

Your Data Protection Compliance Handbook.

4th Edition

01/2022

GDPR compliance made easy.

- An instruction manual for those *without* in-depth data protection knowledge
- Over 200 pages of practical information and instructions how to do the job
- Shift more DP work to local staff
- For demonstrating your compliance (principle of "accountability")
- Customize as desired
- With many ready-to-go templates
- Updates offered on an ongoing basis

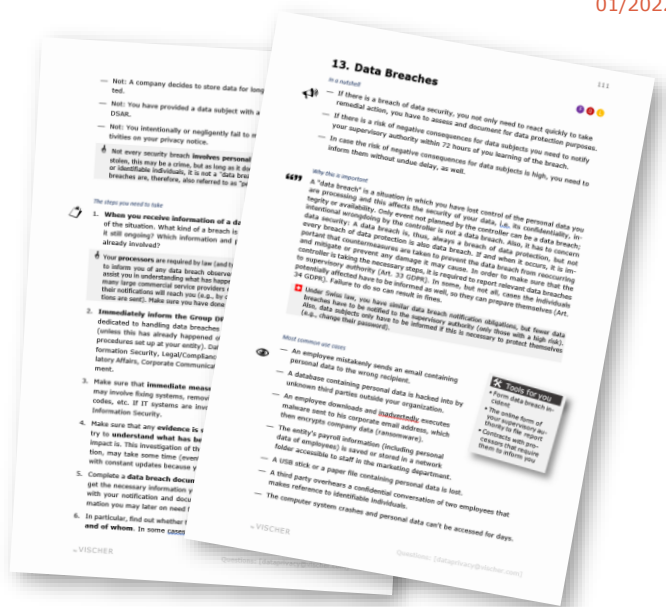


Table of Contents

1.	INTRODUCTION	10
2.	OUR DATA PROTECTION COMPLIANCE SETUP	11
3.	FIRST STEPS	13
4.	RECORDS OF PROCESSING ACTIVITIES	20
5.	POLICIES ON DATA PROTECTION COMPLIANCE	27
6.	DATA PROTECTION TRAINING	34
7.	COMPLIANCE WITH PROCESSING PRINCIPLES	38
8.	DATA PROTECTION STATEMENTS	52
9.	USE OF PROCESSORS	60
10.	JOINT CONTROL	74
11.	CROSS-BORDER TRANSFERS OF DATA	86
12.	DATA SUBJECT ACCESS REQUESTS (DSAR)	107
13.	DATA PROTECTION IMPACT ASSESSMENTS (DPIA)	117
14.	DATA BREACHES	128
15.	INTERVENTION BY DATA SUBJECTS	142
16.	DATA PROTECTION OFFICER (DPO)	160
17.	MARKETING COMMUNICATIONS	168
18.	WEBSITES AND APPS	181
19.	OTHER SITUATIONS IN DAILY BUSINESS	194
20.	GLOSSARY & ABBREVIATIONS	208
21.	LINKS FOR YOU	233
22.	TOOLS FOR YOU	236

All key topics covered.

Covers day-to-day GDPR obligations of your entity, including governance
 VISCHER DPC Handb
 ook_Info.pdf

- With many templates and checklists and other tools for you to make your life easier
- You can remove and rearrange all topics as per your own needs

Designed for easy navigation.

- Each chapter is structured in the same manner
- In a nutshell
- Why the topic is important
- Practical tools
- Most common use cases
- Step-by-step instructions

	but IGDTAs are more popular because they are easier to implement.
ISO 27001	The most widely established international standard for data security. It describes an information security management system (ISMS), i.e. a concept to make sure that an organization has the necessary data security in place. It does not say which specific data security measures an organization has to implement, but apart from defining how to govern data security, it in an annex lists over 110 "controls" across over a dozen areas such as "Asset Management", "Access Control", "Cryptography", "Operational Security" or "Supplier Relations" that define which practices or safeguards should be performed to ensure data security. They are implemented in the form of technical and organizational measures of data security (TOMS), e.g., backups, antivirus software, policies, NDAs, SLAs, CCTV cameras, locks, awareness trainings. A company can have its ISMS audited (including for effectiveness) and certified. When relying on ISO 27001 certifications, it is important to understand the scope (i.e. which processing activities are covered) and that the ISMS has also been verified for effectiveness.
Joint Controller	Two or more entities jointly determining the purposes and means of a data processing activity (instead of each controller holding the <i>entire</i> part of the data processing

- Glossary with over 20 pages

7. Compliance with Processing Principles

In a nutshell

- Data protection law requires that each activity involving personal data has a legal basis and complies with certain principles.
- Together with the business, you need to check and document compliance with these prerequisites.
- Since you cannot do all at once, you should follow a risk-based approach.

