PUBLIC SECTOR LAW

Schulung zum Datenschutz

Evangelisch-reformierte Landeskirche
& Kirchgemeinden Graubünden

RA Dr. Esther Zysset
zysset@publicsector.ch

Überblick und Ziel

Wieso ist Datenschutz für die Kirche **relevant**?

Was sind die wichtigsten **Prinzipien** und **Regeln** des Datenschutzes?

Welche **Pflichten** haben die einzelnen Mitarbeitenden im Datenschutz?

Wieso reden wir über Datenschutz?

Wie der Datenabfluss vom Bund zu Xplain zustande kam

Keystone-SDA
Bern, 01.05.2024 - 14:32

Der Hackerangriff auf die Berner Firma Xplain führt zu Datenleck des Bundes. Die Hinter

Durch den Hackerangriff auf die Firma Xplain gelangt

1. Betrieb einer App bei der Spitex

Wenn bei einem Spitex Klient festgestellt wird, dass eine psychiatrische Pflegeleistung angezeigt ist, zieht die Spitex externe Fachpersonen zu. Die Spitex hat dazu mit den Psychatrischen Diensten Graubünden (PDGR) einen Vertrag abgeschlossen. Die PDGR Fachpersonen handeln in diesem Fall im Auftrag der Spitex und werden dafür auch von dieser Organisation bezahlt. Seitens der Spitex Organisation wird eine Klientendatenbank über App betrieben. Der Zugriff über diese App ermöglicht den Zugriff auf alle in der App verwalteten Personen. Derzeit ist es softwaremässig nicht möglich, die Berechtigung auf einen bestimmten Personenkreis einzuschränken. In der Konsequenz haben alle Personen, welche die App nutzen auf alle Klientendaten Zugriff.

in
verwickelt

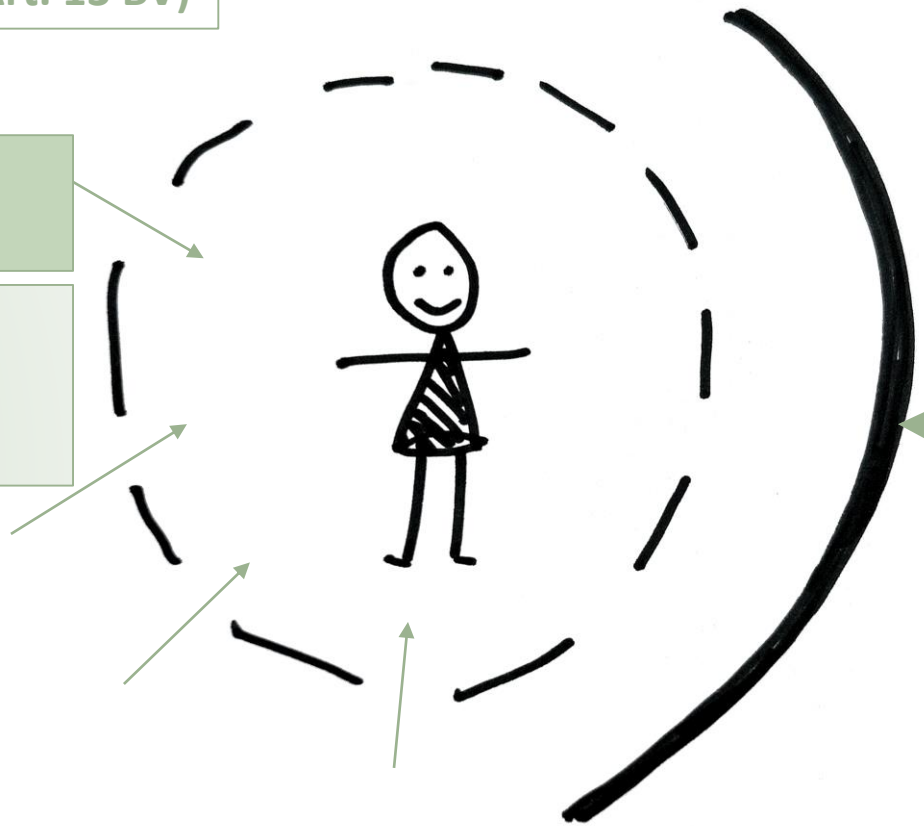
dynummern von Polizeibeamten
elandet sein.

