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. Rusné 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

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,

— the right to erasure,

— the right to restrict processing,

— the right to data portability,

— the right to object,

— rights in relation to automated decision making and profiling.

3.3
DPA
Data Protection Authority

3.4
DPIA
Data Protection Impact Assessment

3.5
DPO
Data Protection Officer

3.6
GDPR
General Data Protection Regulation

3.7
identifiable natural person
one who can be identified, directly or indirectly, in particular, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

3.8
Micro-enterprise(s); Micro-SME(s)
enterprises with less than 10 employees and an annual turnover below €2 million.

Note 1 to entry: Micro-enterprises are considered as a sub-category of small and medium-sized enterprises (SMEs).

Note 2 to entry: For more information, see Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, 2003/361/EC, Annex, Article 2.

3.9
personal data
in general, any information that allows to identify a natural person and any information that can be linked to an identifiable natural person (3.7).

Note 1 to entry: The GDPR[6] describes personal data as information relating to an identified or identifiable natural person (the 'data subject', see 3.1).

[6]) Article 4(1) GDPR.

3.10
processing (of personal data) [7]
any (active or passive) operation or set of operations performed on (sets of) personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

NOTE

Processing must be interpreted very broad and includes any (even possible) contact with such data, such as storing personal data for a third party without having access to the unencrypted data.

3.11
Traditional Micro-SME(s)
Micro-SME(s) (see 3.8) defined by the following cumulative characteristics:

a) Their business is focussed on "brick-and-mortar" and physical services and the personal data they process is mainly used to provide these services.

b) Their online presence is limited (mainly website and social networks) or inexistent.

c) If present online, they may provide limited online services, generally supporting their "brick-and-mortar" business, mostly through standardized third-party services.

Note 1 to entry: Examples of standardized third-party services are booking apps (for example used by restaurants or hairdressers), rating apps, digital fidelity cards/apps or basic web shops.

d) They are organized in a low-tech and non-data-intensive way; They mainly process the personal data of their customers, suppliers and their limited number of employees; Their processing of sensitive personal data (see 3.12) is limited.

e) They may use their customers' personal data for digital advertisement purposes.

Note 2 to entry: Direct mail, search engines, telemarketing or social media ads are examples of how Traditional Micro-SMEs generally use customers' personal data for digital advertisement purposes, if they are using personal data for marketing purposes at all.

Note 3 to entry: It is unlikely at this moment for Traditional Micro-SMEs as defined in this CWA to use more advanced online marketing techniques such as mail automation, tailor made profiling, or enhanced digital advertisement that requires a further going use of the personal data. However, as the digitization process of all business and the access to digital marketing products and services keeps growing and is even further pushed by the Covid19 pandemic, it is to be expected that the use of such techniques will also rise among Traditional Micro-SMEs.

f) Their number of employees remains more or less stable.

Note 4 to entry: Generally, Traditional Micro-SMEs qualify as Micro-SMEs throughout their entire lifecycle.

Note 5 to entry: Micro-SMEs active in fields that require the processing of sensitive or high amounts of personal data, are excluded from this definition. Such excluded Micro-SMEs are, for example, Micro-SMEs providing health care related services or products (such as doctors, physiotherapists and pharmacies), Micro-SMEs providing digital

[7]) Article 4(2) GDPR.

services (such as online marketing services or data analytics services) and Micro-SMEs providing legal or accountancy services.

3.12
sensitive personal data
all personal data that has a more sensitive nature and to which processing restrictions apply.

Note 1 to entry: Sensitive personal data includes the special categories of personal data defined in Article 9 of the GDPR, personal data relating to criminal convictions and offence (Art. 10 GDPR) and other personal data of which processing is particularly sensitive and/or may be specifically regulated, such as location data or social security numbers[8)].

Note 2 to entry: For more information on sensitive data and special categories of personal data, see 4.2.4.6.

4 Guidelines for Micro-SMEs' GDPR Compliance

4.1 Overview of the practical requirements for the GDPR implementation for Traditional Micro-SMEs

This section translates the key GDPR requirements (described below in sections 4.2 and 4.3) into a practical list of required policies/documents for the GDPR implementation.

Complying with these practical requirements helps Traditional Micro-SMEs to apply and demonstrate their compliance with the GDPR (see Table 1).

As the GDPR imposes on Traditional Micro-SMEs to demonstrate their compliance with the GDPR, these practical requirements should also be materialized/documented (on paper or digital). Such materialization occurs for example in the form of a written or drafted table, process, template to be used in the future or guideline.

Table 1 — List of practical requirements for the GDPR implementation for Traditional Micro-SMEs

Name of the practical requirement	Required action
<u>Customers and website</u>	
a) Privacy Policy/Privacy Notice/Privacy Statement	A Traditional Micro-SME should inform its customers, website visitors, prospects, etc. in advance about the use it makes of their data and how it protects them. This is normally done via the Privacy Policy. The information provided to the data subjects should provide a useful overview of the processing a Traditional Micro-SME carries out, in a clearly visible, understandable and legible form. The GDPR also encourages the use of icons. A Privacy Policy should therefore contain the following information: 1) What personal data does a Traditional Micro-SME collect? Under this title all the *categories* of personal data that are processed by the Micro-SME should be mentioned and briefly explained.

8) Traditional Micro-SMEs shall verify national law to know what types of data can only be processed if additional requirements are met or cannot be processed at all. The processing of social security numbers, for example, is limited in many EU member states.

Name of the practical requirement	Required action
	Typical examples for Traditional Micro-SMEs: — Contact details; — Technical information: such as IP address or operating system when using a website or app; — Customer surfing behaviour on a website; — Billing and payment details, when amounts are to be charged; — Other information that are communicated by a customer. 2) How does the Traditional Micro-SME collect data? In particular a Traditional Micro-SME may collect data (for example): — When using its website; — When communicating with it; — By using its services; — From public sources; — [Other]. 3) How does a Traditional Micro-SME use data? It can use personal data to (for example): — Provide its services/products; — Communicate; — Make its website work. 4) On what legal basis does a Traditional Micro-SME process data? 5) Which third parties process data? For example: — Hosting and website; — Analysis of website traffic; — Supporting business service providers, such as for administrative and accounting purposes, if their access to personal data is strictly required; — E-mail services, couriers. 6) Where is data stored and processed? For example: — On the servers and computers we use within the EU; — On the systems of the listed third parties processing the data. In such a case a Traditional Micro-SME should ensure that they provide an adequate level of protection. 7) Information about data subject rights and the procedures to exercise these rights and a right to complain about the use of personal data. 8) How long does a Traditional Micro-SME keep data? 9) Information about cookies and other tracking technologies.
b) Cookie policy, cookie banner and cookie preference centre	Traditional Micro-SMEs should ask for consent for the use of cookies and other tracking mechanisms on their websites. A Traditional Micro-SME should inform website visitors transparently about the cookies it uses, ask permission

Name of the practical requirement	Required action
	to use them (via a cookie banner) before they become active and give them the opportunity to refuse them. Cookie Management Platform tools (CMP) allow to implement this in an automated manner. The GDPR requires that this information is presented to the client in a clearly visible, understandable and legible form. In doing so, the GDPR encourages the use of icons. For this reason, the Cookie Policy has been split up into a concise, easy-to-understand part that is ideally included in the cookie banner and a more detailed part. To correctly use cookies, a Traditional Micro-SME should implement: — a cookie policy, explaining a.o. how cookies are used and what cookies are, — a cookie banner (or cookie notice), that pops up on the website, provides some basis information and is used to obtain consent of the website visitor for the use of cookies, — a cookie preference centre, allowing website users to manage their cookie preferences at any moment. Cookie banners constitute the means by which a website informs users about the use of cookies and other tracking technologies (the first layer). They are a prerequisite for obtaining valid, opt-in consent for the use of cookies, given that consent under the GDPR and e-Privacy Directive has to be 'informed'. As with regular privacy notices under the GDPR, cookie banners have to be drafted in a clear and intelligible language so that the average individual (non-privacy expert) is able to understand what the notice is saying, and importantly, to what processing they are called to consent. There are different possibilities for cookie notice implementation, as for example, a short cookie banner with basic information about cookies usage, allowing the user to accept all of them (opt-in), refuse all of them unless some are necessary for the functioning of the website or configure options for the usage of different cookies in a more detailed cookie notice (second layer). It is a good practice to group the information of cookies according to their purpose. For example, cookies that are necessary to make the website usable, cookies for user preferences, cookies for usage analytics, and cookies for marketing and unclassified cookies. User shall be able to accept (or not accept) the usage of cookies by groups separately. For example, a user should be able to accept analytics cookies and refuse the usage of marketing cookies easily based on the previous classification. If the number of cookies is very high, having to accept or refuse the usage of every cookie separately may be very impractical and not recommended. Another good practice is to show a button to accept all the cookies and a button to refuse all the cookies. It is recommended it is as easy for the user to refuse the usage of cookies as it is to accept their usage.
	In the second layer, the cookie policy, the following information shall be displayed for every cookie on each group (see example below): ☑ Name

<table>
<tr><th>Name of the practical requirement</th><th>Required action</th></tr>
<tr><td></td><td>
☑ Provider: own cookies or third party
☑ More technical details and information regarding the specific purpose
☑ Session or persistent
☑ Type: HTTP cookie, flash cookie, local storage cookie
☑ Retention period
Finally, it´s recommended that the information provided in the (dynamic) cookie banner is also be available on a static webpage, to allow website visitors to review the earlier choices made with regard to the use of cookies and to allow them to withdraw earlier provided consents. The cookie preference centre shows the current state of cookie configuration to the user and allows to change or withdraw the consent.
E.g.: “Currently you are accepting all the cookies. You can change or withdraw your consent for cookies of category X by clicking here” or “Currently you are accepting Necessary cookies and Analytics cookies. You can change or withdraw your consent here”.
The cookie banner can include the following statements and request for consent (for example):
Our website uses cookies to provide you with an excellent user experience, to analyse and optimise the use of our website, to provide you personalized content and to continue to improve our services.
We therefore recommend that you accept all cookies.
Please indicate below which cookies may be used:
<table>
<tr><td>ON
Always on</td><td>Strictly necessary cookies: we use these cookies to [XXX]</td></tr>
<tr><td>OFF</td><td>Functionality cookies: we use these cookies to [XXX]</td></tr>
<tr><td>OFF</td><td>Analytical and performance cookies: we use these cookies to [XXX]</td></tr>
<tr><td>OFF</td><td>Advertising and social media cookies: we use these cookies to [XXX]</td></tr>
</table>
<table>
<tr><td>I accept ALL cookies [<-button]</td></tr>
<tr><td>I accept the cookies selected above [<-button]</td></tr>
</table>
If you reject some or all of the above cookies, this may disrupt the use of (parts of) our website.
</td></tr>
</table>

Name of the practical requirement	Required action
	You can find more information about how we process your data and use cookies in our Cookie Policy and Privacy Policy [<- links to Cookie Policy and Privacy Policy]. Note that the non-essential cookies above should not be pre-ticked to 'on' and that these cookies cannot be installed until the website-visitor has accepted the use thereof. The Cookie Policy should start with a summary and further contain the following sections, it may include the following example text: 1) What are cookies: *"Cookies are small (text) files that your computer downloads when you visit a website. Cookies are sent back with each subsequent visit to this website or to another website that recognizes this cookie.* *Thanks to cookies, a website can recognize you.* *Cookies are used, among other things, to allow you to navigate between pages efficiently, to remember your preferences, to increase your general ease of use or to show you online advertisements that match your profile."* 2) What type of cookies does a Traditional Micro-SME use: *"We use the following types of cookies:* *— Cookies necessary for the proper functioning of our Website.* *— Cookies that analyse how our Website is used.* *— Cookies to remember your preferences (such as language).* *— [Cookies to analyse your browsing behaviour and display your customized advertisements]."* 3) Why does a Traditional Micro-SME use cookies: *"We use the following types of cookies for the following purposes:* *— Strictly necessary cookies. These cookies are necessary for the operation of our Website. They enable you to log in, to use a shopping cart].* *— Analytical cookies/performance cookies. These cookies analyse the way our Website is used, which pages are visited the most, where problems occur, etc. This allows us to improve our Website and keep your user experience optimal].* *— Functionality cookies. These cookies are used to recognize individual users and remember their preferences. For example, they allow us to remember your choice of language and any other settings you change, so that they look good the next time you visit].* *— Targeted cookies or advertising cookies. These cookies analyse your surfing behaviour (on our and other websites) in order to show you advertisements that match your interests and profile. Such cookies generally come from third parties (such as [mention one or more internet search engines or social media platforms]) who collect this information and are also responsible for the advertisements based on it]."* Note that cookies can also be broken down:

Name of the practical requirement	Required action
	— First party cookies. These cookies originate from ourselves. For example, they control and remember the display of the website in your preferred language or remember the contents of a shopping basket. — Third party cookies. These cookies are set by others. They are often used to track online behaviour across different websites, such as cookies placed by internet search engines or social media platforms. 4) What specific cookies does a Traditional Micro-SME use: "We use the following cookies: ***(1) [our website.be]:*** *o First party cookies* *o Purpose: [to improve the operation and functioning of the website]* *o Data: [your behaviour on our website, technical identification data, preferences, etc. No data that could lead to identification will be permanently stored here]*
	o Validity: [They include both session cookies (which expire after closing the page) and permanent cookies which expire after 1 year] ***(2) [website analytics service provider]*** *(i) Third-party cookies.* *(ii) Purpose: [Analysis of your use of our website, how you get to us, which device you use, from which location you visit our website, etc.].* *iii) [We have set up [analytics service provider] in such a way that the findings of this service are only shared with [analytics service provider] anonymously].* *(iv) Type: [Analytical cookies] [Advertising cookies [if data is shared non-anonymously with the service provider]].* *(v) Data: [technical identification data and behaviour (both on our website and on other websites). We ourselves have no access to the information collected, only to resulting statistics].* *vi) Validity: [These contain both session cookies and cookies that expire after 2 years].* ***(3) [name of the service provider and names of the cookies]*** *(i) [Third-party cookie/first-party cookie].* *(ii) Purpose: [define purpose].* *(iii) Type: [describe type].* *(iv) Data: [what data are collected].* *(v) Validity: [how long do the cookies remain valid].* ***[(4) Etc.]***
c) Data Subject Access Requests (DSAR)	A Traditional Micro-SMEs should define the processes on how it will react to requests of data subjects who want to perform their rights under the GDPR, such as access, correction, portability, etc. and prepare standard forms and templates to be used during that process.

