Allgemeine Infos zum Datenschutz nach DSGVO

Basics

Seit dem 25.05.2018 gilt eine Datenschutz-Grundverordnung (DSGVO) der EU. Folgend wurde auch das Bundesdatenschutzgesetz angepasst (BDSG bzw. BDSG-neu). Im Vergleich zum alten BDSG gibt es nicht besonders viele Neuerungen, sodass wir grundsätzlich gut aufgestellt sind, aber es gibt einige wesentliche Neuerungen, z.B. wann ein*e Datenschutzbeauftragte*r bestellt werden muss und was seine*ihre Aufgaben sind, was bei Verstößen passiert (höhere Bußgelder) und strengere Nachweispflichten. Insgesamt wird die neue DSGVO als positiv eingeschätzt, weil sie tatsächlich dazu taugen kann, dass unser aller Daten besser geschützt sind. Es kommt aber auch ein bisschen Arbeit auf uns zu.

Im folgenden habe ich einige Infos & Quellen zusammengefasst. Es folgt eine Checkliste.

Diese Info wird zur Zeit überarbeitet.

Disclaimer: Diese Informationen sind gründlich recherchiert, aber: Wir beschäftigen keine Jurist*innen und können keine rechtsverbindlichen Informationen geben.

Inhalt

Grundinfos

Gilt das für uns?

Ja. Die DSGVO gilt für alle. Sie betrifft alle Institutionen, d.h. auch Vereine, egal ob sie eingetragen (e.V.) sind oder nicht. Also *auch alle Stämme!* Jeder Stamm muss sich um seinen Datenschutz selbst kümmern. Wir als LV wollen euch dabei aber so gut wie möglich unterstützen!

Worum geht's?

Es geht um **personenbezogene Daten**, die wir ganz, teilweise oder nicht automatisiert **verarbeiten**. Für die Verarbeitung gibt es **Verantwortliche**. Die Verantwortlichen werden kontrolliert von einer*m internen **Datenschutzbeauftragten** und extern durch die **Aufsichtsbehörde**. Bei der Datenverarbeitung kann es vorkommen, dass man **Auftragsverarbeiter*innen** einschaltet. Unsere Datenverarbeitung muss **rechtmäßig** sein und nach bestimmten **gesetzlichen Vorgaben** erfolgen. **Betroffene** von Datenverarbeitung haben ein Recht auf Information, d.h. wir haben eine **Informationspflicht**. Die Betroffenen haben außerdem einige weitere Rechte uns gegenüber, sog. **Betroffenenrechte**. Um diese und unsere **Auskunftspflicht** gegenüber der Aufsichtsbehörde zu gewährleisten, brauchen wir ein **Verzeichnis der Verarbeitungstätigkeiten** (das ist durch die DSGVO vorgeschrieben). Um außerdem der Verletzung des Datenschutzes vorzubeugen, müssen wir **technische und organisatorische Maßnahmen (TOM)** treffen und eine **Datenschutz-Folgenabschätzung** durchführen.

Hä? Was ist das denn für Zeug? – Definitionen

Begriff	Definition
personenbezogene Daten	• alle Daten, anhand derer man eine Person identifizieren kann, z.B.: Name, Adresse, IP-Adresse, aber auch Bilder! (zu Bildern siehe unten) • **besonders schützenswerte Daten** sind u.a. die sexuelle Orientierung oder Gesundheitsdaten
Datenverarbeitung	• ist alles, was wir mit diesen Daten tun: Erheben, Speichern, Ändern, Nutzen, Übermitteln, Verknüpfen oder Löschen. • Dabei macht es keinen Unterschied, ob wir sie automatisiert, d.h. mit dem Computer, oder nicht automatisiert, d.h. auf Papier, verarbeiten. Es geht also um digitale wie analoge Datenverarbeitung

Quellen

- der Text der DSGVO: https://dsgvo-gesetz.de/
- die DSGVO als PDF: https://www.datenschutz-grundverordnung.eu/wp-content/uploads/2016/04/CONSIL_ST_5419_2016_INIT_DE_TXT.pdf
- grundlegender Wikipedia-Artikel: https://de.wikipedia.org/wiki/Datenschutz-Grundverordnung
- Datenschutz im BdP vom Bund: Datenschutz im BdP_Stamme.pdf
- "Erste Hilfe zur Datenschutz-Grundverordnung für Unternehmen und Vereine", hrsg. v. Bayerischen

Verantwortliche*r	• ist regelmäßig der Vorstand eines Vereins • Der Vorstand kann die Umsetzung schriftlich delegieren, bleibt am Ende aber trotzdem verantwortlich, wenn was schief geht • **Datenschutz ist Chefsache!** Er muss euch wichtig sein!
Datenschutzbeauftragte*r (DSB)	• wird benötigt, sobald **mindestens 10 Personen regelmäßig Daten verarbeiten**. Da jede*r Sippenführer*in bei der Anmeldung zur Sippenfahrt Daten verarbeitet, kann man relativ schnell auf 10 kommen. Selbst wenn nicht 10 Personen Daten verarbeiten, braucht man eine*n DSB, wenn man z.B. Gesundheitsdaten verarbeitet und ohne die seine Arbeit nicht machen kann (z.B. Fahrten und Lager) • wird vom Vorstand schriftlich berufen • ist dafür zuständig, die Umsetzung und Einhaltung des Datenschutzes zu überwachen • steht als Ansprechpartner*in für die Betroffenen zur Verfügung und steht deshalb auf der Homepage • es darf keinen Interessenskonflikt geben, d.h. er*sie darf nicht selbst Administrator*in oder Vorstand sein, kann aber durchaus auch selbst Daten verarbeiten (aber eben nicht an zu herausragender Stelle) • ⚠️ Wir sind auf Landesebene gerade am Prüfen, wie wir euch an dieser Stelle bestmöglich unterstützen können! Ihr erhaltet dazu in den nächsten Tagen weitere Infos.
Aufsichtsbehörde	• ist eine externe Kontrollstelle des Landes Niedersachsen. Sie heißt: Landesbeauftragte für den Datenschutz (LfD) Niedersachsen, wird geleitet von Barbara Thiel und hat auch eine Homepage: https://www.lfd.niedersachsen.de/startseite/ • Sie ist in bestimmten Fällen zu informieren (z.B. bei einer Verletzung des Datenschutzes), steht für Fragen zur Verfügung und kann unangekündigt Kontrollen durchführen. Erfahrungsgemäß sind Aufsichtsbehörden eher kooperativ und wollen euch unterstützen.
Auftragsverarbeitung	• ist, wenn ich eine externe Stelle beauftrage, zu einem bestimmten Zweck bestimmte Daten auf eine bestimmte Art und Weise zu verarbeiten • Mit diesem muss ein Vertrag über die Datenverarbeitung geschlossen werden und ihr müsst das auch kontrollieren können (ihr solltet also nicht einfach das billigste Unternehmen nehmen, sondern das beste!) • Beispiel: Hoster meiner Website, aber (meistens) nicht Facebook. • mehr dazu, siehe unten
Rechtmäßigkeit	• Um Daten verarbeiten zu dürfen, gibt es drei Möglichkeiten: 1. die betroffene Person hat wirksam (!) eingewilligt (s.u.) 2. es ist zur Erfüllung eines Vertrags (z.B. die Teilnahme an einer Veranstaltung, wozu die Anmeldung der Vertrag ist) oder einer rechtlichen Verpflichtung (z.B. wenn ihr Daten an die Stadtjugendpflege übermittelt, um Zuschüsse zu bekommen) notwendig. 3. ihr habt berechtigte Interessen, die "die Interessen der betroffenen Person überwiegen", z.B. überwiegt das Interesse des Stammes, die Kontaktdaten der Meutenführung zu veröffentlichen, damit die Eltern sie erreichen können • darüber hinaus gilt: ◦ Die Daten dürfen nur für einen bestimmten Zweck verarbeitet werden (**Zweckbindung**). Dieser muss im Vorfeld feststehen und den Betroffenen mitgeteilt werden. Es dürfen auch nur Daten verarbeitet werden, die für diesen Zweck wirklich notwendig sind. Und dabei geht es immer um die Frage: Welche Daten braucht Person X für ihren konkreten Zweck genau? Z.B.: Ein Küchenteam braucht Ernährungshinweise, aber nicht den Wohnort. ◦ Die Daten müssen **richtig** sein (logisch, oder?). Ihr solltet dafür sorgen, dass sie richtig sind! ◦ Ihr dürft **nur die** Daten speichern, die ihr **wirklich braucht**. Was ihr für einen bestimmten Zweck nicht mehr braucht, müsst ihr löschen, sofern es keine Aufbewahrungsvorschriften gibt (z.B. Aufbewahrung von Buchhaltungsunterlagen), oder so ändern, dass sie nicht mehr personenbezogen sind. Es ist z.B. kein Problem eine Statistik zu führen darüber, wie sich die Altersstruktur auf euren Stammesvollversammlungen über die letzten 20 Jahre entwickelt hat – nur ohne Namen halt. ◦ Ihr müsst im Zweifelsfall **Rechenschaft ablegen** können, wenn z.B. die Aufsichtsbehörde mal nachfragt. Dazu dient u.a. das Verzeichnis von Verarbeitungstätigkeiten