Wie funktioniert der Datenschutz?

Schutz der Privatsphäre (Art. 13 BV)

Datenbearbeitung im privaten Sektor

Datenbearbeitung ist zulässig, sofern die Prinzipien und Pflichten eingehalten werden.



Datenbearbeitung im öffentlichen Sektor

Datenbearbeitung ist nur mit einer gesetzlichen Grundlage (bzw. zur Erfüllung einer öffentlichen Aufgabe) zulässig.

Graubünden reformiert
Grischun refurmà
Grigioni riformato

Welches Recht findet Anwendung?

Prinzipien und Regeln (wie?)

Kantonales Datenschutzrecht
(KDSG, Bildüberwachungsverordnung VBÜ)

Öffentliche Aufgaben (warum?)

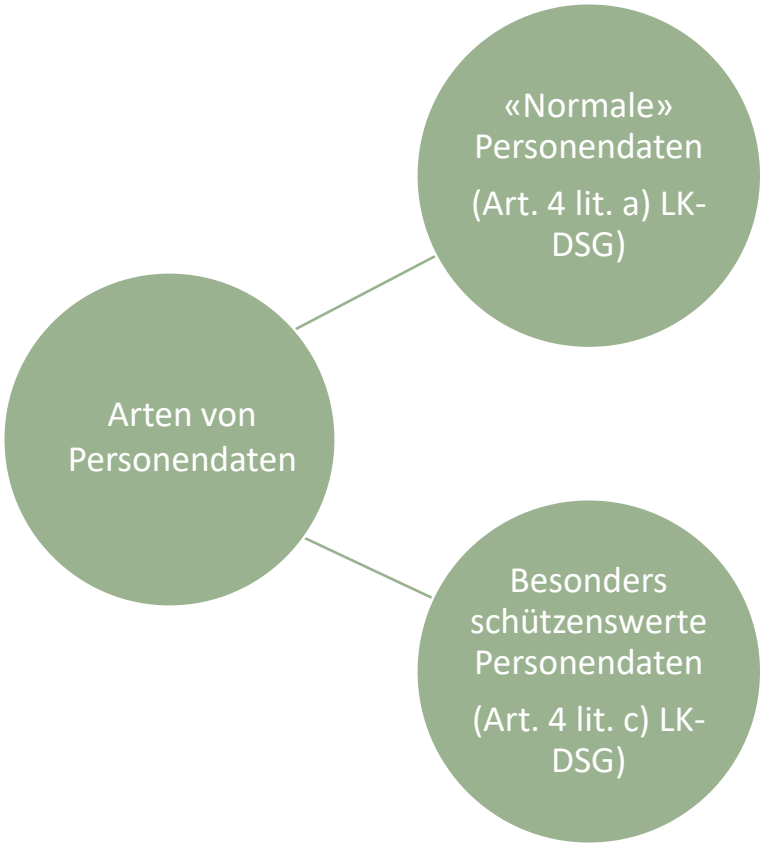
Sachgesetze und kirchliche Erlasse
(Verfassung, Kirchengesetze,
Kirchgemeindeverordnungen,
Wegleitungen)

Landeskirchliches Datenschutzgesetz
(LK-DSG)
Konkretisiert das KDSG

:

