Roter Baum e. V.

Brandstr. 15
04277 Leipzig

Dokumentation

„Datenschutz für NPOs – ein Forum für Expert*innen und Praktiker*innen“
am 13.12.2018 von 16:00 bis 20:00 Uhr in der Harkortstr. 10, 04109 Leipzig

Inhaltsverzeichnis

1 Entstehungshintergrund

Die Entstehungsgeschichte des Forums geht zurück auf einen DSGVO-Einführungsworkshop im Juni 2018, der vom Netzwerk Tolerantes Sachsen in den Räumen des Antidiskriminierungsbüro Sachsen e. V.s in Leipzig veranstaltet wurde. Bei einem informellen Gespräch im Anschluss an die Veranstaltung fanden sich einige Personen aus verschiedenen Vereinen zusammen, die ein geteiltes Interesse an einer vertieften Auseinandersetzung mit Datenschutz im Vereinskontext hatten.

Daraus entstand der lose Zusammenschluss „Datenschutz und jetzt?“, der seitdem einige Male in unregelmäßigen Abständen zusammen gekommen ist. Mittelfristiger Plan ist die Entwicklung einer Strategie zur Stärkung des Datenschutz-Niveaus in der sächsischen Vereinslandschaft durch die Schaffung zugänglicher und nachhaltiger Beratungs- und Weiterbildungsangebote.

Das Forum war als Auftakt zur Entwicklung dieser Strategie konzipiert. Seine Ziele bestanden auf der Erhebung eines Ist-Zustands auf drei Ebenen:

1. Problembewusstsein: Welche Relevanz wird Datenschutz in lokalen Vereinen beigemessen und welche realen Gefahren gibt es?
2. Praxis: Was sind häufige Probleme und welche Lösungsansätze gibt es?
3. Vernetzung: Wer sind lokale Expert*innen und Anlaufstellen? Welche Vereine beschäftigen sich intensiver mit Fragen des Datenschutzes?

Als Veranstalter des Forums fungierte der Rote Baum e. V.; Kooperationspartner*innen waren plus humanité e. V., das Netzwerk Tolerantes Sachsen und die Freiwilligen-Agentur-Leipzig e. V. Aus dem Kreis dieser Vereine wurden für das Jahr 2019 außerdem ein Finanzantrag zur Einrichtung einer Datenschutz-Sprechstunde über die Stadt Leipzig gestellt.

2 Problembewusstsein

Das Forum begann nach einleitenden Worten zur Entstehung der Veranstaltung und dem geplanten Ablauf mit einem Erfahrungsaustausch in Kleingruppen. Leitfragen waren, welche Bedeutung Datenschutz in der eigenen Organisation hat und in welchen Zusammenhängen Datenschutz-Fragen bereits diskutiert wurden.

2.1 Kollektive Bedarfsanalyse

Motivation für diesen Erfahrungsaustausch war es, konkret zu ermitteln, welche Bedarfe für Beratung und Qualfizierung im Bereich Datenschutz bei den beim Forum vertretenen Vereinen bestehen. Der Austausch war in allen Kleingruppen rege und förderte ein breites Bild an Beratungs- und Weiterbildungsbedarfen zu Tage, das einen guten Ausgangspunkt für die Entwicklung einer langfristigen Strategie zur Stärkung des Datenschutz-Niveaus in sächsischen NPOs liefert.

Als Schwerpunkte ergaben sich die Bereiche Informationspflichten/Datenschutzerklärungen, Einwilligungen in Datenverarbeitungen, Verschlüsselung von Kommunikation und gespeicherte Daten sowie die Sicherung der Daten von Mitgliedern und Unterstützer*innen.

Als übergeordnete, allgemeine Punkte wurden Fragen nach umfassender Weiterbildung zum Thema und nach Möglichkeiten zur Prävention von Angriffen aufgeworfen. Außerdem wurde Klärungsbedarf zu Datenschutz beim Fotografieren und bei der Sicherung analoger Unterlagen sowie Unklarheiten bei Zugriffsrechten und beim Begriff der „besonders sensiblen Daten“ vorgemerkt.

2.2 Input: Warum Datenschutz?

Der erste Input des Forums stellte den zweiten Teil des Blocks Problembewusstsein dar. Nach der gemeinsamen Sammlung konkreter Herausforderungen beleuchtete Rainer Rodewald vom Bündnis Privatsphäre Leipzig e. V. aus verschiedenen Perspektiven die Notwendigkeit von Datenschutz.

Er zeigte zunächst moderne Rechtsgrundlagen auf und machte dann Herausforderungen und Bedrohungen in der von ihm als „Überwachungskapitalismus“ bezeichneten Gesellschaft der Gegenwart deutlich. Diese Gesellschaftsformation sei durch zunehmenden Verhaltenskontrolle und -manipulation, die sich auf große Datensammlungen stütze, und durch die Kommerzialisierung und Monopolisierung des Geschäfts mit diesen Daten, gekennzeichnet.