Landesamt für Datenschutzaufsicht, bearb. v. Thomas Kranig u. Eugen Ehmann, 2017 (gedruckt in der LGS).
- Leitfaden vom Bayerischen Jugendring (BjR): 2018_04_25_Datenschtutz_in_der_Jugendarbeit.pdf
- Datenschutz im Sportverein vom LSB NRW: IP-Datenschutz-im-Sportverein_2018_01_30.pdf
- Was ist mit **WhatsApp**? Merkblatt_WhatsApp_im_Unternehmen.pdf
- zur Datenschutzerklärung auf Homepages: https://www.impulse.de/recht-steuern/rechtsratgeber/datenschutzerklaerung/2393294.html
- https://www.tagesschau.de/ausland/eu-datenschutz-faq-101.html
- https://www.facebook.com/business/gdpr
- https://www.lda.bayern.de/tool/start.html#

Links & Dateien

- https://www.lda.bayern.de/de/erste-hilfe.html hier sollen irgendwann zu finden sein: ein Muster für das **Verzeichnis von Verarbeitungstätigkeiten** sowie ein Muster eines **Auftragsverarbeitungsvertrags**
- https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/Sicherheitsirrtuemer/sicherheitsirrtuemer_node.html klassische Sicherheitsirrtümer enttarnt vom BSI
- https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Verschluesselung/Verschluesselung_node.html Empfehlungen zum Thema Verschlüsselung des BSI
- Checkliste DSGVO BJR.pdf**Checkliste zum Anfangen** vom BJR
- Muster LSB NRW.pdf diverse **Muster** für alles mögliche vom LSB NRW
- Checkliste und Muster Erste Hilfe zur DSGVO.pdf**Checkliste**, Muster für **Checkliste von Verarbeitungstätigkeiten** und Muster für **Kontrollbogen** der Aufsichtsbehörde.

Präsentation zur stute 2018

gesetzliche Vorgaben	• sind die neue Datenschutz-Grundverordnung (DSGVO) sowie das darauf aufbauende neue Bundesdatenschutzgesetz (BDSG-neu) • viele Vorschriften aus der DSGVO sind so oder ähnlich schon im alten BDSG zu finden, also eigentlich schon längst Gesetz
Betroffene	• sind die Personen, deren Daten verarbeitet werden
Informationspflicht	• ist eure Pflicht gegenüber Betroffenen, sie darüber zu informieren, was mit ihnen Daten geschieht und welche Betroffenenrechte sie haben • wie und worüber ihr genau informieren müsst, s.u.

Betroffenenrechte	• Betroffene haben ein Recht auf
	  ◦ Auskunft
	  ◦ Berichtigung, Löschung und Einschränkung der Verarbeitung
	  ◦ Datenübertragbarkeit (d.h.: sie dürfen verlangen, dass ihr Daten, die ihr habt, jemandem anders mitteilt)
	  ◦ Widerspruch gegen die Verarbeitung
	  ◦ Recht, keiner automatisierten Entscheidung unterworfen zu werden
	• was ihr tun müsst, wenn ein*e Betroffene*r eins davon von euch verlangt, findet ihr unten

Auskunftspflicht	• Wenn die Aufsichtsbehörde kommt, dann müsst ihr Auskunft geben über eure Datenverarbeitung
Verzeichnis von Verarbeitungstätigkeit	• ist ein Verzeichnis, in dem ihr jede Verarbeitungstätigkeit auflistet. Hier darf die Aufsichtsbehörde reinschauen. • Eine Verarbeitungstätigkeit ist z.B. die Durchführung eines Stammeslagers • Eine Vorlage findet ihr unten
technische und organisatorische Maßnahmen (TOM) gegen die Verletzung des Datenschutzes	• es gibt ein paar Maßnahmen, die ihr treffen solltet, um eure Daten auch sicher zu halten, z.B. solltet ihr ausreichend sichere Passwörter haben (im Computer, im WLAN, in nds.meinbdp, bei eurem E-Mail-Konto usw.) und bei E-Mails an alle Mitglieder nicht alle Empfänger*innen einer E-Mail ins An-Feld setzen (sondern in BCC!) – letzteres gab schon in der Vergangenheit Abmahnungen! • Mehr dazu findet ihr unten
Datenschutz-Folgenabschätzung	• ist eine Einschätzung eurerseits, was passieren könnte, wenn mal irgendwo ein Leck ist. Dadurch soll euch klar werden, wo ihr vielleicht noch bessere vorbeugende Maßnahmen treffen könnt, und wie ihr reagieren könnt, wenn etwas passiert. Verschiedene Autor*innen schlagen sogar vor, einen Testlauf zu machen • was ihr tun müsst, wenn es zu einer Verletzung kam, findet ihr unten

Und wie geht das jetzt?

