IT Security & Compliance

Essentials

for (Jewish) Non-Profit Organistions

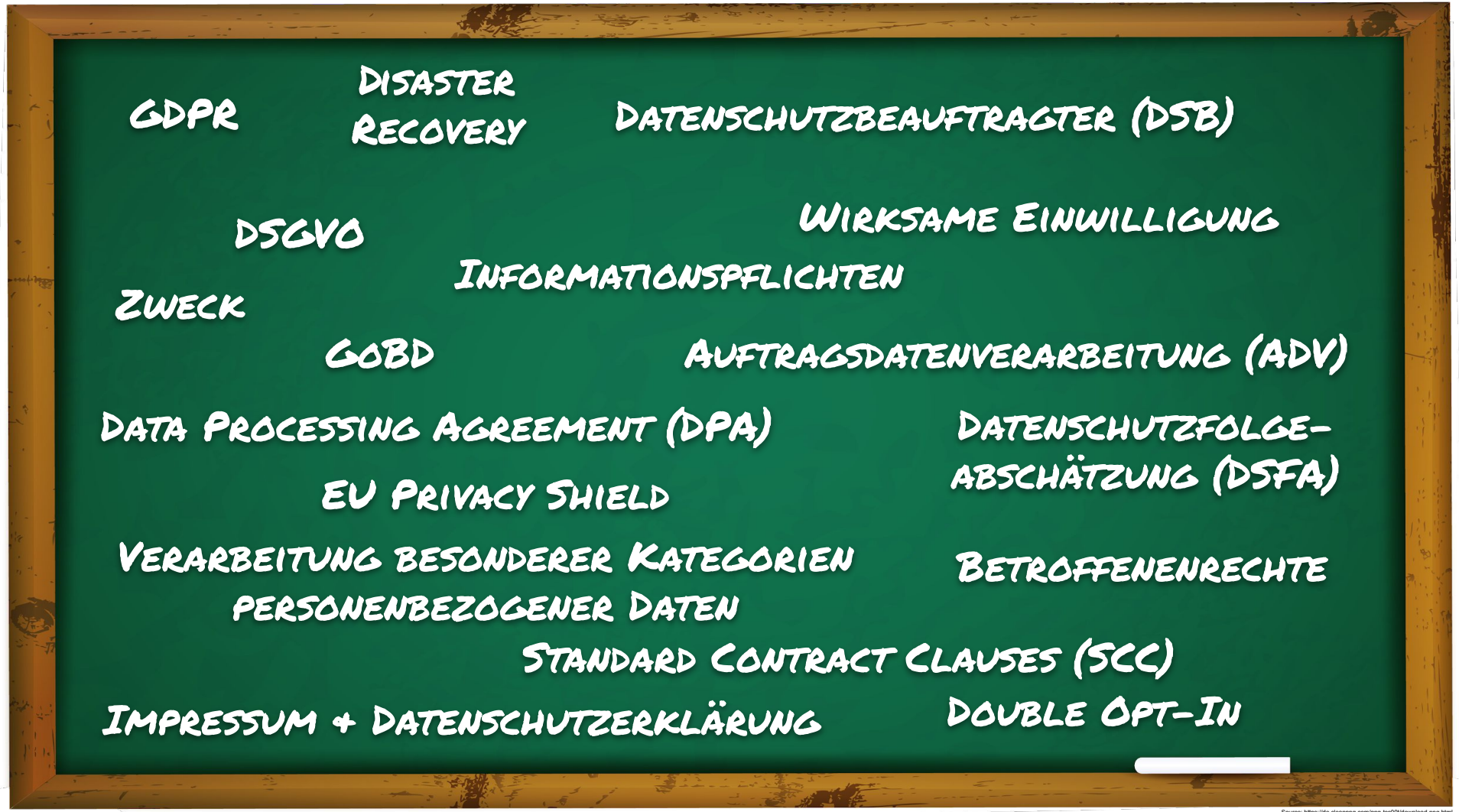
(in Germany)