Anschließend ging er auf die Potentiale und Grenzen der Schutzmöglichkeiten durch Verschlüsselungssysteme ein. Zur konkreten Entscheidung für das Ausmaß technischer Sicherheitsmaßnahmen im Vereinsalltag plädierte er für „Bedrohungsmodelle als Mittel zur Selbstermächtigung“. Ausführlich legte er einen praktischen Ansatz dar, der in konkreten Konstellationen erlaubt, die jeweiligen schützenswerten Güter, potentiellen Angreifer*innen, Risiken bei Schutzversagen und die möglichen Angriffswege zu identifizieren. Diese Grundlage erlaube eine fundierte Entscheidung für technische Maßnahmen, bei denen Risiko und Aufwand in angemessenem Verhältnis stünden.

Die vollständige und anhand der Folien gut nachvollziehbare Präsentation ist einsehbar unter `https://privatsphaere-leipzig.org/slides/Dateschutz-fuer-NGOs/#/`.

3 Praxis

Nachdem die Vorstellung des Ansatzes zur Entwicklung von Bedrohungsmodellen bereits zum Praxisteil übergeleitet hatte, folgten drei Inputs, die mit je unterschiedlichen Schwerpunkten Handlungsoptionen zur Stärkung des vereinseigenen Datenschutz-Niveaus aufzeigten.

3.1 Input: Datensparsamkeit und eigene Infrastruktur

Den Anfang machte herr flupke von der dezentrale e. V., den er als „Verein für technologische Selbstermächtigung und rabiates Basteln“ vorstellte. herr flupke war angefragt, um einen Einblick in die Datenschutz-Praxis der dezentrale als mit hohem Problembewusstsein und technischem Know-how ausgestatteter Hackerspace zu geben. Er hat seinen Input im Nachhinein ausformuliert und uns für diese Dokumentation zur Verfügung gestellt:

> Wir sind ein Hackerspace, aber lasst euch davon nicht verwirren. Im Grunde sind wir nur Hippies mit Computern. Nun leben wir schon einige Zeit mit Rechnern und Netzwerken und haben (kulturell) Wissen und Erfahrung angesammelt. Dies lässt sich unter anderem mit dem folgenden Satz zusammenfassen: Personenbezogene Daten sind der radioaktive Abfall unserer Zeit. Ja, man kann sie sammeln und tolle Dinge damit machen, aber sie bleiben radioaktiver Abfall. Wenn man etwas mit ihnen anstellt, sollte man vorsichtig sein. Nicht nur vorsichtig, sondern auch faul - so richtig faul.
>
> Daten, die man nicht hat, muss man nicht schützen. Um Daten, die man nicht erhebt, muss man sich nicht kümmern. Daten, für die man sich nicht interessiert, binden keine Aufmerksamkeit und Ressourcen. Das deutsche Stichwort ist „Datensparsamkeit“.
>
> Datenschutz betreiben wir offensiv und defensiv. Offensiv sind alle Maßnahmen, deren Ergebnis wir direkt beeinflussen können. Defensiv sind alle Maßnahmen, in denen wir trotz ihrer inhärenten Problematik versuchen, die Nachteile (z. B. erhobene Daten) zu minimieren. Offensiv ist z. B. der Umgang mit Personendaten. Im Verein gibt es zunächst keine Klarnamenpflicht. Jede Person kann unter einem beliebigen Namen auftreten. Das schützt zum einen die legale Identität (was wir nicht kennen, kann uns auch nicht abhanden kommen) und es ermöglicht einen sozialeren Umgang. Gerade wenn man online und offline auftritt, möchte man das etwas abgrenzen. In (sozialen) Gruppen etablieren sich ohnehin schnell Spitznamen, die niemand gegen einen Ausweis überprüft. Warum also Ausweisdaten überhaupt erheben? Die einzigen in der dezentrale mit Klarnamen vermerkten Personen sind aus dem Vorstand bei juristischer Notwendigkeit (z.B. im Umgang mit dem Amtsgericht). In Parteien kann man z. B. auch unter Pseudonym eintreten. Die Notwendigkeit für Datenerhebung (siehe auch vorhin: „Zweckgebundenheit der Datenverarbeitung“) ist häufig deutlich geringer als die meisten Menschen glauben. Das bedeutet natürlich wieder: weniger Daten - weniger Arbeit ... Wir sind halt nur Hippies mit Computern.
>
> Wir haben eine Webseite unter `https://dezentrale.space`. Da geht es bei uns schon los. HTTP**S**. Das ’S’ deutet die Verwendung einer verschlüsselten Verbindung (mittels TLS) an. Von Außen kann z. B. der Internetanbieter nicht sehen, **was** von unserer Seite abgerufen wird. (Der Umstand, dass dezentrale.space besucht wird, ist allerdings nach wie vor sichtbar.) Die Verschlüsselung mittels TLS ist dank „let’s encrypt“ heutzutage kein Problem mehr (und auch kostenlos).
>
> Webseiten, besonders wenn sie de facto nur Visitenkarten im Internet sind, kann man sehr schmal bauen. Hier sieht man mal die Systemlast unseres Webservers. Mir ist klar, dass die wenigsten mit diesem Bild vertraut sind, aber nur ein Punkt ist wichtig: „CPU 0,3%“. Mit all den Dingen, die wir (nicht) machen, haben wir kaum Last auf der Maschine. Das bedeutet, dass z. B. mehrere Vereine eine Webseite oder mehrere Dienste auf einem Server betreiben können. Vielleicht kann auch ein befreundetes Technikkollektiv, sich um die Infrastruktur kümmern. Anbieter, bei denen man sich eine Webseite durch Klötzchen-Schieben auf dem Bildschirm bauen kann, sind die Hölle - nicht nur aus Datenschutzsicht, sondern auch aus Performance-Gründen.

