23.01.2023 Augen auf und durch! Datenschutz fürs Ehrenamt

Handout für „Alles im Griff – sicher mit Daten umgehen“ von Olav Seyfarth

- Spoiler: Am Ende sind einige der im Vorfeld und in den Slots gestellte Fragen schriftlich beantwortet. Dennoch ist es logischer, dieses Handout vorwärts zu lesen / zu überfliegen :)

Erwartungen der Teilnehmenden (allgemein)

- Ziel: gewisse Selbstsicherheit für das eigene Handeln in Bezug auf Datenschutz
- Erfahrungsaustausch: Lösungen andere Akteure, Ideen / Produkte kennenlernen, übersehene Punkte entdecken → eigene Herausforderung und Umgang damit beschreiben
- Ausprobieren von workadventu.re ;)
- Arbeitsfähig bleiben → risikobasierter Ansatz, Was kann man nicht wegargumentieren?
  Aufwand reduzieren durch smarte Tools?
- Take-Aways: Umsetzung **Theorie → Praxis**, praktische technische Hilfsmittel (z.B. webbkoll, F12, DS-Generator?), Best Practices, Vorlagen (z.B. für Datenschutzerklärungen (z.B. für Mitarbeiter)), empfehlenswerte Dienste und Dienstleister, einfache Schulungen für Mitarbeiter?

Rahmen / Versachlichung

- Datenschutz ist nicht machbar → Ausrede oder falsch verstanden
  Angst davor, etwas falsch zu machen / Haftung bei Nichtstun → anfangen und besser werden

  "Gefordert ist, was wir uns selbst auch von anderen wünschen: Transparenz über das, was mit Informationen zu unserer Privatperson geschieht und dass diese Informationen von denen, die damit umgehen, sensibel behandelt werden."
- Ideen nicht aus Angst verwerfen (vorauseilender Gehorsam, "Das geht eh nicht wegen Datenschutz") → Stattdessen das Was und Wie beschreiben, dann Risiko für die Betroffenen.
  Daraus Maßnahmen ableiten, sodass ein "akzeptables" Risiko (Sicht der Betroffenen!) verbleibt.
- Dieses kurze Seminar ersetzt keine Datenschutzausbildung!
  Als Einstieg lesenswert: Leitfaden "Das Datenschutzrecht" des ZDH
  Danach das Buch "Datenschutzgrundverordnung für Dummies" (Wiley, auch als eBook)
  Und natürlich die Materialien der Stiftung Datenschutz :)
  Danach / kontinuierlich: Blogs, Newsletter, Konferenzen

Kontext / Datenschutz-Basics

- Was ist in jedem Fall **mindestens** zu tun? Datenschutzkonzept? Löschkonzept?
  Eher nicht (als erstes). Erst mal anfangen zu sammeln und (irgendwie) aufzuschreiben.
  Siehe Säulenmodell (PDF) (Verfahren→Technik→Verträge), darauf aufbauend ggf. DS-Prozesse
- Die für das gesamte Thema Datenschutz benötigten Ressourcen (Zeit, Geld und KnowHow) sind abhängig von der Größe der Organisation und der Sensibilität der Daten
  Rollenklärung! Verantwortlichkeiten und Prozesse! Benennung und Aufgaben DSB(+DSK!)
  Betroffene sind: Mitarbeitende, Mitglieder, Kunden/Gäste/Teilnehmende, Dienstleister/Dritte
- Datenschutz ≠ Verteidigung gegen Rechtsansprüche
  Dokumentation der **Verfahren** und der **Maßnahmen**, nicht der Daten / Rechte / Akteure!
- Betroffenenrechte: Aufwand bei Auskunfts-/Löschersuchen
  Speicherung planen, Suche/Löschung technisch unterstützen
- Social Media: TikTok, Instagram, Twitter, Facebook, Mastodon → andere Slots

Technisch-organisatorische Maßnahmen als Anforderung der DSGVO

- „**TOM**“ kann man übersetzen mit „IT-Sicherheit“ (bewusst zu stark vereinfacht)
- „**Risiko**“ bedeutet im Datenschutz das „Risiko für die Grundrechte und Grundfreiheiten der Betroffenen“, nicht das „Risiko für einen Serverausfall“ oder das „Risiko für den Verein, ein Bußgeld zu bekommen“
- typisch: **technisch** wenig Möglichkeiten(?) bzw. wenig umgesetzt / gefordert
  wenn überhaupt etwas gemacht wird, dann oft „**organisatorisch**“ – schriftlich?!
- DSGVO erlaubt **risikobasierten** Ansatz – und fordert, dass **geeignete** TOM ergriffen werden
  → Verweis auf Dokumentationspflicht bei Kirstin
- IT-Ausstattung im Vereinbüro: Gefahr "wegtragen" nicht vergessen", "übliche" Maßnahmen wie (Router- und Windows-)Firewall, Virenscanner (der von W10/11 reicht), regelmäßig Updates!
  Sinnvoll wäre auch: IT-(Sicherheits-)Richtlinien, ein:e IT-Sicherheitsnbeauftragte:r
- Sicherheit, z.B. für Cloudspeicher, am Risiko aus Sicht der Betroffenen ausrichten
  Wenn man weiß, dass Passwörter ein Problem sind, dann Zugänge ohne Passwort nutzen, und für Cloud-Zugriff per Browser 2FA/MFA. Ja, unbequem, aber wenn der Zugang missbraucht wird…
- Vertraulichkeit / Integrität: Absicherung / Zugriffsrechte: Wer darf was sehen, bzw. nutzen?
  Beitragszahlungen etc.: nur Kassenwart? Grundsätzlich: "Need-to-know". Aber: Nicht übertreiben! Es muss handhabbar bleiben – und der Vorstand soll doch evtl. sowieso die Nichtzahler anrufen!?
- Verfügbarkeit: Datensicherung! No Backup, no mercy. Evtl. Redundanz (RAID, Sync-Clients).
  Eigene PCs/Server vs. professionelle IT as a Service – gerade bei kleinen Vereinen eher auslagern!

