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

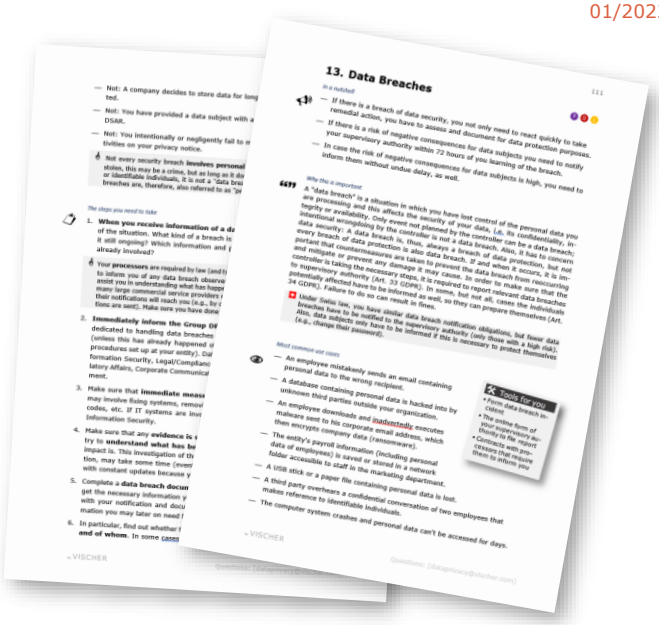


Table of Contents

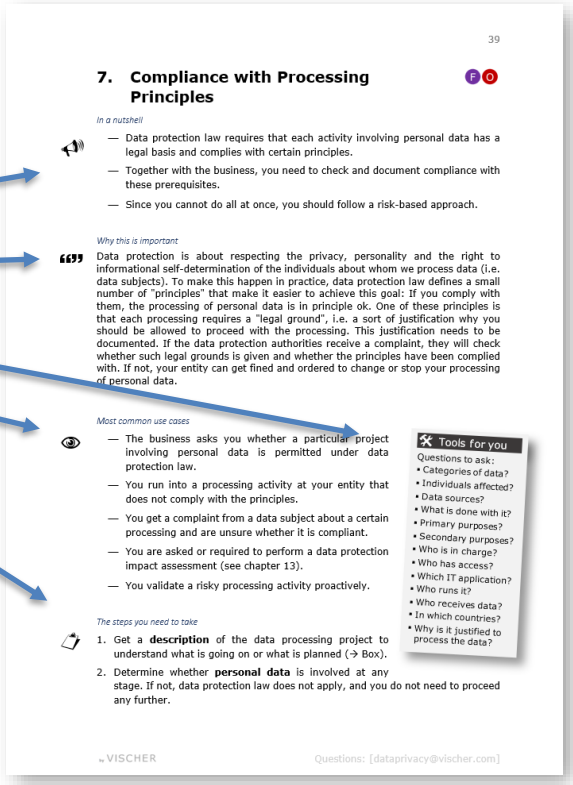
All key topics covered.

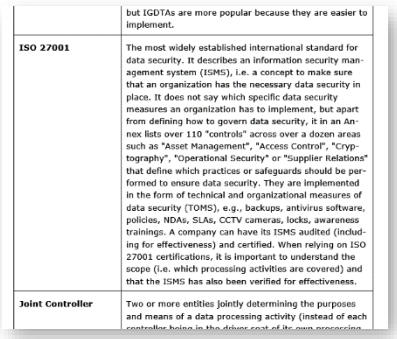
https://www.rosenthal.ch/downloads/VISCHER_DPC_Handbook_Info.pdf

- Covers day-to-day GDPR obligations of your entity, including governance
- 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





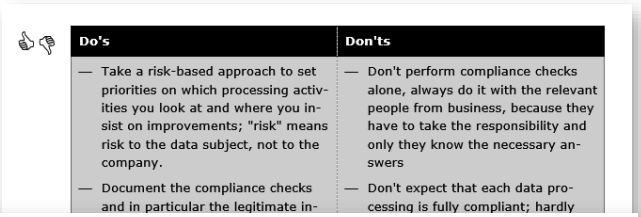
	but IGDTAs are more popular because they are easier to implement.
ISO 27001	The most widely established international standard for data security. It describes an information security management system (ISMS), i.e. a concept to make sure that an organization has the necessary data security in place. It 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

- Glossary with over 20 pages

by VISCHER

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

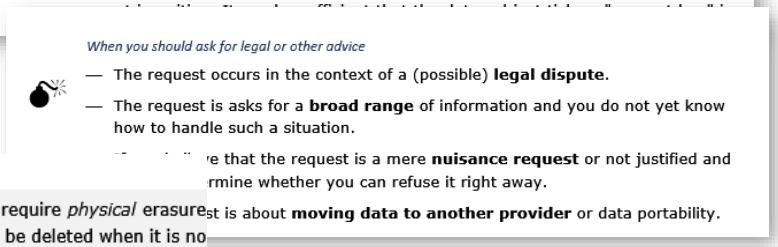


Do's	Don'ts
— Take a risk-based approach to set priorities on which processing activities you look at and where you insist on improvements; "risk" means risk to the data subject, not to the company.	— Don't perform compliance checks alone, always do it with the relevant people from business, because they have to take the responsibility and only they know the necessary answers
— Document the compliance checks and in particular the legitimate in-	— 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