Zunächst: **Don't Panic!** Die Aufsichtsbehörden werden nicht am 25.05. hier aufschlagen und direkt eine Sanktion in Millionenhöhe verordnen. In der Vergangenheit haben sie sich als recht hilfsbereit erwiesen, wenn man von sich aus auf sie zugeht (vgl. Erste Hilfe zur DSGVO). Es könnte aber durchaus sein, dass jemand uns ans Bein pissen möchte und deshalb, allein weil keine Datenschutzerklärung auf der Homepage steht, einen Abmahnanwalt losschickt. Also: Wenn wir bis zum 25.05. eine gute Basis geschaffen haben, sind wir gut dabei – ein verbessertes Bewusstsein, ein perfekter Datenschutz lässt sich nicht in 10 Tagen schaffen; Rom wurde auch nicht an einem Tag erbaut!

Es gibt einige Hilfestellungen, Mustervorlagen usw.usf. Die sind rechts in der Link- & Dateiensammlung untergebracht. Außerdem habe ich bereits einige eigene erstellt, die ihr auf den untergeordneten Seiten findet. Eine eigene Checkliste findet ihr unten genauso wie die ersten 17 Schritte.

Die Maßnahmen, die wir treffen müssen, liegen im Bereich der Bürokratie/Verwaltung (z.B. Verzeichnis der Verarbeitungstätigkeiten), im Bereich der IT-Sicherheit, der Kommunikation (z.B. E-Mails), der räumlichen Gegebenheiten (z.B. in der LGS oder im Stammesheim) sowie möglicherweise im organisatorischen Bereich. Das ganze wird Veränderungen mit sich bringen, aber was uns klar sein muss: Es kann im Endeffekt nur nützlich sein! Spätestens wenn der Stammesratsraum nicht mehr mit alten Akten vollsteht oder ihr plötzlich mehr Speicherplatz auf dem Rechner habt, werden wir es merken 🙂

Checkliste

Diese Checkliste könnt ihr im Verlauf eurer Arbeit immer mal wieder machen, um zu schauen, wo ihr gerade steht.

Checkliste zum Runterladen:

- Checkliste DS.docx
- Checkliste DS.pdf

Frage	Antwort	Anmerkungen & Notizen
Wer ist für Datenschutz verantwortlich?		
Ist ein*e Datenschutzbeauftragte*r benannt?		
Ist eine Bestandsaufnahme erfolgt, wo Daten verarbeitet werden? (möglichst exakt benennen)		
Wisst ihr, auf welche Rechtsgrundlage ihr Verarbeitungen stützt? (Artikel der DSGVO)		
Habt ihr ein Verzeichnis der Verarbeitungstätigkeiten?		
Habt ihr eine Datenschutzerklärung für Online-Präsenzen?		
Habt ihr eine Allgemeine Datenschutzerklärung für Veranstaltungen?		
Gibt es auf Anmeldungen ein Feld zum Ankreuzen, dass man in die Datenverarbeitung einwilligt?		
Welche Auftragsverarbeitungen habt ihr?		

Bestehen Verträge mit allen Auftragsverarbeiter*innen?		
Könnt ihr sämtlichen Betroffenenrechten jederzeit nachkommen?		
Wisst ihr, was ihr tun müsst, wenn es zu einer Datenschutzverletzung gekommen ist?		
Könnt ihr dem in der gesetzlich vorgegebenen Zeit jederzeit nachkommen?		
Habt ihr eine Datenschutz-Folgenabschätzung vorgenommen und werdet ihr sie regelmäßig evaluieren?		
Habt ihr technisch-organisatorische Maßnahmen vorgenommen, um für Datenschutz und -sicherheit zu sorgen?		
Habt ihr diese dokumentiert?		
Gibt es Schulungen und Belehrungen für Menschen, die mit personenbezogenen Daten zu tun haben?		

Was mach ich denn jetzt konkret? – Der 17-Punkte-Plan

1. Macht euch bewusst, dass Datenschutz **wichtig** ist und auch etwas kosten kann.
2. **Findet heraus,** wo ihr überall Daten verarbeitet.
3. Beruft eine*n **Datenschutzbeauftragte*n** und meldet ihn*sie an die LGS sowie an die Aufsichtsbehörde
4. Legt für alles ein **Verzeichnis der Verarbeitungstätigkeiten** an und arbeitet euch an den darin geforderten Punkten ab. Wenn ihr mal nicht weiter wisst, schaut ihr hier auf diese Seite.
5. Erstellt zwei **Datenschutzerklärungen**
    a. eine für Online-Präsenzen
    b. eine für Veranstaltungen (z.B. so)
6. Überarbeitet eure **Anmeldeformulare**: Fügt Einwilligungskästchen hinzu (z.B. wie in dieser Vorlage)
7. Legt klare Abläufe fest, wann Daten wie **vernichtet** werden sollen.
8. **Vernichtet** Daten, die ihr nicht mehr braucht.
9. Habt ihr **Auftragsverarbeiter**? Mit Sicherheit! Dann schließt Verträge. Bewahrt diese gut auf!
10. Legt für alle eure Gruppenleiter*innen **TOM**-Richtlinien fest. Haltet sie schriftlich fest!
11. Lasst eure*n Datenschutzbeauftragte*n an einer **Schulung** teilnehmen.
12. **Belehrt** eure Gruppenleiter*innen, was sie datenschutzrechtlich dürfen und was nicht (das kann der*die DSB übernehmen, z.B. in einer Einheit beim Stammesrat). Macht allen Gruppenleiter*innen bewusst, dass diese Belehrungen Pflicht sind. Dokumentiert die Belehrungen.
13. Legt einen **regelmäßigen** Rhythmus für Belehrungen fest (z.B. 1-2mal im Jahr für alle Gruppenleiter*innen)
14. Überlegt euch klare Abläufe, was ihr macht, wenn jemand **Betroffenenrechte** geltend machen möchte. Haltet sie schriftlich fest und bewahrt sie gut auf!
15. Überlegt euch klare Abläufe, was ihr macht, wenn es zu einer **Datenschutzverletzung** gekommen ist. Haltet sie schriftlich fest und bewahrt sie gut auf!
16. Macht eine **Datenschutzfolgenabschätzung** und überarbeitet ggf. das, was ihr bisher erarbeitet habt.
17. Entwickelt einen Prozess, dass euer (nun fertiges) Datenschutzkonzept regelmäßig **evaluiert** und angepasst wird.

Erläuterungen

Datenschutzerklärung

Wir empfehlen, **zwei Datenschutzerklärungen** zu machen. Dadurch wird alles etwas übersichtlicher. Außerdem sind die Verarbeitungen und die Zielgruppen teilweise unterschiedlich.