Beispiele für typische Probleme, konkrete Lösungsmöglichkeiten

- **Datenaustausch** per E-Mail und USB-Stick → Google-Drive, Dropbox, Nextcloud, …
  Verweis auf „Verarbeitung im Auftrag“ → **Vertrag** mit Google, Dropbox, Hoster, …?!
- Wenn man Server oder Cloud-Dienste hat, dann braucht es ein „Rollen- und **Rechtekonzept**“,
  z.B. „Dinge, die nur der Vorstand sehen sollte“ vs. „dürfen alle lesen“ (und schreiben/löschen?)
- Meist gibt es nebenläufige lokale Kopien: Vorsitzende hat ihre Dateien, Kassenwart seine, …
  Sinnvoll wären **Strukturen**: an Prozessen/Zugriffsrechtenrechten orientierte Verzeichnisse
  einheitliche Nomenklatur, sprechende Verzeichnis- und Dateinamen
  Vermüllen: z.B. Zwischenstände entsorgen → **Löschregeln** festlegen
- **Datensicherung** – was ist das, warum braucht man das, wie macht man das sinnvoll?
  Archivierung und Backup – als Verein – planen (keine „persönlichen Backups“)!
- **Verschlüsselung** – was ist das und in welchen Fällen könnte das sinnvoll sein?
  Wie kann man das einfach/handhabbar machen? Was geht nicht gut (E-Mail)?
  Alternativen (Beispiele):
  - Bestätigung, dass ein Dokument vorgelegt/geprüft wurde statt dessen Speicherung
  - auf Privat-PC: separates Benutzerkonto mit Passwort statt VeraCrypt-Container
  - Messenger (Signal, Nextcloud Talk, …) statt verschlüsselter E-Mail verwenden

Verpflichtung auf das Datengeheimnis

- Oft werden **privat Geräte und Cloud-Dienste** verwendet. Nur OK, wenn
  1. keine kritischen Daten erfasst/gespeichert werden,
  2. Daten bzw. Systeme sinnvoll technisch gesichert sind und
  3. alle Akteure geeignet vergattert wurden.
- In der Praxis sehen wir irgendwelche heruntergeladenen **Verpflichtungserklärungen**
  ggf. datenschutzrechtlich unwirksam, juristisch unpassend oder gar für den Verein schädlich
- Sinnvolle Verpflichtung: Unterweisung→Verpflichtung, **Muster** (zur Verfügung stellen)
  Beweisbarkeit Pflicht? Nein, das kann Verein entscheiden.

Auftragsverarbeitung

- Jeder Anbieter ist angeblich "DSGVO-konform". Man aber braucht entweder ein Gutachten (oder zumindest eine Aussage) eines sachverständigen unabhängigen Dritten – oder man muss selbst prüfen. Das ist nicht **so** schwer, muss aber **dokumentiert** werden! Prüfschritte:

  1. Verarbeitung im Auftrag vs. Datenweitergabe, gemeinsame Verantwortung?
  2. Verträge inkl. Anlagen und Nachweisen einsehbar?! Sonst anfordern …und dort:
  3. Gegenstand sinnvoll? Ungewünschte/Einseitige Verpflichtungen?
     Verfahren/Ansprechpartner sinnvoll geregelt? Unterverarbeiter genannt und sinnvoll?
  4. Findet die Datenverarbeitung im EU-Ausland statt (z.B. globale Rechenzentren)?
     Sind (wesentliche) Unterauftragsverarbeiter im EU-Ausland? (→ **aktuelle** SSC inkl. TIA)
     Ist eine Muttergesellschaft (mit Weisungsrecht) im EU-Ausland?

  Tipp: Auf av-vertrag.org kann man zumindest schon mal schauen, ob der Anbieter einem AV-Vertrag haben sollte, inkl. einer ersten (unverbilndlichen) Empfehlung.

  Wenn Punkt 4 zutrifft (Datentransfer in "unsichere Drittstaaten") sollte ein Profi gefragt werden.
  Und ja, die IP-Adresse wird als personenbezogenes bzw. personenbeziehbares Datum gewertet.