Auf dieser nächsten Seite sieht man auch, welche Seiten von unserem Server abgefragt wurden. Diese Übersicht wird direkt auf dem Server (aus den Logdaten) erzeugt. Es gibt keinen Grund Dienste von Google o. ä. dafür zu nutzen. Die Datenschutzerklärung wird kürzer und die Performance steigt. Auch die Zeile mit der „14“ ist interessant. Hier wird die Schriftart für die Darstellung der Webseite von unseren Servern geladen. Sehr viele Vorlagen (oder Templates) holen sich diese Schriftarten bei Google oder von dedizierten Anbietern. Das bedeutet, das Nutzerdaten (IP, Browserkennung etc.) an diese dritte Partei übertragen werden. Die Datenschutzerklärung wird länger und wir müssten sicherstellen, dass dieser Drittanbieter datenschutzkonform arbeitet. Das ist Aufwand. Wir sind Hippies und faul. Deshalb haben wir das gleich bei uns auf dem Server, den wir kontrollieren. Wieder Arbeit vermieden.

Die Logdaten werden bei uns 14 Tage gespeichert. Das reicht, um ggf. Probleme nachzuverfolgen. Der Rest interessiert uns nicht. Wenn alles einmal läuft, kann man Logging auch gleich abschalten. Daten, die man nicht hat, muss man auch nicht aufwändig schützen.

Wir betreiben auch Mailinglisten. Hier kann sich jeder mit einer beliebigen E-Mail-Adresse (und Namen) registrieren. Es gibt ein Archiv, aber neugierige MitbürgerInnen finden einen nicht sofort, wenn man nicht seinen Klarnamen verwendet. Das ist kein absoluter Schutz, aber eine nützliche Indiskretion. Wir brauchen keine Klarnamen für den Betrieb, systembedingt aber eine E-Mail-Adresse. Wo die wieder mit welchen Daten registriert ist, interessiert uns nicht (und können wir auch kaum nachprüfen). Wir vermeiden auch hier wieder personenbezogene Daten.

Bei uns gibt es auch die Überlegung eines sogenannten „Datenbriefes“: Einmal im Jahr soll einer Person proaktiv mitgeteilt werden, welche Daten wir zu welchem Zweck gespeichert haben und wer (warum) darauf Zugriff hat. Das ist zum einem eine Geste an unsere Mitglieder und NutzerInnen. Zum anderen zwingt einen dieser Prozess, einmal im Jahr die Datenbestände zu durchforsten und ggf. zu löschen.

Datenschutz umfasst bei uns auch defensive Maßnahmen. Am Anfang erwähnte ich unsere Adresse in der Dreilindenstraße 19. Wir verweisen natürlich auf eine Karte und die meisten erkennen sofort den Lindenauer Markt. Interessant ist aber, dass wir dafür OpenStreetMap nutzen. Zum einen sind die Daten frei verfügbar, zum anderen werden auf dem Kartenserver deutlich weniger Daten erhoben und gespeichert als bei z. B. Google Maps. Hier können wir die Datenerhebung nicht verhindern, aber durch eine geschickte Anbieterwahl die Nachteile für unsere NutzerInnen minimieren.

Das alles ist schön und gut, aber wie kommt man durch dieses Datenschutz-Nirvana? Ganz einfach: Zettel und Stift. Ich empfehle allen, einfach mal übliche Interaktionen/Prozesse im Verein zu durchlaufen und zu notieren, welche Daten in jedem Schritt erhoben werden. Das sollten im Idealfall mehrere Personen unabhängig voneinander machen, um ein besseres (Lage-)Bild zu bekommen. In einem Verein sind Mitgliederaufnahme, Ladungen zu Sitzungen, Mitgliederaustritt und das Informieren über den Verein als interessierte Neue (z. B. auf der Webseite) gute Startpunkte für diese Datensafari.

Zusammenfassend lässt sich folgendes sagen: Personenbezogene Daten sind der radioaktive Abfall unserer Zeit. Dem Datenschutz sollte man sowohl offensiv (durch Datenvermeidung/-sparsamkeit) als auch defensiv (durch Nachteils- und (strategische) Arbeitsvermeidung) begegnen.

