CEN

WORKSHOP

AGREEMENT

CWA 17858

March 2022

ICS 03.160; 35.030; 35.240.63

English version

Guidelines for Traditional Micro-SMEs' GDPR Compliance

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties, the constitution of which is indicated in the foreword of this Workshop Agreement.

The formal process followed by the Workshop in the development of this Workshop Agreement has been endorsed by the National Members of CEN but neither the National Members of CEN nor the CEN-CENELEC Management Centre can be held accountable for the technical content of this CEN Workshop Agreement or possible conflicts with standards or legislation.

This CEN Workshop Agreement can in no way be held as being an official standard developed by CEN and its Members.

This CEN Workshop Agreement is publicly available as a reference document from the CEN Members National Standard Bodies.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Ref. No.:CWA 17858:2022 E

Contents

Page

European foreword

This CEN Workshop Agreement (CWA 17858:2022) has been developed in accordance with the CEN-CENELEC Guide 29 "CEN/CENELEC Workshop Agreements – A rapid prototyping to standardization" and with the relevant provisions of CEN/CENELEC Internal Regulations - Part 2. It was approved by a Workshop of representatives of interested parties on 2022-01-25, the constitution of which was supported by CEN following the public call for participation made on 2021-01-28. However, this CEN Workshop Agreement does not necessarily include all relevant stakeholders.

The final text of this CEN Workshop Agreement was provided to CEN for publication on 2022-02-16.

Results incorporated in this CWA received funding from the European Commission's Horizon 2020 – The Framework Programme for Research and Innovation (2014-2020) under grant agreement No 786741.

The following organizations and individuals developed and approved this CEN Workshop Agreement:

— Mr. Brahim Bénichou - Chairman

— UNE, Spain, Ms. Marta Fernández- Secretary

— Apave Certification, France, Mr. Benoit Phuez

— Cleopa GmbH, Germany, Mr. Detlef Olschewski

— EURECAT, Spain, Ms. Rosa María Araujo

— KU Leuven, Belgium, Ms. Lidia Dutkiewicz

— Maticmind S.p.A. Italy, Mr. Andrea Praitano

— MB Asmens duomenų apsauga, Lithuania, Ms. Rusnė Juozapaitienė

— Studio Tumietto, Italy, Mr. Daniele Tumietto

— R.I.C.S EDV GmbH, Austria, Mr. Manfred Woehrl

— Universidad Politécnica de Madrid, Spain, Mr. Yosd Samuel Martín

Attention is drawn to the possibility that some elements of this document may be subject to patent rights. CEN-CENELEC policy on patent rights is described in CEN-CENELEC Guide 8 "Guidelines for Implementation of the Common IPR Policy on Patent". CEN shall not be held responsible for identifying any or all such patent rights.

Although the Workshop parties have made every effort to ensure the reliability and accuracy of technical and non-technical descriptions, the Workshop is not able to guarantee, explicitly or implicitly, the correctness of this document. Anyone who applies this CEN Workshop Agreement shall be aware that neither the Workshop, nor CEN, can be held liable for damages or losses of any kind whatsoever. The use of this CEN Workshop Agreement does not relieve users of their responsibility for their own actions, and they apply this document at their own risk. The CEN Workshop Agreement should not be construed as legal advice authoritatively endorsed by CEN/CENELEC.

Introduction

0.1 General

The basis for guidelines covered by this CEN Workshop Agreement (CWA) has been developed in the SMOOTH Project (GA no. 786741) funded by the European Commission's Horizon 2020 – The Framework Programme for Research and Innovation (2014-2020). SMOOTH[1)] aims to assist Traditional Micro-Enterprises (Traditional Micro-SMEs) to comply with key requirements of the General Data Protection Regulation ('GDPR') by designing and implementing an easy-to-use and affordable cloud-based platform service[2)].

0.2 The GDPR

The General Data Protection Regulation (GDPR) was adopted in April 2016 to set a uniform level of data protection across the EU that is fit for the digital age. After a two-year transition period, it entered into force on 25 May 2018. The GDPR is directly applicable in Member States. As a regulation, it does not need to be implemented by the Member States. However, as explained by the Recital 10 of the GDPR, this Regulation provides a 'margin of manoeuvre' for Member States to specify its rules. There are more than 30 GDPR provisions, where Member States have the freedom to adapt their laws as they see appropriate. To that end, the GDPR does not exclude Member State law that sets out the circumstances for specific processing situations, including determining more precisely the conditions under which the processing of personal data is lawful[3)].