Übersicht aktuelle Software, Alternativen zu den (oft US-)Marktführern

- Betriebssysteme: Windows → Installation ohne Microsoft-Konto mit Rufus, ShutUp10
  Alternativen: MacOS, Linux → Anleitung der Computertruhe, MicroOS, Solus, Mint
- Office: "gemeinsame Dokumentenablage" vs. "kollaboratives Arbeiten"
  Alternativen: LibreOffice/OpenOffice, SoftMaker, OnlyOffice, iWork, … "absolute" Kompatibilität nötig?
- Anforderungen bei PDFs: lesen, kommentieren/abzeichnen, schwärzen, umstellen, bearbeiten?
  Alternativen zu Adobe Reader: Sumatra, Okular, MasterPDF Editor, …
- OneDrive, Dropbox & Co. → Verschlüsselung (z.B: mit Cryptomator) oder Alternative: luckycloud, DRACOON, YourSecureCloud, pCloud
- All-in-one-Kollaborations-Suiten: Microsoft 365, Google Workspace ("Documents") → Komplexe Verträg! Notwendige Einstellungen! Ständige Änderungen! KnowHow nötig! Alternative: Empfehlung: dPhoenixSuite von dataport, Alternativen: ownCloud (neues Backend!), Nextcloud (als "hosted": z.B. bei einem der NC-Partner, ownCube, Ionos, Hetzner, Telekom, … – auf dem eigenen Webspace: ssh-Zugang sinnvoll, Empfehlung: manitu – oder eigenem Server: nur mit IT-Profi)
- Internet-Provider: In Deutschland eher kein Problem (TKG); Hoster für Webseite(n) und E-Mail (kein GMail / Freemail) → Erfahrungen der TN, Alternativen: mailbox.org, eclipso, grommunio, Zimbra
- Webserver: US-Transfer: Consent-Tools wie UserCentrics und Cookiebot machen es eher schlimmer → Videos, Fonts und Einwilligung möglichst vom eigenen Server (AddOn/PlugIn für CMS, z.B. Maps/Video abblenden, selbst hosten oder alternativer Anbieter, 2-Klick-Lösung für Social Media-Widgets); SocialPlugins?; CAPTCHA: ReCaptcha → FriendlyCaptcha, eher nicht: hCaptcha; Google Maps (Standortfreigabe für google.com!?) → SmartMaps
- Newsletter-Tools: MailChimp → Alternativen: Empfehlungen: Rapidmail (DE, AVV), Inxmail (DE, AVV auf Anfrage), OK / komische Verträge: GetResponse (PL, SVK?, AVV, UAV, DPR); unklar: CleverReach (DE, kein AVV?, Rabatt für Non-Profit-Organisationen), KlickTipp (UK, AVV+SCC im Kundenkonto, diverse UAV), Sendinblue (nur Marketing-Bla, AVV: Hosting bei Google); "Double-OptIn" ist keine Forderung des Datenschutzes, aber dennoch sinnvoll als Missbrauchs-Sperre!
- Videokonferenz-Systeme: Teams, Skype, Zoom, Whereby, edudip, alfaview, collocall, vOffice, Veeting, visavid, BBB: bbbserver, Senfcall, Jitsi (Software, SaaS von 8x8=USA)
- Umfragen: (Google/Microsoft Forms → s.o.), Typeform, SurveyMonkey → Lamapoll, LimeSurvey, TerminBW, OpenSource: Framadate, dudle – werden aber derzeit beide nicht weiterentwickelt
  Terminvergabe: Doodle, Calendly → calendso, Terminland, online-anmeldeformular
- Spezial-Software: Verein, CRM, Datei/Mail-Archiv, Bank, Zahlungsdienstleister: Stripe → Giropay, Payone, PayPal Europe, eher nicht: Klarna (Datenleck, extensives Tracking)
- Passwörter: Prüfen, ob eigene Daten "im Netz" sind: haveibeenpwned, HPI; sicher speichern: selbst: KeePass(XC), pass, SaaS: Bitwarden, Passwork, 1Password, …
- IM: WhatsApp, Telegram; Signal, Wire, Threema, Matrix, XMPP, Briar, SMS → seriöse Anbieter (z.B: sms77), Überlegungen des BSI, diverse Vergleiche, z.B. DataGuard, AVG, Kuketz-Blog, geschlossene IM-Lösungen?, Kollaborations-Messenger: Slack → Mattermost
- Online-Kreativwerkzeuge: PLACEm, miro → Conceptboard, Padlet → Taskcard, Mentimeter / Slido → SlideLizard, Edkimo, Tweedback
- Weitere Tipps: diverse Online-Tools (bbb), nette Übersicht (wirecloud), Empfehlungen im Kuketz-Blog , Empfehlungen (Klaudia Zotzmann-Koch), VK-Tool-Vergleich (ActiveMind, 03/2021), Liste interaktiver Tools für Webinare (ohne DS-Bewertung!), Selbst-Hosting-Liste,