Name of the practical requirement	Required action
	Requests of data subjects to exercise their data subject rights have to be complied with even if they are not expressed in writing by the data subject. A Traditional Micro-SME should be able to provide each person whose data it is processing with an integral copy of all the data in its possession that that person has provided: — Information that has been communicated directly (e.g., in a form or contract); — Information collected based on that person's behaviour; and — Information when the data was collected. Examples of such personal data: — Data about what a customer buys (such as purchase history in a shop); — Data on the behaviour of a customer: how much does a certain customer spend per month, which products does he usually buy, which advertisements does he click on in a webshop, etc; — An energy company that keeps track of the consumption history of its customers; — A “smart watch” application on a smartphone that keeps track of users' performance so that they can evaluate their results and progress. A Traditional Micro-SME shall only communicate personal data and raw data without violating the rights of others. Further restrictions may apply as per national law implementing the GDPR. A Traditional Micro-SME may let the person download the information himself/herself (e.g., download it from the customer section of the website) or provide it on request (e.g., via web form or request template). A Traditional Micro-SME should only give this information to the person in question or to others that have been duly authorised to act on their behalf. A Traditional Micro-SME should verify the requesting person’s identity to a reasonable extent, but cannot impose unreasonable obligations. For example, it should not ask for the request to be sent by post if the registration is digital, nor should it put in place other delaying or complicating mechanisms, such as requiring a copy of the identity card of the data subject, when this is not justified by (for example) the kind of services that are provided, the sensitivity or volume of the personal data, the secure and individualized access the data subject has to an online client zone, etc. A Traditional Micro-SME acting as a data processor who receives a data subject request should inform the data controller and should not fulfill the DSAR without the agreement of data controller.
d) Processing personal data of children	The processing of personal data of minors under 13 years of age (in Belgium, in some other countries this limit is 14, 15 or 16 years) is particularly protected

Name of the practical requirement	Required action
	and should meet additional conditions[9]. If a Traditional Micro-SME offers digital services that may be used by minors in more than one country, it should always check which is the minimum age in each country. The following points of attention apply to processing of personal data of minors: — when explaining how the personal data are being processed, an additional effort is expected so that the explanation is clear to the child as well. This may include, for example, visual aids such as short films or cartoons; — where digital services or products (e.g., online games, platforms, online shops for real goods, etc.) are provided to a child, the consent of 'the holder of parental responsibility' is required;[10] — the consent of the holder of parental responsibility: if the child is younger than 13-16 years old (see above), you should ask permission from the "parents". The child should not be able to do it on behalf of the "parents". In practice a statement "I give permission to my child as a parent" supplemented with the possibility to use the credit card and code of the "parents", can be considered as a sign that the "parents" have given permission; — codes of conduct: the GDPR allows organizations representing a particular sector or group to draw up binding codes of conduct containing additional measures. Such codes of conduct may specifically define how to deal with children. It is recommended to check with a specific sector or professional association whether they have drawn up a code of conduct.
e) Record of data breaches and a Data Breach Policy/Procedures	A (personal) data breach means any accidental or unlawful unauthorized disclosure, loss, destruction, alteration of, or access to, personal data you process in any way, including during transmission or storage. Some of the common examples include: — a file with personal data is sent to the wrong person; — an unauthorized person has had access to your systems and may have been able to access, copy, view, destroy, etc. personal data; — an account of an employee has been hacked and you cannot determine with certainty if the hacker accessed the personal data that the employee has access to; — a logfile or directory of your website containing personal data was accessible on the internet for anyone who visited the right url and you cannot ascertain for sure that it has not been viewed by anyone;

[9]) The age as from which children can consent under the GDPR to have their personal data processed in the context of the provision of information society services can vary between 13 years old and 16 years old. For an overview of the applicable ages as from which a child can freely consent in this context in each EU-country, please visit: https://www.gdprhandbook.eu/consent-and-children-data .

[10]) The 'holder of the parental responsibility', as defined under Article 8 GDPR, can be any person entitled under national law to lawfully represent the minor. National law shall be verified to establish who has such authority.

Name of the practical requirement	Required action
	— a laptop or storage media is lost (such as a USB-stick), even if the device is encrypted; — a file that contains personal data cannot be retrieved; — the password of an encrypted file with personal data is lost and there are no other, accessible copies of the file. A personal data breach should be notified to the data protection authority within 72 hours, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of the concerned persons. If the breach is not notified within 72 hours, the controller should inform the data protection authority of the reasons for the delay. A notification may be made in phases, i.e., the available information can be part of the initial information and additional information can be added to the file later. The notification should include at least the following information: — the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; — (where applicable) the name and contact details of the data protection officer or of another point of contact from which further information can be obtained; the likely consequences of the breach; — the measures taken or proposed by the controller to address the data breach including, where appropriate, measures to mitigate any possible adverse effects. A Traditional Micro-SME should adequately document all personal data breaches, including the related facts, effects and the remedial measures taken. When a personal data breach is likely to result in a risk to the rights and freedoms of natural persons, the controller should inform the data subjects of the breach without undue delay. A Traditional Micro-SME should describe, in clear and plain language, the nature of the personal data breach and indicate: — the name and contact details of the data protection officer or other point of contact from which further information can be obtained; the likely consequences of the personal data breach; — the measures taken or proposed by the controller to address the breach including, where appropriate, measures to mitigate any possible adverse effects. A Traditional Micro-SME does not need to inform the data subjects of the personal data breach if: — it has implemented appropriate technical and organizational protection measures which were applied to the personal data affected by the breach, in particular measures, such as encryption, that render the personal data unintelligible to any person who is not authorized to access them;

Name of the practical requirement	Required action
	— it has subsequently taken measures to ensure that a high risk to the rights and freedoms of the data subjects is no longer likely to materialize; or — doing so would involve disproportionate efforts, in which case it should make a public communication or take similar measures to ensure that the data subjects are informed in an equally effective manner. The Traditional Micro-SME should describe in a Data Breach Policy/Procedures which the data breach response plan is, i.e., how its employees or third party processor and data processors should react when a data breach occurs, who they should inform etc. Employees should be informed about the content of this policy. Simplified, such response plan should contain at least the following information for a Traditional Micro-SME who is a data controller (only relevant in Traditional Micro-SMEs with more than 1 employees): — the name and emergency contact details of the person responsible for the handling and the follow up on data breaches must be explicitly mentioned in the procedure, — what to do and who to contact *immediately* upon discovery of a data breach, such as the ICT service provider, besides the person described above and who to contact if one or more of these persons are unavailable, — undertake (if possible) the first preliminary protective measures to avoid further exposure, risk and damage, — preliminary evaluation extent of the breach and the risks for the data subjects and evaluate if a notification to the data protection authority and the data subjects has to take place, — collect further information about the breach, the exposed personal data, log files, etc., obtain information from data processors if they are involved in the data breach, — if required, take additional protection and recovery measures, — decide if notification to the data protection authority is required (this must be done within 72 hours upon discover by the data controller), — decide if a notification to the data subjects is required, how this can/must be done and within which timeframe this must take place, — if applicable, prepare the notification, justify why the delay of 72 hours is exceeded and (where applicable) why not all information about the breach can be provided), and submit it in due time, — if applicable, prepare the notification to the data subjects and send it out in due time, — perform a final assessment of the data breach, the causes, the damage etc. and implement (if required) additional organizational and technical measures, including using this information (if useful) to raise awareness among employees and service providers, — add the data breach to the record of data breaches.

Name of the practical requirement	Required action
	A record of data breaches should be established. In this record, a Traditional Micro-SME should not only note the data breaches that required notification, but also data breaches that remained below the notification threshold. A Traditional Micro-SME should: — Assess the technical and operational security measures in place and make the appropriate adjustments, if necessary; — Establish a Data Breach Policy and a record of data breaches; — Have IT systems tested regularly by an external party; — Put in place an appropriate data breach notification procedure; — Train its employees and contractors in security awareness; — It is advisable to consult the national legislation and the national websites of these DPAs to establish how a data breach should be notified to a specific DPA. NOTE Some national DPAs (e.g., Luxembourg, Belgium) have published data breach notification forms.
<u>Newsletter</u>	
f) Newsletter subscription information	When someone who is not a customer or contracting party of the Traditional Micro-SME concerned signs up to the Traditional Micro-SME's website (or in any other way) to receive a newsletter (or other informative e-mails), the Traditional Micro-SME should ask for permission ('consent') to do so and is obliged to provide certain information. A Traditional Micro-SME should: — obtain consent for this. This should be done separately if the personal data is going to be used for multiple purposes; — expressly state that such consent may be withdrawn at any time; — explain what it is going to be done with the data; — not require to fill in more data than the data actually needed to carry out the processing operations for which you collect the data. For example, a Micro-SME may not compulsorily ask someone for their gender, address or date of birth if that information is not necessary for the intended processing, i.e., sending the newsletter. Boxes to be ticked to obtain consent should never be ticked in advance. The Traditional Micro-SME should give an individual the option to unsubscribe from emails at any time and change his/her preferences. This can be done via the unsubscribe link that should be provided in each e-mail and ideally also via an online 'preference center' where all communication preferences can be managed. The link to a Privacy Policy should also always be provided.
g) Confirmation e-mail newsletter subscription	In order to confirm that the permission and information have been given effectively, it is recommended that Traditional Micro-SME sends an e-mail about this (ideally, this process is automated). In this e-mail the Traditional Micro-SME it´s recommendable to also ask the recipient to confirm his e-mail address and his wish to receive the Micro-SME's newsletters ("double opt-in")

Name of the practical requirement	Required action
	by clicking on a confirmation button. This way, the Micro-SME ensures that the person who registered has access to the e-mail address provided. A Traditional Micro-SME can (for example) include the following statements in a confirmation e-mail for newsletter subscription: "*Thank you for subscribing to [our newsletter].* *We will be happy to keep you informed about [X].* *Please confirm your email address via this button?:* *Confirm [/link]* *We value your privacy and we will only use your data to send you communications (about actions, newsletter, information) according to your preferences, [/taking into account your profile if applicable].* *If you would like to read more on [what exactly those preferences are and] how we guarantee your privacy, you can do so via the link[s] below to our Privacy Policy.* *Don't hesitate to contact us if you have any further questions."* It is recommended and may result from national e-commerce legislation that if it is not clear from the e-mail that it has a commercial purpose, the message "Advertising" should be added (ideally at the top).
h) Unsubscribe e-mail	When someone signs up for a newsletter on your website they should be given the opportunity to unsubscribe. Unsubscribing should be easy and accessible. It should be at least as easy as signing up. If someone subscribes by email, they should also be able to unsubscribe by email. When someone unsubscribes, a Micro-SME is no longer allowed to send them e-mails and should avoid doing so at all costs. In every commercial e-mail, your recipient should be given the opportunity to unsubscribe from subsequent mailings, for example, with the following sentence: *"Do you no longer wish to receive our emails? Then you can unsubscribe via this link [/link]. You can manage the emails you receive in our Preference Center [/link]".* If your recipient clicks on one of the two links, he will be taken to an unsubscribe page or a preference centre, where his details have already been (pre-)filled in. It is recommended that in the Preference Center, a recipient is given the opportunity to unsubscribe specifically for certain communication options. If he only wants to unsubscribe from the weekly newsletter, he can, for example, continue to receive "information about events". This can be done in the following way (for example): *"I want to unsubscribe with the following e-mail address [e-mail address is pre-filled - to be modified by user in case there is a wrong address] from the following communications:* □ *Monthly newsletter [on [subject]];* □ *Weekly newsletter [on [subject]];* □ *[New blog entries that appear on your website];*

Name of the practical requirement	Required action
	□ *[Interesting events [near me];* □ *I want to unsubscribe from all communications [/Link button + bold or colour]. (This button disables all of the above options - please note that if you select this button, you will no longer receive any communication from us.)* *Send / Confirm [/ button with link]* *You can unsubscribe from our emails at any time and change the above preferences. If you uncheck the above choices, you will no longer receive any communication from us.* *We will only use your data in accordance with your preferences indicated above and strictly in accordance with the privacy legislation. Read our Privacy Policy [/link] for more information."*
<u>Suppliers and third parties</u>	
i) Privacy clause(s) in contracts and terms and conditions	In any cooperation with a client, contractor, partner, etc., both sides process personal data to a limited extent, even if the actual order does not relate directly to the processing of personal data. Such limited processing does not require a separate processing agreement to be drawn up, but it is sufficient to regulate the privacy obligations in the contract or the applicable terms and conditions. A Traditional Micro-SME can, for example, insert the clauses below in its contracts, general terms and conditions, purchase conditions, etc., to inform contract partners how a Micro-SME processes the received data. *"The parties confirm that they will use the personal data provided by them in the execution of the [contract/ general terms and conditions/other]:* *— received from each other: will at all times process strictly in accordance with the Privacy Regulations applicable to that data/processing at that time;* *— transmit to each other: may transmit to each other in accordance with the applicable Privacy Regulations.* *As soon as the scope of the data transferred or the processing carried out so requires, the Parties will enter into a processing agreement for this purpose, which will take precedence over the privacy provisions in this [contract/general terms and conditions/other].* *Indemnification* *Each Party shall indemnify the other Party against all damages and claims of third parties (including from any (privacy) authority) to the extent and to the extent such damages or claims originate from the (alleged) breach by the indemnifying Party of its obligations under Privacy Regulations.* *Sub processors* *Each Party has the right to have personal data received from the other Party processed by third parties ("Sub-processor(s)"):* *(i) within the EU to the extent that [prior approval is obtained from the Responsible Person] [these are notified in advance to the Responsible Person] and the requirements set forth in the Privacy Regulations are met;*

Name of the practical requirement	Required action
	ii) outside the EU to the extent that [prior approval is obtained from the Responsible Person] [these are reported in advance to the Responsible Person] and the requirements set out in the Privacy Regulations have been met. *If the processing of the personal data received from another Party is very limited and incidental and does not involve any risk for the data subjects, that Party shall not proactively inform the other Party of (or obtain permission for) a change of Sub-processor, but shall be able to provide an overview of the Sub-processors upon request.* *These Sub-processors, like the receiving Party, shall strictly comply with the Privacy Regulations and the privacy obligations imposed on the receiving Party and may under no circumstances process these personal data for their own use."*
j) Data processing agreement	— When a Traditional Micro-SME acts as a data controller and has personal data processed by a data processor it should enter into a data processing agreement, which should clarify that: • the processor will process personal data only on written instructions from the Micro-SME; • the processor uses all appropriate technical and organizational measures to protect the security and confidentiality of the data; • [if applicable] the processor will not subcontract to another processor unless instructed to do so in writing by the Micro-SME or unless this possibility is explicitly provided in the data processing agreement, in which case the processor may be required to pro-actively inform the data controller about such new intended processor (if desired). In any case, the processor shall provide an overview of all (sub-)processors to the data controller upon the latter's request; • the processor will collaborate with the Micro-SME to uphold their obligations under the GDPR, particularly concerning data subjects' rights; • the processor will assist the controller in ensuring compliance with the obligations regarding the security of personal data and, if applicable, compliance with data protection impact assessments, taking into account the nature of processing and the information available to the processor; • the processor will inform the data controller if he has suffered a data breach; • the processor will inform the data controller if he has received a DSAR and will assist the data controller in fulfilling the request; • the processor agrees to delete or destroy all personal data upon the termination of services or return the data to the Micro-SME; • the processor will allow the Micro-SME to conduct an audit and will provide whatever information necessary to prove compliance. — When using data processors to process personal data on behalf of the Traditional Micro-SME, the latter should need to ensure that the data are

Name of the practical requirement	Required action
	processed within the European Economic Area or in countries that are subject to an adequacy decision, or ensure that appropriate safeguards are in place[11)]. — When a Traditional Micro-SME acts as a service provider it may process personal data for its clients, for example it may: • manage its client's customer data (e.g., administrative support, sending emails, accounting, etc.); • contact clients of clients (e.g., call centre services). — In that case a Traditional Micro-SME will process personal data on behalf of a data controller, with whom it should clearly agree in writing what it may and may not do with the data and whether it may use subcontractors. A Micro-SME's acting as such a service provider will process these data on behalf of its clients. A Traditional Micro-SME should make clear (written) data processing agreements with its contractors about (see above): • what it can and cannot do with those data; • how to secure that data; • how long it is allowed to keep the data.
<u>Management</u>	
k) DPO appointment guidance	A Traditional Micro-SME may need to appoint a DPO under the GDPR if its core business requires such Traditional Micro-SME to: — regularly and systematically monitor data subjects on a large scale; — process sensitive personal data on a large scale. Very few Traditional Micro-SMEs are expected to appoint a DPO, as the requirement for a DPO applies to organizations carrying out specific processing activities that are not common to Micro-SMEs. A Traditional Micro-SME should however include in their privacy policies an email, phone number or postal address that individuals could use in order to contact them for data protection matters, for example: *"For all matters regarding personal data and this Privacy Policy you can contact us using the address: privacy@Micro-SME.com".*
l) DPIA assessment and guidance (DPIA)	Prior to high-risk personal data processing, a DPIA should be performed to ensure that the processing can be performed under the GDPR and that all requirements are met. When a new (potential) high risk processing of personal data is started or there is a modification of an existing one, a Traditional Micro-SME needs to evaluate whether that processing can have a major impact on the privacy of the persons whose data is being processed. A Traditional Micro-SME needs to evaluate and document: — whether the planned processing poses a privacy risk; — whether and how the risks will be adequately covered.