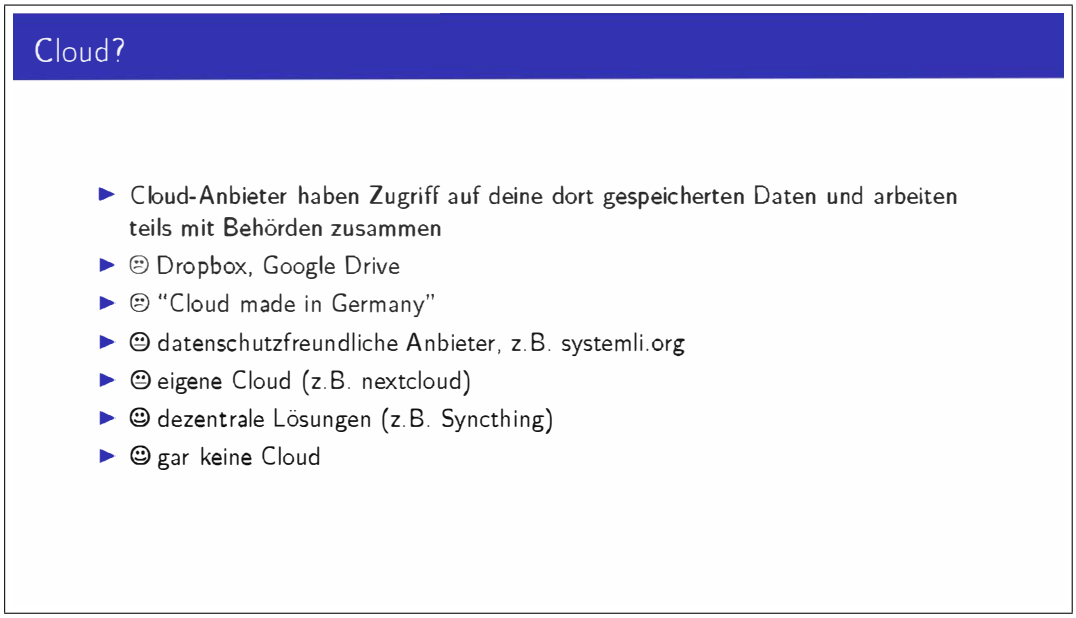
Verantwortungsvoll handeln, heißt auch zu wissen, wessen Auto man im Notfall anzünden kann* und auch sich sicher zu sein, dass niemand einen Grund hat nach dem eigenen Fahrzeug

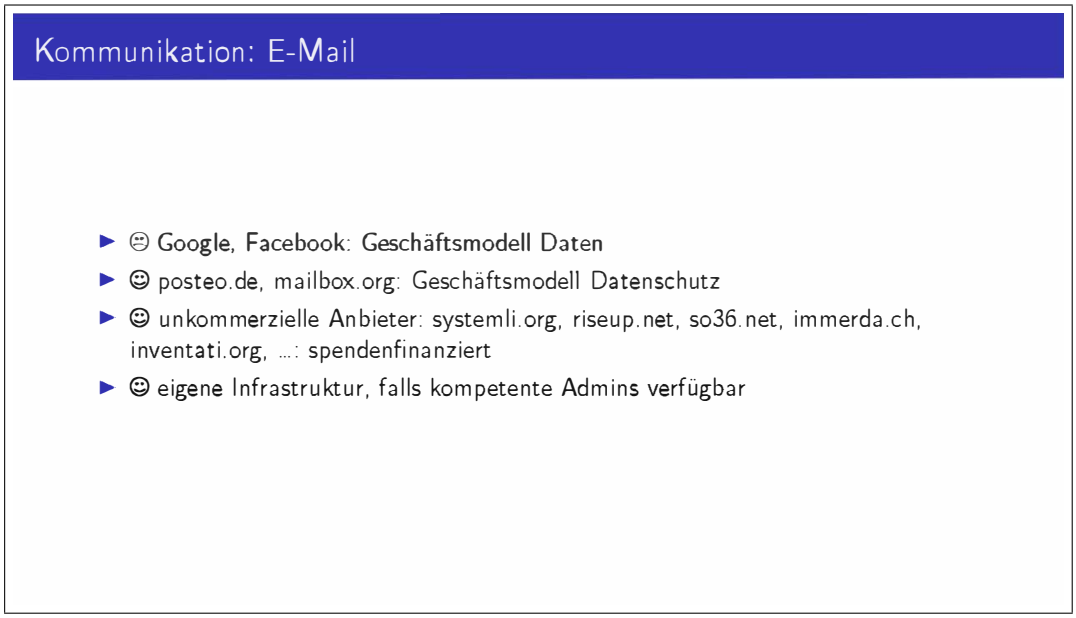
zu trachten, weil man Daten schützt.