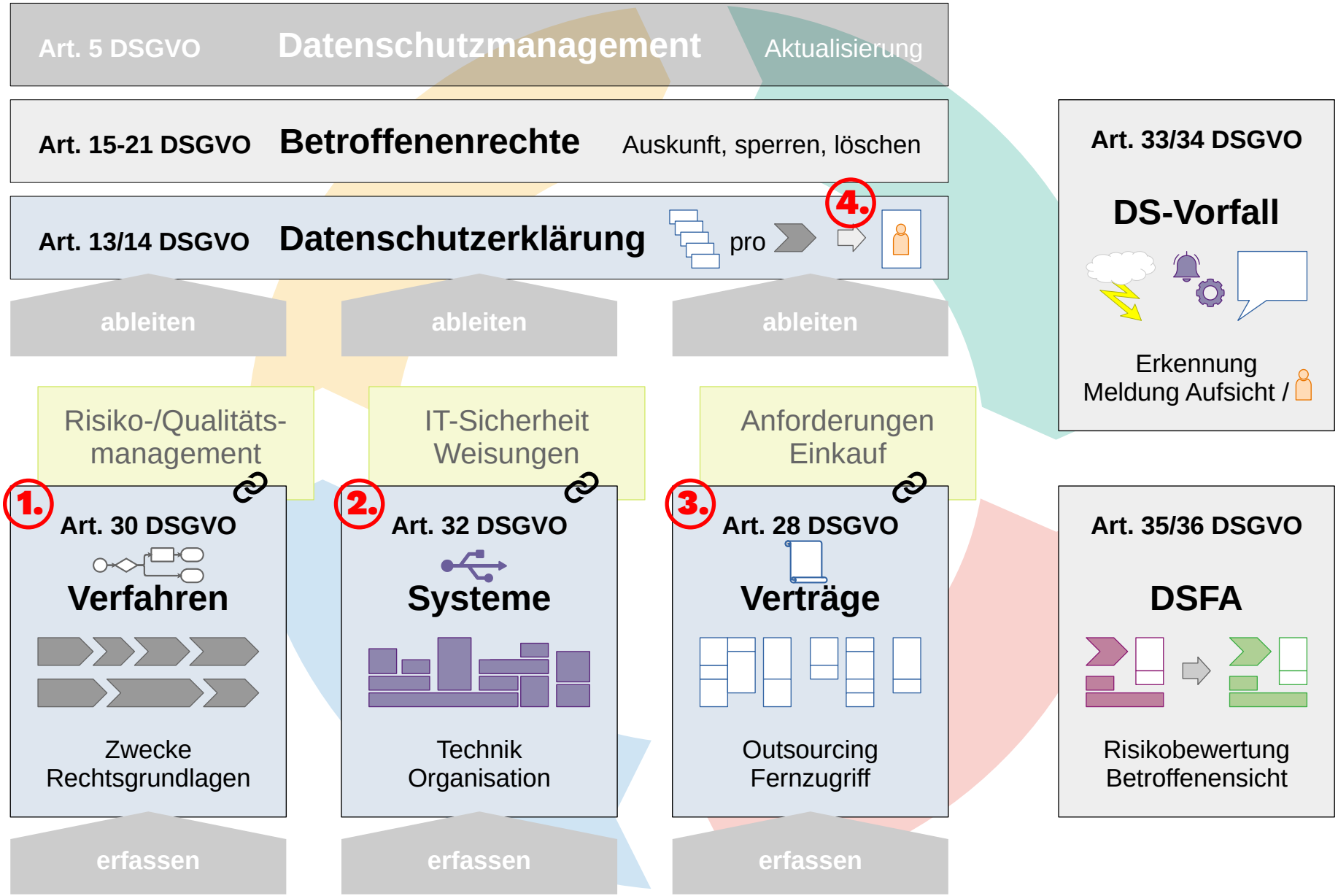
Konkrete Fragen und schriftliche Antworten

- Müssen Dokumente, die per E-Mail versendet werden, durch Kennwort geschützt werden? Wäre eine Cloud-Ablage eine Alternative? Die DSK vertritt in der OH E-Mail von 2021 die Auffassung, dass Transportverschlüsselung für "normale Mails" reicht. Wenn die Dokumente sensibel sind, kann zusätzlich ein "Öffnen-Passwort" gesetzt werden. Ja, das Versenden von Links zum passwortgeschützten Abruf aus einer Cloud ist eine Alternative. Da der Link aber aus Versehen in falsche Hände geraten kann, muss der Empfänger entweder ein Konto in der Cloud haben, oder das Passwort (oder Teile davon) müssen auf einem **zweiten Kanal** zugestellt werden, z.B. per Messenger oder SMS. Wenn eine Messenger erreichbar ist, kann man überlegen, ob man das Dokument nicht gleich darüber schicken kann.
- Gibt es einen Unterschied zwischen manuell versendeter E-Mail (TO/CC/BCC) und Mailinglisten / Newsletter-Tools? Hinsichtlich der Sicherheit der E-Mails nicht, manche Tool-Anbieter setzen aber standardmäßig **Tracking** ein. Prüfen und abschalten wenn nicht nötig, sonst als Verfahren und in die Datenschutzerklärung aufnehmen!
- Fotos: Klären von wem sie aufgenommen wurden (engagierter Fotograf vs. Gäste) und ob einzelne/alle Fotos "geteilt" werden sollen. Weniger ist mehr. Keiner schaut sich später hunderte Fotos an. Gleich ausmisten und beschriften (taggen). Festlegen, wann welche gelöscht werden.
- Wie lange müssen / dürfen p.b. Daten aufbewahrt werden? Solange es ein Verfahren gibt, dessen Zweck und Rechtsgrundlage greifen, z.B. wenn Aufbewahrungspflichten bestehen oder ein (dokumentiertes!) "berechtigtes Interesse" noch vorliegt. Anders gesagt: Alles was man nicht braucht **muss** weg!
- Was ist bei der Entsorgung / Löschung von Daten zu beachten. Was sollte vorher geregelt sein? Löschen bedeutet "physisches Löschen", nicht "sperren". Es reicht aber, Daten EIN Mal z.B. mit Nullen (oder Zufall – langsam!) zu überschreiben. Ein "normales" Löschen einer Datei löscht diese nicht, bei "normalen" (Art. 6-)Daten ist das aber bereits angemessen. Bei Art. 9-Daten ggf. nicht. Für die Entsorgung gibt es konkrete Vorschriften und Normen, siehe DIN 66399.