11) See 4.2.4.5.

Name of the practical requirement	Required action
	A DPIA should be carried out when a new or modified use of personal data "probably poses a high risk" to those whose personal data are being processed. According to the GDPR and an opinion of the privacy authorities, a DPIA should at least be carried out when: — there is doubt as to whether or not it is required; — an organization systematically and comprehensively assess personal aspects of natural persons, based on automated processing (such as profiling) and base decisions affecting them; — there´s large-scale processing of sensitive data (health data, political affiliation, ethnicity, biometric data, criminal convictions, etc.); — there´s systematic and large-scale monitoring of publicly accessible areas. It is not very likely that Traditional Micro-SMEs, as defined in the CWA (see 3.11), will be involved in high-risk processing.
m) Data Security Policy	It is recommended that a Traditional Micro-SME defines how it ensures the organizational and technical security of the personal data it processes, including the security of the used information technology (devices, applications and networks). In order to demonstrate how a Traditional Micro-SME is complying with the security principle, having a Data Security Policy in place is recommended. A Traditional Micro-SME should protect the personal data processed by taking technical and organizational security measures: — Confidentiality • Traditional Micro-SME's staff should be trained to handle confidential data; • A Traditional Micro-SME should take technical measures to prevent data breaches or damage when breaches occur by encrypting data, strictly securing access to systems and buildings, etc. — Integrity • Traditional Micro-SME's staff should be trained to process data safely and with minimal risk of errors; • Traditional Micro-SME should use technology to monitor and safeguard the integrity of the IT environment, including the personal data processed (e.g. Firewalls, Virus scanners...). — Availability • Traditional Micro-SME's staff should be trained to process data in order to ensure a high level of availability; • Traditional Micro-SME IT systems should have a high degree of redundancy; • Risk management; • Micro-SME should take measures in view of the degree of data sensitivity and potential risks of the data breach it processes.

Name of the practical requirement	Required action
n) Retention Policy/Documentation	This policy describes how long each category of personal data is stored by a Traditional Micro-SME. The GDPR does not dictate how long personal data should be kept. However, a Micro-SME needs to establish and document standard retention periods for different categories of information it holds, wherever possible. Specific examples of retention times for different processing activities based on the above, could include storing: — customer financial and tax data for the purpose of compliance with tax regulations for the period specified by tax laws; — employee files and records for as long as required by relevant employment and social security and social protection laws; — direct-marketing customer data for a specifically defined period, e.g., 1 year, unless the customer objects/opts-out sooner, does not show any engagement or actively opts-in for the data to be used for another defined period; — consumers' contract, service, or delivery data for as long as the contract is in force or services or products are provided; — processing data necessary for the establishment, exercise or defense of legal claims. A Traditional Micro-SME should consider any legal or regulatory requirements. There are various legal requirements and professional guidelines about keeping certain kinds of records – such as information needed for income tax and audit purposes. It is also recommended for a Traditional Micro-SME to also consider any relevant industry standards or guidelines. A Traditional Micro-SME should verify if it complies with the storage limitation principle. Personal data can be kept as long as one of the purposes applies, but it should not be kept indefinitely 'just in case'. If data is no longer needed, a Traditional Micro-SME should either erase it, or anonymise it so that it is no longer in a form which permits identification of data subjects. [12)] A Traditional Micro-SME should review whether it still needs personal data at the end of any standard retention period, and erase or anonymise it unless there is a clear justification for keeping it for longer. It is also good practice to review a retention of personal data at regular basis and take the time to perform such review into account in the initial retention period if personal data is to be stored for several years. For example, if data retention of data stored for a longer time is checked once a year, than the retention period of personal data that must be stored during 5 years by law should ideally be set to 6 years. This provides a buffer of one year to the Traditional Micro-SME to be able to organize the deletion and destruction of personal data.
o) Record of processing activities (RoPa)	A Traditional Micro-SME, as defined under this CWA (see 3.11), is not obligated to maintain a RoPa unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is

12) See 4.2.2.3 and the footnote under that part with regard to pseudonymisation and anonymisation.

Name of the practical requirement	Required action
	not occasional, or the processing includes special categories of data or personal data relating to criminal convictions and offences. Some Traditional Micro-SME may need to maintain a RoPa. The RoPa lists and describes the processing activities of the Traditional Micro-SME, both as a data processor and as a data controller. The information that should be mentioned in the RoPa is different when relating to the processing activities as a data processor compared to the processing activities of the Traditional Micro-SME as a data controller. The information required from data controllers is more extensive than that required from data processors. In particular, when it comes to data controllers, that record should contain all of the following information: — the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer; — the purposes of the processing; — a description of the categories of data subjects and of the categories of personal data; — the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations; — where applicable, transfers of personal data to a third country; — where possible, the envisaged time limits for erasure of the different categories of data; — where possible, a general description of the technical and organizational security measures. Such records should be kept on paper or in electronic form.
	It is recommended to consult websites of the national DPAs which have issued RoPa templates[13]).

[13]) Some useful templates can, for example be found on the websites of:

— ICO, the UK data protection authority: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/documentation/how-do-we-document-our-processing-activities/,

— CNIL, the French data protection authority: https://www.cnil.fr/en/record-processing-activities,

— The Belgian Data Protection Authority: https://www.autoriteprotectiondonnees.be/publications/modele-de-registe-des-activites-de-traitement.xls (in French) and https://www.gegevensbeschermingsautoriteit.be/publications/model-voor-register-van-verwerkingsactiviteiten.xls (in Dutch).

The RoPa of the European Data Protection Supervisor (EDPS) can also be looked at as an interesting example of an actual RoPa. Note that the scope of data processing performed by the EDPS exceeds any data processing activities of any Traditional Micro-SME by far, causing that the EDPS' RoPa is be much more complex than any Traditional Micro-SME's RoPa needs to be. On a side note, also note that the EDPS is not subject to the GDPR.

Name of the practical requirement	Required action
p) Legitimate interests assessment (LIA) guidance	Legitimate interests is the most flexible lawful basis for processing. A wide range of interests may be legitimate interests. The GDPR specifically mentions use of client or employee data, marketing, fraud prevention, intra-group transfers, or IT security as potential legitimate interests. However, if a Traditional Micro-SME chooses to rely on legitimate interests, it has to take on extra responsibility for considering and protecting data subjects rights and interests. It should: — identify a legitimate interest; — show that the processing is necessary to achieve it; and — balance it against the individual's interests, rights and freedoms. If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override legitimate interests. This legitimate interest assessment or LIA can be broken down into a three-part test: — Purpose test: are you pursuing a legitimate interest? — Necessity test: is the processing necessary for that purpose? — Balancing test: do the individual's interests override the legitimate interest? A Traditional Micro-SME should include details of legitimate interests used as legitimate processing basis in its Privacy Policy. If a Traditional Micro-SME wants to rely on legitimate interests, it should use the LIA described above to assess whether it applies. A Traditional Micro-SME should perform the LIA before the start of the processing. It is recommended to consult websites of the national DPAs which have issued LIA templates[14]).
Employees	
q) Employee policies	A Traditional Micro-SME with employees should have a number of policies to ensure it complies with the GDPR when processing the personal data of these employees and to ensure that its employees handle personal data in a GDPR compliant manner. Note that national legislation, employment law in particular, should always be taken into account when applying data protection principles, rights and obligations to the employee-employer relationship. These include: 1) A data policy Employees of a Traditional Micro-SME which processes personal data, should be informed how they have to handle personal data to ensure that it is being processed in a GDPR compliant way. It should contain information on:

[14]) For example the one of the ICO, the UK data protection authority: https://ico.org.uk/media/for-organisations/forms/2258435/gdpr-guidance-legitimate-interests-sample-lia-template.docx .

Name of the practical requirement	Required action
	— what personal data are processed as part of the business of the Traditional SME (e.g., a name, a photograph, an ID card number, an IP address, a professional e-mail address, etc.); — what is the legal basis for data processing; — where the data is stored; — how long personal data is retained and when it should be deleted; — rules on use of e-mail and communication; — information on ICT devices, security policies and password guidelines; — “Bring Your Own Device”; — unwanted information sharing; — contact information. The Data Policy may be (and is often) integrated in the ICT Policy. 2) An ICT Policy An ICT Policy defines how the employees are allowed to use the ICT environment (networks, devices, applications, software) of the employer. An ICT Policy has the following objectives: — to let employees handle the ICT infrastructure in a well-considered manner and make them aware of the importance of the protection of (personal) data, the possible risks and the damage that can occur when the ICT infrastructure is being used incorrectly; — to allow ICT infrastructure to be used in a secure and lawful manner; — to promote the optimal and efficient use of the ICT infrastructure; — to ensure safe handling of personal and non-personal data. it´s recommendable that the ICT Policy provides guidance on the following matters: — policy of use of devices (e.g., encryption and password guidelines, backup and maintenance, private use); — policy on reporting incidents when using the ICT infrastructure (e.g. possible loss of or damage to a Device (computer, USB stick, smartphone, etc.), any suspicious communication (such as possible phishing emails) received); — connecting own devices (such as laptops, tablets, phones, storage media, etc.) in accordance with the BYOD Policy; — use of a professional e-mail address and other means of communication; — use of the Internet (e.g., guidelines on personal use, security, use of public Wi-Fi networks); — use of social and other media; — [if applicable] control and monitoring of the ICT infrastructure; — [if applicable] camera surveillance. 3) The employee privacy policy

Name of the practical requirement	Required action
	The employee privacy policy is the Privacy Policy (see above) applicable to the processing of personal data of the employees. It explains: — What categories of personal data related to the employees are collected by the Traditional Micro-SME – employer, e.g.: • personal identification and contact details, such as name, address, date of birth, gender, professional photos and private telephone number; • immigration and residence status and the right to work; • contact details in case of emergency; • education and training information, such as diplomas, certificates and licenses, professional files and attendance at internal training courses; • work-related information, such as number of years of service, timesheets, badges, work location, employee ID number, work file, holidays and contracts; • recruitment and performance-related information, such as objectives, assessments, comments, feedback results, career history, work equipment, career and succession planning, skills and competences and other work-related qualifications; • information relating to use of resources, including computers and telecommunication systems and internet traffic; • information necessary for compliance with standards and laws, risk management, including disciplinary reports, background reports and safety data; • payroll administration and payment or information about bonuses obtained, such as salary and insurance information, social security number or tax information, details of bank account and employee bonus schemes, information of family and dependents; • travel details and passport information; • photos. — Legal grounds for data processing (performance of the employment contract, legal obligation, legitimate interest, consent, note that using consent is difficult in an employment context as an imbalance of power exists between the employer and the employee); — How a Traditional Micro-SME obtains personal data (communication with the employee, collected as a result of the employee's use of infrastructure, collected as a result of the employee's performances, indirect knowledge; — How a Traditional Micro-SME uses employee's data (e.g., to keep payroll records, payment of wages, insurance, to evaluate employee's performance etc.);

Name of the practical requirement	Required action
	— Which third parties process employee's personal data (e.g., hosting and backup service providers, administration personnel and secretariat, cloud services etc.); — Technical safety and organizational measures; — Data retention; — Employees data subject rights, Human Resources (HR) department contact information and the right to complain about the use of data. Specific rules should be taken into account when processing sensitive personal data. The employees should be informed that the following sensitive data are being processed (if applicable): — National number; — Information about employee's health in the event of absence due to illness; — Union membership; — The existence or absence of criminal convictions and prosecutions, but only to the extent that a Micro-SME is legally obliged to do so (if not, the processing of such information will generally be prohibited, please verify the applicable national legislation). 4) Employment contract It can be useful to insert a few general clauses about data processing in the new employment contracts to be concluded, related to both the importance the employer attaches to the data protection rights of the employee and to the importance attached to the way the employee will handle personal data processed as part of the business of the employer. Reference should be made to the work rules and the applicable policies in which these principles and the rights and rules relating hereto are substantiated. 5) Work Rules Depending on the applicable national legislation, the Micro-SME should provide more information on the data protection rights of the employees and on the compliance of the employees with the applicable data protection rules and policies in the work rules.
r) Specific information to be provided to applicants	Applicants should also be informed about the processing of their personal data. For example, the following information can be included in the vacancy (or on a page to which reference is made): "*We process the personal data you provide us with (in writing or orally), which result from tests and which we collect ourselves, such as publicly available data on the Internet or when verifying references. We only use this data for the processing of your application, treat it confidentially and keep it for [12] months after your application. If we wish to add you to our recruitment reserve, we will ask your consent to do so]. You will find more information in our Privacy Policy [/link to website privacy policy], the principles of which apply accordingly."*

Name of the practical requirement	Required action
	Candidates, just like clients, can exercise their right of correction, inspection, etc. on the personal data collected by a Traditional Micro-SME. It is recommended to keep applicants' details for a sufficiently long period in case there is a subsequent discussion about, for example, discriminatory treatment in the application. Always verify national law to evaluate what personal data may be processed about job applicants, what their data protection rights are, etc. Also note that local data protection authorities may 'recommend/require' different applicable legal grounds to process personal data and may differ in opinion on how long applicant data may be stored after the job application is closed.

4.2 Key GDPR requirements for Traditional Micro-SMEs

4.2.1 Main processing purposes and categories of personal data

This CWA provides an overview of the main processing activities and purposes carried out by Traditional Micro-SMEs, as well as on categories of personal data. Table 2 below shows the main categories of data subjects linked to the processing activities of Traditional Micro-SMEs.

