgarian-Italian consortium and for which the Italian Privacy Authority is a partner in Italy with the University of Roma Tre, it was set up to prepare SMEs, their associations and their legal advisors for the effective application of the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC) through awareness raising, multiplication of training and sustainable development of skills. In particular, one of the objectives of this project is to ensure the necessary sustainable sectoral knowledge through the development of self-assessment and awareness-raising tools.

This document presents draft common criteria for the development of a self-assessment tool that aims to provide SMEs of different sizes and belonging to different economic sectors support for GDPR compliance; In particular, it finalizes Activity 3 of the Work Package 3 (*Work Package 3: Self-assessment tool for sustainable awareness based on SME's. Activity 3: Draft common criteria applicable to different economic sectors*).

In order to propose an applicable multi-sectoral self-assessment tool, the project takes the inputs of a specific survey (Activity 1) previously carried out on SMEs and their trade associations https://smedata.eu/wp-content/uploads/2019/05/D3.1_SMEDATA_Survey_Report.pdf.

The SMEDATA WP3 Activity 2 and Activity 3 are characterized as follows.

Activity 2: Identification of sets of multiple criteria to cover different economic sectors

In order to propose multi-sector applicable tool, SMEDATA Project Partners team will examine and assess the results from the previous Activity 1.

Based on expert judgment they will provide first draft of **set of multiple criteria for self-assessment and awareness tool in different economic sectors**. It is planned to have more than one set of criteria at this stage of the project execution considering that the raw data will be collected from different business sectors and the tool should be designed to cover common processing issues. Each set will contain two types of criteria:

(i) Type 1: Criteria related to the **regulated subjects** (controller, processor, data subjects, etc.), and,

(ii) Type 2: Criteria related to the **processing procedures.**

The results of Activity 2 formed the base of Activity 3.

Activity 3: Preparation of draft common criteria applicable to different economic sectors (GPDPIT) (M10-M13)

The results of Activity 2 have been discussed during organized expert workshops and considering comments and suggestions from Consortium Members

Two workshops were held in Rome (4 and 9 November 2019) with round 70 participants representing:

- SMEs,
- academia,

- SMEs associations,

in order to reach to and elaborate **draft common set of criteria** applicable to different economic sectors.

This document contains the draft common criteria applicable to different SMEs economic sectors

2. Results of the survey conducted on SMEs as data controllers in light of GDPR

The Report on the survey analysis of SMEs as data controllers in light of GDPR indicates 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.

Interviews also reported that understanding

- the types of personal data that are collected by the organization,
- the records and systems in which it is stored,
- and why and how it is used,

are very important and challenging to ensuring compliance.

Moreover, 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.

In relation to the self-assessment tool, the interviewees were asked to comment on the format, content, and structure deemed most appropriate and useful for a process of self-assessment and awareness raising. The results are as follows:

Format

Most respondents (58%) find that the most appropriate structure of the self-assessment tool is that of a tool available online, preferable to other formats such as paper format or a mobile application.

Content

Among the following options:

- "easy driving" with the bases of the GDPR,
- tools containing references to the articles of the GDPR and other legal information materials,
- in-depth analysis of complex issues concerning the application of the GDPR,
- guide to the GDPR based on questions and answers,
- tools containing elements of practical knowledge and suggestions,
- sector-specific information tools,
- other,

the answers in order of preference were:

1. tools containing elements of practical knowledge and suggestions;
2. guide to the GDPR based on questions and answers;
3. "easy driving" with the bases of the GDPR.

The SMEDATA Project is funded by the European Union's Rights,
Equality and Citizenship Programme (2014-2020)

Target Audience

Regarding the target audience to whom the tool should be destined, the following options have been submitted to the interviewees:

- Legal professionals within SMEs,
- Management of SMEs,
- Data protection officers,
- Others.

the answers, in order of preference, were the following:

1. Management of SMEs,
2. Legal professionals within SMEs,
3. Data protection officers.

3. Results of the feedbacks from Experts and Academia

The following criteria includes the feedbacks gathered from Academia and experts from SMEs' associations in two different meetings held in Rome the 4 and the 9 October 2019 with round **70 participants**. Further comments and suggestions from SMEDATA consortium Partners have been also considered to draft the present document. The overall considerations from SMEs on the criteria structure are mainly related to the necessity to represent their specific context business and to develop a tool easy to use and able to support their privacy management operational context. Particular attention is on the necessity to have an effective guidance to compliance requirements for small business including the necessity to identify a sound and smart approach to evaluate the personal data protection risk of their processing activities.