Die Bearbeitung von Personendaten

Was sind Personendaten? 1/2



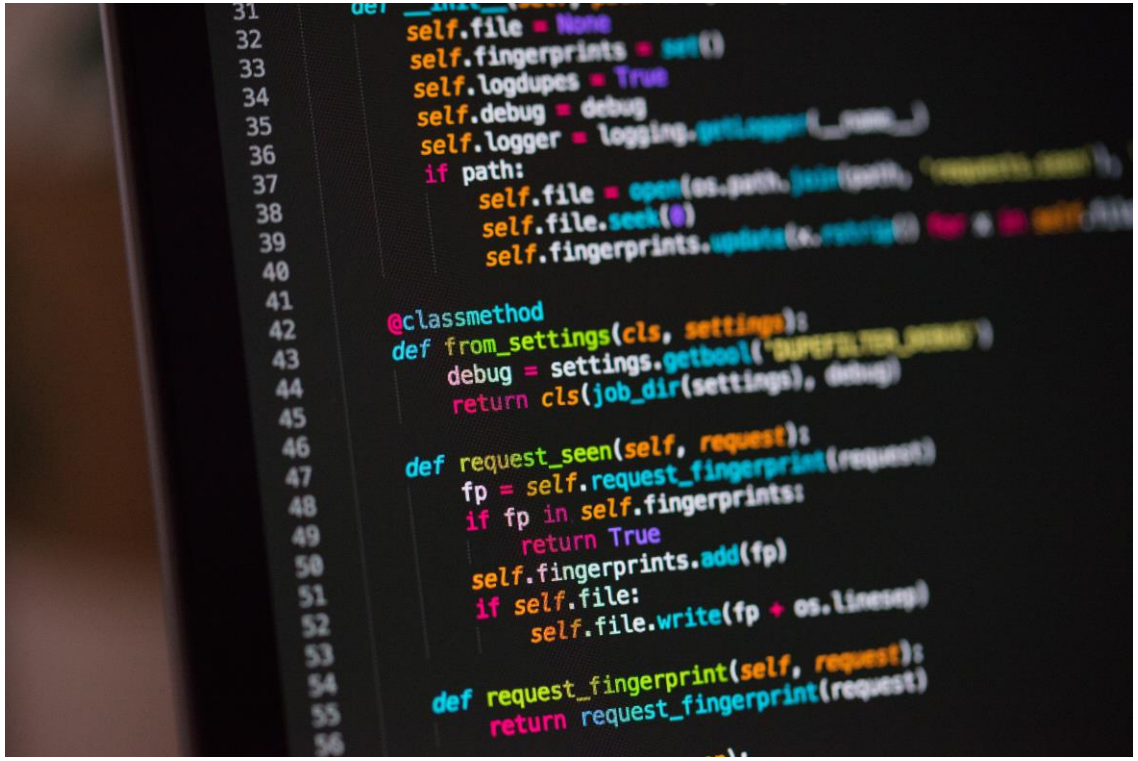
Informationen über eine **bestimmte** oder **bestimmbare** Person

1. Daten über **religiöse**, **weltanschauliche**, **politische** oder **gewerkschaftliche** Ansichten oder Tätigkeiten,
2. Daten über die **Gesundheit**, die **Intimsphäre** oder die Zugehörigkeit zu einer **Ethnie**,
3. **genetische** Daten,
4. **biometrische Daten**, die eine natürliche Person eindeutig identifizieren,
5. Daten über verwaltungs- und **strafrechtliche Verfolgungen** oder Sanktionen,
6. Daten über Massnahmen der **sozialen Hilfe.**

\+ Persönlichkeitsprofile
\+ Profiling

Was sind Personendaten? 2/2

- E-Mail-Adresse
- Vor- & Nachnamen
- Telefonnummern
- IP-Adresse
- Religionszugehörigkeit
- Zivilstand
- Lohn
- Etc.



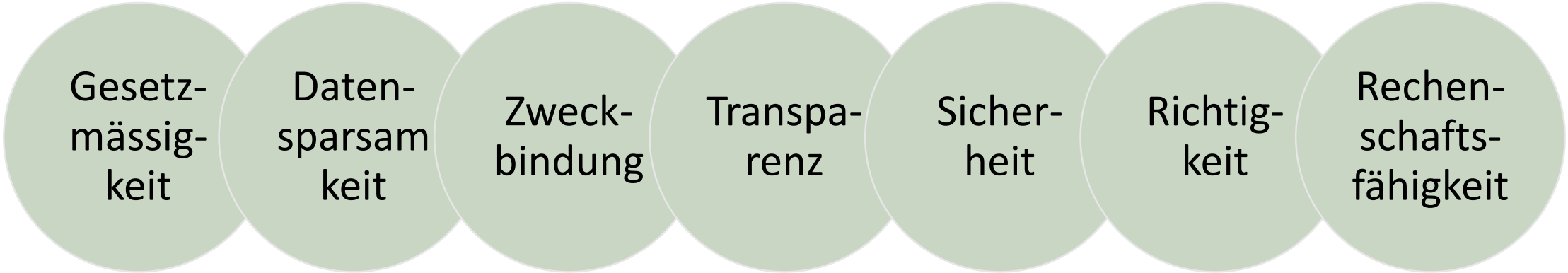
Was ist Bearbeitung?