Table 2 — Processing Activities

Relevant categories of data subjects	Purpose of processing activity
Customers	Manage relationship with customers, such as: — invoicing — providing a product or service — advertising, marketing and promotion communications (email, calls or post) — promoting events — after-sales service — loyalty
Potential customers	Manage relationship with potential customers, such as: — advertising, marketing and promotion communications (email, online, calls or post) — promoting events
Employees	Manage employment relationship, such as: — employee administration — payroll management — employee evaluation — absence registration and management — training
Applicants	Manage relationship with applicants
Suppliers	Manage relationship with suppliers, such as: — purchase of services and/or goods

	— payment
Visitors	Manage persons visiting the Traditional Micro-SME, such as: - visitor registration - resource management (for example, meeting rooms and calendars)
Persons filmed by video surveillance tools	Security of goods and persons

4.2.2 Principles relating to processing of personal data

Article 5 GDPR sets the principles that shall be respected by all organizations processing personal data, regardless of the risk of the processing activities. They are thus also relevant for Traditional Micro-SMEs.

4.2.2.1 Lawfulness, fairness and transparency

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject[15]):

4.2.2.1.1 Lawfulness

Lawfulness entails that processing of personal data shall only take place if covered by at least one 'lawful/legal basis for processing'. Article 6 GDPR establishes six legal bases on which controllers shall rely. Processing operations under GDPR will only be lawful if they are based on one or more of the six legal bases exhaustively listed in Article 6(1) GDPR and take into account the limitations under Article 9 and Article 10 GDPR. Which one(s) of these legal bases is (are) most appropriate to use will depend on the Traditional Micro-SMEs' processing purposes (e.g., commercial, employee management) and relationship with the individual (e.g., contractual relationship, potential future customer). In today's business world, companies may conduct several processing operations for different purposes. This entails that Traditional Micro-SMEs may rely on different legal bases for their different processing activities.

i. **Consent**

Traditional Micro-SMEs may ask their customers, suppliers, prospective clients to consent to the processing of (some of) their personal data. To be valid, consent shall (cumulatively) be freely given, specific, informed, unambiguous and given by a statement or by clear affirmative action[16]).

It is important to take into account that processing based on consent does not provide a perpetual right to the Traditional SME to keep processing the personal data the consent relates to. First of all, consent can be withdrawn by the data subject at any moment (see below), putting an immediate end to the right to further continue the processing based on such consent if no other lawful basis for data processing exists. But even if the consent is not explicitly withdrawn, it is considered to degrade over time and the principles of data minimisation, storage limitation and accuracy (see below) may require stopping the consent-based processing or to ask for a new consent ('consent renewal' or 'reconsenting'). This will be the case, for example, if the context in which the consent was provided does not justify a continued processing or if the continued processing goes against the data subject's rightful expectations.

NOTE Practical example

---

[15]) Article 5(1)(a) GDPR.

[16]) Article 4(11) GDPR.

If a Traditional Micro-SME sends newsletters or direct marketing to existing or potential customers based on their consent, it will have to evaluate if this processing is still useful and complies with the expectations of the addressees. If an addressee has, for example, not reacted to a promotion, not opened a newsletter or has not shown any significant engagement in response to such mailings, the lawfulness of the further consent-based processing is at stake. In that case, the Traditional Micro-SME may, for example, sending the data subject a last message to assure that the data subject is still interested. This message can be a commercial message, explaining that the Traditional Micro-SME has noticed that it has not heard from the addressee for over a year, asking the addressee to confirm (by clicking a button) that it still wants to receive interesting promotions, the newsletter, etc. If the data subject does not confirm its consent, its personal data can no longer be processed on this basis and no more promotions, newsletter, etc. shall be sent.

In addition to the above, consent may also be requested for definite duration, in which case the validity of it automatically expires when the end date is reached. Further processing is only allowed in that case if a new consent is obtained prior to the expiration of the previous consent. Some data protection authorities would recommend this way of working. The upside of working with a fixed duration is that it is very clear during what period the personal data can be processed. The downside however is that reconsenting will be required for any consent-based processing, even if there's no doubt about the relevance, and that, if no new consent is obtained prior to the expiration data, any further processing will almost automatically become illegal. A challenge for the Traditional Micro-SME will also be to keep track of the dates on which consent was provided.

Table 3 below compiles the elements for valid consent under the GDPR explained above into a checklist that guides the efforts of Traditional Micro-SMEs to achieve compliance.

Table 3 — Traditional Micro-SMEs consent checklist

GDPR consent element	Traditional Micro-SMEs obligations
Freely given	Traditional Micro-SMEs shall assess whether there is an imbalance of power in their relationship with the individual. They shall not rely on consent as the lawful basis for data processing if there is an imbalance (notably in the employment context, except in specific circumstances), but have to look for alternative legal bases in Article 6. Traditional Micro-SMEs shall not make consent a precondition for performing a contract or service. Traditional Micro-SMEs shall ensure that individuals who refuse to give consent can do so without facing any detriment or negative consequences such as extra costs, downgrading of a service or not being allowed to participate to a contest.
Specific	Traditional Micro-SMEs shall ensure that they request consent for a specific purpose. Where a processing operation serves multiple purposes, or where a Traditional Micro-SME wishes to carry out several operations for several purposes, the Micro-SME shall give the option to consent separately to the different purposes. Traditional Micro-SMEs shall ensure that the requests for consent are easily identifiable, i.e., they are separate from the acceptance of other terms and conditions.
Informed	The information that shall be provided, includes specifically the following information.

	Traditional Micro-SMEs shall ensure that they present individuals with the following information when requesting consent: — Name of their company and of any third-party controller (this can be another company or organization) that will be relying on consent. — The types of personal data that will be collected and used (e.g., email, phone number, bank account). — The purpose of each of the processing operations for which they ask consent. — The right for individuals to withdraw consent at any time without any negative consequences. See below (Section 4.2.3.1) for the further information to be provided. Traditional Micro- SMEs shall always use clear and simple language that is easy to understand and tailored to their audience. They shall avoid the use of lengthy documents and legal jargon.
Unambiguous and active	Traditional Micro-SMEs shall not rely on pre-ticked boxes, opt-outs or any other type of default or passive consent to obtain consent. They shall rely on a clear positive act, i.e., 'a statement or a clear affirmative action', out of which clearly results that individuals opt-in, consent with the intended processing. Note that this clear affirmative action can be circumstantial and can, for example, be inferred from someone's actions, if, out of such actions clearly results that such person is consenting to the processing.
Explicit	Processing of sensitive personal data on the basis of consent shall meet the requirements for 'explicit' consent under the GDPR. In addition to the high standard applicable to 'consent' in general, explicit consent requires the data subject to explicitly confirm, in a statement, that he or she agrees with the intended processing of specific types of personal data. Contrary to 'consent' in general, 'explicit consent' cannot be inferred from 'a clear affirmative action'. This statement with the explicit consent can be written or oral, but the data controller must be able to prove that the 'explicit consent' was obtained, so some kind of materialization is required. It can also be provided in a digital way, for example by e-mail or by clicking an 'Accept' button under a statement in which is explicitly explained what processing the data subject explicitly consents to. In certain circumstances, it may even be required to have the consent statement (digitally) signed to obtain an explicit consent.[17)]

NOTE Soft opt-in and unsolicited e-mails

Following the rules on unsolicited communications set out in Art. 13 of the e-Privacy Directive (see 4.3), it is only allowed to communicate for direct marketing communications (including electronic communications, calls and facsimiles) through automated calling and communication systems if the addressees have given their prior consent to receive such communications.

17) For more information on the notion of 'explicit consent', see for example European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, adopted on 4 May 2020 and ICO, Guide to the General Data Protection Regulation (GDPR), What is 'explicit consent'?.

In derogation of this prohibition to send unsolicited e-mails, consent can be presumed to have been given, except if the addressees have opted-out of receiving such direct marketing communications. This is the so-called 'soft opt-in' principle. Processing based on the soft opt-in principle is actually not based on 'consent' as a legal basis under the GDPR, but on 'legitimate interest' (see 4.2.2.1.1, iv), as no valid consent in the meaning of the GDPR is provided.

Following this principle, a Traditional Micro-SME which has obtained electronic contact details (such as e-mail addresses) from its customers in the context of the sale of a product or a service, is allowed to use these contact details for direct marketing purposes:

- of its own *similar* products or services,

- provided that the customers are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use of their contact details:

o at the time of their collection ('opt-out'), and

o on the occasion of each direct marketing message based on the soft opt-in principle ('unsubscribe').

The soft opt-in principle can be implemented in a different way in different member states so national legislation has to be verified[18)] .

In practice, the soft opt-in principle allows for a Traditional Micro-SME, for example a local gift shop, to send e-newsletters to their existing customers with publicity for the products sold in the gift-shop, if the customer has had the chance to object against such use when the e-mail address was provided, for example via an 'opt-out' checkbox. If the owner of the gift shop has other business of provides other services, it cannot use the soft opt-in principle to send publicity for these other shops or services to the gift shop customers. Also, the gift shop has to ensure that each e-mail that is sent under the soft opt-in principle clearly provides the possibility for the customers to object against further use for direct marketing purposes (i.e., each e-mail must provide an unsubscribe link or button).

[18)] Note that the e-Privacy Directive is not directly applicable in the EU member states and has been implemented in the member states through national legislation. Consequently, national legislation must be verified to understand how the soft opt-in principle is implemented and applicable in specific member states. See 4.3 for more information.

ii. **Contract**

Micro-SMEs often process personal data of their customers, employees or suppliers in order to be able to **perform their contractual obligations** to these persons. Where this is the case, Micro-SMEs shall rely on 'contract' (Article 6(1)(b)) as the most appropriate legal basis. The contract legal basis shall also be used by Traditional Micro-SMEs carrying out **pre-contractual requests** from potential clients (e.g., a potential client asks a home repair Traditional Micro-SME to provide a quote to paint his house). Processing must be necessary for the performance of the contract or for addressing the pre-contractual request to be able to process the personal data on the 'contract' legal basis (= the data minimisation principle)[19]).This necessity limits the amount of personal data that can be lawfully processed under the 'contract' legal basis. Which personal data are necessary shall be determined on a case-by-case basis. Personal data that is not strictly necessary for these purposes, shall only be processed if another legal basis for such processing is available.

> ***Example***: Traditional Micro-SME A is a small shop selling cameras. Customer X buys two cameras that are currently out of stock and asks for them to be delivered to his home address when available. To deliver the goods, the Traditional Micro-SME A needs to process the customer's name and address – this is necessary to allow it to perform the contract.
>
> Traditional Micro-SME A wants to store and process the customer's data even after the delivery so as to send by mail promotional material such as leaflets and catalogues. This processing is not necessary for the contract's performance, and the Micro-SME must use a different legal basis that is appropriate to processing for marketing purposes, such as consent or legitimate interest.

iii. **Legal obligation** to which the controller is subject

In some circumstances, the law imposes the processing of personal data. For example, a Traditional Micro-SME needs the social security number of its employees to report to social security or tax authorities[20]). It shall therefore rely on the legitimate processing basis 'legal obligation' to process such social security number.

To rely on 'legal obligation' as processing basis, the obligation to process the personal data must be directly imposed by law (EU or national act) and be mandatory.

iv. **Legitimate interests**

Where personal data processing is necessary to pursue legitimate interests of a Traditional Micro-SME or a third party, those legitimate interests shall serve as the legal ground for such processing, provided that the interests and fundamental rights of the data subject (3.2) are not overriding (see below).

---

[19]) For more information about the data minimisation principle and how it applies on processing based on different legal bases, see 4.2.2.3

[20]) Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, adopted on 9 April 2014, p. 19.

The GDPR[21)] and the Article 29 Working Party[22)] provide the following examples of legitimate interest:

— processing for direct marketing purposes and other forms of marketing or advertisement[23)],

— processing to prevent fraud,

— employee monitoring for safety or management purposes and processing for physical security,

— IT and network security.

National legislation should be verified, as it may define situations in which, for example, the use of legitimate interests as legal ground may be excluded.

Necessity of processing. A Traditional Micro-SME relying on 'legitimate interests' shall demonstrate that the processing is necessary for the interests it wants to pursue and that the interest in itself is legitimate. Necessity requires the Traditional Micro-SME to consider whether there are less intrusive ways to achieve the same result.

The balancing test. Having identified a legitimate interest and demonstrated the necessity of the processing, the GDPR requires organizations to carry out a balancing test in which the interest of the Traditional Micro-SME's interest to process the personal data and the data subject's interest not to have its data processed, are balanced against each other. The test requires a **context-specific risk-benefit assessment** and implementation of potential **mitigation measures**.

Among the elements Traditional Micro-SMEs shall consider when assessing the balance, are[24)]:

— their relationship with the individual and whether the individual could expect them to use personal data in that way (for instance, in a company/customer relationship the customer could reasonably expect that the company may analyse and use his or her personal data for specific advertising purposes),

— the nature of the personal data processed and whether it is sensitive or private,

— the possible impact on individuals,

— whether the Traditional Micro-SME can adopt safeguards to minimize the impact.

Because of its context-specific nature and the need to carry out a balancing exercise, it is difficult to automatically assess whether or not a Traditional Micro-SME correctly uses legitimate interest as a legal basis.

---

21) Recital (47) GDPR.

22) Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, adopted on 9 April 2014, p. 25.

23) Some Member States (e.g. Lithuania) provide that the legal basis for processing personal data for direct marketing purposes can only be done based on consent. It is advised to always check the national legislation implementing the GDPR.

24) ICO, Guide to the General Data Protection Regulation (GDPR) – Lawful basis for processing: Legitimate interests.

v. **Protection of vital interests** of the data subject or of another natural person

The 'vital interests' lawful basis is to be used exceptionally, in actual situations of emergency, for example if someone faints and needs help or if someone is in danger. Thus, it shall not justify regular processing activities carried out by a Traditional Micro-SME.

vi. **Public interest and official authority**

Performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

'Public interest' mainly concerns processing by public authorities and is therefore of no real relevance for Traditional Micro-SMEs.

4.2.2.1.2 Fairness

Fairness requires controllers to only handle personal data in ways that the individuals would reasonably expect and to take account of the interests and reasonable expectations of data subjects. What is actually processed by an organization shall match up with what the organization declares (through its consent forms and privacy policies) to be processing. Fairness is closely interlinked with the lawfulness and transparency requirements.

It would for example be (among other things) unfair if a Traditional Micro-SME uses personal information from a data subject who requests a quotation, for example, the address of the data subject, to raise the applicable prices based on this information if it has not been made very clear to the data subject that this would be a price-determining element.

4.2.2.1.3 Transparency

Transparency is closely linked to, and even a prerequisite for fairness. It is also necessary for giving individuals meaningful control over their personal data and enabling them to exercise their rights. The transparency principle requires controllers to be open and clear about personal data processing: individuals should be made aware of the risks, safeguards, their rights in relation to the processing of personal data, why their data is being processed and who is processing it. The transparency obligations and specific information controllers have to communicate to individuals are further detailed in the GDPR (Articles 12-14).

Many obligations under the GDPR are (at least partly) implementations of the transparency requirement, such as the information obligations about data subject rights (see 3.2) and most of the data subject rights themselves (see 4.2.3.1), the general information obligations towards data subjects (see 4.2.3.2), the information obligation when processing personal data based on the consent of the data subject (see 4.2.2.1.1), etc. The transparency obligation leads to the requirement to provide more information on the processing of personal data, for example through the privacy policy (see 4.1, Table 1, a), the cookie policy (see 4.1, Table 1, b) and the notice when someone subscribes to a newsletter (see 4.1, Table 1, f).