4. Criteria Model

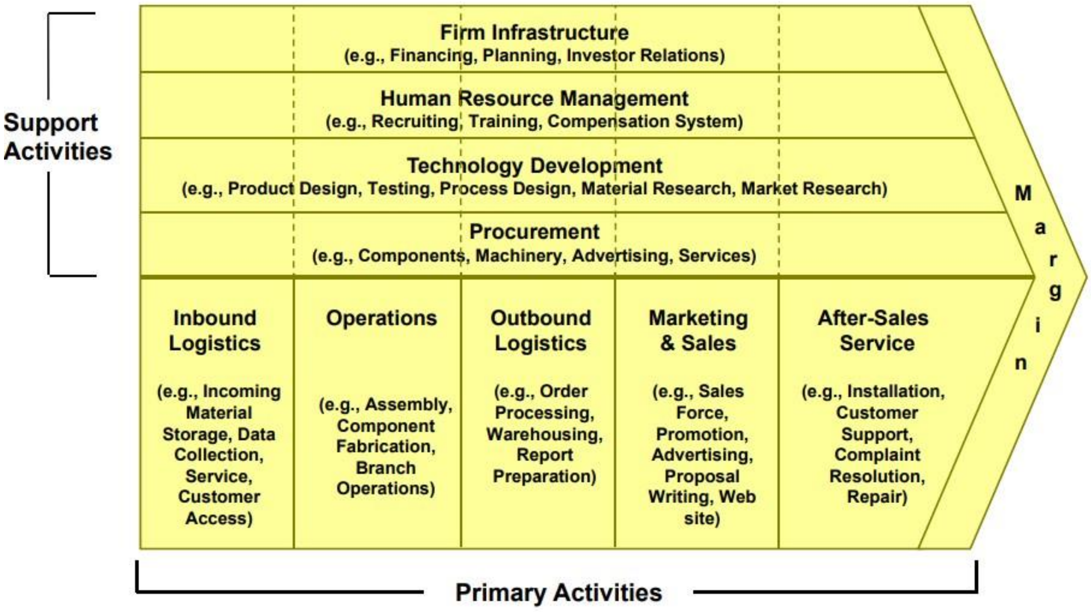
In order to identify criteria on how to cover different economic sectors here we introduce a general model to design a multi-sector self-assessment tool.

This model is based on:

- the main activities that characterize an overall company business process,
- the regulated subjects,
- the processing procedures and the categorization of personal data processed,
- the main activities to perform in order to be compliant to the GDPR.

4.1 Main Activities characterizing the business process

The main activities that characterize a company’s business process are here explained in order to identify the potential procedures for processing personal data related to the performance of each specific activity. These activities are derived from the Michael Porter value chain framework, as shown in the following picture.



Support Activities
Firm Infrastructure
(e.g., Financing, Planning, Investor Relations)
Human Resource Management
(e.g., Recruiting, Training, Compensation System)
Technology Development
(e.g., Product Design, Testing, Process Design, Material Research, Market Research)
Procurement
(e.g., Components, Machinery, Advertising, Services)
Inbound Logistics
(e.g., Incoming Material Storage, Data Collection, Service, Customer Access)
Operations
(e.g., Assembly, Component Fabrication, Branch Operations)
Outbound Logistics
(e.g., Order Processing, Warehousing, Report Preparation)
Marketing & Sales
(e.g., Sales Force, Promotion, Advertising, Proposal Writing, Web site)
After-Sales Service
(e.g., Installation, Customer Support, Complaint Resolution, Repair)
Margin
Primary Activities

Source: Professor Michael E. Porter - Harvard Business School

The SMEDATA Project is funded by the European Union’s Rights,
Equality and Citizenship Programme (2014-2020)

The model here provided explicates the processing procedure of personal data correlated with each main business activity. The processing procedures are correlated with the categories of personal data processed and the data subjects involved. According to these processing procedures specific checklist may be provided by the Self- Assessment Tool.

