



GDPR

Information material
for SMEs

November 2020

DISCLAIMER

THE INFORMATION AND VIEWS SET OUT IN THIS REPORT ARE THOSE OF THE AUTHORS AND DO NOT NECESSARILY REFLECT THE OFFICIAL OPINION OF THE COMMISSION. THE COMMISSION DOES NOT GUARANTEE THE ACCURACY OF THE DATA INCLUDED IN THIS PAPER. NEITHER THE COMMISSION NOR ANY PERSON ACTING ON THE COMMISSION'S BEHALF MAY BE HELD RESPONSIBLE FOR THE USE WHICH MAY BE MADE OF THE INFORMATION CONTAINED THEREIN.

Table of Contents

Introduction	4
1. GDPR: a short overview	5
What is GDPR?	6
What is personal data?	6
What constitutes data processing?	7
What are Data Protection Authorities (DPAs)?	8
2. Links to Resources for Business and Organisations	9
What must your organisation do to comply with EU data protection rules?	10
3. Initiatives for SMEs	12

Introduction

Dear entrepreneur,

This paper is part of the ConsumerLaw Ready project addressed specifically to micro, small and medium-sized companies that interact with consumers.

The ConsumerLaw Ready project is a European-wide project managed by EUROCHAMBRES (the association of European Chambers of Commerce and Industry), in a consortium with SMEunited (Crafts and SMEs in Europe) and BEUC (the European Consumer Organisation). It is funded by the European Union with the support of the European Commission.

The ConsumerLaw Ready project aims to enhance the knowledge of traders, in particular of SMEs, regarding consumer rights and their corresponding legal duties.

The objective of the project is indeed to assist you in complying with the requirements of EU consumer law, by providing you with five different training modules. Each one deals with one particular topic of EU consumer law:

- Module 1 deals with the rules on pre-contractual information requirements
- Module 2 presents the rules on the consumer's right to withdraw from distance and off-premises contracts
- Module 3 concentrates on the remedies which traders must provide when do not conform with the contract
- Module 4 focuses on unfair commercial practices and unfair contract terms
- Module 5 introduces alternative dispute resolution and the Online Dispute Resolution (ODR) platform, an official website managed by the European Commission dedicated to helping consumers and traders resolve their disputes out-of-court.

The website consumerlawready.eu contains learning tools, such as videos, quizzes and an e-test through which you can obtain a participation certificate. You can also connect with experts and other SMEs through a forum.

GDPR – Information material for SMEs is a further resource whose aim is to provide you with a selection of available resources and links which could support you to find the correct information on the General Data Protection Regulation. It is not part of CLR training. The provided content is for information only and does not provide legally binding advice.

We hope that you find the information provided useful.

1. GDPR: a short overview

THE CONTENT PROVIDED IS FOR INFORMATION PURPOSE ONLY AND IT DOES NOT PROVIDE LEGALLY BINDING ADVICE.

FOR FURTHER INFORMATION, PLEASE HAVE A LOOK AT THE WEBPAGES OF THE EUROPEAN COMMISSION ON DATA PROTECTION ([HTTPS://EC.EUROPA.EU/INFO/LAW/LAW-TOPIC/DATA-PROTECTION/](https://ec.europa.eu/info/law/law-topic/data-protection/))

What is GDPR?

“Regulation (EU) 2016/679 of the European Parliament and of the Council¹, the European Union’s (‘EU’) new General Data Protection Regulation (‘GDPR’), regulates the processing by an **individual, a company or an organisation** of **personal data** relating to **individuals** in the EU.

It doesn’t apply to the processing of personal data of deceased persons or of legal persons.

The rules don’t apply to data processed by an individual for purely personal reasons or for activities carried out in one’s home, provided there is no connection to a professional or commercial activity. When an individual uses personal data outside the personal sphere, for socio-cultural or financial activities, for example, then the data protection law has to be respected”².

When the regulation applies A company with an establishment in the EU provides travel services to customers based in the Baltic countries and in that context processes personal data of natural persons.

When the regulation doesn’t apply An individual uses his/her own private address book to invite friends via email to a party that he/she is organising (household exception).

What is personal data?