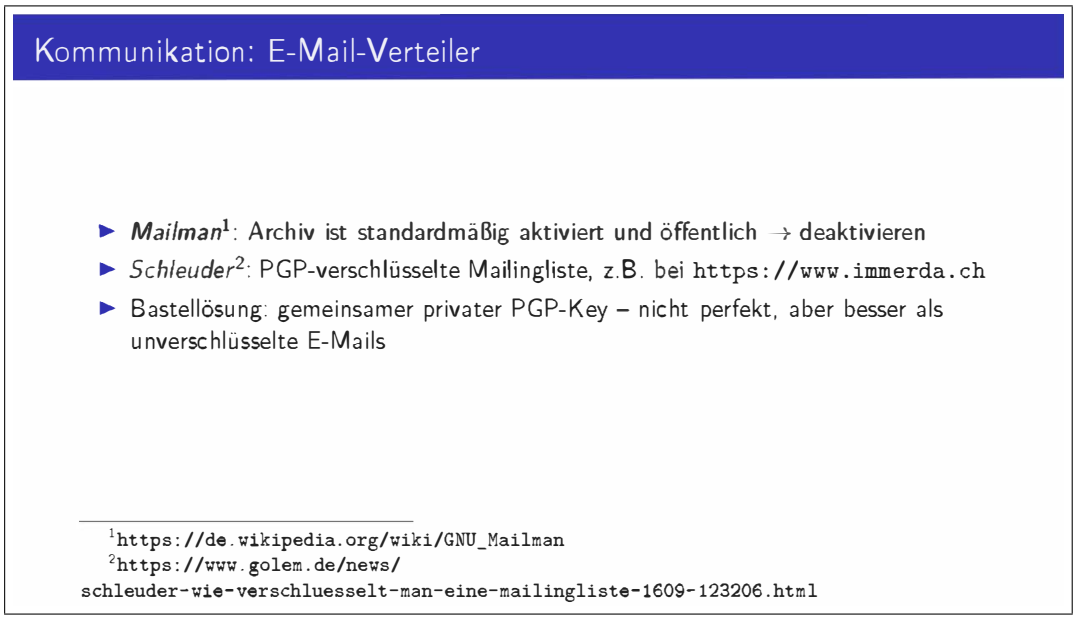
* Schon mal bei Google probiert? Wenn ihr nicht wisst, wie ihr die erreicht, denen ihr (indirekt) Daten zuschanzt, sollte man ins Grübeln kommen.

3.2 Input: Technische Ansätze für mehr IT-Sicherheit

Als nächster Referent nahm Ralph, der für mehrere sächsische NPOs die IT-Infrastruktur betreibt, die Bereiche Cloud, E-Mail- und Messenger-Kommunikation in den Blick und stellte jeweils vergleichend gängige und alternative Optionen in Hinblick auf die damit verbundene Sicherheit gegenüber. Die entsprechenden Folien seiner Präsentation sind im folgenden abgebildet:



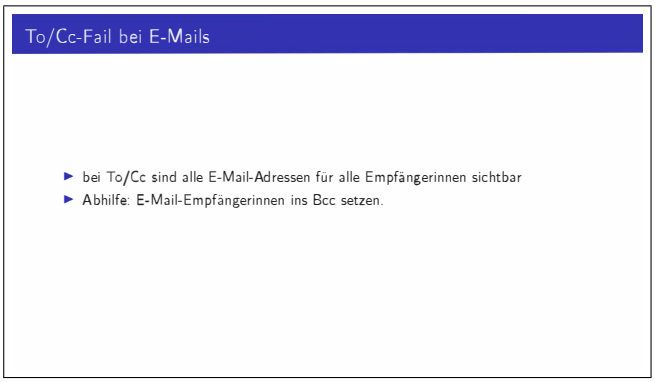


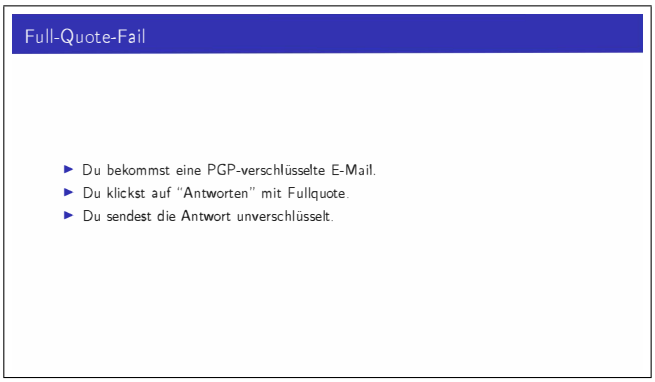


Im Rahmen dieser Ausführungen gab es von Ralph ein eindeutiges Plädoyer zur Nutzung von PGP für verschlüsselte E-Mail-Kommunikation zum Schutz der Kommunikationsinhalte. Für den weitaus schwierigen Schutz der Metadaten der Kommunikation empfahl Ralph den Rückgriff auf die in den Folien aufgeführten, vertrauenswürdigen Anbieter. In Bezug auf Messenger-Apps sprach er sich eindeutig für die Nutzung von Signal aus und machte deutlich, dass er Telegram nicht für einen vertrauenswürdigen Messenger hält.