Why this is important

Data protection is about respecting the privacy, personality and the right to informational self-determination of the individuals about whom we process data (i.e. data subjects). To make this happen in practice, data protection law defines a small number of "principles" that make it easier to achieve this goal: If you comply with them, the processing of personal data is in principle ok. One of these principles is that each processing requires a "legal ground", i.e. a sort of justification why you should be allowed to proceed with the processing. This justification needs to be documented. If the data protection authorities receive a complaint, they will check whether such legal grounds is given and whether the principles have been complied with. If not, your entity can get fined and ordered to change or stop your processing of personal data.

Most common use cases

- The business asks you whether a particular project involving personal data is permitted under data protection law.
- You run into a processing activity at your entity that does not comply with the principles.
- You get a complaint from a data subject about a certain processing and are unsure whether it is compliant.
- You are asked or required to perform a data protection impact assessment (see chapter 13).
- You validate a risky processing activity proactively.

The steps you need to take

1. Get a **description** of the data processing project to understand what is going on or what is planned (→ Box).
2. Determine whether **personal data** is involved at any stage. If not, data protection law does not apply, and you do not need to proceed any further.

Tools for you

Questions to ask:

- Categories of data?
- Individuals affected?
- Data sources?
- What is done with it?
- Primary purposes?
- Secondary purposes?
- Who is in charge?
- Who has access?
- Which IT application?
- Who runs it?
- Who receives data?
- In which countries?
- Why is it justified to process the data?

Tons of supporting information.

- Over 120 questions and answers across all chapters
- Do's and Don'ts in every chapter
- Many useful hints based on practical experience
- Tells your people when to consult your experts
- Where the revised Swiss DPA deviates from the GDPR

Do's	Don'ts
<ul style="list-style-type: none"> — Take a risk-based approach to set priorities on which processing activities you look at and where you insist on improvements; "risk" means risk to the data subject, not to the company. — Document the compliance checks and in particular the legitimate in- 	<ul style="list-style-type: none"> — Don't perform compliance checks alone, always do it with the relevant people from business, because they have to take the responsibility and only they know the necessary answers — Don't expect that each data processing is fully compliant; hardly

Questions and Answers

Q18. How do we get consent in a valid manner?

A: Under the GDPR, consent is only valid if it is "freely given, specific, informed and unambiguous" (Art. 4 (11) GDPR). This does not mean though, that you have to get

When you should ask for legal or other advice

- The request occurs in the context of a (possible) **legal dispute**.
- The request is asks for a **broad range** of information and you do not yet know how to handle such a situation.

... are that the request is a mere **nuisance request** or not justified and ... rmine whether you can refuse it right away.

The term **"deletion"** does not necessarily require *physical erasure* of data. Personal data is usually considered to be deleted when it is no longer accessible, with reasonable means, to identify the persons to whom the data relates. This can also be achieved by properly anonymizing information or by "logical deletion" means physically the personal data is moved to another provider or data portability.

+ Under Swiss law, the same rules and conditions. Consequently, both the Swiss DPA and the GDPR apply to the processing, as well.

19. Other Situations in Daily Business

Customer Events	
When organizing a customer event, you will have to send invitations. If you send them by e-mail, make sure you comply with the restrictions on marketing e-mails (see chapter 17).	
Put a reference to the data protection statement on the invitation that describes the data you will be processing for the event (such as guest lists, dietary requirements, photographs) and the purposes you wish to use it for (including company publications, social media).	
In the invitation reply form (or corresponding only form), only ask for the information you absolutely need. If this includes sensitive personal data (such as certain dietary requirements, indicating religious belief), include the sentence "I consent to the processing of the above data for the purpose of [describe purpose], which I can withdraw at any time by contacting [contact details]." If consent is withdrawn, you have to delete such data.	
Use the data you received only for the purposes you have indicated on the invitation reply form (e.g., organizing the event). If you want to include it also in your CRM, say so.	

Tools ready to use in practice.

- Separate section covering data protection aspects of daily business situations
- Over two dozen templates, forms, samples, checklists and other documents
- Tools complement the step-by-step instructions in the chapters
- They make it easy for you to document your compliance with the GDPR
- Continuously expanded

Ready for customization.

- You get editable files you can freely adapt to fit your needs
- Benefit from the experience and learnings across our client base (both B2B and B2C)
- Group-wide usage permitted, perpetual license available
- Ongoing updates and additions
- Day-to-day advice and support upon request

Contact:

dataprivacy@vischer.com
David Rosenthal & VISCHER DP team