Jeder Umgang mit Personendaten, (…),
insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten (Art. 4 lit. d LK-DSG).

Prinzipien des Datenschutzes

Was ist bei der Datenbearbeitung zu beachten?

Die 7 Grundprinzipien des Datenschutzes



Prinzip der Gesetzesmässigkeit 1/2

Gesetz-
mässig-
keit

- Bearbeitung von Personendaten, soweit dies zur **Erfüllung kirchlicher Aufgaben nötig** ist (Art. 5 Abs. 1 LK-DSG).
- Für die Bearbeitung **mit besonderen Risiken** ist **Gesetz im formellen Sinn** erforderlich (Art. 5 Abs. 2 LK-DSG).

Prinzip der Gesetzesmässigkeit 2/2

Gesetz-
mässig-
keit

Ausnahmen

- Bearbeitung **ohne grosse Risiken** (Art. 5 Abs. 3 LK-DSG).
- Bei **Einwilligung**
- **Schutz höherwertiger Interessen** (Art. 5 Abs. 4 LK-DSG).

Prinzip der Datensparsamkeit

Daten-
sparsam-
keit

So wenig Personendaten wie möglich bearbeiten!

Prinzip der Zweckbindung

Zweck-
bindung

Bearbeitung von Personendaten grundsätzlich nur im **Zusammenhang** mit dem **Zweck der Erhebung** (Zweckänderungsverbot).

Prinzip der Transparenz

Transpa-
renz

Betroffene Personen werden, wo nötig, über die Bearbeitung **informiert**.

Prinzip der Sicherheit

- **Schutz** vor **Verlust**, **Verfälschung** und **unbefugtem Zugriff**.
- Ergreifung von technischen und organisatorischen Massnahmen (TOMs).

Prinzip der Richtigkeit

Personendaten müssen korrekt sein.

Prinzip der Rechenschaftsfähigkeit

Rechen-
schafts-
fähigkeit

- Sicherstellen, dass intern die nötigen **Prozesse und Verfahren** umgesetzt werden.
- **Nachweis gegen Aussen**, dass die gesetzlichen Pflichten umgesetzt und eingehalten werden.

Kirchgemeinde Hintertupfingen

Gian Casanova kümmert sich um die Einführung einer neuen Mitarbeiterin. Dazu schickt er den Lebenslauf der neuen Mitarbeiterin per E-Mail an seine Kollegin Mia Caduff von der Kommunikation, u.a. damit sie die Daten und das Foto für den externen Newsletter nutzen kann.

- Sind Personendaten betroffen?
- Findet eine Bearbeitung statt?
- Welche Datenschutzprinzipien sind tangiert?

Jetzt wird es konkret: Pflichten im Einzelnen

Konkrete Pflichten

1. Wann muss man eine **Datenschutz-Folgenabschätzung (Evaluation)** durchführen?
2. Was ist ein **Datenschutzvorfall** und was muss man tun?
3. Was muss ich tun, wenn ich **Dritte** beiziehe?
4. Welche **Rechte** haben **betroffene Personen** und wie muss man damit umgehen?
5. Was umfasst die **Informationspflicht**?

Kirchgemeinde Hintertupfingen

Mia muss diese Woche auch noch eine Offerte einholen für eine Cloud-Lösung für die Geschäftsdaten der Kirchgemeinde.

Sie schaut sich verschiedene Lösungen an und entscheidet sich für das Angebot „CloudBox“ einer US-Anbieterin.

Evaluation (DSFA) und (Vorab-) Konsultation

Evaluation (DSFA) 1/2

Was ist eine Evaluation / DSFA?	Ein «Nachdenken» über eine Bearbeitung von Personendaten, das hilft, Risiken zu erkennen und reduzieren.
	Ein Planungsinstrument.
	Ein Nachweis nach aussen.