  Aufwändiger sind die Überlegungen, wann man was löschen sollte, da Aufbewahrungsfristen zu und berechtigte Interessen zu beachten sind. Idealerweise denkt man die Löschung bereits bei der Erhebung mit. Daher gilt die Löschung / Entsorgung als der "heilige Gral" bei den Verfahren im Datenschutz. Hinweise zum Löschkonzept: DIN 66398, Empfehlung: Podcast-Folge (fast 1,5h!).
- Was ist zum Datenschutz als Protokollant und Schriftführer im Verein zu beachten? Überlegen, ob / was namentlich notiert werden muss, wie lange was aufbewahrt werden soll und wann was wie vernichtet wird. Die Entscheidung kann sein, dass z.B. Abstimmungen und Wortmeldungen nicht namentlich protokolliert werden. Dann ist auch kein Risiko erkennbar…
- "Datenschutzgerechte Archivierung, z.B. von Protokollen"? Siehe vorherige Frage. Bei Dateien reichen (bei "normalen" Protokollen) aus meiner Sicht korrekt gesetzte Zugriffsrechte.

  Anmerkung zu Archivierung: "Revisionssicher" bedeutet nicht, dass man nichts löschen darf… Wenn Daten nach DSGVO gelöscht werden müssen (und keine Aufbewahrungspflichten dagegen stehen), dann darf die Löschanforderung nicht von der Technik des Archivsystems verhindert werden!
- Wie gehe ich mir Daten von Spender*innen um, die ich für später noch aufbewahren möchte? → Zweck klären, mögliche Technik: Verschlüsselung, z.B. symmetrisch mit ZIP oder VeraCrypt oder asymmetrisch mit GnuPG. Bei ZIP beachten, dass die standardmäßige Verschlüsselung "ZIP2.0" leicht zu brechen ist. Wenn der Inhalt sensibel ist, muss AES verwendet werden. AES-verschlüsselte ZIPs können aber nicht direkt von den im Windows/macOS/Android eingebauten Entpacker gelesen werden. Empfehlung: 7zip, **nicht** WinZIP. Alternative unter Windows: Total Commander, unter MacOS: Keka.
- ADFC / Codierung von Fahrrädern: Was ist zu beachten bei der Datenspeicherung von Bürgern durch Mitglieder und die anschließende Verarbeitung durch den Verein? Geeignete Technik?
  Bzgl. Technik: Könnte man Pseudonymisierung verwenden? Falls ja: Vier-Augen-Prinzip anwenden, ggf. Treuhändermodell, ggf. digitale Signaturen. Unterweisung der Mitglieder? Ja. Reicht aber einmalig. Kontrolle? Eigentlich schon, aber das kommt sicher komisch. Je nach angewendeter Technik ist das aber kaum nötig, z.B. könnte die Erfassung schon vorab zu Hause erfolgen, und dann nur ein Code verknüpft werden.