Eure Datenschutzerklärung muss **leicht verständlich** sein. Schließlich muss man auch fähig sein, in sie einzuwilligen.

1. Datenschutzerklärung für Online-Datenverarbeitung

Diese muss seit dem 25.05.2018 auf allen euren Internetseiten von der Startseite aus unter dem Namen "Datenschutz" (oder Datenschutzerklärung) erreichbar sein. Die muss enthalten:

- Wer ist verantwortlich? – die Stammesführung (Name & Kontaktdaten), also die Person, die "über die Verarbeitung von personenbezogenen Daten entscheidet" (Quelle)
- Wer ist Datenschutzbeauftragte*r? (sofern ihr eine*n habt) – Name und Kontaktdaten
- Welche Daten werden erhoben?
- Wozu werden die Daten verarbeitet? – hier könnt ihr euch auf den Vereinszweck aus der Bundessatzung berufen, denn: Um den Vereinszweck zu erfüllen, müssen wir einige Daten verarbeiten
- Wie werden die Daten verarbeitet?
- An wen werden die Daten übermittelt? – Stichwort: Auftragsverarbeitung
- Wie lange werden die Daten gespeichert *oder* nach welchen Kriterien legt ihr fest, wann sie gelöscht werden sollen?
- Der*die Betroffene hat ein Recht auf Auskunft, auf Berichtigung, auf Löschung, auf Einschränkung der Verarbeitung und auf Widerspruch gegen die Verarbeitung. An wen kann er*sie sich wenden, um diese Rechte geltend zu machen? – die Stammesführung
- Der*die Betroffene hat ein Recht, sich bei der Aufsichtsbehörde zu beschweren (Link zur Behörde)

💡 Wir empfehlen für diese Datenschutzerklärung den Datenschutz-Generator. Orientiert euch gerne auch an der Datenschutzerklärung des BdP (www.pfadfinden.de) sowie unserer Datenschutzerklärung (www.nds.pfadfinden.de).

2. Datenschutzklärung für Veranstaltungen

Diese muss für alle Veranstaltungen, die nach dem 25.05.2018 stattfinden, bei **jeder Veranstaltung** der Anmeldung beigelegt werden. Sie muss grundsätzlich im selben Format vorliegen wie die Anmeldung. Das heißt, bei einer Papieranmeldung muss die Datenschutzerklärung in Papierform, bei einer Online-Anmeldung muss sie online für die Erziehungsberechtigten/Teilnehmer*innen verfügbar sein.

⭐ Für eure Allgemeine Datenschutzerklärung für Veranstaltungen haben wir diese Vorlage gebastelt: Vorlage Datenschutzerklärung für Veranstaltungen.

⚠️ Bei jede*r Anmeldung braucht ihr die Zustimmung jeder*s Teilnehmer*in (bzw. deren Erziehungsberechtigten) zur Datenverarbeitung. Siehe dazu den nächsten Abschnitt.

Passus in Anmeldungen

Jede*r Teilnehmer*in (bzw. deren Erziehungsberechtigten) müssen bei jede*r Veranstaltung der Datenverarbeitung aktiv zustimmen! Das heißt: Es reicht nicht, wenn sie einen Satz im Kleingedruckten unterschreiben, sondern sie müssen ein Kreuzchen setzen (sog. Opt-in-Verfahren). Wie das aussehen kann, seht ihr in der unten verlinkten Vorlage.

💡 **Wir empfehlen**:

1. Gebt den Erziehungsberechtigten und euren volljähigen Mitgliedern einmalig eine Datenschutzerklärung auf Papier und bittet sie, diese gut aufzubewahren. Dokumentiert für jedes Mitglied, dass ihr diese Datenschutzerklärung ausgehändigt habt!
2. Hängt die Datenschutzerklärung in eurem Stammesheim aus, sodass sie von den Mitgliedern und Erziehungsberechtigten regelmäßig eingesehen werden kann.
3. Stellt die Datenschutzerklärung auf eure Homepage.
4. Bei jeder Anmeldung könnt ihr jetzt den Link auf die Anmeldung schreiben und einen Hinweis, dass diese Datenschutzerklärung auch im Stammesheim aushängt oder bei der Gruppenleitung angefordert werden kann.

⚠️ Da ihr auch **dokumentieren** müsst, wer der Verarbeitung der eigenen Daten zugestimmt hat, lohnt es sich, die Anmeldeformulare solange aufzubewahren, wie ihr auch die Daten aufbewahrt! Anschließend sind die Anmeldungen natürlich fachgerecht zu entsorgen (sodass die Müllabfuhr nicht mehr ohne weiteres auf die Daten zugreifen kann).

⭐ Hierfür haben wir eine Vorlage: Datenschutz & Bildrechte im Anmeldeformular.

Einwilligung

Wie bereits gesagt: Die Person muss **von sich aus einwilligen**. Es darf ihr nicht schon vorgegeben sein, dass sie einwilligt (Opt-In-Verfahren). Zu dieser Einwilligung muss sie **fähig** sein; fähig wird man, indem man von euch ausreichend informiert wird (siehe oben Datenschutzerklärung & Passus in Anmeldungen).

Die Person darf die Einwilligung jederzeit **widerrufen**. Was ihr dann tun müsst/könnt, findet ihr unten.

⚠️ Zu allen Daten, die ihr aus einem Aufnahmeantrag in den BdP gewonnen habt, besteht bereits eine Einwilligung! Das gilt auch, wenn die Daten sich geändert haben und die betroffene Person euch die neuen korrekten Daten mitgeteilt hat (z.B. neue Handynummer, neue Adresse usw.). Das heißt: Daten aus der Mitgliederverwaltung dürfen grundsätzlich genutzt werden. Alle weiteren Daten benötigen eine explizite Einwilligung der*s Betroffenen. Das heißt natürlich, dass ihr **nicht irgendwelche Daten in der MV eintragen dürft**, die ihr z.B. aus einer Veranstaltungsanmeldung gewonnen habt. Wenn ihr also feststellt: "Huch, hier in der Anmeldung steht ja eine andere E-Mail-Adresse in der MV", dann fragt einmal nach, ob ihr diese neue E-Mail-Adresse in die MV übertragen dürft.

Verzeichnis der Verarbeitungstätigkeiten

Das Verzeichnis der Verarbeitungstätigkeiten ist etwas neues. Hier müssen wir dokumentieren, in welchem Zusammenhang mit personenbezogenen Daten gearbeitet wird. Natürlich muss es immer aktuell sein! Aber um nachweisen zu können, dass es aktuell ist, ist es sinnvoll, für ca. 1 Jahr eine Versionsgeschichte anzulegen, d.h. nachvollziehbar zu machen, was wann geändert wurde. Hierfür bietet es sich an, nds.meinBdP zu nutzen, da das Programm selbst eine Versionsgeschichte anlegt. Vorstellbar ist eine Speicherung verschiedener Versionen über 1 Jahr.