Evaluation (DSFA) 2/2

Erstellungspflicht:

- **Vor** einer **neuen Bearbeitung** von Personendaten oder
- Bei **wesentlicher Änderung** der bisherigen Bearbeitungsweise

… wenn daraus ein **hohes Risiko** resultiert.

Inhalt: **Beschreibung** der geplanten Bearbeitung; **Bewertung** der Risiken für die betroffene Person; **Massnahmen**, die zur Verringerung der Risiken getroffen werden.

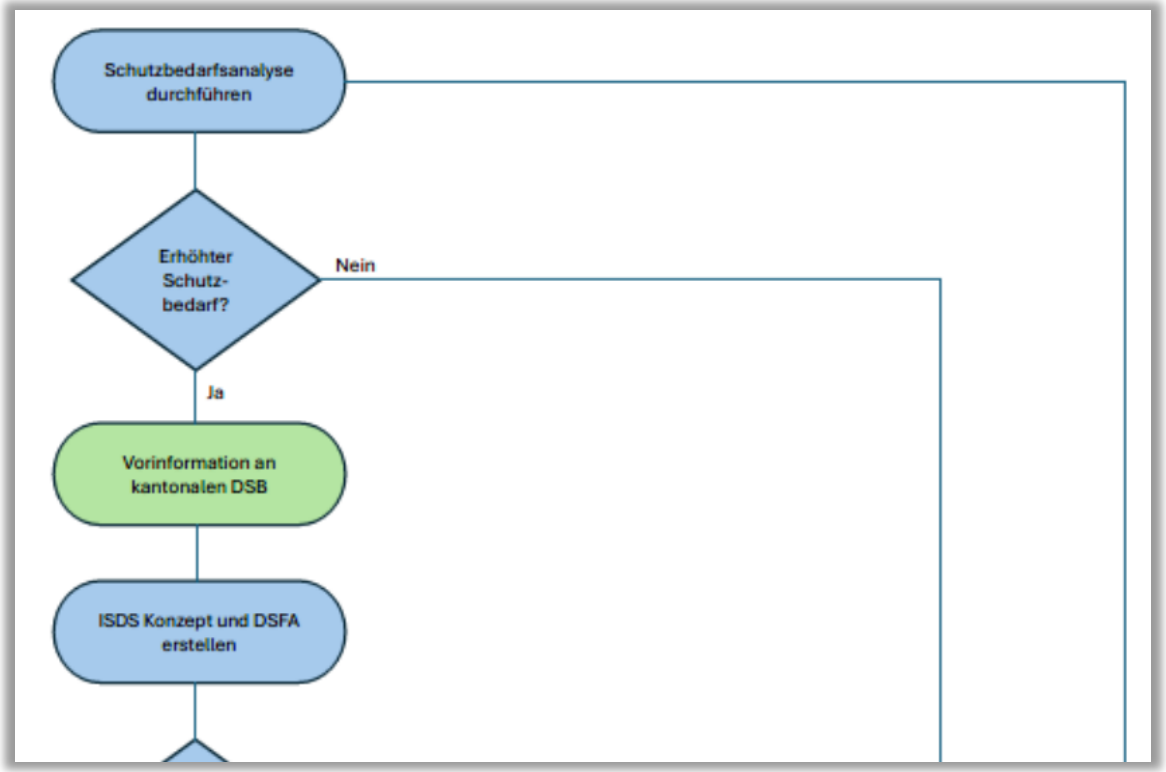
(Vorab-)Konsultation

Vorabkonsultation: Wenn trotz der getroffenen Massnahmen **hohe Risiken verbleiben**, ist die Bearbeitung der **kt. Aufsichtsstelle** zu **unterbreiten**

→ Unterstützung durch **kirchl. DSB** (Art. 28 Abs. 2 lit. b LK-DSG)

Achtung: Die Antwort muss abgewartet werden.
Die Umsetzung des Projekts ist erst **nach Abschluss der Konsultation** der/des kt. Aufsichtsstelle möglich!