Erste Schritte im Datenschutz



Warum gibt es nicht datenschutzkonforme Tools

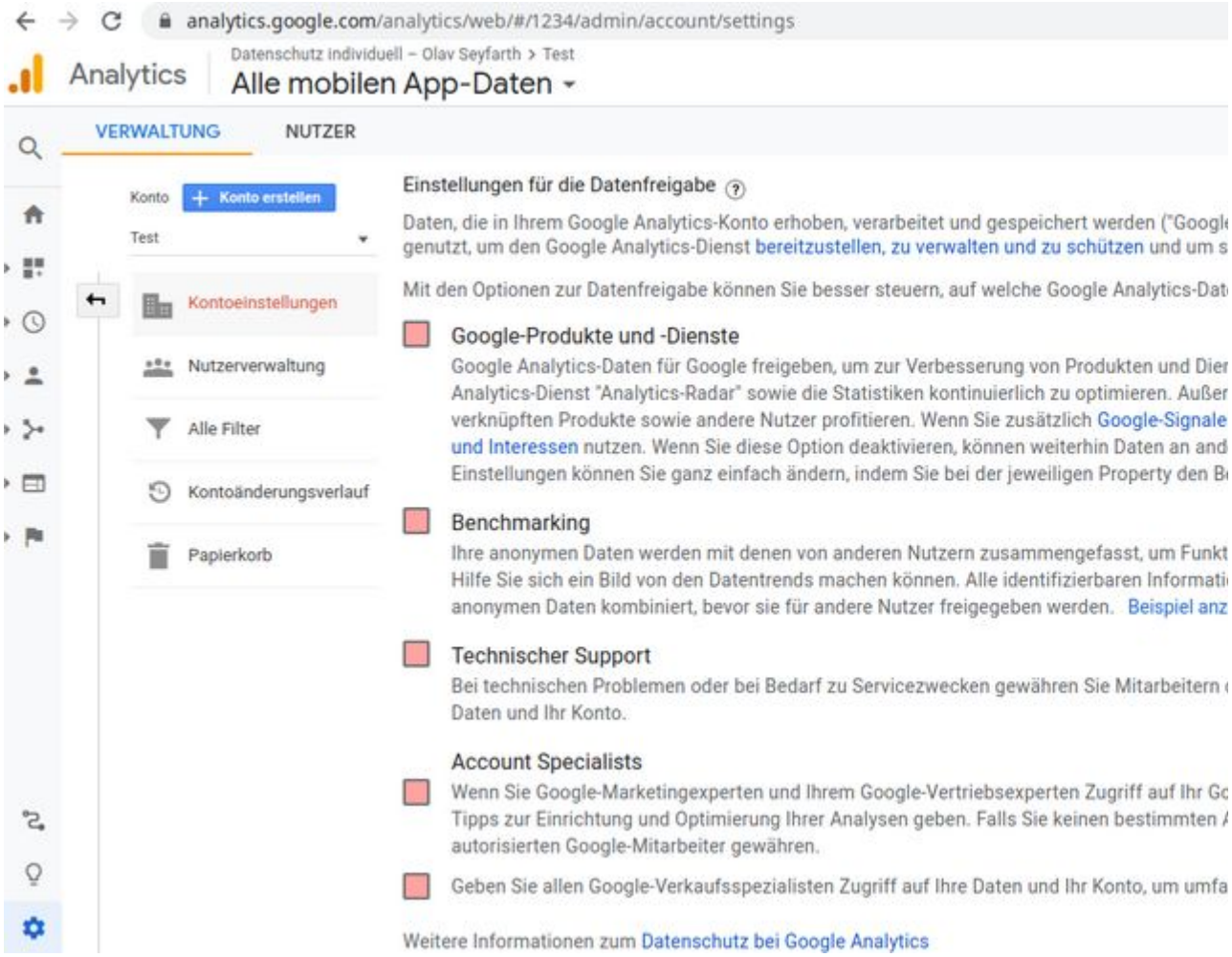
- Unkenntnis der Anfordernden
  - Technik: Kompatibilität zu Landschaft/Strategie, Schnittstellen
  - Recht: z.B. Datenschutz bei Datentransfer in Drittstaaten
  - Lizenzen: privat ≠ geschäftlich, z.T. aktive Messung
  - Veränderung: Evergreen-Modell, Verträge, Firmenkäufe
- Unklarheit in der Organisation
  - Anfordernde haben Erwartungen an die IT bzw. den DSB. Passen diese zum Rollenverständnis der IT bzw. des DSB?
  - Befugnisse zum Einkauf bzw. Verantwortung für den Betrieb von Cloud-Diensten zwischen Prozessverantwortliche und IT abgegrenzt?
- Keine Zeit für Marktvergleich, Test, Verträge lesen, …

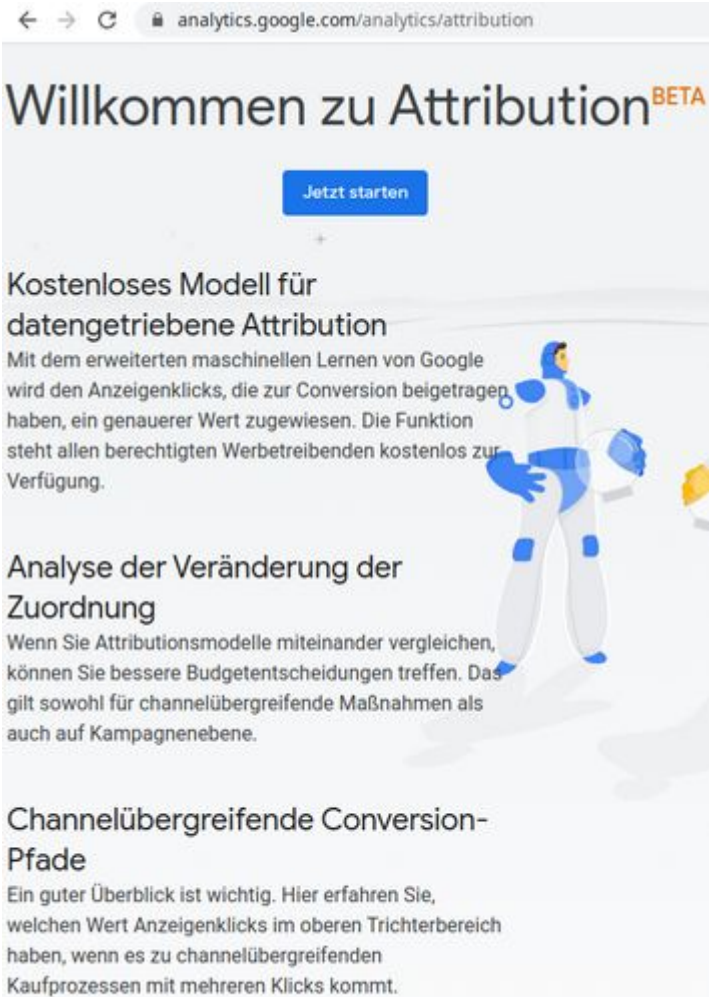
Typische Probleme bei Cloud-Diensten

- Datentransfer in Staaten ohne angemessenes Datenschutzniveau
  - auch Unterauftragnehmer! Selbst bei Speicherung in der EU
  - auch CDN? Schriftarten? Code?
- Datennutzung durch den Verarbeiter für dessen eigene Zwecke, z.B. Telemetriedaten zur Verbesserung der Produktqualität
  - Unterscheidet der Anbieter von sich aus?
  - Was kann (nicht) unterbunden werden?
  - Wer müsste das konfigurieren? (oft Fachabteilung!)
  - Wer kontrolliert die Konfiguration? (tiefe IT-Kenntnis erforderlich!)
- In meinen Augen „seltsam“ – unzulässig?
  - direktes Vertragsverhältnis mit MA, z.B. bei miro, kununu engage