It is therefore required to always consult the national law implementing the GDPR.

The GDPR has a strong(er) focus on protecting and empowering individuals and on safeguarding citizens' rights to data protection and privacy.

It imposes extensive obligations on all organizations processing personal data of EU data subjects[4)] (see 3.1). It applies to natural and legal persons, public authorities, agencies and other bodies that process personal data regardless of their size and revenue, regardless if they process personal data as data controllers or as data processors.

0.3 Traditional Micro-SMEs

Micro-SMEs are a very heterogenic group and cover a broad spectrum of activities with very different risk profiles. Therefore, it is not possible to define the data processing risk profile of all Micro-SMEs in a general way, nor is it possible to generally define the operational requirements that Micro-SMEs need to implement to be GDPR (see 3.6) compliant.

Traditional Micro-SMEs as defined under this CWA (see 3.11) run traditional businesses that are used every day by millions of European citizens. Examples of such companies include brick-and-mortar retail shops, real state agencies, repair shops, restaurants, family businesses, etc. Traditional Micro-SMEs' activities, covered by this CWA, are not data-intensive and they generally only engage in low-risk

---

1) For more information on the SMOOTH platform, visit https://smoothplatform.eu.

2) Whereas the substantial content has been based on the outcome of the SMOOTH Project, the practical templates, information and examples in this CWA have been based on the existing templates and guidelines of the data protection service provider 'My Privacy Specialist' (https://myprivacyspecialist.com).

3) Recital (10) GDPR.

4) The territorial scope of the GDPR is not limited to the EU. The Regulation applies to processing of personal data carried out by a controller or processor established in the EU, as well as to processing of personal data of data subjects located in the EU. Non-EU based controllers or processors offering goods or services to EU data subjects or monitoring their behaviour are also subject to the GDPR. For more information, see Art. 3 GDPR.

processing of personal data. Traditional Micro-SMEs are valuable to EU's economy and societal well-being, contributing to the overall employment and added value.

Compared with more data-intensive Micro-SMEs, public organizations and larger private organizations, Traditional Micro-SMEs generally have both limited resources and limited data protection expertise. These make their compliance efforts more difficult. Traditional Micro-SMEs are particularly vulnerable and risk failing to comply with the GDPR.

0.4 (Data) controllers and (data) processors

In their day-to-day operations, Traditional Micro-SMEs process various categories of personal data for different purposes:

— data of employees for payroll management,

— data of customers and prospective customers to deliver products and/or services, to engage them in fidelity programs or marketing strategies,

— data of suppliers to effect orders and payments,

— data of employees of customers,

— etc.

Traditional Micro-SMEs' obligations differ depending on whether they act as data controllers or data processors when processing personal data. Insofar as a Traditional Micro-SME determines the purposes and means of the processing, such Traditional Micro-SME is to be considered as the "(data) controller" under the GDPR. A Traditional Micro-SME is a "processor" if it processes personal data on behalf ('on instruction') of a controller. Traditional SMEs as defined in this CWA will rarely act as a processor. Whether acting as controllers or processors, because of the lack of expertise in data protection and limited resources, Traditional Micro-SMEs are particularly vulnerable in complying with such a complex and extensive regulation and risk failing to do so.

When a Traditional Micro-SME acting as data controller transfers personal data to another data controller, who will independently define means and purpose of further processing, this transfer is considered as a separate processing operation. Consequently, such transfer must comply with the rules under the GDPR applicable to each processing operation meaning that e.g., a lawful processing basis and defined purpose must be applicable. Note that such transfer is a transfer to a third party and should be treated accordingly.

0.5 Low-risk processing

The GDPR embraces a risk-based approach to data protection. This entails that the measures adopted by controllers to ensure compliance shall be appropriate to the risk level of the activity. Most Traditional Micro-SMEs'[5] processing operations (mostly related to managing their relations with employees, customers, potential customers and suppliers) are low risk.

0.6 e-Privacy Directive

The GDPR is complemented by the Directive 2002/58/EC (the e-Privacy Directive). The Directive mainly contains obligations for electronic communications service providers. At the same time, it includes a provision on cookies and similar tracking technologies which can affect all organizations with an online presence, including Traditional Micro-SMEs.