“Personal data is any information that relates to an **identified or identifiable living individual**. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.

Personal data that has been de-identified, encrypted or **pseudonymised** but can be used to re-identify a person remains personal data and falls within the scope of the GDPR.

Personal data that has been rendered **anonymous** in such a way that the individual is not or no longer identifiable is no longer considered personal data. For data to be truly anonymised, the anonymisation must be irreversible.

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) (OJ L 119, 4.5.2016, p. 1).

² ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_en

The GDPR protects personal data **regardless of the technology used for processing that data** – it's technology-neutral and applies to both automated and manual processing, provided the data is organised in accordance with pre-defined criteria (for example alphabetical order). It also doesn't matter how the data is stored – in an IT system, through video surveillance, or on paper; in all cases, personal data is subject to the protection requirements set out in the GDPR³.

Examples of personal data

a name and surname;

a home address;

an email address such as name.surname@company.eu;

an identification card number;

location data (for example the location data function on a mobile phone) *;

an Internet Protocol (IP) address;

a cookie ID⁴;

the advertising identifier of your phone;

data held by a hospital or doctor, which could be a symbol that uniquely identifies a person.

Examples of data not considered personal data

a company registration number;

an email address such as

info@company.eu ;

anonymised data.

What constitutes data processing?

“Processing covers a wide range of operations performed on personal data, including by manual or automated means. It includes the **collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval,**

³ ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

⁴ Note that in some cases, there is a specific sectoral legislation regulating for instance the use of location data or the use of cookies – the ePrivacy Directive (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 (OJ L 201, 31.7.2002, p. 37) and Regulation (EC) No 2006/2004) of the European Parliament and of the Council of 27 October 2004 (OJ L 364, 9.12.2004, p. 1).

consultation, use, disclosure by transmission, dissemination or otherwise making available, **alignment or combination, restriction, erasure or destruction** of personal data.

The General Data Protection Regulation (GDPR) applies to the processing of personal data wholly or partly by automated means as well as to non-automated processing, if it is part of a structured filing system”⁵.

Examples of processing include:

staff management and payroll administration;
access to/consultation of a contacts database containing personal data;
sending promotional emails⁶;
shredding documents containing personal data;
posting/putting a photo of a person on a website;
storing IP addresses;
video recording.

What are Data Protection Authorities (DPAs)?

“DPAs are independent public authorities that supervise, through investigative and corrective powers, the application of the data protection law. They provide expert advice on data protection issues and handle complaints lodged against violations of the General Data Protection Regulation and the relevant national laws. There is one in each EU Member State.

Generally speaking, the main contact point for questions on data protection is the DPA in the EU Member State where your company/organisation is based. However, if your company/organisation processes data in different EU Member States or is part of a group of companies established in different EU Member States, that main contact point may be a DPA in another EU Member State”⁷.

[Find your National Data Protection Authority online⁸.](#)

Further information and material can be found here:

<https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules/>

⁵ ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_en

⁶ Please remember that to send direct marketing emails, you also have to comply with the marketing rules set out in the ePrivacy Directive

⁷ ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en

⁸ edpb.europa.eu/about-edpb/board/members_en

2. Links to Resources for Business and Organisations

What must your organisation do to comply with EU data protection rules?

Here below you can find a list of resources that can be useful for complying with EU data protection rules.

[Application of the regulation⁹](#)

[Who does the data protection law apply to?](#)

[Do the rules apply to SMEs?](#)

[Do the data protection rules apply to data about a company?](#)

[Principles of the GDPR¹⁰](#)

[What data can we process and under which conditions?](#)

[Purpose of data processing](#)

[How much data can be collected?](#)

[For how long can data be kept and is it necessary to update it?](#)

[What information must be given to individuals whose data is collected?](#)

[Overview of principles](#)

[Obligations¹¹](#)

[Controller/processor](#)

[Are the obligations the same regardless of the amount of data my company/organisation handles?](#)

[What does data protection 'by design' and 'by default' mean?](#)

[What is a data breach and what do we have to do in case of a data breach?](#)

[When is a Data Protection Impact Assessment \(DPIA\) required?](#)

[Data Protection Officers](#)

[What rules apply if my organisation transfers data outside the EU?](#)

⁹ ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation_en

¹⁰ ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr_en

¹¹ ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations_en



How can I demonstrate that my organisation is compliant with the GDPR?