Eine Verarbeitungstätigkeit in diesem Sinne ist "Stammessommerfahrt" (als vorübergehende Verarbeitungstätigkeit) oder "Stammesrat" (als kontinuierliche Verarbeitungstätigkeit). Kontuinuierliche Verarbeitungstätigkeiten sollten kontinuierlich geführt werden. Bei vorübergehenden Verarbeitungstätigkeiten lohnt es sich, das Verzeichnis gleich am Anfang auszufüllen und spätestens zum Ende der Verarbeitungstätigkeit (lies: Veranstaltungsorganisation) noch einmal zu überarbeiten, bevor ihr es abschließt. ⚠️ Achtung: Auch vorübergehende Verarbeitungstätigkeiten werden aus dem Verzeichnis **nicht gelöscht!**

Das ganze Verzeichnis ist **nicht öffentlich**. Es dient in erster Linie euch als Übersicht und Qualitätskontrolle. Es ist aber auch für die Aufsichtsbehörde. Es ist ausdrücklich nicht für Betroffene einzusehen! Das heißt, ihr müsst dieses Verzeichnis auch gut vor Einsicht schützen (auf nds. meinbdp z.B. durch ein entsprechendes Berechtigungsmanagement).

⭐ Wie so etwas auf unsere Bedürfnisse angepasst aussehen kann, findet ihr in Kürze hier.

Grundsätzlich ist es sinnvoll, ein Vorblatt zu erstellen (beinhaltet Angaben zur*m Verantwortlichen & zum*r Datenschutzbeauftragten) sowie je eine Tabelle pro Verarbeitungstätigkeit. Darin geht es dann z.B. darum, wer betroffen ist, welche Daten verarbeitet werden, wer die Daten verarbeitet, wann gelöscht wird und welche technischen und organisatorischen Maßnahmen (TOM) getroffen wurden.

Wer führt das Verzeichnis? Diese Frage müsst ihr für euch selbst beantworten. Sie hängt sehr stark von eurer internen Struktur ab. Das einzige, was wichtig ist, ist, was am Ende rauskommt: Ein **zentrales** Verzeichnis, auf das der*die Verantwortliche und der*die Datenschutzbeauftragte jederzeit zugreifen können, um es ggf. der Aufsichtsbehörde vorzulegen.

Da die Aufsichtsbehörde meistens noch etwas mehr sehen möchte, als nur das, was im Standard-Verzeichnis abgebildet wird, kann es sich lohnen, zu jeder Verarbeitungstätigkeit noch eine zweite Tabelle anzuhängen, ein quasi **erweitertes Verzeichnis**. Darin geht es vor allem um Dokumentationspflichten, z.B. hinsichtlich datenschutzfreundlicher IT-Gestaltung oder hinsichtlich der Geltendmachung von Betroffenenrechten. Hieran dürften sich die Verarbeitungstätigkeiten allerdings wenig unterscheiden, wenn ihr immer unter den gleichen Voraussetzungen arbeitet.

eine*n Datenschutzbeauftragte*n berufen

Was ist & macht ein*e DSB?

Ein*e Datenschutzbeauftragte*r (DSB) unterstützt und kontrolliert den*die Verantwortliche*n in Fragen des Datenschutzes. Dazu sollte er*sie fachlich qualifiziert sein durch z.B. eine Weiterbildung bzw. eine Schulung. **Wir raten dringend davon ab, einfach irgendwen** zur*m DSB zu berufen. Wir als Landesverband sind noch auf der Suche, wie wir euch gerade an dieser Stelle bestmöglich unterstützen können. Bitte wartet hier weitere Infos von unserer Seite ab, bevor ihr jemanden beruft.

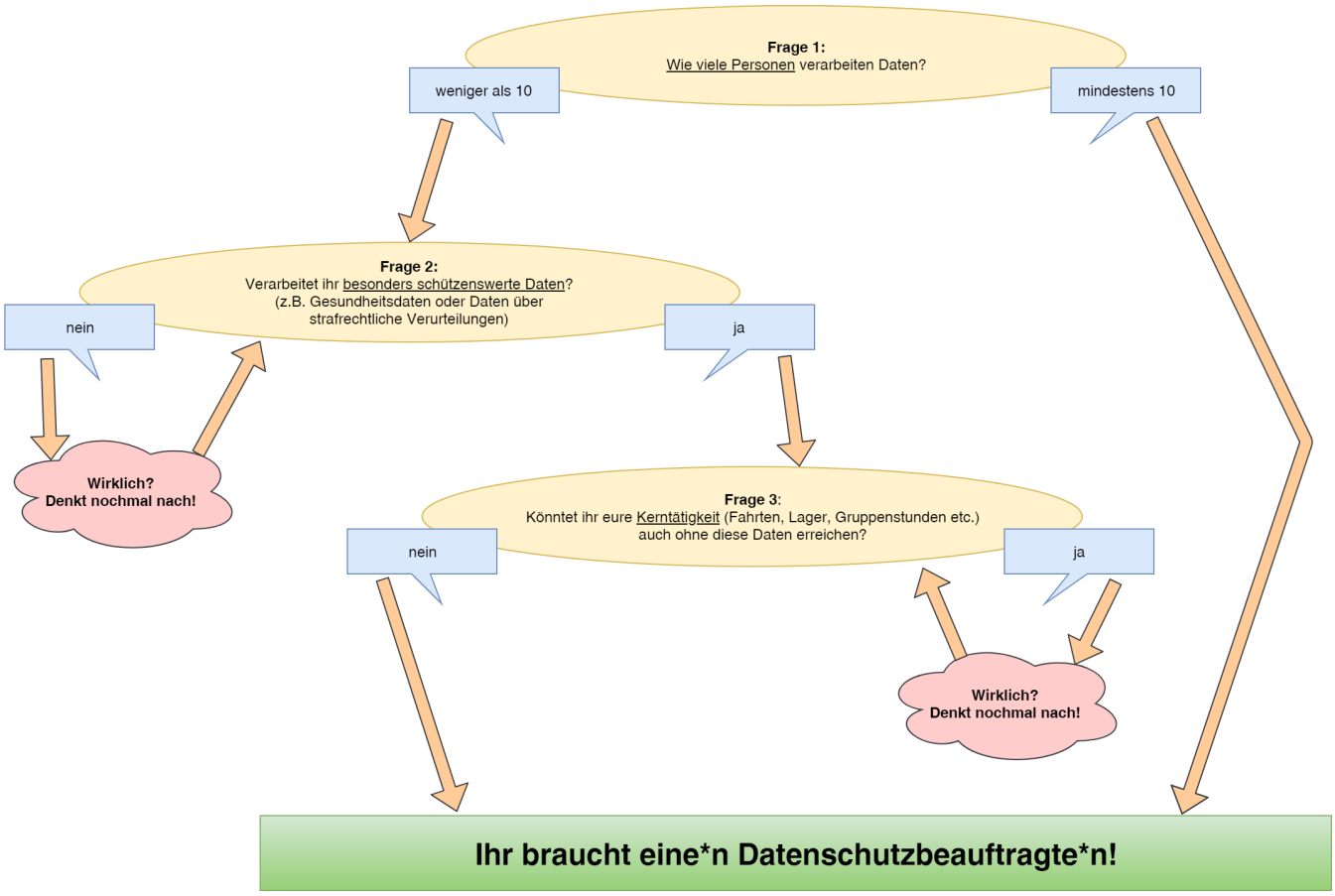
Der*die DSB sollte nicht mit der Landesbeauftragten für Datenschutz verwechselt werden – das ist nicht unsere neue LB Datenschutz, sondern die Aufsichtsbehörde des Landes Niedersachsen!