Hinweis: Merkblatt kt. Aufsichtsstelle



Quelle: [Merkblatt Vorabkonsultation kt. Aufsichtsstelle GR (2024)]

Kirchgemeinde Hintertupfingen

Muss Mia vor dem Einsatz der Software CloudBox eine Datenschutz-Folgenabschätzung durchführen?

Datenschutzvorfall

Kirchgemeinde Hintertupfingen

Mia ist langsam etwas müde vom langen Tag, muss aber als letzte Aufgabe des Tages noch ihren Newsletter verschicken. Gemacht ist gemacht!

Aber oh Schreck, sie hat im Newsletter aus Versehen ein Kirchenvorstandsprotokoll verlinkt, in dem verschiedene vertrauliche Geschäfte beschrieben werden.

Mia wird nervös…. Was muss sie tun?

Datenschutzvorfall 1/3

Begriff: Verlust/Vernichtung, Verfälschung oder **unbefugter Zugriff** auf/von Personendaten.

Beispiele:

- **Verlust** eines USB-Sticks oder eines Laptops mit Geschäftsdaten.
- Daten sind plötzlich **nicht mehr vorhanden** oder stimmen nicht mehr.
- Daten wurden auf einer **nicht zugelassenen** Cloudlösungen gespeichert oder an eine **private** E-Mail-Adressen geschickt.

Datenschutzvorfall 2/3

Sofortige Meldung an kirchl. DSB (auch bei blossem Verdacht)!

→ Die Meldung geht dem Tagesgeschäft immer (!) vor.

→ Mit der Meldung sind keine negativen personalrechtlichen Konsequenzen verbunden.

Datenschutzvorfall 3/3

Meldekette:

Kirchgemeinde → kirchl. DSB → kt. Aufsichtsstelle

Keine Meldepflicht (an **kt. Aufsichtsstelle**): Wenn voraussichtlich kein hohes Risiko für die Grundrechte der betroffenen Person.

→ Diese **Bewertung** übernimmt die/der **kirchl. DSB**.

Information der betroffenen Person:

- Wenn es zu ihrem **Schutz erforderlich** ist oder
- Wenn die/der **kt. Aufsichtsstelle** es **verlangt**

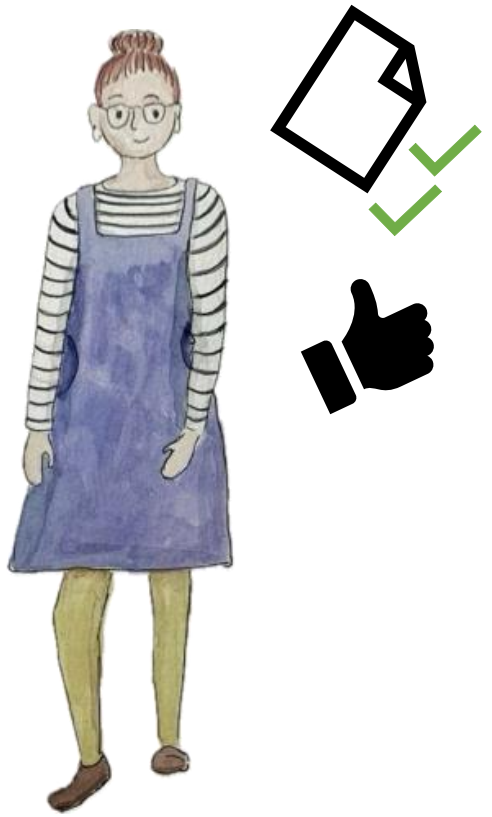
Datenbearbeitung im Auftrag

Kirchgemeinde Hintertupfingen

Zurück zum Vormittag:

Mia klickte sich für den Erwerb der Software CloudBox durch die Eingabefelder und setzt am Ende in einem Pop-up Fenster Häkchen bei „Accept Terms of Use“ und „Accept Privacy Policy“.

Glücklich über den kostensparenden Deal, begann sie bereits verschiedenste Datensätze in die neue Lösung zu importieren.



Kirchgemeinde Hintertupfingen

- Was geschah beim Anklicken des Pop-Up aus rechtlicher Sicht?
- Was müsste Mia tun, bevor sie eine neue Software einsetzt?
- Spielt der Sitz der Anbieterin eine Rolle (hier USA)?