Schlomo Schapiro ✧ Limmud Festival ✧ 09.06.2023

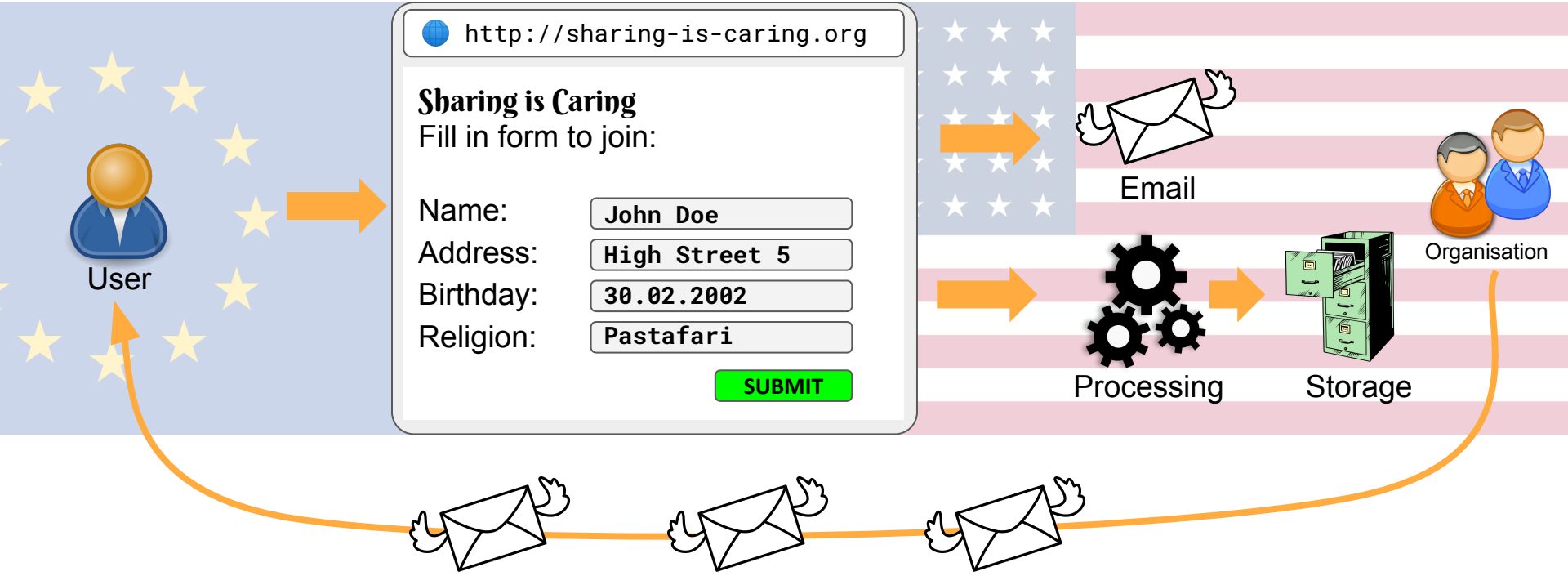
schlomo.schapiro.org

Disclaimer:

I'm not a lawyer, and the information presented here can be wrong. Please get professional advice and help. This information is meant to illustrate the problem space and help you get started.



Common Example: Website, Form & Email Distribution List



Problems?

Transport encryption (HTTPS) missing

Data subject rights & data retention

Purpose

GDPR §9 special category personal information

Multi-Factor Authentication

Effective consent for collection & processing of special category data and for processing data outside of EU

Impressum & Datenschutz-erklärung missing

Double opt-in required for newsletters

Data Processing Addendum (DPA / ADV)

Backup & Disaster Recovery

Standard Contract Clauses

Data Protection

General Data Protection Regulation: 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.

Examples of personal data

- a name and surname; a home address; the date of birth;
- an email address such as name.surname@company.com;
- an identification card number;
- location data (for example the location data function on a mobile phone)*;
- an Internet Protocol (IP) address;
- a cookie ID*;
- the advertising identifier of your phone;
- data held by a hospital or doctor, which could be a symbol that uniquely identifies a person.

Source: https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en

GDPR Art. 9: Special categories of personal data

Processing of personal data revealing racial … origin, … religious or philosophical beliefs, … for the purpose of uniquely identifying a natural person, … shall be prohibited.

Paragraph 1 shall **not apply** if one of the following applies:

- … explicit consent …
- … necessary for a purpose …
- … protect vital interests …
- … legitimate activities with appropriate safeguards by … any other not-for-profit body with a … religious … aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects
- …