We consider the following processing procedures tables pertinent to Controllers of SMEs classified in four different Business Categories:

- MANIFACTURERS;
- SMALL TRADE – CRAFTSMENSHIP;
- HEALTH SERVICES;
- GENERAL SERVICES (Non-Health Services).

Each Category may imply different processing procedures according to Category's specific business characteristic.

It's worth of mention that some specific business activities such as Accounting, Tax and social security obligations, Information technology, Commercial information collection, debt collection, security may be privacy "sensitive" activities managed internally or also outsourced.

The SMEDATA Project is funded by the European Union's Rights,
Equality and Citizenship Programme (2014-2020)

4.2 Categories of regulated subjects

The following tables are designed to support the tool with reference to the Data Controllers. For the other regulated subjects “Processors” and “Data Subjects” may be developed specific checklists based on Article 28 provisions for Processors and based on GDPR sections 2 and 3 (Art. 13-22) for Data Subjects

The SMEDATA Project is funded by the European Union’s Rights,
Equality and Citizenship Programme (2014-2020)

4.3 Tables of processing procedures according to SME Business Category

MANIFACTURERS

BUSINESS PRIMARY AND SUPPORT ACTIVITIES	SUB FUNCTIONS	PROCESSING PROCEDURES	DATA SUBJECTS	PERSONAL DATA CATHEGORIES	PAPER/ELECTRONIC DATA PROCESSING
Finance	• Finance	**• Financing** **• Budget control**	• Customers • Employees • Suppliers	• Personal data	Paper/Electronic
Human resource management	• Personnel Management • Payrolls • Recruiting • Training	**• Attendance recording** **• Performance measurement** **• Payrolls management** **• Tax and social security obligations management** **• Sick and leave management** **• Workplace and personnel health management** **• Recruitment, Selections (includes candidates) and personnel leaving the organization** **• Staff evaluation management**	• Employees • Job Vacancy candidates	• Personal data • Art. 9 Personal data • Art. 10 Personal data	Paper/Electronic
Research And Development	• Production programming and control • Technical - Scientific information collection	**• Production programming and control** **• Acquisition of data from specialized sources (technical and scientific data bases)**	• data subjects involved in data collection and analysis • Employees	• Personal data • Art. 9 Personal data (Pharmaceutical and Other Health business)	Paper/Electronic

The SMEDATA Project is funded by the European Union's Rights,
Equality and Citizenship Programme (2014-2020)

Procurement and Logistics (inbound/outbound)	• Supplier qualification/rating • Procurement • Inventory management • Logistics (Transport and delivery)	**• Suppliers management** **• Purchase order management** **• Inventory control** **• Conveyor management** **• Delivery control**	• Suppliers • Employees	• Personal data • Art. 10 Personal data	Paper/Electronic
Production (Business Operations)	• Production design • Production programming and control • Security management	**• Production programming and Control data management** **• Information systems management** **• Outsourced ICT services** **• Maintenance management** **• Video surveillance** **• Geolocation** **• Access control (Systems and Service area)**	• Employees • Suppliers	• Personal data	Paper/Electronic
Marketing and Sales	• Sales and aftersales management • Marketing	**• Market intelligence** **• Billing** **• Sales reporting** **• Web site management** **• Customer support**	• Customers • Employees • Web site visitors	• Personal data	Paper/Electronic
Business Administration and Internal Control	• Accounting system • Management Control	**• Accounting Management** **• Internal Audit and Control**	• Customers • Employees • Suppliers	• Personal data	Paper/Electronic

The SMEDATA Project is funded by the European Union's Rights,
Equality and Citizenship Programme (2014-2020)