Eigene Zwecke bei Google Analytics

- Profilbildung kann soweit ich weiß NICHT abgeschaltet werden(!)
  Zusätzliche Optionen sollten aus- bzw. nicht eingeschaltet werden:





Eigene Zwecke bei Firebase Cloud Messaging

- Dies muss IMMER abgeschaltet (und dennoch erklärt) werden:

console.firebase.google.com/project/test/settings/privacy

Firebase

Projektübersicht

Entwickeln
Authentication, Firestore Database, ...

Veröffentlichen und beobachten
Crashlytics, Performance, Test Lab ...

Analytics
Dashboard, Realtime, Events, Conve...

Einbeziehen

Predictions
A/B Testing
Cloud Messaging
In-App Messaging
Remote Config
Dynamic Links
AdMob

Test

Projekteinstellungen

Allgemein | Cloud Messaging | Integrationen | Dienstkonten | Datenschutz | Nutzer und Berechtigungen

Dienstdaten

Was sind Firebase-Dienstdaten?

Firebase-Dienstdaten sind die personenbezogenen Daten, die Google während der Bereitstellung und Verwaltung der Firebase-Dienste erhebt und erstellt. Kundendaten und Google Cloud-Dienstdaten zählen nicht dazu. Google nutzt die Firebase-Dienstdaten gemäß seiner Datenschutzerklärung und den anwendbaren Nutzungsbedingungen.
Weitere Informationen

Einstellungen für Firebase-Dienstdaten

Über die folgende Einstellung haben Sie mehr Kontrolle darüber, wie Google Ihre Firebase-Dienstdaten verwendet.

☑ Google darf meine Firebase-Dienstdaten verwenden, um mir umfangreiche Analysen, Statistiken und Empfehlungen zu meiner Nutzung von **Nicht-Firebase**-Diensten von Google zur Verfügung zu stellen und die **Nicht-Firebase**-Dienste von Google zu verbessern.

*Wenn Sie diese Option deaktivieren, werden die Firebase-Dienstdaten trotzdem für Empfehlungen und Verbesserungen der **Firebase**-Dienste verwendet und dazu, Ihnen andere gewünschte Dienste wie Google-Produkte, die Sie mit Ihrem Firebase-Projekt verknüpfen, bereitzustellen und diese zu verbessern.*

Eigene Zwecke: Microsoft 365

- Abgrenzung ist vertraglich weitestgehend erfolgt
  - aktuelle OST müssen beim Lizenzgeber angefordert werden
  - technisch Einflussmöglichkeiten gering, z.T. kostenpflichtig

- DSGVO-konforme Einstellung insgesamt
  - verschachtelte Konfiguration, viele Abhängigkeiten
  - erfordert (gerade initial) zu viel Expertenwissen
  - muss ständig neu bewertet und nachjustiert werden

Indizien für datenschutzfreundliche Tools

- Anbieter
  - aus der EU (oder einem Land mit Angemessenheitsbeschluss)
  - auch alle Unterauftragnehmer – oder E2E-verschlüsselt
  - Informations-, Auskunfts-, Opt-Out- und Löschmöglichkeiten
- Vertrag
  - AVV hinreichend spezifische, zur Leistung passende(!) TOM
  - Abgrenzung AV $\leftrightarrow$ eigene Zwecke, z.B. Telemetrie, Debug/Crash
  - in Ausnahmefällen: gemeinsame Verantwortung?

Alternative – Vergleich mit Marktführer

- in der Regel sehr ähnliche Kernfunktionen
  - in der Regel akzeptabel
- z.T. geringere Performance, Reife oder Integration
  - ggf. problematisch
  - wichtig für IT: direkt benutzbare Schnittstellen (Stripe, Trello)
  - Unterstützung des gesamten Vertriebsprozesses (Livestorm)
- höherer Preis
  - wie viel ist akzeptabel/verfügbar? Warum darf online nichts kosten?
  - Marktführer (wirklich) „kostenlos“? **Geschäftsmodell hinterfragen!**

Webtracking & Co.