4.2.2.2 Purpose limitation

Purpose limitation is the second core principle figuring in Article 5(1) GDPR. According to that principle, personal data shall be collected for specified, explicit and legitimate purposes and shall not be further

processed in a manner that is incompatible with those purposes[25]. Purpose limitation has two building blocks, briefly illustrated in the Table 4 below: i) purpose specification and ii) compatible further use[26].

Table 4 — The purpose limitation principle

Purpose limitation (GDPR)		
Specification	Personal data may only be collected for specified, explicit and legitimate purposes (…)	The data collected shall only be paired with the aims justifying their collection – e.g., a Traditional Micro-SME collects the customer's postal address to perform a delivery. The address shall as a principle only be used for this purpose. If the address is to be used for other purposes, these purposes shall also be communicated and a separate legal processing basis is required. A specified purpose shall be sufficiently defined to delimit the scope of the processing operations. An explicit purpose shall be sufficiently unambiguous and clearly expressed. A legitimate purpose is a purpose that is 'in accordance with the law' in the broadest sense. Law includes all forms of written and common law, primary and secondary legislation, municipal decrees, judicial precedents, constitutional principles, fundamental rights, other legal principles.
Compatibility	(…) and not further processed in a manner that is incompatible with those purposes.	The notion of 'further processing' refers to any processing operation occurring after the initial collection (e.g., storage, use, transfer, etc.). The GDPR calls for a case-by-case assessment of compatibility between the initial purpose of collection and further processing. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, shall take into account, inter alia: (i) any link between those purposes and the purposes of the intended further processing; (ii) the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; (iii) the nature of the personal data; (iv) the consequences of the intended further processing for data subjects; and (v) the existence of appropriate safeguards in both the original and intended further processing operations. Note that, even if the further processing purposes is considered to be compatible, the Traditional Micro-SME will still need to comply with all other GDPR requirements before it can actually process the personal

[25]) Article 5(1)(b) GDPR.

[26]) Article 29 Working Party, Opinion 03/2013 on purpose limitation, WP 203, adopted on 2 April 2013.

Purpose limitation (GDPR)		
		data for this purpose and will, for example, need to have a separate lawful processing basis for the further processing (see 4.2.2.1.1).

With purpose limitation being a fundamental principle of personal data processing, it is important for Traditional Micro-SMEs to understand that **the fact they have lawfully collected personal data for a given purpose does not entitle them to use the data for other purposes**. The GDPR places restrictions on further processing of personal data, and imposes notably to assess (and demonstrate, as per the accountability principle) the compatibility of further processing.

NOTE Practical examples

If a Traditional Micro-SME processes the social security number of its employees to communicate with the social security services, it cannot use this social security number for any other purposes, except if the requirements above are complied with (and, of course, if such processing is allowed by law).

Further processing for archiving purposes in the public interest, for scientific and historical research purposes or for statistical purposes should always be considered as compatible processing.[27)] Compatible processing is also any processing that is reasonably required under normal business activities or to support the service or products provided, for example, when a back-up is made of personal data of customer or when these are processed as part of an internal and external company audit, to the extent of course that the requirements mentioned above are complied with.

4.2.2.3 Data minimisation

Data minimisation requires controllers to ensure that personal data are "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*"[28)]. What data is deemed adequate, relevant and necessary depends on the specific purpose of processing. Having identified the specific purposes, Traditional Micro-SMEs shall make sure that they only process personal data that are suitable and reasonable to accomplish such purposes. They shall also assess whether the purposes could be achieved with either less personal data, with less intrusive data or with properly anonymised or pseudonymized datasets.[29)] In essence, the amount of personal data collected, the detailedness, the (internal and external) accessibility to such data and the data retention period shall be tailored to the identified purposes and all kept as low as possible at any time.

Whether it is necessary for a Traditional Micro-SME to process and store personal data depends on the specified purpose of processing. Traditional Micro-SMEs may process several types of personal data for a variety of purposes. Consequently, automatically assessing the necessity to process the stored data may

---

[27)] Recital 50 GDPR.

[28)] Article 5(1)(c) GDPR.

[29)] Despite pseudonymisation or anonymisation, third parties may still be able to re-identify the data subjects (and 'break' the anonymisation or pseudonymisation). For example, in 2019, researchers were able to correctly re-identify 99.98% of Americans in anonymous datasets, using 15 demographic characteristics (L. Rocher, J.M. Hendrickx and Y. de Montjoye, "Estimating the success of re-identifications in incomplete datasets using generative models", Nature Communication, 2019, vol. 10, nr. 3069, https://doi.org/10.1038/s41467-019-10933-3)

So, simply removing or obfuscating the direct identifiers will generally not be sufficient to avoid re-identification. Generally, especially when anonymizing, more than one anonymization technique should be applied to a data set to ensure proper anonymisation. How personal data should be duly pseudonymized or anonymized exceeds the scope of this CWA. For more information, see, for example the ENISA Recommendation, Pseudonymisation techniques and best practices, adopted in November 2019 or the WP29, Opinion 05/2014 on Anonymisation Techniques, adopted on 10 April 2014.

be challenging; the outcome (necessary vs. unnecessary data) may differ based on each Traditional Micro-SMEs' processing objectives.

At the same time, taking into account the most regular processing operations and purposes carried out by Traditional Micro-SMEs, it should be possible to extract the types of personal data that are necessary or not. An important task to be carried out within the technical work packages is the cross-linking of 'purposes' and 'necessary data'. It is important to note though that assessing 'necessity' in absolute terms may not be possible, because it really is context specific.

We can take as an example a Traditional Micro-SME processing data of applicants to a job position. One could argue that it is necessary for the Traditional Micro-SME to process a candidate's name, unique candidate number (if the applicant is allocated one), contact details, academic and professional data (CV). It could also be easily argued that, in principle, it is not necessary for a Traditional Micro-SME to process a candidate's social security number, bank details and marital status at the recruitment stage because those details are not needed for recruitment purposes. However, it is less evident whether or not processing information on an applicant's age, gender and nationality is necessary, as this information may be relevant in some contexts.

Table 5 below provides examples of possible necessary data and probable unnecessary data.

Table 5 — Data minimisation in practice

Purpose of processing	Possibly necessary data (if applicable)	(Probable) unnecessary data
Manage relationship with customers - invoice	Name (first name and surname) Delivery address Invoice mailing address A means of communication (email address or telephone number) VAT number	Date of birth Nationality Requiring both an email address and telephone number Marital status Age (but the fact that someone is an adult may be required to ensure contractual capacity) Gender/Sex
Manage relationship with job applicants	Name (first name and surname) Means of communication (email address, telephone number) Academic data (CV) Professional data (CV) Social media information NOTE Social media information should always be processed with precaution and care and within justified limits. In most cases, the processing hereof will only be possible on the legal basis 'legitimate interests'.	Gender Social security number Bank details Marital status Criminal record (except if specifically required for the function, verify national law) Social security number

The Traditional Micro-SME should verify at least once per year what processed personal data should be deleted, destroyed or anonymized.

Accuracy

The data accuracy principle provides that personal data shall be "accurate *and, where necessary, kept up to date*"[30]. Controllers shall take every reasonable step to ensure that inaccurate personal data are rectified or erased without delay. They shall also have appropriate processes in place to check accuracy, record the source of the personal data and keep the data updated. Ideally, forms should be created for updating data, procedures should be established for doing so, the person responsible for this task should be appointed (if relevant) and deadlines to review the accuracy of the processed personal data should be set.

The effort a controller shall make to keep personal data up to date depends on what the information is used for. The GDPR refers to taking "every *reasonable* step" to ensure accuracy. The reasonableness of the measures to be implemented depends on the purposes of the processing operations and the kind of personal data being processed. For instance, a Traditional Micro-SME shall update an employee's payroll data if it gives the employee a pay rise, or a customer's delivery address to ensure that products purchased are delivered to the right place. A Traditional Micro-SME dealing with sensitive data shall also pay particular attention to keep data updated, due to the importance of keeping such data accurate. On the other hand, a company keeping postal addresses for marketing purposes does not need to take extreme measures (such as tracing its customer) to check that its records are up to date; it shall be enough to update the records only if the customer informs it of the new address or if it results from other information that the address may be outdated[31], taking into account that personal data that hasn't been used for a longer time and no longer serves a legitimate purpose will need to be deleted anyway in accordance with the storage limitation principle (see below).

4.2.2.4 Storage limitation

According to the storage limitation principle, personal data shall not be kept for longer than is necessary for the legitimate purposes for which they are processed[32]. A longer-than-necessary storage period is permitted only for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of appropriate technical and organizational safeguards. These exceptions are of limited relevance for Traditional Micro-SMEs' processing activities.

The GDPR does not set a specific retention period for different types of personal data. National law however generally dictates that specific types of personal data need to be stored for a minimum duration, for example for tax or social security purposes. The appropriate retention period depends on how long an organization needs the personal data to achieve the specified processing purposes, including purposes imposed by law, and for how long it's justified to pursue such processing. That is why, also for the correct implementation of the storage limitation principle, it is necessary for a Traditional Micro-SME to first determine why it needs the data and if an obligation to store the data for a minimum period of time. It should then establish an appropriate Retention Policy and once the purposes of processing have been fulfilled, ensure that personal data are anonymised or securely deleted.[33]

We can take as an example a Traditional Micro-SME processing data of applicants to a job position. The potential employer generally has a legitimate interest to retain information about applicants after the candidate was refused, for example to contact such candidate later for another job or to avoid inviting the refused candidate when such candidate applies for another function in the future. How long such

---

[30] Article 5(1)(d) GDPR.

[31] ICO, Guide to the General Data Protection Regulation (GDPR) – Principle (c): Data minimisation.

[32] Article 5(1)(e) GDPR.

[33] See 4.2.2.3 and the footnote under that part with regard to pseudonymisation and anonymisation.

information can be retained will depend on the specific situation and the outcome of the balancing exercise. It may also depend on national legislation. However, in practice retention periods between one and two years are very common. A retention period of more than two years based on legitimate interests will be difficult to justify in most cases.

4.2.2.5 Integrity and confidentiality

The integrity and confidentiality principle is essentially about organizational and technical information security. It requires controllers to ensure appropriate security when processing personal data and protect the data against unauthorized or unlawful processing, accidental loss, destruction or damage[34]. The integrity of personal data would for example be compromised if a data breach occurs or if it can no longer be assured that the personal data has not been altered (intentionally or accidentally).

The 'confidentiality' component entails for example that, in principle, personal data shall not be available to everyone within an organization, but only to those needed for the processing activities to take place. It also entails that persons who do have access to the personal data, shall be bound by an appropriate confidentiality obligation. The integrity and confidentiality principle is further substantiated in the GDPR, notably in Articles 32-34 on security of processing and personal data breaches. According to the risk-based approach that is essential to applying the GDPR, the level of security to be implemented by an organization depends on the level of risk of its processing operations.

Also see 4.2.4.3 for more information about safeguarding the integrity and confidentiality of processed personal data.

4.2.2.6 Accountability

Accountability is two-fold, entailing an obligation for controllers to be both responsible for *ensuring* compliance and be able to *prove* compliance[35].

While accountability is an overarching principle, some specific measures organizations processing personal data shall or should adopt to ensure and be able to prove compliance can be found in Chapter IV GDPR, listing the obligations of controllers and processors. The requirements to implement technical and organizational measures (see 4.2.2.5 and 4.2.4.3), to be able to demonstrate that data subjects have been duly informed about the processing of their personal data (see 4.2.2.1.3), to be able to demonstrate that consent obtained for data processing complies with the legal requirements (see 4.2.2.1.1), to comply with data subject requests and to be able to demonstrate that a such requests were adequately addressed (see 4.2.3), to implement data protection by design and by default and prove how this was done, to keep records of processing activities (see 4.2.4.2), conduct a DPIA[36] (see 3.4) and appoint a DPO[37] (see 3.5) where needed are all manifestations of the accountability principle. The accountability measures to be adopted by each organization depend on the risk of processing, with higher risk bringing heightened obligations for controllers. Traditional Micro-SMEs, as defined in the CWA (see 3.11), are conducting low-

---

[34]) Article 5(1)(f) GDPR.

[35]) P. Voigt and A. von dem Bussche, The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International 2017.

[36]) A DPIA or a data protection impact assessment is an assessment that has to be performed under specific circumstances, notably when the processing of personal data is likely to result in a high risk to the rights and freedoms of natural persons (art. 35 GDPR).

[37]) A DPO or a data protection officer shall be appointed by organizations who meet specific requirements, because the legislators is of the opinion that these organizations (are likely to) engage in more riskful processing. This obligation does normally not apply to the Traditional Micro-SMEs (as defined under this CWA, see 3.11) and the subject is therefore out-of-scope of this CWA (see 1 Scope). For more information on DPO's, see Articles 37 to 39 GDPR.

risk processing and benefit from a (somewhat) smaller scale approach to accountability, as they may not need to hold ('full-fledged') records of processing (see 4.2.4.2), normally do not need to appoint DPOs or will only very occasionally need to perform DPIAs.

4.2.3 Rights of the data subjects

4.2.3.1 General

The GDPR strengthened previously existing rights of individuals vis-à-vis data controllers, while also recognizing new digital rights like the right to data portability. The data subject rights (see 3.2) aim to give individuals meaningful control over their personal data.

The GDPR provisions on the data subject rights are not risk-based, meaning that all organizations processing personal data, regardless of the risk of processing, shall accommodate these individuals' rights[38]. The GDPR calls for controllers to "*facilitate the exercise of data subject rights*"[39] and to phrase any communication to data subjects in a concise, transparent and easily accessible form, using clear and plain language[40]. In principle, there is a one-month deadline to react to any request made by the data subject, which may however be extended by two further months when justified by the complexity or number of requests. If a data subject exercises its data subject rights, the controller should verify the requesting person's identity to a reasonable extent, but not impose unreasonable obligations. For example, it shall not ask for the request to be sent by regular post if the registration is digital, nor shall it put in place other delaying or complicating mechanisms, such as requiring a copy of the identity card of the data subject, when this is not justified by (for example) the kind of services that are provided, the sensitivity or volume of the personal data, the secure and individualized access the data subject has to an online client zone, etc.

Finally, controllers are not allowed to charge money for addressing requests – rights shall generally be exercised free of charge[41].

Traditional Micro-SMEs shall provide their (potential) clients, suppliers etc. the means to exercise their rights. To this end, they shall establish processes to follow-up and effectively address data subjects' requests regarding the exercise of their rights, within the time limits prescribed by the GDPR. For instance, a company having a website can provide a specific contact form on its website for receiving requests. Companies without online presence can provide individuals with a telephone number, dedicated email address or postal address. Equally important is the establishment of internal procedures and allocation of responsibilities once a Traditional Micro-SME receives a request from a data subject: the Traditional Micro-SME, i.e. the members of its personnel, shall be able to recognize the request and its importance, identify the personal data concerned (what personal data relating to individual A it processes), examine the substance of the request (if individual A objects to processing, are there overarching reasons that would allow the Traditional Micro-SME to still process his or her data?) and importantly, effectively be able to address the request (if individual A rightfully requests the deletion of his or her data, the Traditional Micro-SME shall have the means to permanently delete the data).

---

[38]) With the exception of Article 22 – Right not to be subject to a decision based solely on automated processing, including profiling, which does not concern all Micro-SMEs but only those engaging in that type of processing.