SMALL TRADE and CRAFTSMENSHIP

BUSINESS PRIMARY AND SUPPORT ACTIVITIES	SUB FUNCTIONS	PROCESSING PROCEDURES	DATA SUBJECTS	PERSONAL DATA CATHEGORIES	PAPER/EELCTRONI C DATA PROCESSING
Finance	• Finance	• **Financing** • **Budget control**	• Customers • Employees • Suppliers	• Personal data	Paper/Electronic
Human resource management	• Personnell Management • Payrolls • Recruiting • Training	• **Payrolls** • **Attendance recording** • **Sick and leave management** • **Tax and social security obligations** • **Workplace and personnel health management** • **Staff evaluation management**	• Employees	• Personal data • Art. 9 Personal data • Art. 10 Personal data	Paper/Electronic
Procurement and Logistics (inbound/outbound)	• Supplier qualification/rating • Procurement • Inventory management • Logistics (Transport and delivery)	• **Suppliers management** • **Purchase order management** • **Inventory control** • **Delivery control**	• Suppliers • Employees	• Personal data • Art. 10 Personal data	Paper/Electronic
Production (Business Operations)	• Production programming and control • **Sales Management** • Security Management	• **Customer management** • **Production Control** • **Billing** • **Information systems management** • **Outsourced ICT services** • **video surveillance** • **Geolocation**	• Customers	• Personal data • **Art. 9 Personal data**	Paper/Electronic
Marketing and Sales	• Marketing	• **Web site management** • **Customer support**	• Customers • Employees • Web site visitors	• Personal data	Paper/Electronic
Business Administration and Internal Control	• Accounting system • Management Control	• **Accounting Management**	• Customers • Employees • Suppliers	• Personal data	Paper/Electronic

HEALTH SERVICES

BUSINESS UNIT PRIMARY BUSINESS ACTIVITIES	SUB FUNCTIONS	PROCESSING PROCEDURES	DATA SUBJECTS	PERSONAL DATA CATHEGORIES	PAPER/EELCTRO NIC DATA PROCESSING
Finance	• Finance	**• Financing** **• Budget control**	• Patiens • Employees • Suppliers	• Personal data • Art. 9 Personal data	Paper/Electronic
Human resource management	• Personnell Management • Payrolls • Recruiting, • Training	**• Attendance recording** **• Performance measurement** **• Payrolls management** **• Tax and social security obligations management** **• Sick and leave management** **• Staff evaluation management** **• Recruitment, Selections (includes candidates) and personnel leaving the organization**	• Employees • Job Vacancy candidates	• Personal data • Art. 9 Personal data • Art. 10 Personal data	Paper/Electronic
Research And Development	• Production programming and control • Technical - Scientific information collection	**• Project management systems** **• Acquisition of data from specialized sources (technical and scientific data bases)**	• data subjects involved in data collection and analysis	• Personal data • Art. 9 Personal data	Paper/Electronic
Procurement and Logistics (inbound/outbound)	• Supplier qualification/rating • Procurement • Inventory management • Logistics (Transport and delivery)	**• Suppliers management** **• Purchase order management** **• Inventory control** **• Conveyor management** **• Delivery control**	• Suppliers • Employees	• Personal data • Art. 10 Personal data	Paper/Electronic

Services provisions	• Health services provisioning • Security Management	• **Patient lists management** • **Health Service provisions** • **Billing** • **National health system reporting** • **Video surveillance** • **Geolocation** • **Access control (Systems and Service area)** • **Information systems management** • **Outsourced ICT services**	• Employees • Patients	• Personal data • Art. 9 Personal data	Paper/Electronic
Marketing and Sales	• Sales management • Marketing	• **Market intelligence** • **Sales reporting** • **Web site management**	• Patients • Employees • Web site visitors	• Personal data	Paper/Electronic
Business Administration and Internal Control	• Accounting system • Management Control	• **Accounting Management** • **Internal Audit and Control**	• Patiens • Employees • Suppliers	• Personal data • Art. 9 Personal data)	Paper/Electronic

GENERAL SERVICES (Non-Health Services)