The e-Privacy Directive had to be transposed into the domestic laws of all Member States. Implementation varied across the EU and led to different interpretations of the e-Privacy cookie rules among Member States. Since January 2017, a proposal is in place to replace the e-Privacy Directive with the e-Privacy Regulation that will apply directly to all Member States. The reform is ongoing and even though the e-Privacy Regulation was supposed to come in force at the same moment as the GDPR, at this moment it is unlikely that the e-Privacy Regulation will be approved soon.

0.7 Verbal forms in the document

In this document, the following verbal forms are used:

— "shall" indicates a requirement;

— "should" indicates guidance on how to comply with the GDPR requirements in a practical way;

— "it is recommended" indicates best practices that go beyond the mere compliance.

— "may" indicates permission;

— "can" indicates a possibility or a capability.

Information marked as "NOTE" is for guidance in understanding or clarifying the associated requirements.

0.8 Structure of this CWA – How to use this CWA?

Due to the limited general legal knowledge available in Traditional Micro-SMEs and their general lack of time and resources to organise GDPR implementation projects themselves, this CWA is primarily and foremost addressed to their service providers, such as their accountants, IT service providers and lawyers.

From a pragmatic point of view, the most practical part of this CWA is section 4.1 (Overview of the practical requirements for the GDPR implementation for Traditional Micro-SMEs).

This section 4.1 provides practical guidance, checklists, templates and examples that are ready to use to support a Traditional Micro-SME on its way to complying with its data protection obligations or to assess if a Traditional Micro-SME meets the requirements.

Sections 4.2 (Key GDPR requirements for micro-enterprises), 4.3 (Most relevant e-privacy requirements for Micro-SMEs) and 3 (Terms and definitions) provide the legal background and explanation required to fully understand how to apply the practical guidelines in section 4.1 and to explain as short and practicable as possible the principles behind the practicalities. This information is provided in an

[5] As defined in this CWA, see 0.3 and 3.11.

accessible and condense manner, taking into account the context in which Traditional Micro-SMEs and their advisors operate.

Finally, section 1 (Scope) defines and provides some background information on the context in which this CWA is applicable, such as about what is to be understood under Traditional Micro-SMEs and about who this CWA is addressed to.

1 Scope

The present CEN Workshop Agreement (CWA) provides GDPR-compliance guidelines for Traditional Micro-SMEs (see 3.11) acting as controllers for low-risk processing (see 3.10) operations. It provides practical guidance on the key GDPR (see 3.6) requirements to be considered by such Micro-SMEs and translates these into the practical recommendations they should comply with, to be GDPR compliant.

The document focusses on legal provisions applicable to such low-risk processing. It does not consider in depth the GDPR provisions applicable to high-risk processing (environments), such as on data protection impact assessments, data protection officers and provisions on automated-decision making and profiling.

NOTE 1 It should be taken into account that provisions applicable to high-risk processing are relevant for Traditional Micro-SMEs when they would be involved in high-risk processing.

This CWA offers guidance only on the most relevant and common e-Privacy rules for Micro-SMEs' (see 3.8) processing activities that are applicable across EU member-states.

NOTE 2 CWA users should always check the implementation of the e-Privacy Directive in national law in the relevant Member State.

This CWA is applicable to Traditional Micro-SMEs. It is mainly addressed to the Micro-SMEs' service providers who assess them or support them to become GDPR compliant (e.g., consultants, trainers, accountants, lawyers, ICT providers, etc.). Due to the limited general legal knowledge present in Traditional Micro-SMEs and their general lack of time and resources to organise GDPR implementation projects themselves, this CWA is primarily and foremost addressed to their service providers.

The use of this CWA will be beneficial to:

— citizens: their rights to privacy and data protection will be safeguarded, even when their data is processed by Traditional Micro-SMEs;

— Traditional Micro-SMEs: being compliant is important from different perspectives, such as regulatory, reputational and economic; the CWA will help them avoiding data breaches and avoiding administrative fines that may be imposed when they're in breach of data protection legislation.

2 Normative references

There are no normative references in this document.

3 Terms, definitions and abbreviated terms

For the purposes of this document, the following terms, definitions and abbreviated terms apply.

3.1
data subject
any identified or identifiable natural person (3.7) to whom personal data (3.9) relates.

3.2
data subject rights
rights for individuals provided by the GDPR:

— the right to be informed,

— the right of access,

— the right to rectification,