[39]) Article 12(2) GDPR.

[40]) Article 12(1) GDPR.

[41]) Article 12(5) GDPR. That provision allows controllers to exceptionally charge a reasonable fee taking into account the administrative costs of taking the action requested where requests are manifestly unfounded or excessive, in particular because of their repetitive character.

The GDPR grants data subjects the following rights. Most of them are triggered once a Traditional Micro-SME receives a request from a data subject.

4.2.3.2 Right to be informed

Organizations shall inform individuals if they are using their personal data. The Traditional Micro-SME shall give this information at the time personal data is collected. Regarding the content of information to be provided, the GDPR distinguishes between cases where the personal data are collected directly from the data subject and cases where the personal data are obtained from another source (indirectly).

This information will normally be provided to the data subjects through the Traditional Micro-SME's privacy policy and privacy notices (see 4.1, Table 1, a)). Some example sentences are provided below that can be used to inform the data subjects about the topics mentioned below.

4.2.3.2.1 Information where personal data is obtained directly from the individual

a) Identification of data controller and data controller contact information

Name and contact details of Micro-SME, for example: *"We, Micro-SME A, registered in Brussels (Micro-SME A SRL., Chaussee de Waterloo 1, Brussels, VAT number BTW BE0000-000-000) process personal data for […]"*

b) (DPO) contact details

Very few Traditional Micro-SMEs are expected to appoint a DPO, as the requirement for a DPO applies to organizations carrying out processing activities that are not common to Traditional Micro-SMEs. If a DPO is appointed, at least one efficient way to contact him or her should be communicated (for example an email address). Traditional Micro-SMEs who did not appoint a DPO should include in their privacy policies an email, phone number (ideally) and postal address that individuals may use in order to contact them for data protection matters:

For example: *"For all matters regarding personal data and this privacy policy you can contact us using the address above or via email on the address: privacy@Micro-SME.com".*

c) Purpose(s) of processing

The Privacy Policy shall enable individuals to understand easily why their personal data is processed. Even though GDPR requires purposes to be 'specified', the level of detail a Traditional Micro-SMEs shall use when explaining a purpose depends on the complexity of its processing operations. Given that most Traditional Micro-SMEs do not engage in complicated processing (large scale, use of algorithms, profiling) a limited description of purposes may suffice:

"We process your email and postal address to be able to send you marketing and promotion communications"; "We process your basic contact details (name, email and postal address) because we need them to perform the contract between us, such as mailing you the products you purchase"; "As your employer, we need to keep and process information about you for employment purposes. Processing this information enables us to comply with the employment contract and to comply with any legal requirements".

d) Lawful basis for processing

Privacy policies should explicitly indicate which of the legal bases of Article 6 GDPR are applicable to the processing carried out by the Traditional Micro-SMEs. Note that if a Traditional Micro-SME relies on consent, the Privacy Policy shall include information on the right of individuals to withdraw consent and how this can be exercised.

If a Traditional Micro-SME relies on legitimate interest to process personal data, the Privacy Policy shall indicate what these legitimate interests are. When the legitimate interest invoked is 'marketing', the Privacy Policy shall include information on the right to object to direct marketing and how it can be exercised.

For example: *"We process your personal data for direct marketing and security of our systems based on our legitimate interest. You can ask us to stop sending you marketing messages at any time by following the opt-out (unsubscribe) links on any marketing message sent to you or by emailing privacy@Micro-SME.com confirming you wish to stop receiving marketing messages".*

e) Storage period and criteria

For how long will the personal data be processed? The GDPR requires specifying of a concrete storage period or at least the criteria used to determine that period. The Traditional Micro-SME shall in any case internally define specifically and in detail what storage periods apply. Also, if a data subjects request information about specific storage periods, the Traditional Micro-SME shall be able to provide this information. If personal data shall be retained by law during a fixed period, an extra delay is ideally added to allow the Traditional Micro-SME to organise the deletion of the personal data. If such extra delay is not provided for, the Traditional Micro-SME will have to delete such data on the day that it is no longer required to retain it. By, for example, always adding an extra delay of (if justifiable) one year, the Traditional Micro-SME can organise itself and delete once a year al the data that had to be retained until the year before.

For example: *"We retain your transaction data for a period of six months after performing our contract with you […]".*

"To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements. By law, we have to keep basic information about our customers (including Contact, Identity, Financial and Transaction Data) for six years after they cease being customers for tax and other legal purposes. Personal data that we are not required to process anymore, will be deleted not later than one year after that moment."

f) Information about the data subjects' rights and how to exercise those rights

By means of the Traditional Micro-SMEs' Privacy Policy, individuals shall be informed about their 'data subject rights' under the GDPR. It is important to note that the rights available to individuals may differ depending on the legal basis used for processing, as indicated below. Therefore, the information on the lawful basis provided in the Privacy Policy should be cross-checked with the information on rights. The impact of the data subject rights on processing based on the most common legal processing bases for Traditional Micro-SME's (see 4.2.2.1) can be found below (see Table 6). Processing based on legal obligations is not included in this overview, because national law can affect the applicability of data subject's rights on processing based on the legal processing basis 'legal obligation'.

Table 6 —Legal processing based on consent, 'contract' or legitimate interests and how they are impacted by data subject rights

Right			Consent	Contract	Legitimate interests
	Access		☑	☑	☑

	Rectification		☑	☑	☑
	Erasure		☑	☑	☑
	Restriction		☑	☑	☑
	Data portability		☑	☑	
	Object		Not applicable, except if used for direct marketing purposes. Consent can always be withdrawn however, what has the same result (=no more processing).	Not applicable, except if used for direct marketing purposes	☑

For example:

"Your rights:

Under certain circumstances, you have a right to:

1) *access your personal data, which means that you can ask us to provide you information regarding the personal data we hold about you;*

2) *request a copy of the personal data we hold about you;*

3) *ask that we correct your personal data if you can show that the personal data we process about you is incorrect, incomplete or outdated;*

4) *request the erasure of your personal data;*

5) *object to the processing of your personal data (e.g., for marketing purposes);*

withdraw your consent at all times (e.g., unsubscribe from a newsletter);

If you would like to exercise any of these rights, we ask that you send us an e-mail. You can reach us at privacy@Micro-SME.com.

We will promptly inform you of having received your request. We will notify you as soon as reasonably possible and at the latest thirty (30) days after having received the request. If we need more time to answer your request, we can extend this period by 2 months. We will also inform you of this within the aforementioned period.

If we consider your request invalid, we will inform you about this within the same delay.

g) Information about the right to lodge a complaint with a supervisory authority

Privacy policies shall mention the individuals' right to file a complaint with the relevant supervisory authority. Individuals have the right to address their complaint to any DPA (see 3.3). Usually, complaints are lodged with the DPA of the Member State where individuals reside.

h) If relevant, information about the use (or non-use) of automated decision-making, including profiling, as well as about the logic involved in automated decision-making. These practices most likely do not take place in Traditional Micro-SMEs

Automated decision-making consists of evaluating personal aspects relating to an individual based solely on automated processing. Profiling is a category of such processing and consists of any form of automated processing of personal data, evaluating personal aspects relating to an individual, to analyse or predict aspects concerning his or her personal preferences or interests, reliability or behaviour, location or movements. In the case of Traditional Micro-SMEs, the more likely situation is the use of profiling for direct marketing, for example through the use of social media or through marketing campaigns conducted by third parties and targeting a specific audience, consisting of existing and/or potential customers. In these cases, Traditional Micro-SMEs will act as controllers and shall take the applicable provisions into account.

i) Information about recipients or categories of recipients of the personal data

If the Traditional Micro-SME shares the personal data it collects with any other organization this shall be clearly stated in the Privacy Policy. It is allowed under the GDPR (and advised) to name 'categories of recipients' rather than listing the specific names of all companies having access to the data.

For example:

"For the employment, contractual and related purposes set out above, we will need to share your personal data with third parties. The categories of persons we share your personal data with are: our payroll provider, our pension's provider, work-related benefits providers, our IT service provider, service providers who support our general business processes if access is required for them to deliver such services, […]".

j) Information about international transfers

Controllers intending to transfer personal data to a third country shall inform data subjects about the transfer and safeguards they plan to implement to ensure protection of their data. For Traditional Micro-SMEs, international transfers could arise when they rely on non-EU based processors.

For example:

"Some of our external service providers, e.g. our website analytics provider, are based outside the European Economic Area (EEA), so their processing of your personal data may involve a transfer of data outside the EEA. Whenever we transfer your personal data out of the EEA, we adequately ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

We will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission. For further details, see European Commission: Adequacy of the protection of personal data in non-EU countries.

(…)

Where we use providers based in other countries, we may transfer data to them if they provide other safeguards that provide similar protection to personal data in accordance with the GDPR, such as, if applicable, by entering into the Standard Contract Clauses with them."

4.2.3.2.2 Additional information where personal data have not been obtained from the individual

It is possible that Traditional Micro-SMEs process personal data which they have not collected directly from the concerned individuals but from third parties (e.g., a marketing agency). The GDPR provides additional information where personal data have not been obtained from the data subject. Entities shall provide all information listed above and in addition, information about:

a) Categories of personal data involved

What categories of personal data does the Traditional Micro-SMEs process? Examples of personal data categories are contact data, transaction details, purchase history, technical information (IP address, login information, browser type and version) and details of visits to the Traditional Micro-SMEs' website.

b) Information about the source of the personal data

From where does the personal data originate?

For example:

"We collected the personal data about you directly from you or your interactions with us, our websites or social media sites. We also obtain personal data about you from [social media platform] (public profile, email and likes) when you use your [social media platform] account to login on our website."

If the data has been obtained from a third party, the Traditional Micro-SME should inform the data subjects concerned specifically from which source they obtained it.

Article 12(1) of the GDPR requires information relating to processing to be provided to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Accessibility and intelligibility are essential requirements under the GDPR: to fully comply with the GDPR, Traditional Micro-SMEs' information policies shall not only include all the elements of information mentioned in Articles 13 and 14, but also be drafted in a way that enables individuals to fully understand the information. Presenting information in an unclear, vague or non-transparent way constitutes a breach of the GDPR.

The Article 29 Working Party guidelines on transparency clarify the meaning of the following notions:

— The 'concise and transparent' element refers to the fact that controllers shall present the information efficiently and thereby avoiding the provision of excessive information (*information fatigue*). It also entails that the information on data protection matters shall be clearly differentiated from other non-privacy related information, such as contractual provisions or general terms of use. The use of layered information policies is recommended, as it allows individuals to easily navigate through the Privacy Policy and access more detailed information if they wish so.

— 'Intelligibility' mandates the use of clear and plain language. The Privacy Policy shall be understood by an average member of the intended audience, which in the case of Traditional Micro-SMEs will likely be consumers, suppliers, employees, in their vast majority non-privacy experts. The use of legal jargon and complicated sentences is thus to be avoided. Clarity also requires that information is concrete and definitive. Finally, for information to be intelligible for the intended audience, it shall also be provided in the language of the persons to whom it is addressed, or, under specific circumstances (for example communication to a specific group of highly educated persons in de professional context) a language that is supposed to be easily understood by them are that is generally used to communicate with them. National legislation may also need to be taken into account when deciding on the appropriate language, for example consumer law or employment law may also define what language should be used when these are applicable.

— 'An easily accessible form' means that "it should be immediately apparent to [individuals] where and how this information can be accessed". Traditional Micro-SMEs shall ensure that the entirety of information is available in one single place or one complete document, which can be easily accessed.

4.2.3.3 Right of access

This is the right of individuals to find out if an organization is using or storing their personal data in any way[42]. In practice, this right is exercised by asking an organization: i) whether it holds any personal data relating to a particular person and ii) to provide a copy of such data. This is commonly known as making a 'data subject access request', abbreviated as 'DSAR'.

Firstly, following a subject access request, individuals shall be made aware of the use of their personal data by an organization. The right of access goes beyond the provision of general information. Individuals shall be able to obtain access to the personal data processed and more precise information about the processing, notably about:

a) the purposes of processing;

b) the categories of personal data concerned;

c) the recipients or categories of recipients to whom the personal data have been or will be disclosed;

d) the envisaged period for which the data will be stored or criteria to determine that period;

e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

f) the right to lodge a complaint with a supervisory authority;

g) where the personal data are not collected from the data subject, any available information as to their source;

h) the existence of automated decision-making, including profiling.

4.2.3.4 Right to rectification

This is the right of individuals to ask for an organization to correct the personal data held or used by the organization[43]. It is a specification of the principle of data accuracy (see *supra*), which provides that personal data processed shall reflect reality at any time. Individuals can challenge the accuracy of their personal data and ask for it to be corrected. If the data is incomplete, individuals may also ask for the organization to complete it by adding more details.

The right to rectification is important because inaccurate data could have particularly negative consequences for an individual in certain cases. For example, the keeping of inaccurate creditworthiness data for an individual could deny him or her a credit. Accuracy is especially important for information of a sensitive nature.

4.2.3.5 Right to erasure

This is the right of individuals to ask for an organization that holds data about them to delete that data and, under some circumstances, the organization shall proceed to delete it[44]. This right is also referred

[42]) Article 15 GDPR.

[43]) Article 16 GDPR.

[44]) Article 17 GDPR.

to as “the right to be forgotten”. The GDPR does not specify the meaning of ‘erasure’ nor does it point out to specific techniques for erasing personal data.

The right to erasure applies in the following circumstances indicated in Table 7.

Table 7 — Applicability of the right to erasure

Personal data is no longer necessary for the original purpose of collection or processing	☑ Right to erasure
Individual withdraws consent to the processing *(where processing was based on consent)*	☑ Right to erasure
Individual objects to the processing and the controller does not have an overriding legitimate interest to continue this processing *(where processing was based on legitimate interest)*	☑ Right to erasure
Individual objects to the processing for direct marketing purposes	☑ Right to erasure
Controller has processed personal data unlawfully *(without an appropriate lawful basis)*	☑ Right to erasure
Controller has processed the personal data to offer information society services to a child	☑ Right to erasure

Note that in most of the circumstances described above, the data controller should in fact already have pro-actively ended the processing of the personal data, based on the lawfulness, data minimisation and storage limitation principles. Also note that some information shall need to be erased from use for a specific purpose, but that other legal grounds and purposes may justify for such information to be kept for these other purposes.

4.2.3.6 Right to restriction of processing

This right enables individuals to limit the way an organization uses their personal data when they are concerned about the accuracy of the data or how it is being used[45]. It can also be used to stop an organization deleting personal data. Restriction of processing does not require nor allow the organization to delete the personal data: a Traditional Micro-SME that complies with a rightful request to restrict processing, shall still store the personal data, but is not anymore allowed to use it for any other purpose.

A Traditional Micro-SME can for example be asked to temporarily limit the use of personal data when the data subject is considering a challenge the accuracy of the data, to object against the (unlawful) use of the data or may want to file a complaint at the DPA.

A Traditional Micro-SME can also be asked to limit the use of the data if the individuals concerned want the Traditional Micro-SME to keep it in order to prepare, exercise or defend legal claims.

As to the practical implementation of this right, the GDPR mentions some indicative methods by which the processing of personal data could be restricted. These include temporarily moving the data concerned to another processing system, making the data unavailable to users, or temporarily removing published personal data from a website[46] Therefore, a Traditional Micro-SME should implement technical means to ensure that while the restriction is in place, the relevant data cannot be processed or changed.