Er machte außerdem deutlich, warum er eine Trennung von privaten und dienstlichen IT-Geräten für unerlässlich hält: Beim Verlust privater, unverschlüsselter USB-Sticks oder Computer (etwa durch Diebstahl) ist die weitere Verwendung der darauf befindlichen Daten genauso unkontrollierbar wie in dem Szenario, dass eine Person mit Daten auf ihren Privatgeräten den Verein verlässt - womöglich sogar im Streit. An seine Vorredner anschließend leitete er hieraus einen Appell zu Verschlüsselung, Datensparsamkeit und dem Entwickeln von Bedrohungsszenarien ab.

Zum Abschluss seines Kurzvortrags stellte Ralph eine Reihe typischer Anwendungsfehler vor, die zu Sicherheitslücken trotz sicherer Software führen:





Schlüssel-Fail

- Du benutzt einen verschlüsselnden Messenger oder PGP.
- Dein Handy/Computer ist nicht verschlüsselt.
- Du verlierst das Gerät.

Verschlüsselung nutzlos, wenn der Schlüssel daneben liegt.

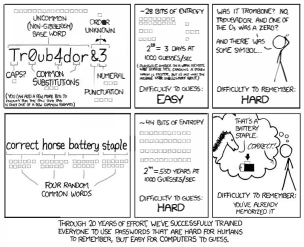
Passwort-Fail

Das Passwort

- ist zu kurz / zu einfach
- besteht aus Daten, die sich über dich in Erfahrung bringen lassen: Name des Haustiers, Geburtstag, ...
- klebt an deinem Bildschirm
- ist bei jedem Dienst (fast) das gleiche

Ein geeigneter Ort zum Speichern eurer Passwörter ist ein **Passwortmanager**, z.B. *KeePassX*. Keine Onlinedienste!

Was ist ein gutes Passwort?



https://xkcd.com/936

Passwort-Vergessen-Fail

- Du hast ein sicheres Passwort bei einem Webdienst.
- *Passwort vergessen* → *Wie lautet der Geburtsname Ihrer Mutter?*

Passwörter bei Vereinen/NGOs

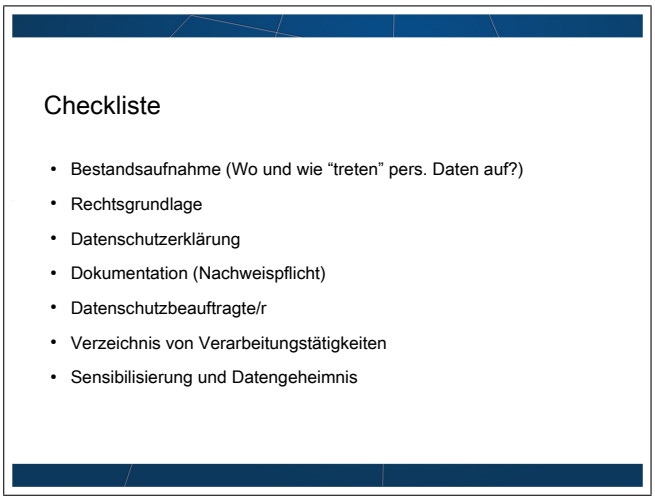
- Problem: Manchmal teilen sich mehrere Leute ein Passwort (z.B. E-Mail-Account, verschlüsselter Bürorechner)
- Tipp: an möglichst wenigen Stellen ein gemeinsames Passwort erfordern
  - Beispiel: Bürorechner verschlüsselt, darauf KeePassX-Container: lieber das selbe komplexe Passwort als zwei verschiedene einfache
- Tipp: Passwörter gelegentlich ändern

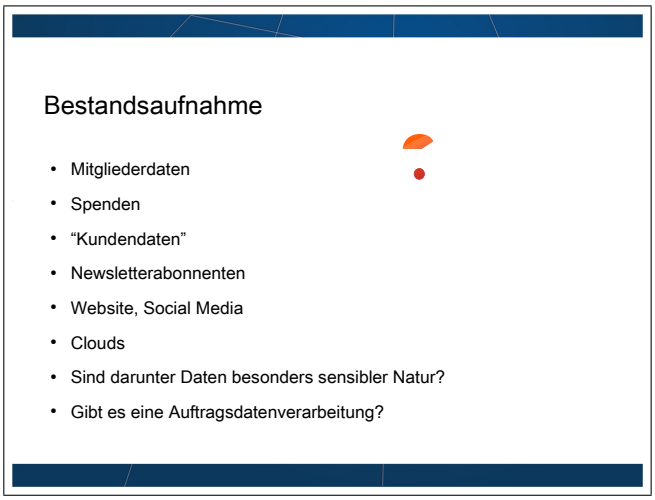
Backups

- regelmäßig
- auf verschlüsselten externen Speichermedien
- an verschiedenen Orten
- automatisiert – mit Software wie *BackInTime* (Linux), ...