Der*die DSB ist **nicht** für die Umsetzung des Datenschutzes zuständig, sondern (wie gesagt) dafür, euch dabei inhaltlich zu unterstützen und zu kontrollieren. Außerdem können sich Betroffene bei ihm*ihr melden, wenn sie sich über euch beschweren wollen.

Die genauen Aufgaben einer*s DSB findet ihr weiter unten.

Muss ich eine*n DSB berufen?

Mit 99%iger Sicherheit **ja**. Macht gern selbst einmal den Test:



Anmerkungen:

- zu Frage 1 – Hier geht es wirklich um jede Person. Wenn die Heimwartin nur einmal im Jahr eine E-Mail an alle Mitglieder schreibt, dann verarbeitet sie Daten, ist also mitzuzählen. Es könnte also gut sein, dass ihr schnell auf 10 Personen kommt (gerade, wenn man alle Gruppenleitungen mitzählt, die Handynummern ihrer Sipplinge haben).
- zu Frage 2 – Sicherlich verarbeitet ihr nicht die sexuelle Orientierung, Gewerkschaftszugehörigkeit oder die ethnische Herkunft, aber wenn ihr auf Anmeldungen zu Lagern und Fahrten benötigte Medikamente oder gesundheitliche Einschränkungen abfragt, dann verarbeitet ihr Gesundheitsdaten; und wenn ihr die erweiterten Führungszeugnisse einsehen müsst, dann verarbeitet ihr Daten über strafrechtliche Verurteilungen.
- zu Frage 3 – Ob wir auf Fahrt gehen könnten, wenn wir nicht in Führungszeugnisse blicken? Nein, denn wir dürften es nicht. Ob wir auf Fahrt gehen könnten, ohne zu wissen, welche Medikamente unsere Wölflinge kriegen müssen? Nein, definitiv nicht. Also: Ohne Gesundheitsdaten und ohne Führungszeugnisse könntet ihr eure Kerntätigkeit nicht erreichen.

Wer kann DSB werden?

Ein*e DSB muss nicht selbst Teil des Stammes sein, sondern kann auch völlig extern sein – ihr könntet theoretisch sogar eine*n professionelle*n Dienstleister*in aus Berlin–Mitte damit beauftragen und bezahlen. Wir sind gerade dabei zu prüfen, ob wir eine*n DSB auf Landesebene finden, der*die auch dafür zur Verfügung stünde, von euch ebenfalls berufen zu werden. Bitte wartet also weitere Infos von uns ab!

Ein*e DSB kann nebenbei natürlich auch andere Aufgaben im Verein haben, z.B. als Gruppenleiter*in. Aber das darf keine Aufgabe sein, bei der es zu einem **Interessenskonflikt** kommt! Ein solcher Interessenskonflikt liegt vor, wenn z.B. der*die nds.meinBdP-Admin oder der*die Mitgliederverwalter*in oder ein Mitglied der Stammesführung DSB ist. Eine endgültige juristische Klärung steht zwar noch aus, wann ein Interessenskonflikt genau vorliegt und wann nicht, aber grundsätzlich können wir vermutlich sagen: Wenn du daran beteiligt bist, das Datenschutz-System an zentraler Stelle mitzugestalten oder verantwortlich bist für den sämtlichen Datenschutz, dann darfst du nicht DSB werden. Wenn du nur in geringerem Maße Daten nutzt, z.B. eine Anmeldung zu einer Fahrt verwaltest oder eine Handynummer in deinem Handy speicherst, dann kannst du DSB werden.

Wie berufe ich jemanden zur*m DSB?

Zunächst mal: Fragen. Wenn Du dann jemanden gefunden hast, lohnt es sich, die Person schriftlich zu berufen oder auf eurer Stammesvollversammlung zu wählen oder zu bestätigen. Auch in letzterem Fall lohnt sich eine genaue Aufgabenbeschreibung, die von beiden Seiten (der Stammesführung einerseits und der*m DSB andererseits) unterschrieben wird. Das alles schriftlich zu machen, ist es deshalb sinnvoll, weil ihr dann gegenüber der Aufsichtsbehörde nachweisen könnt, dass ihr wirklich und zu jedem Zeitpunkt (ab dem 25. Mai 2018) eine*n DSB gehabt habt. Wie eine solche schriftliche "Bestellung" aussehen kann, findet ihr hier.

Wie gesagt: Wartet bitte noch wenige Tage ab, bis wir auf Landesebene weitergekommen sind!

Anschließend müsst ihr eure*n DSB an die Aufsichtsbehörde melden, damit die weiß, an wen sie sich wenden kann. Dafür wird es ein bundeseinheitliches Formular geben, das, sobald es fertig ist, auf dieser Seite des niedersächsischen Landesbeauftragten für den Datenschutz veröffentlicht wird. Auch das werden wir für euch im Auge behalten.

Was sind die genauen Aufgaben einer*s DSB?

Die genauen Aufgaben werden in Art. 39, Abs. 1 DSGVO geregelt:

- Der*die DSB unterrichtet und berät die Stammesführung und alle Mitglieder, die Daten verarbeiten, hinsichtlich dessen, was sie tun müssen für den Datenschutz.
- Der*die DSB kontrolliert, dass die gesetzlichen Datenschutzvorschriften eingehalten werden.
- Der*die DSB berät die Stammesführung, wenn sie eine Datenschutzfolgenabschätzung durchführt (siehe unten unter "Was tun, wenn der Datenschutz verletzt wurde?")
- Der*die DSB arbeitet mit der Aufsichtsbehörde zusammen und ist Ansprechpartner*in für sie.
- Der*die DSB berät betroffene Personen in allen Fragen rund um Datenschutz (siehe auch Art. 38, Abs. 4 DSGVO).

Damit all das möglich ist, muss man natürlich die **Kontaktdaten der*s DSB veröffentlichen**. Das geschieht sinnvollerweise auf der Homepage und kann außerdem auf den Anmeldeformularen zu Veranstaltungen geschehen. Aber: Es wäre natürlich nicht im Sinne des Datenschutzes, wenn ihr die persönliche Anschrift veröffentlicht! Es bietet sich an, eine Funktions-E-Mail-Adresse einzurichten wie z.B. datenschutz@stamm-zuckerberg.de.