---

[45]) Article 18 GDPR.

[46]) Recital (67) GDPR.

4.2.3.7 Right to data portability

Data portability allows individuals to receive their personal data from a controller in order to transfer it to another service provider or request to send the data directly to such other service provider in a way that is machine-readable. This right only applies to data that is held electronically and that was provided to the controller by individuals, including data that has been gathered from monitoring individual activities when they are using a device or service (i.e. website usage data or raw data gathered from wearable devices). This right complements the individuals' right of access, by allowing them to receive personal data stored by a data controller for further personal use[47]). The fact that data subjects also have a right to transmit personal data from one data controller to another data controller empowers data subjects as consumers and enhances competition and avoids that individuals 'cannot' leave a supplier (vendor-lock-in), because all their usage data is stored by that supplier and they would have to 'start over again' when transferring to a new supplier. Transmitting personal data from one controller to another should be done using structured, commonly used and machine-readable formats, using secure methods[48]).

Only processing operations based on the individual's consent or on a contract to which the individual is party fall under the scope of the right to data portability[49]).

Data portability might be challenging for Traditional Micro-SMEs on a technical level, as data controllers should offer different implementations of the right. Article 29 Working Party indicates in its guidelines on data portability that controllers should explore and assess two different and complementary ways to make portable data available: a direct transmission of the overall dataset of portable data (or several extracts of parts of the global dataset) and an automated tool that allows extraction of relevant data[50]). However, as the business and services of Traditional Micro-SMEs will generally not really rely on personal data or be data focussed and will not process large volumes of data, data portability is in practice less relevant for most such enterprises, even though that they have to be able to comply with it under the circumstances set out above.

NOTE General example

A general example of when data portability would apply and be relevant, is when a data subject intends to switch or is switching from one energy providers to another. The data subject may want to submit its historical energy consumption data from its previous or existing provider to the potential new provider, to obtain a better pricing plan.

4.2.3.8 Right to object

Individuals have the right to object to the processing of their personal data in some circumstances)[51]). Once requested, the organization shall stop processing the data for that purpose unless it can give overriding and legitimate reasons to continue using that data despite the individual's objections. In order to deny a request, organizations have to engage in a balancing exercise, weighing the individual's interests and rights with their own legitimate grounds for processing: only if the latter overrides the

---

[47]) *Ibid*., p. 5.

[48]) *Ibid*.

[49]) Article 20(1)(a) GDPR.

[50]) Article 29 Working Party, Guidelines on the right to data portability, WP 242, as last revised and adopted on 5 April 2017, p. 16.

[51]) In the case of Micro-SMEs, the right to object only applies when the lawful basis of the processing is the legitimate interest of the controller, especially when the processing purpose is direct marketing.

former, a Traditional Micro-SME may refuse the right to object. In that case, the decision shall be explained to the individual along with information on their right to complain to the supervisory authority.

The situation is different, however, when a Traditional Micro-SME processes personal data for direct marketing on the basis of legitimate interests, which may be particularly relevant for Traditional Micro-SMEs. Traditional Micro-SMEs may process personal data of their customers for direct marketing without obtaining their consent, by relying on their 'legitimate interest' and the 'soft opt-in principle' (see 4.2.2.1.1, i). However, the GDPR establishes an absolute right to object to processing for direct marketing and an organization cannot invoke overriding grounds that prevail over the individual's rights and interests: *"[Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing"]*[52)].

Therefore, where an individual objects to the processing of his personal data for direct marketing, Traditional Micro-SMEs shall ensure that the individual's personal data are no longer processed for that purpose.

4.2.3.9 Right not to be subject to a decision based solely on automated processing, including profiling

The final right provided in GDPR is the right of individuals not to be subject to a decision that is based solely on automated processing if the decision affects their legal rights or other equally important matters[53)] (for instance, the automatic refusal of an online credit application, and e-recruiting practices without human intervention). This type of decision-making is only allowed where the decision is: (i) necessary for the entry into or performance of a contract; or (ii) authorised by domestic law applicable to the controller; or (iii) based on the individual's explicit consent. In the cases referred to in points (i) and (iii) the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

Individuals must be able to understand the reasons behind decisions made about them by automated processing and the possible consequences of the decisions and be able to object to profiling in certain situations, including for direct marketing.

In the case of Traditional Micro-SMEs this right could be of limited relevance. Traditional Micro-SMEs day-to-day data processing operations are unlikely to include such solely automated decision-making. The more likely situation is the use of profiling for direct marketing for example on social media, to own or potential customers through marketing campaigns that may be conducted by third parties and target a specific audience. In this case, both the platform the Traditional Micro-SMEs will remain controllers with regard to the processing of the personal data of the target audience.

4.2.4 Obligations of controllers

4.2.4.1 General

This section will focus on accountability requirements that are relevant for all Traditional Micro-SMEs:

— Keeping records of processing activities.

— Implementing (at a minimum) basic security measures to the processing.

---

52) Article 21(2) GDPR.

53) Article 22 GDPR.

— Establishing a procedure for managing personal data breaches and notifying the DPA and data subjects where necessary.

— Having contractual terms to regulate their relationship with data processors.

— Processing of special categories of data.

4.2.4.2 Documentation of processing activities (records of processing activities)

Any organization processing personal data should 'know its data'. Keeping track of the personal data stored or otherwise processed, information on the purpose of processing, to whom it is disclosed etc. is a prerequisite for implementing meaningful data protection measures and enabling individuals to exercise their rights. Accordingly, the GDPR places the obligation on both controllers and processors to keep records of their processing activities[54]). Records shall be kept in writing, including in an electronic form. They shall also be regularly kept up to date to reflect the current processing operations of an organization.

Because records maintenance may prove time-consuming and potentially costly, especially for (Micro-) SMEs having insufficient financial and human resources, the GDPR provides for an exception for any enterprise or organization with less than 250 employees. The exception however is very unlikely to result applicable, because any (Micro-)SME shall still keep records in the following situations:

- **For processing operations that are not occasional**

  Processing is 'occasional' if it only occurs once or for a short period of time and only plays a subordinate role on the activity of an organization[55]). Some of the processing operations carried out by Traditional Micro-SMEs cannot be classified as 'occasional' because of their continuity and regularity. For instance, even small businesses possibly process personal data regarding their employees or customers (e.g., addresses for delivery of orders) on a regular basis[56]). It should be assessed on a case-by-case basis whether these processing operations are occasional and whether or not they should be recorded. If records of processing need to be maintained, ideally all processing activities are listed in it (also the occasional ones), but that's is not an obligation.

- **For processing likely to result in a risk to the rights and freedoms of data subjects**

  Importantly, the Regulation here refers to 'risk' rather than 'high-risk', which possibly means that only activities with minor risks are excluded.

- **For processing of special categories of personal data or personal data relating to criminal convictions**

  Whenever a Micro-SME processes sensitive personal data the processing shall be documented.

The type of information that shall be documented in the records **differs** depending on whether an organization is a **data controller** or **data processor**. In line with the GDPR's approach to place more responsibilities on controllers, the latter shall keep more information in their records than processors.

---

[54]) Article 30 GDPR.

[55]) P. Voigt and A. von dem Bussche, The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International 2017, p. 45.

[56]) Article 29 Working Party, Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR, p. 2.

Table 8 shows the information of processing activities to be kept in records.

Table 8 — Information to keep in records of processing activities

Information to keep in records	Controller (Art. 30(1))	Processor (Art. 30(2))
Name and contact details of the organization, its representative and DPO	☑	☑
Purposes of processing	☑	
Categories of processing		☑
Description of categories of data subjects and of categories of personal data	☑	
Categories of data recipients	☑	
Transfers of personal data to a third country/international organization and suitable safeguards	☑	☑
Envisaged time limits for erasure of the different categories of data	☑	
General description of the technical and organizational security measures	☑	☑

Because documentation can help organizations comply with other GDPR provisions, such as to effectively implement the rights of data subjects and improve their personal data governance in general, most DPAs, including the ICO encourage all organizations to document other aspects of the GDPR as a best practice[57]. A Traditional Micro-SME should additionally document the location and source of the personal data, the lawful basis for the processing, the records of consent (which individual consented to which processing) and the contracts it has with processors.

To guide organizations in their compliance efforts, some DPAs have published documentation templates, guides and tools that could be easily downloaded or used by Traditional Micro-SMEs and their service providers[58].

As described above, maintaining records of processing is always a good idea, even if it is not imposed, because it will help the Traditional Micro-SMEs understand what processing activities they're engaging in and demonstrate their compliance in accordance with the accountability principle. Also, if a Traditional Micro-SME does not have much processing activities, drafting and maintaining records of processing activities will not be very difficult, nor will it take much effort.

4.2.4.3 Security of processing

All organizations processing personal data shall implement appropriate technical and organizational measures to ensure security of processing[59]. The GDPR embraces a **risk-based approach to security**, stipulating that in assessing the appropriate level of security an organization shall take into account the risks that are presented in the processing. Other factors to consider when determining the appropriate

[57]) ICO, Guide to the General Data Protection Regulation (GDPR) – Documentation.

[58]) See ICO, Documentation template for controllers and processors; APD, Registre des activités de traitement and AEPD, Facilita RGPD.

[59]) Article 32 GDPR.

security measures are the **state of the art** (what is the state-of-the-art technology for comprehensive data security?), the **costs** of implementation and the nature, scope and purposes of processing.

As to the concrete measures to be adopted, the GDPR does not come with an exhaustive list. It indicates, however, a few indicative measures that should be implemented as appropriate, such as the pseudonymisation and encryption of personal data, the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and the ability to restore availability and access to personal data in a timely manner in case of a physical or technical incident[60]).

Therefore, there is no one-size-fits-all solution to security; the appropriate security level is to be decided by organizations on a case-by-case basis upon performing a risk assessment of their data processing operations. Organizations engaging in high-risk processing activities (e.g. profiling) or processing special categories of personal data are expected to implement a more thorough security strategy than organizations in low-risk data processing only. The risk-based approach is particularly important for Traditional Micro-SMEs and the risk of each separate processing activity has to be assessed. As the processing activities carried out by most Traditional Micro-SMEs are low risk, they may not need to invest significant resources and time in security.

At the same time, all Traditional Micro-SMEs are required to implement adequate security measures according to their processing activities. Below, Table 9 and Table 10 provide with some organizational and technical measures that should be adequate for most of the Traditional Micro-SMEs[61]).

Traditional Micro-SMEs shall verify if under national law any minimum security requirements or recommendations exist, for example, under the form lists published by a national DPA.

Table 9 — Suggested organizational measures for security

Organizational measures	All Traditional Micro-SMEs shall ensure that their employees involved in processing/having access to personal data are informed about and duly aware of their obligations under data protection law, notably their duty on secrecy and confidentiality and that certain organizational measures automatically protect the processed personal data.
	— Personal data shall not be exposed to third parties. Staff shall be cautious and avoid unattended electronic screens and unattended paper documents in public areas. When they are absent from the workstation, the screen should be blocked or the session should be closed.
	— Both paper documents and electronic files shall be stored securely on a 24/7 basis. Secure storage entails the use of lockers or restricted access rooms.
	— Electronic documents or media such as USB sticks, CDs, hard disks etc. containing personal data shall not be discarded without guaranteeing their destruction.
	— Personal data or personal information shall not be transferred to third parties and staff shall pay attention not to disclose such data during telephone conversations or email exchanges.
	— The secrecy and confidentiality duties transcend the employment relationship. Employees remain bound by these duties even after their employment contract with the Traditional Micro-SME ends.

[60]) Article 32(1) GDPR.

[61]) The measures are based on the recommendations of AEPD on basic security measures to be adopted by organizations, given as part of the RPDP Facilita compliance report.

	— Employees are informed about the procedure to handle requests from data subjects to exercise their rights.
	— Employees are informed and able to understand what a personal data breach is and notify the management when they realise that a security breach occurred.
	— Management sets the example in the use of personal data and emphasises the importance of data protection.
	— Adequate policies are in place and duly communicated to the personal and inhouse service providers, such as an ICT-Policy, a Data Policy, a Password Policy, a Retention Policy, Data Breach Policy, BYOD Policy, Role Policy, etc.

Table 10 — Suggested technical measures for security

Technical measures	All Traditional Micro-SMEs shall implement certain technical security measures in their processing systems. These measures will essentially relate to the access to systems, networks and data, the storage of data, communication, Software Policy and control.
	Access to systems, networks and data
	— Protect the network environment from third party and unauthorised access, with detection. Access and access patterns are actively monitored and analysed and preservation/protective measures can be activated both automatically and manually. Externals only have access to a separate guest-network, not to the company network.
	— In general, an adequate Password Policy shall be set up, requiring anyone accessing a device (computer, smartphone, etc)., the company network (local, distant and virtual access) or online and local applications that process personal data to individually identify with a unique username and password (ensuring unambiguous identification). The password shall comply with the at the given moment current standards for safe-password usage under which the complexity, uniqueness and temporariness of passwords are guaranteed. Where possible and especially when accessing personal data or providing external access, this shall be combined with at least one other authentication method (active or passive 2-factor authentication).
Technical measures	— When a computer or other device is used for the processing of personal data and for personal use purposes, Traditional Micro-SMEs should create different profiles or different users for each purpose, i.e., to keep professional and personal uses of the device separate.
	— It is recommended to have profiles with administration rights for the system installation and configuration for certain persons and users without privileges or administration rights to access personal data.
	— Role Policy and authorisation management: access to the actual personal data will be limited to persons who need to have effective access to them ("need-to-know"), with individual access. For this purpose, job descriptions should reasonably identify the information that should be available to each profile. Others will only have access to pseudonymised or anonymised data (see also 4.2.2.3 and the footnote under that part with regard to pseudonymisation and anonymisation).
	— Detection of and automated actions against suspicious login attempts.

	— Provide active detection of and protection against threats from all forms of viruses, malware, attacks, etc.
	— Logging and auditing: access to personal data should be logged and monitored.
	— Access control: access to buildings and sensitive areas should be controlled and recorded electronically, mechanically and visually.
	— Access rights of persons leaving the company shall be revoked immediately.
	— Paper and storage media are destroyed before being disposed of.
	— Ensure that a (if possible physical) firewall protects the company network and that firewalls are activated on computers and devices in which personal data are stored or otherwise processed to avoid undue remote access to that data.
	Storage of (personal) data
	— Use state-of-the-art encryption to guarantee the confidentiality of the data to avoid unauthorized access to information, especially if it is necessary to transfer personal data outside the facilities where they are processed through electronic communication means. Make sure that any device on which personal data can be accesses, stored or processed is encrypted (including computers, handhelds, storage media, etc). Also refresh the encryption (key) periodically, to avoid, for example, risks linked to long-term encryption keys and revoke access by former employees.
	— Computers and devices shall be kept updated as possible and also be equipped with anti-virus systems to protect against malware and prevent, as far as possible, the theft and destruction of information and personal data. The anti-virus system should be updated periodically.
	— Provide intelligent organization of storage so that personal data and sensitive data are stored in a logical and user-friendly manner in the designated place.
	— Data retention policies shall be in place to comply with data retention periods and to identify which data may be outdated.
	— Backup periodically, on a second and separated medium other than the one used for daily work. The copy shall be stored in a safe place different to the one in which the computer with the original files is located and cannot have an open direct connection with the main system, so as to avoid contamination and allow the recovery of personal data in case of loss of information. The functionality of the back-up shall be tested.
Technical measures	**Communication**
	— Secure emailing and other communications with encryption, spam and phishing protection.
	— Personal data is only shared via a file-sharing platform, via temporary and/or personalised hyperlinks.
	— The website provides a secure connection.
	— Communication and logging on to the website always take place via a secure connection.
	Software Policy
	— A Software Policy is enforced so that only trusted and approved software is used.