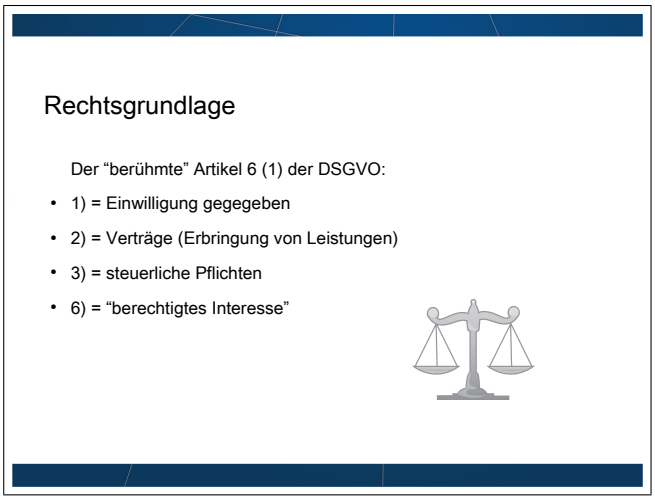
3.3 Input: Auf dem Weg zum DSGVO-konformen Verein

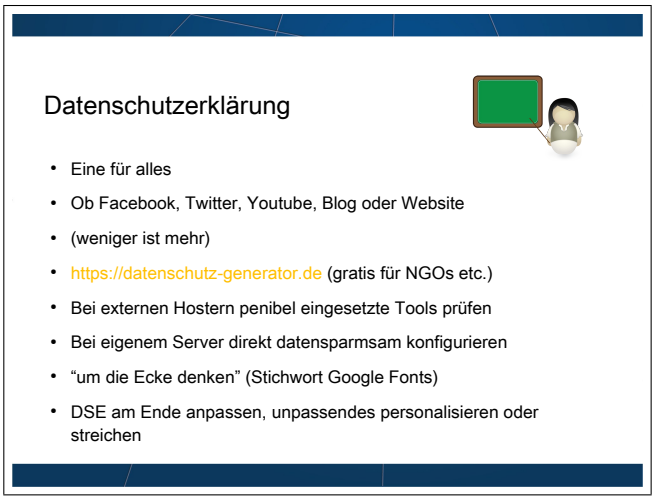
Der letzte Input des Forums fokussierte die rechtliche Perspektive, die vielen Teilnehmenden in Bezug auf ihre Vereinspraxis am drängendsten erschien. Gregor Henker, der als Datenschutzbeauftragter ausgebildet und tätig ist, gab mit seiner Präsentation eine Checkliste an die Hand, die Prioritäten und Aufgaben auf dem Weg zu einer rechtssicheren Praxis aufzeigte. Die Checkliste sieht als ersten Schritt eine Bestandsaufnahme vor, um sich bewusst zu machen, welche Datenverarbeitungen im eigenen Verein überhaupt stattfinden. In diesem Zuge empfiehlt er, gleich festzuhalten, welche dieser Verarbeitungen besonders sensible Daten betreffen und welche von Dritten weiterverarbeitet werden und damit einen Auftragsdaten-Verarbeitungsvertrag brauchen.





Als nächsten Schritt gilt es, für jede Verarbeitungstätigkeit zu prüfen, auf welcher Rechtsgrundlage sie erfolgt. Anschließend könne eine Datenschutzerklärung erstellt werden, die über die entsprechenden Verarbeitungstätigkeiten informiert. Dazu empfahl Gregor Henker einen Generator, der rechtssichere Formulierungen liefere und hilfreich sei, um versteckte Datenverarbeitungen in der Online-Präsenz aufzuspüren. Die vom Generator erstellte Erklärung bedürfe aber definitiv der Strukturierung und Kürzung, um einigermaßen verständlich zu sein.





Im Anschluss gab er Hinweise zur Dokumentation von Vorgängen, die sich aus der Kommunikation mit Betroffenen ergeben. Hierbei ging es einerseits um Nachweise der Einwilligung in Verarbeitungen sowie um erbetene Löschungen und Änderungen von Datensätzen. Unter dem Schlagwort „Buchhaltung schlägt Datenschutz“ machte Gregor Henker auf ein Beispiel für die Grenzen von Löschungswünschen Betroffener aufmerksam: Bei Datenverarbeitungen, die zur Erfüllung der steuerrechtlichen Buchführungspflichten erforderlich sind, ist eine Löschung vor Ablauf der zehnjährigen Aufbewahrungsfrist ausgeschlossen. Auf diese Ausführungen folgten Hinweise zur Notwendigkeit und dem Aufgabenprofil von Datenschutzbeauftragten.

Dokumentation

- Alle Dienste und Services neu dokumentieren und Nachweise sichern (Newsletter, Verteiler, Infopost etc.)
- Nachweise maschinenlesbar und sicher aufbewahren
- Lösch- oder Änderungsvorgänge dokumentieren
- “Buchhaltung schlägt Datenschutz”
- Je nach Umfang der Tätigkeit, theoretisches Konzept vorbereiten

  (“Best Practice” - Was passiert wie, wenn wer was...)