Dealing with citizens¹²

How should requests from individuals exercising their data protection rights be dealt with?

What personal data and information can an individual access on request?

Do we always have to delete personal data if a person asks?

What happens if someone objects to my company processing their personal data?

Can individuals ask to have their data transferred to another organisation?

Are there restrictions on the use of automated decision-making?

Enforcement and sanctions¹³

Enforcement

Sanctions

Disclaimer¹⁴

Library of related documents¹⁵

¹² ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/dealing-citizens_en

¹³ ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions_en

¹⁴ ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/disclaimer_en

¹⁵ ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en#library



3. Initiatives for SMEs

Since the entry into application of the GDPR, the **European Data Protection Board (EDPB)** has adopted various opinions and guidelines to clarify fundamental provisions of the GDPR and to ensure consistency in the application of the GDPR.

The EDPB acknowledges that the implementation of the GDPR has been challenging, especially for small actors, most notably SMEs. Therefore, they have developed and recollected several tools to support SMEs in complying with the GDPR¹⁶.

Here below you can find a selection of Member State initiatives for SMEs (source: Contribution of the EDPB to the evaluation of the GDPR under Article 97). Wherever possible, we provide a link to the project to help you find additional information¹⁷.

AUSTRIA

- Publication of guidance material and FAQs on SAs website.
- Adoption of DPIA lists.

BELGIUM

- 2018: publication of a GDPR brochure for SME's.
- 2019: large-scale SME consultation to identify their needs concerning GDPR compliance.
- 2020: the BOOST-project, co-financed by the European Commission, will seek to produce guidance and tools for the topics of transparency, DPIA and the concept of controllership.

BULGARIA

- Permanent hot-line for consultations.
- [SMEDATA project](#)¹⁸: the aim is to ensure the protection of personal data through innovative tools for SMEs and citizens.
- [GDPR in your pocket](#)¹⁹, a mobile application.

CZECH REPUBLIC

- Publication of EDPB Guidelines & Opinions on the SA's website.
- Adoption of DPIA lists (35.4 and 35.5 GDPR)
- Hotline for consultations.

GERMANY

- Permanent individual advice upon request by controllers, processors and data protection officers of SMEs, including start-ups.

¹⁶ Contribution of the EDPB to the evaluation of the GDPR under Article 97, February 2020
edpb.europa.eu/sites/edpb/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf

¹⁷ The text is quoted here from the EDPB contribution, including any acronyms and abbreviations that were contained in the original text.

¹⁸ smedata.eu

¹⁹ smedata.eu/index.php/2019/09/30/the-beta-version-of-the-smedata-mobile-application-is-now-available-for-free-download

- Publication of a wide range of guidance material and Q&As aimed for SMEs on various websites of DE SAs.

DENMARK

- Development of an interactive guide to assist SMEs with their GDPR compliance (the Privacy Compass).
- Publication of information addressed to SMEs on its website.
- Telephone hotline.
- Podcast with topics focusing on SMEs
- Checklists, FAQs, guidelines and other publications.

ESTONIA

- Guidance materials and consultations.
- Joint-trainings with different professional associations.
- Hot-line for data subjects and data controllers/processors.

SPAIN

- [Hotline](#)²⁰ for consultations for controllers and processors.
- Consultation with SMEs to know the main impact of GDPR.
- Publication of several [guidelines](#)²¹ and [tools](#)²² aimed at supporting SMEs in their adaptation to the GDPR.
- [FACILITA RGPD](#)²³: an online questionnaire with which companies and professionals can verify through a series of questions that the processing operations they carry out can be considered of low risk and obtain the minimum essential documents to facilitate the application of the GDPR at the end of the test.

FINLAND

- Issued guidance materials and provided feedback on sector-specific guidance.
- Hotline for consultations (data subjects and stakeholders) and hotline for controllers and processors.
- In the process of finalizing a DPIA-tool directed to the needs of SMEs.