	— Software is always kept up to date.
	Control
	— General monitoring and control measures that are in place to take into account the data protection rights of the employees and other monitored persons and their rights under local employment law.

4.2.4.4 Notification of personal data breaches

The GDPR introduces an obligation on all data controllers to report to the supervisory authorities personal data breaches[62]. It defines personal data breach as "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed*"[63]. The definition is particularly broad in that it does not require intent or negligence – it covers any security incident involving personal data no matter how or why it takes place, including accidental breaches. As emphasized by the ICO, a personal data breach entails more than just the loss or theft of personal data. Access to the data by an unauthorized third party, accidentally sending personal data to an incorrect recipient, having a person altering personal data without permission and even the loss of availability of personal data can constitute data breaches[64].

Because of the breadth of the definition, personal data breaches are likely to occur in any business. Like all organizations processing personal data, Traditional Micro-SMEs should be able to **prepare** for**,** instantly recognize and **respond** to a breach on a very short notice. Preparing means that, as a first step, the Traditional Micro-SME's staff is able to recognize a personal data breach and understands the broad scope of the breach notion under the GDPR. A response plan should then be in place for addressing any breach and the employees should be aware of how they shall act in accordance with this response plan.

The duty to report the breach to the supervisory authority does not always apply. The GDPR exempts breaches "*unlikely to result in a risk to the rights and freedoms of natural persons*" from the notification requirement[65]. To decide whether notification is necessary Traditional Micro-SMEs should have in place a process to assess the possible risk to individuals that the breach could cause. The criteria recommended by WP29 to guide this analysis include[66]:

— Type of the breach: a breach whereby confidential information is disclosed to unauthorized parties possibly has more serious consequence than a breach consisting of the temporary unavailability of the data in the local server.

— Nature, sensitivity and volume of personal data: breaches involving data about a person's health, ID documents details or financial data are likely to cause risk to individuals.

---

[62]) Article 33 GDPR.

[63]) Article 4(12) GDPR.

[64]) ICO, Guide to the General Data Protection Regulation (GDPR) – Personal data breaches.

[65]) Article 33(1) GDPR.

[66]) Article 29 Working Party, Guidelines on Personal data breach notification under Regulation 2016/679, WP250, adopted on 3 October 2017, pp. 20 – 22. We also refer to the ENISA-guidelines for useful information on how to evaluate the severity of data breaches, such as the 2013 guide 'Methodology for the Assessment of the Severity Level of Personal Data Breaches', available on the following website: https://www.enisa.europa.eu/topics/data-protection/personal-data-breaches (note however that this guide predates the GDPR and that this methodology is not considered mature enough by some data protection authorities).

— Ease of identification of individuals: where personal data are pseudonymised or encrypted, without the decryption key or pseudonym the data would be unintelligible to unauthorized persons. This reduces the possibility of individuals being identified in case of a breach and the risks they could face as a result thereof.

— Severity of consequences for individuals: where a breach could result in identity theft, fraud, damage to reputation etc. its consequences shall be considered particularly severe.

— Special characteristics of the affected individuals: breaches involving personal data of children or other vulnerable persons may entail higher risks due to the vulnerability of these individuals.

— Number of affected individuals: arguably, the more individuals are affected, the greater the impact a breach can have. At the same time, the number of affected persons shall not be the only criterion in the assessment of risk: a breach involving a very small number of persons can still entail a risk to their rights and freedoms, if for instance the data involved are of particularly sensitive nature.

— Special characteristics of the data controller: risks can vary depending on the organization processing the personal data. The likelihood of risk for individuals is greater for a small cabinet of doctors dealing with medical data than for a Traditional Micro-SME operating in the retail sector that suffers a breach involving its newsletter mailing list.

Following this assessment, if a Traditional Micro-SMS establishes that the breach is likely to result in risks for the individuals affected it shall notify the competent supervisory authority within 72 hours. The notification shall be accompanied with a series of information:

i) a description of the nature of the breach, with information (where possible) on the categories and approximate number of affected individuals and personal data records;

ii) a description of the likely consequences of the breach;

iii) an overview of the measures taken or proposed to be taken to deal with the breach; and

iv) the name and contact details of the DPO or other contact point where the supervisory authority could revert to obtain further information if needed.

Acknowledging that it can be impossible to fully investigate the breach within 72 hours, the GDPR allows controllers to provide this information in phases: immediately notify the supervisory authority and submit further information as soon as it becomes possible.

In addition to the obligation to notify the supervisory authority, **in certain circumstances** controllers are also required to **communicate the breach to the individuals affected**[67]. This applies if the breach is likely to result in 'high risk' to the individuals' rights and freedoms. To determine whether there is 'high risk' a Traditional Micro-SME shall consider the same criteria as explained above. Breaches involving confidential information, medical data and credit card details are likely to result in high risk.

The main purpose of notifying the affected individuals in those cases is to enable them to take steps to protect themselves from the possible negative effects of the breach (e.g. if they know that their credit card details have been stolen, they may cancel that card). Therefore, the Traditional Micro-SME shall describe the nature of the breach in simple and clear language, providing a description of the possible consequences for the individual, of the measures it has taken or proposes to take to deal with the breach, as well as the names and contact details of a contact person for the individual to get more information.

---

[67]) Article 34 GDPR.

A record documenting all data breaches, including those that do not need to be notified to the DPA, shall be held[68]. This record may be linked to (or even physically 'integrated' in) the records of processing activities (see above) and shall mention the facts relating to the personal data breach, the effects of the data breach and the remedial action taken.

4.2.4.5 Obligations when involving a processor

Many of the processing activities of small businesses may not be carried out by the business itself but are 'delegated' to a data processor. Traditional Micro-SMEs can rely on processors for payroll management, for processing online payments, for delivering orders etc. They can also use cloud service providers for email communications and storage of personal data. The GDPR allows the use of processors; however, data controllers have the responsibility to select processors who can provide 'sufficient guarantees' that they will meet the GDPR requirements and respect individuals' rights. Therefore, Traditional Micro-SMEs shall show diligence when choosing and appointing a third organization as processor.

The GDPR provides that whenever a controller involves a processor, a written contract shall be in place. The contract, often referred to as 'data processing agreement' or 'controller-processor agreement', shall enable both parties to understand their respective duties, responsibilities and liability with regard to the data processing.

Controller-processor agreements shall include all of the following information[69]:

— Subject matter and duration of the processing.

— Nature and purpose of the processing.

— Types of personal data involved.

— Categories of data subjects involved.

— Obligations and rights of controllers.

In addition, it is compulsory to include clauses stipulating the following:

— The processor shall only act on the written instructions of the controller. This will be a general clause, likely drafted in a broad way – e.g., the Data Processor may only act and process the Personal Data in accordance with the documented instruction from the Data Controller.

— The processor shall ensure that persons authorised to process the personal data will do so in a confidential manner (confidentiality clause) – e.g., the Data Processor undertakes to fulfil the following obligations: (…) To maintain a duty of secrecy with respect to the personal data to which the Data Processor has access.

— The processor shall take all measures required under Article 32 GDPR regarding security of processing (security clause) – e.g., the Data Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

---

[68]) Article 33, 5 GDPR.

[69]) Some DPAs and other organizations have shared template data processing agreements online, see for example: https://gdpr.eu/data-processing-agreement.

— The processor shall only engage a sub-processor with the prior agreement of the controller and will have a written contract in place to govern the processor-sub-processor relationship (sub-processing clause).

— The processor shall help the controller in addressing requests from individuals to exercise their rights (assistance clause – data subjects rights).

— The processor shall help the controller in meeting its GDPR obligations under Articles 32-36 (security of processing, data breaches notifications, data protection impact assessments) (assistance clause – security).

— The processor shall delete or return (at the choice of the controller) all the personal data to the controller after the end of the provision of services related to processing and delete existing copies unless EU or national law requires storage of the personal data (clause on deleting or returning personal data).

— The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations under the contract and allow (and enable) for audits and inspections by the controller or other auditor (audits clause).

Processing outside of the EU.

Extra care shall be taken into account when working with a non-EU service provider who will process personal data or with an EU-based service provider processing personal data outside the EU.

This will, for example, be the case in the following examples:

— The hosting service provider of the Micro-SME uses servers outside of the EU and does not guarantee that the Micro-SME's website, database, backups, etc. will only be hosted on servers located in the EU.

— The Micro-SME uses an automated mailing solution, that uses or may use servers located outside the EU to provide its services.

— The Micro-SME uses social media service providers of which the servers are or may be located outside the EU.

Such processing (e.g., transfer) of personal data outside of the EU is only allowed in the following circumstances, most relevant for Traditional Micro-SMEs[70]):

— **EEA**

  The transfer occurs to countries that are part of the European Economic Area (EEA), because the GDPR is directly applicable in these countries. This is the case for Liechtenstein, Norway and Iceland.

— **Adequacy decision**

  The European Commission has decided that the third country, a territory or one or more specified sectors within that third country ensure an adequate level of protection for personal data. In December 2020 the European Commission has recognized the following countries as providing

[70]) Art. 44 et. seq. GDPR.

adequate protection: Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay[71]).

Note that until recently, US based entities that were (self) certified under the Privacy Shield framework[72]) were also considered to provide adequate protection. The Privacy Shield framework was however invalidated by the Court of Justice of the EU in its so-called Schrems II decision of 16 July 2020[73]). Since that date and until a new adequacy decision would be in place, US-based entities can no longer be considered as providing adequate protection following an adequacy decision.

— **Appropriate safeguards – Standard Contractual Clauses**

Personal data can also be transferred if appropriate safeguards are in place and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. The appropriate safeguards most relevant for Traditional Micro-SMEs are the so called 'Standard Contractual Clauses' (SCC), which are stand clauses approved by the European Commission[74]).

Traditional Micro-SME's will generally not be in the position to negotiate service and/or data processing agreements with service providers based outside of the EU. Therefore, to comply with the GDPR with regards to the processing of personal data outside of the EU, Traditional Micro-SME's shall have to be careful to:

— either use services provided by data processors who will only process the personal data only within the EU, the EEA or countries that are considered providing adequate protection,

— either, if the personal data is processed in other countries, verify if adequate safeguards are in place, for example by applying the SCC.

In any case, it is the responsibility of the Traditional Micro-SME to ensure that the personal data are processed and transferred under the requirements described above.

4.2.4.6 Processing of special categories of data – additional requirements for Traditional Micro-SMEs

The GDPR recognizes that some personal data are, by their nature, particularly sensitive and merit enhanced protection because their processing could create significant risks to the fundamental rights and freedoms of individuals[75]). These are referred to as 'special categories of personal data' (another broader term commonly used is 'sensitive data'), and cover information revealing a person's racial or ethnic

---

[71]) See here for the full and up to date list of countries providing adequate protection: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[72]) See https://www.privacyshield.gov.

[73]) Schrems II, CJEU, Case C-311/18, 16 July 2020, https://curia.europa.eu/juris/documents.jsf?num=C-311/18#.

[74]) The applicable SCC are available here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en. The European Commission is currently updating the SCC, see here for more information: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries.

[75]) Recital (51) GDPR.

origin, political opinion, religious or philosophical beliefs, trade union membership, genetic and biometric data, health data and data concerning sex life or sexual orientation[76]).

The special regime applicable to special categories of personal data is as follows: in principle, their processing is prohibited under Article 9(1); this general prohibition is lifted only if one of the justifications enumerated in the Article 9(2) applies. The list of justifications is exhaustive, meaning that if an organization processes a special category of personal data in any other situation not covered by Article 9(2), the processing is unlawful. The processing of other types of sensitive personal data, such as data related to prior criminal convictions, social security numbers and location data, is often limited or even prohibited by other national or international rules.

Therefore, before starting to process sensitive data Traditional Micro-SMEs shall assess if these are covered by Article 9 and if any of the justification grounds apply. Not all grounds are relevant for Traditional Micro-SMEs or generally for processing for commercial purposes, but Traditional Micro-SMEs would most commonly be able to rely on the following grounds:

— Explicit consent of the individual (Article 9(2)(a)).

— Processing in the field of employment and social security law (Article 9(2)(b)). Micro-SMEs will be able to rely on this ground only if specific legislation is adopted in their Member State authorizing processing of sensitive data for those employment and social security purposes.

— Processing for the assertion of legal claims (Article 9(2)(f)).

— Processing for individual health care purposes (Article 9(2)(h)).

If any of the abovementioned grounds applies, a Traditional Micro-SME is permitted to process the sensitive data these grounds relate to. The processing shall also comply with all GDPR requirements applicable to 'regular data': for instance, Traditional Micro-SME shall ensure that the data is processed for a specified purpose and not further used (purpose limitation), that it only collects data necessary to fulfil those purposes (data minimisation) and that it informs individuals about the processing and on how to exercise their rights (transparency).

It is important to stress that according to Article 9(2) of the GDPR, the processing of special categories of data for purposes of employment and social security law, as well as for purposes for individual health care, is allowed only if it is authorized by national (or EU) law. Therefore, for assessing compliance with the rules on processing special categories of personal data, it is always necessary to consult national law in addition to the GDPR. Several Member States have adopted legislation implementing certain provisions of the GDPR, including the conditions for the processing of sensitive data.

4.3 Most relevant e-privacy requirements for Traditional Micro-SMEs

The GDPR is a **horizontal** piece of legislation that applies across sectors. The EU also has in place **sector-specific privacy legislation** which aims to supplement the horizontal framework: Directive 2002/58/EC ("e-Privacy Directive").

The Directive applies to the processing of personal data in connection with the provision of publicly available electronic communications services and public communications networks. In essence, the scope of the e-Privacy Directive is limited to the transmission of content, rather than the content itself.

---

[76]) *Ibid*.

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[77]). Article 5(3) requires Member States to ensure that "*the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing*".

This consent requirement does not apply to "*technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service*".

This means that consent will always be required to use cookies, except if the (very limited) exception grounds described above apply.

[77]) Article 5(3) of the e-Privacy Directive has general application and is not specific to providers of particular types of service.

Bibliography

[1] 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 (General Data Protection Regulation)

[2] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

[3] Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, adopted on 9 April 2014

[4] Article 29 Working Party, Opinion 03/2013 on purpose limitation, WP 203, adopted on 2 April 2013

[5] Article 29 Working Party, Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR

[6] Article 29 Working Party, Guidelines on the right to data portability, WP 242, as last revised and adopted on 5 April 2017

[7] ICO, Guide to the General Data Protection Regulation (GDPR)

[8] Voigt P., von dem Bussche A. The EU General Data Protection Regulation (GDPR) – A Practical Guide. Springer International, 2017

[9] European Data Protection Board. Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, adopted on 4 May 2020.