- Analytics / Heatmaps
  - Google[1], Adobe[2]
  - Mouseflow[1], Hotjar[2]
- Soziale Netzwerke
  - Facebook[1], LinkedIn[2]
- Sonstige
  - ReCaptcha[1]
  - Cookiebot[1], UserCentrics[2]

- Analytics / Heatmaps
  - matomo[2], Plausible[2], fathom[3], Snowplow, Ackee[4], GoAccess[4]
  - smartlook[15], Open Web Ana.[4]
- Landing Pages / Redirects
- Sonstige
  - Friendly Captcha[6]
  - Pixelmate[2], Moove[1], Osano

[1] freemium, [2] SaaS kostenpflichtig, [3] kostenpflichtig, nicht OpenSource
[4] kein SaaS, [5] nutzt AWS, [6] Basic nutzt CloudFlare
Übersichten: Plausible Blog (hervorragend!), Kinsta, Monster Insights

Für viele Anwendungen gibt es gute Alternativen

Hinweis: Alle Links dieser Seite wurden ins Handout übernommen und sind dort z.T. vollständiger

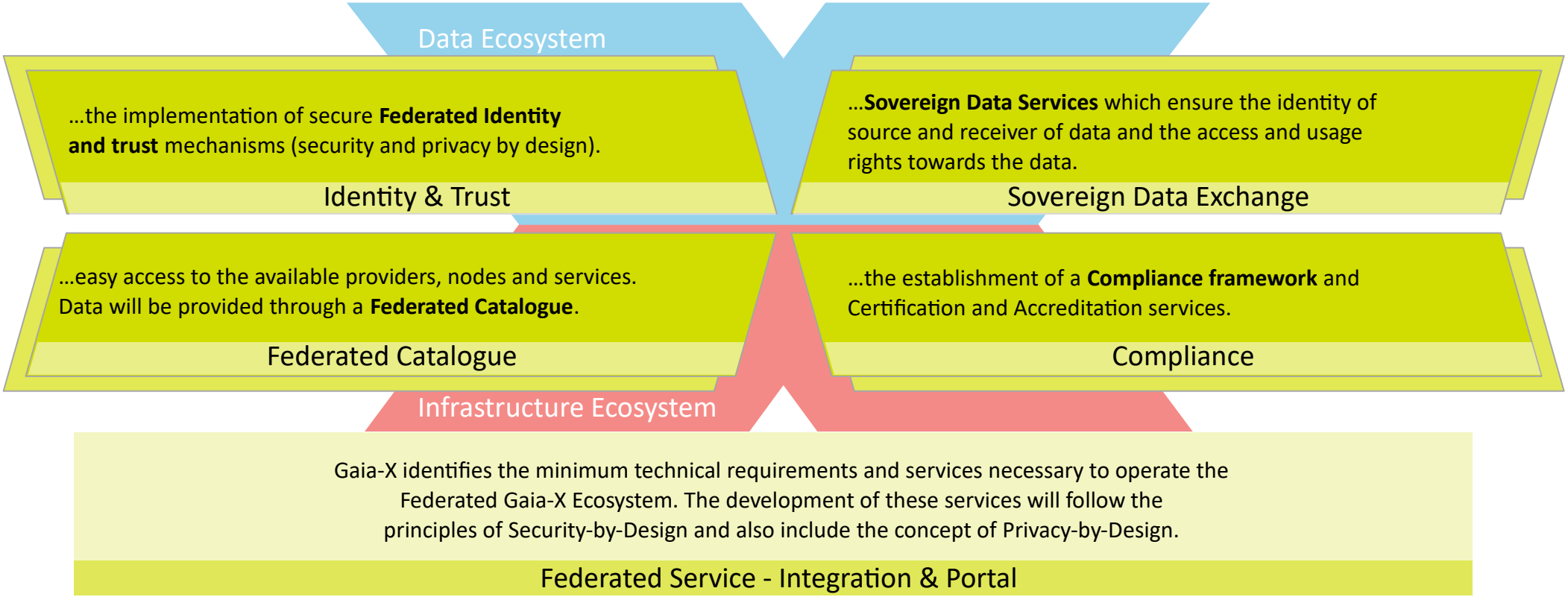
Cloud-Speicher & Zusatzfunktionen	Dropbox, Google Drive OneDrive, iCloud, Box	luckycloud, DRACOON, YourSecureCloud, pCloud
Groupware: E-Mail, Kalender, Kontakte	Google Workspace, Microsoft 365	Nextcloud, mailbox.org, eclipso, grammm, Zimbra[1]
Videokonferenzen	Webex, Teams, Skype, Zoom, GoToMeeting	edudip, alfaview, collocall, bbbserver, vOffice, Veeting
Collaboration	Slack, miro	Mattermost[1], Conceptboard
Umfragen, Terminvergabe	Google, Typeform, SurveyMonkey, Doodle, Calendly	Lamapoll, LimeSurvey, –[2], calendso[1], Terminland, online-anmeldeformular.de
Zahlungsabwicklung	Stripe	Payone, PayPal Europe

[1] nur datenschutzkonform, wenn selbst oder bei EU-Provider gehostet

[2] Framadate und dudle: derzeit keine aktive Weiterentwicklung

Gaia-X – Heilsbringer oder Totgeburt

The technical implementation of these Federation Services focuses on…



Quelle: https://events.bwcon.de/events/sig-cloud-computing-gaia-x/

https://gaia-x.eu/

Olav Seyfarth

- Dipl.-Informatiker (FH), CISO (ISTA)
  Externer DSB für kleinere Unternehmen
  Lehrbeauftragter am ZfS der Uni FR
- OpenSource und Nerd:
  Nextcloud, Arch Linux
- Netzpolitik und Ehrenamt:
  freiburg.social, Computertruhe

https://datenschutz-individuell.de/