Bearbeitung im Auftrag 1/4

Wer bearbeitet Personendaten?

Lokale (native) Applikation:

Web-Applikation und Cloud-Dienste:

Personendaten

Bearbeitung im Auftrag 2/4

Verkauf der Daten

Kirche

Personendaten

- Datenbearbeitung zu kirchlichen Zwecken.
- Einhaltung des Datenschutzes (inkl. Amtsgeheimnis).

Dienstleister:in

Marketing

Bearbeitung im Auftrag 3/4

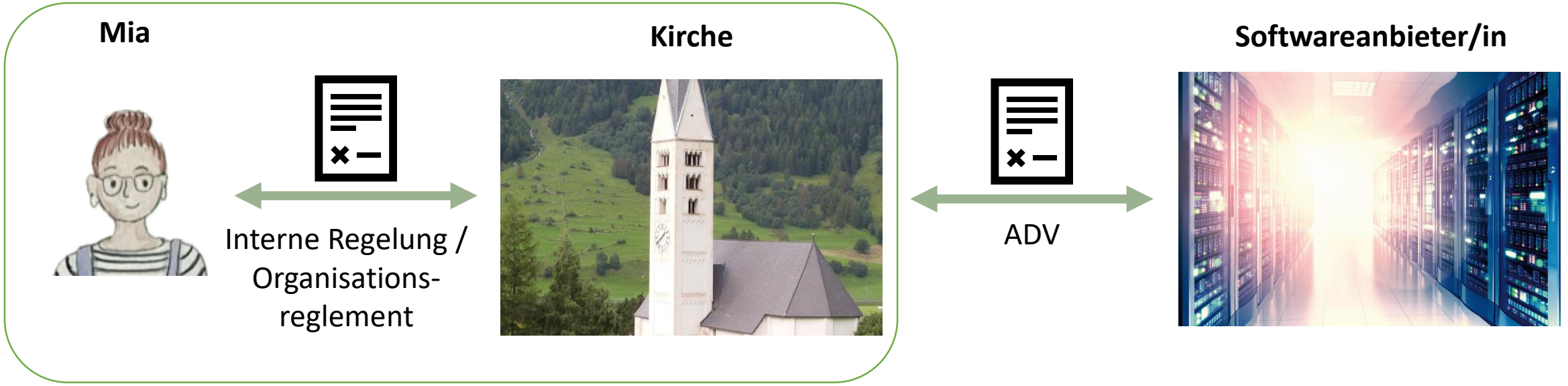
Auftragsdaten-bearbeitungsvertrag (ADV)

Inhalt eines ADV:

- Klare Vorgaben zum Umgang mit Personendaten!
- Weisungen
- Sicherheitsmassnahmen
- Etc.

Bearbeitung im Auftrag 4/4

Die Kirche bleibt für den Datenschutz verantwortlich!