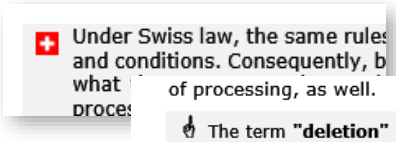
When you should ask for legal or other advice

— The request occurs in the context of a (possible) **legal dispute**.

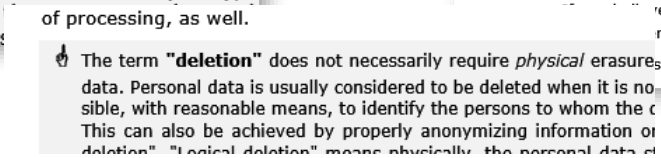
— The request is asks for a **broad range** of information and you do not yet know how to handle such a situation.

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

st is about **moving data to another provider** or data portability.

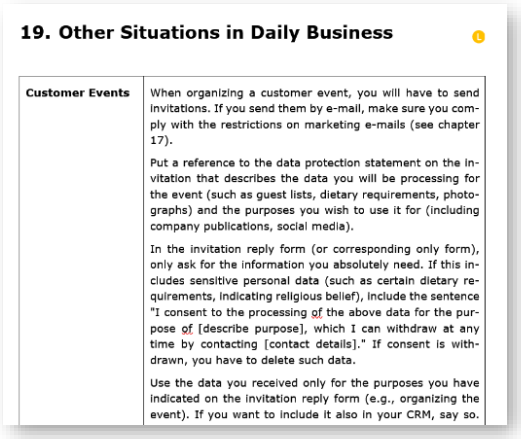


Under Swiss law, the same rules and conditions. Consequently, b what proces



of processing, as well.

The term **"deletion"** does not necessarily require *physical* erasure data. Personal data is usually considered to be deleted when it is no sible, with reasonable means, to identify the persons to whom the c This can also be achieved by properly anonymizing information or deletion". "Logical deletion" means physically, the personal data c



19. Other Situations in Daily Business

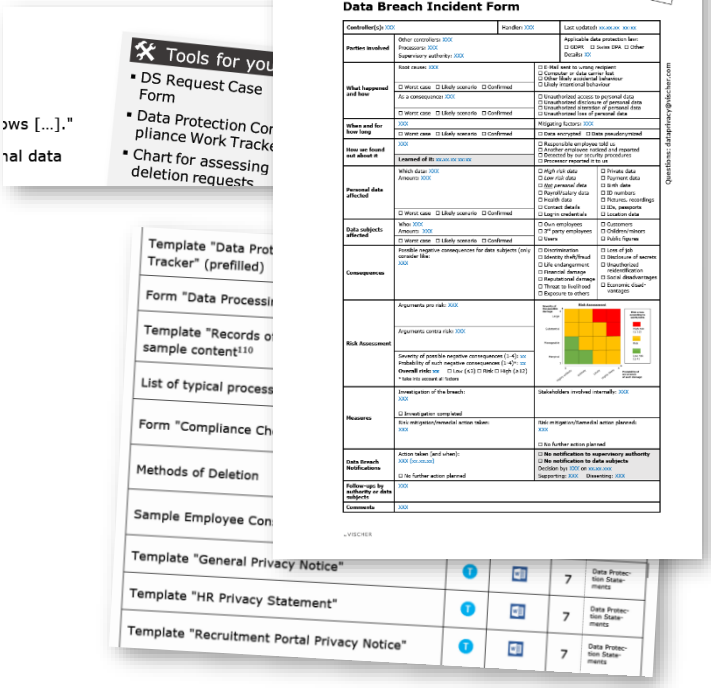
Customer Events	When organizing a customer event, you will have to send invitations. If you send them by e-mail, make sure you comply with the restrictions on marketing e-mails (see chapter 17). Put a reference to the data protection statement on the invitation that describes the data you will be processing 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



Tools for you

- DS Request Case Form
- Data Protection Compliance Work Tracke
- Chart for assessing deletion requests

ows [...]."

nal data

Template "Data Prot Tracker" (prefilled)

Form "Data Processi

Template "Records o sample content[110

List of typical process

Form "Compliance Ch

Methods of Deletion

Sample Employee Con

Template "General Privacy Notice"

Template "HR Privacy Statement"

Template "Recruitment Portal Privacy Notice"

Data Breach Incident Form

Contact:

dataprivacy@vischer.com
David Rosenthal & VISCHER DP team

by VISCHER