Datenschutzbeauftragte/r

- Bei mehr als 10 Aktiven so oder so verpflichtend
- Allerdings: bei besonders sensiblen Daten auch!
- DSB ist nicht Geschäftsführer und nicht im Vorstand
- DSB braucht geeignete Fachkenntnis
- Aber: Verantwortlich bleibt der Vorstand/Geschäftsführung: “Für die Verarbeitung Verantwortliche/r”
- DSB berät, schätzt ein, “wirkt darauf hin”, ist Ansprechpartner

Als weitere Elemente der DSGVO-Anforderungen wies Gregor Henker auf die - in der Praxis für jeden Verein gegebene - Notwendigkeit eines Verarbeitungsverzeichnisses sowie auf die Forderung der Sensibilisierung und Schulung von Mitarbeiter*innen hin.

Verzeichnis von Verarbeitungstätigkeiten

- Laut Artikel 30 der DSGVO eigentlich nur von Nöten, bei mehr als 250 Angestellten/Mitarbeitern (Definition!)
- Aber: Bei besonders sensiblen Daten oder regelmäßiger automatischer Datenverarbeitung doch
- Regelmäßige Datenverarbeitung? z. B.: periodischer Infobrief, Newsletter, Spenden, Mitgliederbeiträge etc.
- Da Datenschutzerklärung eh Pflicht ist, können Bestandteile übernommen werden

Sensibilisierung und Datengeheimnis

- Aktive und Mitarbeiter sollten oder müssen über Datenschutz und Datensparsamkeit sensibilisert werden
- Verpflichtung auf Datengeheimnis ist ratsam (obschon nicht mehr explizit erwähnt in DSGVO)
- In der DSGVO stecken viele verklausulierte Hinweise “rechtmäßige Verarbeitung, nachvollziehbare Weise, technische und organisatorische Maßnahmen etc.”
- Nicht als einmaliges Angebot sehen, sondern in Intervallen wiederholen

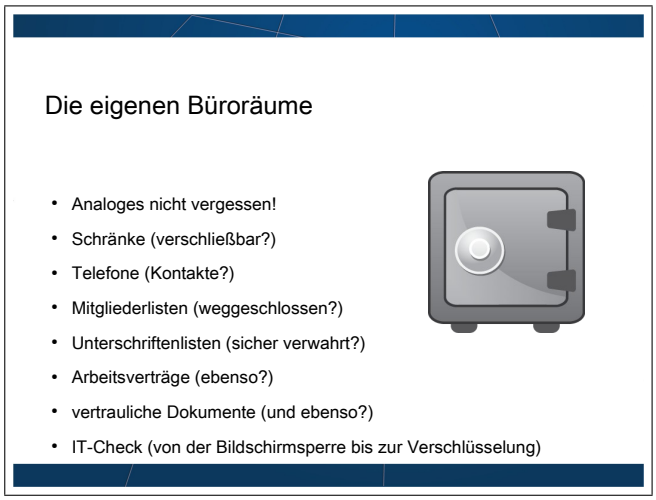
Abschließend streifte er noch das Thema Datenschutz-Folgeabschätzung, machte Vorschläge zum Umgang mit Auskunftsersuchen und schloss mit einer Checkliste zur Sicherheit der eigenen Büroräume.

“Datenschutzfolgeabschaetzung”

- Sollte man oder besser muss man tun, werden besonders sensible Daten verarbeitet
- Übrigens: Wenn Datenschutzfolgeabschätzung, dann Datenschutzbeauftragte/r
- Im Prinzip geht es um “Die W-Fragen” (siehe 1. Input heute)

Auskunftpflicht

- DSGVO hat Rechte und Möglichkeiten von Betroffenen gestärkt
- Es sollte klar definierte Abläufe für mögliche Anfragen geben
- Nicht verunsichern lassen
- Im Zweifel lieber solidarisch sein, als Paragraphen zu reiten
- Definitionen kennen (Löschen, Sperren, Ändern etc.)



4 Vernetzung und nächste Schritte

Zum Abschluss des Forums gab es einen kleinen Ausblick zur weiteren Vernetzung. Es wurde mehrfach der Wunsch nach weiteren ähnlichen Veranstaltungen sowie nach einem dauerhaften Beratungsangebot für Vereine geäußert.

Mehrere Teilnehmende äußerten Interesse, an einem Treffen zum Austausch über weitere Projektideen teilzunehmen. Ein solches Treffen wird im ersten Quartal 2019 stattfinden; ein genauer Termin ist noch nicht gefunden. Interessierte können sich zur Kontaktaufnahme an info@plushumanite.de wenden. Weitere öffentliche Veranstaltungen werden dann erneut über die Kanäle von plus humanité e. V., dem Roten Baum Leipzig e. V., dem Netzwerk Tolerantes Sachsen, der Freiwilligen-Agentur-Leipzig e. V. sowie ggf. neuer Kooperationspartner*innen beworben.