Auftragsverarbeitung

"Auftragsverarbeitung liegt vor, wenn eine natürliche oder juristische Person (z.B. GmbH, KG, AG), Behörde, Einrichtung oder andere Stelle personenbezogene Daten im Auftrag eines Verantwortlichen verarbeitet" (Erste Hilfe zur Datenschutz-Grundverordnung, S. 24).

Das heißt: Immer, wenn ihr jemandem außerhalb eures Stammes Daten gebt, die er*sie in eurem Auftrag verarbeiten soll, oder ihr jemandem Einblick in eure Daten gebt, liegt eine Auftragsverarbeitung vor. Unterschiedliche Ebenen des BdP müssen untereinander in keinem Fall einen Auftragsverarbeitungsvertrag schließen. Beispiele wären z.B. wenn ein Elternteil, das nicht Mitglied ist, eure Kasse führt und deshalb personenbezogene Daten verarbeitet. Es liegt nicht vor, wenn ihr externe Fachleistungen in Anspruch nehmt.

Wenn Auftragsverarbeitung vorkommt, dann:

- solltet ihr vorher gut **prüfen**, ob der*die Auftragsverarbeiter*in hinreichend garantieren kann, dass die Daten geschützt werden. Hier gilt: Qualität vor Quantität – der günstige Preis rechtfertigt keine Verletzung des Datenschutzes! Denn am Ende könnte es hintenrum doch teuer werden für euch, denn: Wenn ein*e Auftragsverarbeiter*in Mist baut, dann haftet ihr vor sein*ihr Fehlverhalten, wenn er*sie in eurem Auftrag gehandelt hat
- solltet ihr einen **Vertrag** über die Auftragsverarbeitung schließen. Darin muss klar gelegt sein, dass ihr dem*r Auftragsverarbeiter*in sagt, was er*sie tun soll/darf und was nicht (Weisungsrecht), was der*die Auftragsverarbeiter*in tun soll, dass er*sie die Daten vertraulich und sicher behandeln muss, und was mit den Daten geschieht, wenn der Auftrag abgeschlossen ist. Ein Muster dafür findet ihr hier.
- solltet ihr euch **Kontrollrechte** einräumen lassen. D.h.: Ihr müsst einfach so unangekündigt bei dem*r Auftragsverarbeiter*in reinschneien dürfen und mal gucken, ob er*sie denn auch alles richtig macht. Dieses Recht solltet ihr euch nicht nehmen lassen, denn schließlich müsst ihr ja gerade stehen, wenn er*sie Mist baut.
- solltet ihr am Anfang schon **ans Ende denken** und klar regeln: Wann endet der Auftrag? Was passiert mit den Daten danach? Wie sind die Daten zu löschen? Usw.usf.

Hier kommt wahrscheinlich die große Frage auf, ob Webseitenhoster, Facebook, Instagram, E-Mail-Server usw. Auftragsverarbeiter*innen im Sinne der DSGVO sind. Hier steht noch weitere Klärung aus.

Betroffenenrechte geltend machen

Betroffene haben Rechte. Sie sollen in der Lage sein zu erfahren, "wer welche Informationen über sie zu welchem Zweck gespeichert hat und wie er sie nutzt." (Erste Hilfe zur Datenschutz-Grundverordnung, S. 40). Finden wir das nicht super? Eigentlich schon. Aber welche Rechte haben Betroffene eigentlich? Und was machen wir, wenn sie die einfordern?

Recht auf transparente Information

Dieses Recht bezieht sich auf die Datenschutzerklärung und den Passus in der Anmeldung (s.o.). Das sind Sachen, die wir als Verantwortliche den Betroffenen von uns aus geben müssen.

Recht auf Auskunft

Dies ist das grundlegendste Betroffenenrecht (logischerweise, denn erst, wenn man weiß, was andere über einen wissen, kann man z.B. verlangen, es zu löschen). Was müsst ihr tun, wenn jemand Auskunft verlangt?

1. Liegt ein konkreter Antrag vor? – Es lohnt sich ein standardisiertes Formular zu haben (Beispiel siehe hier).
2. Ist der*die Antragsteller*in überhaupt die Person, die sie vorgibt zu sein? – Ihr müsst darauf achten, dass ihr nicht einfach irgendwem die Daten von Marco Mühlstein gebt, nur weil jemand sagt, dass er*sie Marco Mühlstein ist.
3. Habe ich überhaupt Daten? – meistens ja. Wenn nicht, musst du es der Person trotzdem mitteilen!
4. Sammle die Daten zusammen (hierfür soll es einen Report in der MV geben, aber auch dein Verzeichnis der Verarbeitungstätigkeiten hilft dir dabei). Dinge, die du Marco Mühlstein jetzt mitteilen musst sind:
    a. Welche Daten habe ich von dir?
    b. Wozu brauche ich die? (Zweck der Verarbeitung)
    c. Wer arbeitet mit diesen Daten (Empfänger*in der Daten)
    d. Wie lange werde ich diese Daten noch haben (geplante Speicherdauer)
    e. Welche weiteren Betroffenenrechte hast du? Bei welcher Aufsichtsbehörde kannst du dich über mich beschweren?

⚠️ Dabei muss auch der konkrete Inhalt benannt werden. Also nicht: "Ich habe von dir Name, Telefonnummer, Anschrift", sondern "Ich habe von dir Marco Mühlstein, 01234-5678909, Mühlenstraße 6, 26123 Oldenburg")

5. Übermittle der*m Betroffenen das Ergebnis als schriftliche oder elektronische Zusammenfassung (z.B. in einem Worddokument per E-Mail). Eine Kopie ist nicht ausreichend! Der*die Betroffene erhält das ganze kostenlos!

Recht auf Berichtigung, Löschung und Einschränkung der Verarbeitung

Nehmen wir an: Marco Mühlstein merkt, du hast eine falsche Adresse von ihm, dann musst du die auf seinen Wunsch hin korrigieren.

Nehmen wir an: Marco Mühlstein ist der Meinung, dass du seine Schuhgröße nicht mehr brauchst, weil der Besuch im Bundestag jetzt schon drei Jahre her ist. Dann ist offensichtlich der ursprüngliche Zweck nicht mehr vorhanden und du musst löschen.

Nehmen wir an: Marco Mühlstein möchte nicht mehr, dass in der Excel-Tabelle mit den Anmeldungen zum Sommerlager steht, dass er evangelisch ist. Du stellst fest: Stimmt, diese Information ist vollkommen irrelevant, und du musst löschen.