FRANCE

- A [dedicated pack available on the website of the CNIL](#)²⁴, with a practical guide and forms.
- A [video](#)²⁵ with a Youtuber on how to apply the GDPR.
- A simplified register (available [in French](#)²⁶ and [in English](#)²⁷).
- A [MOOC](#)²⁸.
- [Specific content concerning security and a guide](#)²⁹.

²⁰ aepd.es/herramientas/informa.html

²¹ aepd.es/guias/index.html

²² aepd.es/herramientas/index.html

²³ aepd.es/es/guias-y-herramientas/herramientas/facilita-rgpd

²⁴ cnil.fr/fr/la-cnile-et-bpifrance-sassocient-pour-accompagner-les-tpe-et-pme-dans-leur-appropriation-du-reglement

²⁵ cnil.fr/fr/video-le-youtubeur-cookie-connecte-repond-vos-questions-sur-larrivee-du-rgpd

²⁶ cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement

²⁷ cnil.fr/en/record-processing-activities

²⁸ cnil.fr/fr/la-cnile-lance-sa-formation-en-ligne-sur-le-rgpd-ouverte-tous

- Other general tools, widely used by SMEs:
 - a hotline;
 - FAQs on the website;
 - the DPIA software;
 - the white list for processing exempted from DPIA;
 - a notification form available online (developed within the EDPB).

CROATIA

- Promotion of the EDPB guidelines, opinions, promo materials among the SMEs.
- Publication of the DPIA list.
- In cooperation with partners from Ireland and Belgium, planned implementation of a project co-financed by the European Commission, titled ARC- Awareness Raising Campaign for small and medium enterprises. The main objectives of the Awareness Raising Campaign for SMEs (ARC project) are: raising awareness of SMEs about the GDPR obligations, helping SMEs to comply with those obligations and answering their questions about the implementation of the GDPR. These objectives will be achieved through the following activities planned within the project: running a survey to identify SMEs needs, preparation of educational materials about the GDPR (based on a previous survey of needs), organization of onsite consultations in all major Croatian regional centres, during which SMEs will be able to receive direct support to resolve their specific problems, organization of two international conferences to exchange experiences and show best practices and preparation of publications on outcomes of the project. The overall expected direct result of the ARC project is increased knowledge and understanding among SMEs on the principles of data protection.

HUNGARY

- NAIH is operating a hotline for SMEs between 15 March 2019 and 15 March 2020 to assist them in compliance with the GDPR. In this period NAIH provides information for SMEs regarding the interpretation and proper application of the GDPR. This EU co-funded project is taking place in a framework of a consortium including several stakeholders. The responses shall be formulated to provide graspable assistance in the interpretation of law applicable relevant to the merit of the question, and to highlight the relevant aspects in the application of law related to the given question, the factors to be considered among them, and their significance. The answer shall contain no opinion as to the lawfulness of any concrete data processing.
- The consortium is also drafting an innovative handbook for SMEs based on the questions and answers in the indicated period.

IRELAND

- A joint initiative with HR SA for the next 2 years, to provide support to the SMEs, supported by a Commission grant.
- Guidance on the website.

²⁹ cnil.fr/fr/securite-des-donnees

ITALY

- SMEDATA project: development of a mobile application as a free open-source software tool assisting citizens and SMEs in understanding and complying with GDPR.

LITHUANIA

- Publication of guidance material and FAQs on SAs website.
- SolPriPa project, promoting high standards of data protection as a fundamental right and central factor of consumer trust in digital economy, co-financed by the European Commission.

LUXEMBOURG

- Providing general advice via e-mail and phone hotline for SMEs contacting CNPD for guidance.
- Monthly newsletters to 1700 subscribers.
- A simplified and structured form for Databreach notifications designed in a way to guide controllers in their analysis of the data breach;
- Development of a GDPR maturity self-assessment tool (for businesses in general) which is an innovative, intuitive solution enabling users to check the level of coverage of their organizations against the GDPR requirements.
- Joint trainings for business owners of SMEs with their professional business association on identifying their stakeholders in the context of GDPR.
- Publication of guidance for employers and employees on surveillance in the working place.