BUSINESS UNIT PRIMARY BUSINESS ACTIVITIES	SUB FUNCTIONS	PROCESSING PROCEDURES	DATA SUBJECTS	PERSONAL DATA CATEGORIES	PAPER/EELCTRONI C DATA PROCESSING
Finance	• Finance	**• Financing** **• Budget control**	• Customers • Employees • Suppliers	• Personal data	Paper/Electronic
Human resource management	• Personnell Management • Payrolls • Recruiting, • Training	**• Attendance recording** **• Performance measurement** **• Payrolls management** **• Tax and social security obligations management** **• Sick and leave management** **• Staff evaluation management** **• Insurance management** **• Recruitment, Selections (includes candidates) and personnel leaving the organization**	• Employees • Job Vacancy candidates	• Personal data • Art. 9 Personal data • Art. 10 Personal data	Paper/Electronic
Research And Development	• Production programming and control • Technical - Scientific information collection	**• Project management systems** **• Acquisition of data from specialized sources (technical and scientific data bases)**	• Data subjects involved in data collection and analysis	• Personal data	Paper/Electronic
Procurement and Logistics (inbound/outbound)	• Supplier qualification/rating • Procurement • Inventory management • Logistics (Transport and delivery)	**• Suppliers management** **• Purchase order management** **• Inventory control** **• Conveyor management** **• Delivery control**	• Suppliers • Employees	• Personal data • Art. 10 Personal data	Paper/Electronic
Production (Business Operations – Services provisions)	• Services provisions • Security management	**• Customer management** **• Services provisions procedures** **• Information systems management**	• Employees • Customers	• Personal data	Paper/Electronic

The SMEDATA Project is funded by the European Union's Rights,
Equality and Citizenship Programme (2014-2020)

		• **Outsourced ICT services** • **Video surveillance** • **Geolocation** • **Access control (Systems and Service area)**			
Marketing and Sales	• Sales management • Marketing	• **Market intelligence** • **Sales reporting** • **Web site management** • **Customer support**	• Customers • Employees • Web site visitors	• Personal data	Paper/Electronic
Business Administration and Internal Control	• Accounting system • Management Control	• **Accounting Management** • **Internal Audit and Control**	• Customers • Employees • Suppliers	• Personal data	Paper/Electronic

The SMEDATA Project is funded by the European Union's Rights,
Equality and Citizenship Programme (2014-2020)

4.4 Main activities to be carried out for the purposes of compliance with the GDPR

Below follows a list of main activities that organizations, identifying the most appropriate implementation methods, considering the size, the different operational context and the human and technical resources available, should perform the reach GDPR compliance.

- Mapping of data and processing activities;
- Respect of Data protection Principles;
- Data communication management;
- Management of outsourced data processing;
- Risk analysis and management: risk assessment, DPIA and security measures;
- Management of the data subject's rights;
- Management of personal data breaches;
- Organization, roles and responsibilities assignment;
- Adoption of "Privacy by design and by default" approach;
- Enforcing procedures necessary to comply with adopted Codes of Conduct and Certifications.

5. Criteria proposal: concluding remarks

1. For data controllers, the processing procedures characteristic of the business types, the categorization of personal data processed and the activities related to the GDPR provisions may be identified as the set of primary criteria on which develop the self-assessment tool. For the other types of regulated subjects, the considerations in paragraph 3.2 apply.
2. The tables here considered are designed to provide possible classes of personal

The SMEDATA Project is funded by the European Union's Rights,
Equality and Citizenship Programme (2014-2020)

data processing activities according to major business categories, in order to make these available to end users, that necessary will select the most appropriate to his particular business and dimension and, where necessary, may add further specific processing categories.

3. The implementation of these criteria is strictly related to the logic of the assessment tool the will be identified. A possible implementation mechanism may be for example a step by step guide, where the user is invited to identify his business category, the processing procedures of personal data related to his specific business context including the applicable further ones, the personal data categories, the data subjects involved, the characteristics of the processing and the main pertinent activities to be carried out to reach GDPR Compliance including a quick guide with description and implementation guidance of each of these activities. Moreover specific distinctions would be considered if the processing activities are carried out internally by or it’s outsourced to a third party as an external service.
4. Particular attention should be provided in guiding the end user in evaluate the risk of the personal data processing in order to providing of the right knowledge of the actions required to prevent consequences on freedom and rights of data subjects.
5. Some suggestions have come about providing this document with examples on how these criteria should be put in place. Since the way to operationalize such criteria is tightly related to the functional model of the tool we believe that, in order to have a better picture on how the tool may work, to postpone those examples to the first functional prototypes of the tool.