Source: https://gdpr-info.eu/art-9-gdpr/

Data Collection & Processing Done Right

- Minimise the data collected and processed
  - Coarse data can be enough, e.g. ask for age instead of birthday
  - Limit the scope of the data processing, delete as soon as possible
- Make the reason and purpose of data collection and processing transparent
  - “We collect your contact details to send you the information that you asked us for”
  - “We analyse your shopping habits on our website to make you better informed offers”
- Determine the legal base for collecting and processing personal data
  - Necessary for the performance of a contract
  - Willingly given consent
  - Legal obligations
  - …
- Inform about the rights of the data subject
  - Access, rectification, erasure, restriction, notification, portability, object, profiling …
- Inform about data controller and processing
  - Identity of controller, data protection officer, sub-processors, data exports …
- Implement technical and organisational measures to safeguard data
  - Minimise access
  - Implement IT-security good practices
  - Data processing by 3rd party sub-processors requires data processing addendum
  - Data transfer to the USA requires Standard Contract Clauses

Data of Minors and Children

Child acting alone

- 16 and older: treat like adults
- Below 16: cannot give effective consent!
- Parents / legal guardians must give consent
- You must make “reasonable effort” to verify parental consent!

Parents acting on behalf of their child

- Age doesn’t matter
- Parents / legal guardians responsible
- Same rules apply for reason of processing

Source: https://gdpr-info.eu/art-8-gdpr/

Data Protection - Datenschutz

Everybody must deal with this, regardless of size or purpose

≥ 20 people dealing with data? → a data protection officer is obligatory!

- Process & tooling documentation
- Technical & operational measures
- Professional software solutions, data processing addendums
- Contact person for inquiries

You'll need data privacy notices and consents, and manage them ✍

You must classify all data and explain the purpose of collecting and processing it

You must give the data subjects the legally mandated rights about their data

Anything is better than nothing 💪

IT-Security

IT Security - Datensicherheit

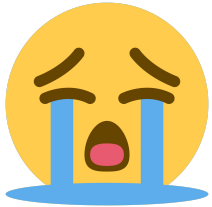
Everybody must deal with this, regardless of size or purpose

All data has value and must be protected (or delete immediately)

- Access control via multi-factor authentication
- All data must be processed and stored in systems belonging to the organisation **or** by 3rd party subcontractors with appropriate contracts (data processing addendum, Standard Contract Clauses for US vendors)
- Systems must be operated professionally
- Must have a backup and restore / disaster recovery plan implemented for all data
- Ensure people who stop working for the organisation also stop having access to the data
- Prevent mixing of organisation data with other / private data

Anything is better than nothing 💪

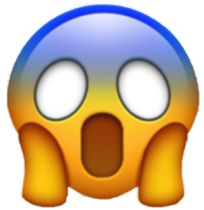
Data privacy & IT security do not earn money, but avoids unwanted costs and embarrassment



- Yes, correct
  - You won’t make more money due to better compliance
  - Nobody will ever praise you for great data privacy and security compliance
  - Nobody will deal with that pro-bono or for fun
  - Nobody wants to be responsible for it
- No, wrong!
  - You significantly reduce and limit the **personal** liability of the management & leadership
  - You prevent costly fines for data privacy violations
  - You prevent accidentally sharing/exposing your member’s/donor’s/customer’s data
  - You really don’t need a data privacy scandal that will forever tarnish your name

Gain the trust of your members, customers, partners and donors to handle their data and money with professionalism and integrity! 💪

Did you ever think about…



- Is your IT secure and how can you be sure of that?
- How can you know about others accessing your data?
- Is all the data protected by multi-factor authentication and backups?
- How easy is it to steal the data of your sponsors, members or your email distribution list?
- What happens if your laptop gets stolen or is lost? If all your data is gone?
- Did you ever share data anonymously with a link that anybody can use?
- How do you off-board employees and effectively remove their access to data?
- How long do you need to retain documents and invoices?

“There are only two types of companies: those that know they’ve been compromised, and those that don’t know.”

Thank you | Further reading (selection)

Basiswissen: Datenschutz im Verein | Stiftung Datenschutz

Checkliste zum Datenschutz im Verein | Deutsches Ehrenamt

Anforderungen der (DS-GVO) an kleine Unternehmen, Vereine, etc., LDA Bayern

Datenschutz im Verein nach der Datenschutz-Grundverordnung (DSGVO), LDI NRW

Datenschutz-schule.info, not only for schools

Personenbezogene Daten und das Schutzstufenkonzept | Datenschutz-Praxis

Besondere Kategorien personenbezogener Daten | Datenschutz-Praxis

Vereinsbuchhaltung & Rechenschaftspflicht | Deutsches Ehrenamt

Leitfaden zur Basis-Absicherung nach IT-Grundschutz | BSI

Grundsätze zur ordnungsgemäßen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenschutz (GoBD) | BSB.VIBSS

Please get professional advice and help

bit.ly/limmud23compliance