LATVIA

- Since 2018: LV SA participates as the Leading Authority in the European Commission's Project on "General Data Protection Regulation possibilities and responsibilities for small and medium-sized enterprises (SMEs); rights and risks for minors (DPSME)". The Project aims to improve the readiness of small and medium-sized enterprises and to fulfil the requirements of the GDPR. The project's time frame is 24 months (01.12.2018 - 30.11.2020).
- a [Guide to Data Processing](#)³⁰ for SMEs.
- Inspectorate participates also in a project of the European Commission - GDPR Compliance - Cloud Platform for Micro Enterprises as a partner for the Leading authority – Spanish Company. The time frame of the Project is 01.05.2018-31.10.2020 and the aim is to develop a cloud platform and a handbook for micro-enterprises to ensure compliance with GDPR.
- The most common way of providing the information is also the Inspectorate's ability to provide a written answer to a person's applications, on-the-spot consultations (on previously agreed time frame) and phone consultations. Any interested person (also SMEs) is welcomed to clarify information on different questions on personal data protection.

MALTA

³⁰ dvi.gov.lv/en/general/recommendation-celvedis-data-apstrade-smalland-modernem

- Development of a 24 months project which, in part, is specifically dedicated to assisting SMEs in complying with the GDPR. EU-funded project (an online compliance tool will be developed).

NETHERLANDS

- Starting in 2018 an information campaign to inform the general public and organisations about the upcoming GDPR, [Hulp bij privacy](#)³¹ (help with privacy).
- Several tools were developed. For example <https://rvo.regelhulpenvoorbedrijven.nl/avg/#/welkom>. Step by step organisations could find out what to do to prepare for the GDPR.
- Online privacy videos.
- [Webapp](#)³², smartphone challenge.
- Educational material to be used in combination with smartphone challenge.

POLAND

- Infoline and website, which provide information on the latest positions and communications of the PL SA and access to the database of administrative decisions.
- Thematic studies on the [website](#)³³, including guidelines and manuals.
- Cooperation with DPOs.
- Special hotline for consultations.
- Thematic newsletters (more than 6000 subscribers).
- Monitoring of the legislative process and issuance of opinions on the compliance of the draft regulations with the data protection law.

PORTUGAL

- Development of two models of the register provided by Article 30 GDPR (one for controllers and the other for processors).
- General basic guidance through FAQs section in its website.

ROMANIA

- In 2018, RO SA has launched Guidelines for the application of the General Data Protection Regulation by the data controllers issued by the National Supervisory Authority for Personal Data Processing.
- In 2018, RO SA adopted Decision no. 174 of 18 October 2018 on the list of the kind of processing operations which are subject to the requirement for a data protection impact assessment.
- In 2019, RO SA has launched Guidelines on questions and answers regarding the application of Regulation EU 679/2016.

SWEDEN

³¹ hulpbijprivacy.nl

³² jetelefoondebaas.nl

³³ uodo.gov.pl/

- Development of an interactive guide for SMEs to assist them with GDPR compliance.
- A national privacy report illustrated the different problems for SMEs to comply with the GDPR.
- The website, checklist, FAQs, guidelines and other publications are tailor-made to have an easy and understandable language, specifically bearing in mind data subject and SMEs.

SLOVENIA

- Support for SMEs is provided by guidelines and other materials/activities
 - guidelines: 6,
 - infographics: 6,
 - forms (templates): 6,
 - pro bono lectures for data controllers and processors: more than 150,
- An EU project RAPID.si is also being implemented, with the focus on SMEs, providing:
 - articles in SME related magazines: 8,
 - monthly LinkedIn publication and newsletter for SMEs,
 - a dedicated SME helpline: 1008 calls received
 - a [website](#)³⁴ specifically oriented towards SMEs.
 - seminars and lectures for SMEs, organized in partnership with the Chamber of Commerce and Industry of Slovenia.

SLOVAKIA

- Publication of EDPB Guidelines & Opinions on the SA's website.
- Adoption of DPIA lists (35.5 GDPR) .
- Providing advice via email to SMEs that contact the SK SA for guidance.

³⁴ upravljavec.si



Consumer Law Training for European SMEs