Rechte der betroffenen Person

Recht auf Information

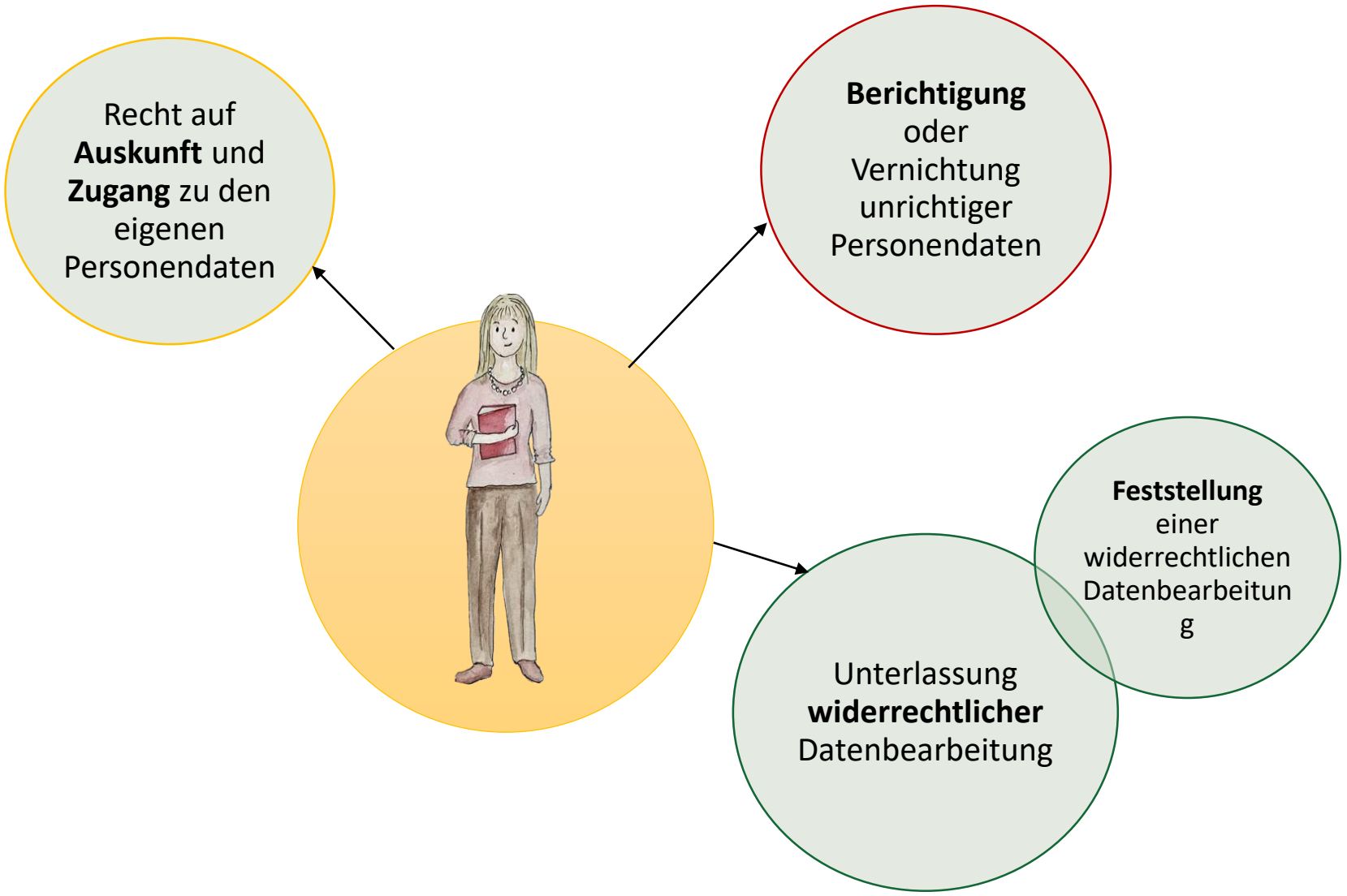
Betroffene Personen sind bei der **Beschaffung von Personendaten** angemessen zu informieren über:

- Die verantwortliche **Behörde**
- Die beschafften **Daten**
- Die **Rechtsgrundlage** und die **Zwecke** der Datenbearbeitung
- **Herkunft** und allfällige **Empfängerinnen**
- Die **Rechte** der betroffenen Personen

Informationspflicht kann **unter** bestimmten **Umständen entfallen**

(Art. 17-18 KDSG).

Betroffenenrechte 1/2



Betroffenenrechte 2/2

Verweigerung der Auskunft/Einsicht möglich, wenn:

- das Auskunftsgesuch offensichtlich **unbegründet** ist,
- überwiegende **öffentliche Interessen** vorliegen oder
- überwiegende **Interessen Dritter** bestehen.

- **Öffentliche Interessen**: Öffentliche Sicherheit, Gesundheit, Amtsgeheimnisse, etc.
- **Interessen Dritter**: Privatsphäre Dritter, Berufs- oder Geschäftsgeheimnisse.

Zurück zum Anfang!

Wieso ist Datenschutz für die Kirche **relevant**?

Was sind die wichtigsten **Prinzipien** und **Regeln** des Datenschutzes?

Welche **Pflichten** haben die einzelnen Mitarbeitenden im Datenschutz?

Danke
für Ihre Aufmerksamkeit!

Fragen und Anmerkungen zur Schulung gerne an zysset@publicsector.ch.