Nehmen wir an: Marco Mühlstein möchte, dass du sämtliche Daten von ihm direkt nach der Sommerfahrt löschst und auf keinen Fall weitergibst. Dann gibt es aber noch eine andere Rechtsgrundlage für dich: Ihr müsst der Stadtjugendpflege die Daten übermitteln, um Zuschüsse zu erhalten. Aber du musst in diesem Fall die Datenverarbeitung einschränken, d.h.: Sie werden noch gespeichert, solange es nötig ist, aber du verwendest sie ausschließlich für die rechtlich zulässigen und nur absolut notwendigen Zwecke.

In allen Fällen musst du Marco hinterher mitteilen, dass du seinem Auftrag nachgekommen bist; bei geänderten Daten lohnt es sich, ihm einfach die neuen Daten zu schicken.

Recht auf Datenübertragbarkeit

Marco Mühlstein kann beantragen, dass er die Daten von dir "in einem gängigen Format" (also z.B. Excel) zur Verfügung gestellt bekommen, oder sogar, dass du diese Daten an jemand anderen weitergibst, z.B. an die Stammesführung vom Stamm der Amazonen, weil ihr ja zusammen ein Lager organisiert und die Stammesführung vom Stamm der Amazonen halt Marcos Handynummer braucht. Was ihr dem Stamm der Amazonen aber nicht mitteilen dürft, ist, welche Erkenntnisse ihr aus der Arbeit mit Marco gesammelt habt (z.B. dass er immer erst ab 13 Uhr erreichbar ist, weil er solange schläft).

Recht auf Widerspruch gegen die Verarbeitung

Nehmen wir an, ihr verarbeitet Daten auf Basis einer Interessensabwägung und veröffentlicht den Namen und die Handynummer von eurer Meutenführerin auf eurer Homepage, damit Eltern sie erreichen können. Die Meutenführung findet das aber nicht gut und widerspricht – dafür muss sie plausible Gründe nennen (z.B.: Ich werde ständig von einer marokkanischen Nummer angerufen!). Jetzt seid ihr in der Pflicht, neue Gründe zu finden, warum ihr die Handynummer doch veröffentlichen müsst. Solltet ihr keinen Grund finden, müsst ihr die Handynummer runternehmen. (In diesem Fall könnte eine Lösung sein, dass ihr euch gemeinsam auf die E-Mail-Adresse einigt, vielleicht sogar eine Funktionsadresse wie z.B. meute.insta@stamm-zuckerberg.de).

Recht, keiner automatisierten Entscheidung unterworfen zu werden

Klingt kompliziert, ist aber einfach – und für uns wahrscheinlich höchst irrelevant: Wir haben alle einen Anspruch darauf, dass kein Computer alleine darüber entscheidet, was mit unseren Daten passiert.

Das trifft z.B. nicht zu, wenn Brittje in der LGS jemanden in den Verteiler für den Stammesversand hinzufügt, weil die Person gerade Stammesführung geworden ist, denn: Brittje ist kein Computer! Die Entscheidung ist also nicht automatisiert, sondern passiert von Hand.

Recht auf Widerrufen der Einwilligung

Betroffene können, wenn sie eine Einwilligung gegeben haben, diese jederzeit widerrufen. Was heißt das für euch?

Da die Einwilligung nur eine (wenn auch die beste und wichtigste!) Form ist, auf die ihr Datenverarbeitung gestützt werden kann, solltet ihr zunächst prüfen:

- Welche Daten sind von dieser Einwilligung betroffen?
  - Eine Einwilligung ist immer spezifisch! Das heißt: Jemand willigt ein, dass Daten für die Sommerfahrt genutzt werden, und widerruft diese Einwilligung später. Davon sind aber nur die Sommerfahrtsdaten betroffen – alle anderen bleiben davon unberührt!
- Könnt ihr ohne diese Daten vertragliche Verpflichtungen erfüllen (Art. 6 Abs. 1 lit. b DSGVO)?
  - Eine Anmeldung zu einer Veranstaltung ist ein Vertrag zwischen euch und dem Mitglied bzw. dessen Erziehungsberechtigten über die Teilnahme an der Veranstaltung, in denen ihr beide gegenseitig einander etwas versprecht: Das Mitglied nimmt teil und ihr sorgt für sein Wohl. Das könnt ihr nur, wenn ihr seine Daten verarbeitet.
- Könnt ihr ohne diese Daten gesetzliche Verpflichtungen erfüllen (Art. 6 Abs. 1 lit. c DSGVO)?
  - Dass ihr euch um das Wohl der euch anvertrauten Kinder und Jugendlichen kümmern müsst, ist auch ein gesetzlicher Auftrag!
- Könnt ihr ohne diese Daten "lebenswichtige Interessen" der*s Betroffenen sichern (Art. 6 Abs. 1 lit. d DSGVO)?
  - Wenn ihr nicht wisst, welche Allergien jemand hat, könnt ihr nicht dafür sorgen, dass er*sie Essen vorgesetzt bekommt, dass er*sie auch verträgt. Es ist ein "lebenswichtiges Interesse" einer betroffenen Person, dass für seine Gesundheit gesorgt wird. Dafür braucht ihr Daten.
- Habt ihr selbst als Stamm "berechtigte Interessen", die wichtiger sind als die Interessen, Grundrechte und Grundfreiheiten der*s Betroffenen (Art. 6 Abs. 1 lit. f DSGVO)?
  - Ihr wollt Zuschüsse beantragen? Dann braucht ihr auch die Daten dieser Person.
- **Aber**: Fragt euch bei jeder dieser Fragen auch: Auf welche Daten könnten wir zu diesem Zweck verzichten?
  - Beispielsweise braucht ihr für das Beantragen von Zuschüssen nicht die Allergien der betroffenen Person. Andererseits könnt ihr auch gut ein laktosefreies Essen kochen, ohne das Alter der betroffenen Person zu wissen.

Ziel sollte sein, dass ihr der betroffenen Person klar sagt, dass ihr die Datenverarbeitung auf die absolut notwendigen Fälle einschränken werdet, dass ihr das aber auch dürft. In der Vorlage Datenschutzerklärung für Veranstaltungen, die ihr für euch ja nutzen könnt, ist das ja auch beschrieben, die Betroffenen haben dem zugestimmt.

technische und organisatorische Maßnahmen (TOM)

Um Daten zu schützen, müssen wir auch einige so genannte **TOMs** treffen. Diese TOMs haben neben dem Datenschutz noch einen ganz anderen Zweck: Sie bewahren den BdP und euren Stamm vor Schaden! Nämlich vor Schäden, die mit einem Leak oder ähnlichem einhergehen könnten. Einmal die falsche Liste an die Zeitung geschickt und schon habt ihr einen Skandal in eurem Provinzkäseblatt. Da muss nicht mal Runde Hack-Braten von Stamm Moskau versuchen, eure Stammesführungswahl zu manipulieren.

> ⚠ Alle TOMs gelten sowohl für eure **Stammes**räume, als auch für eure **Privat**räume sowie für **Stammes**computer als auch für **private** Devices vom Smartphone bis zum Tower-PC.

Ziele und Vorbereitung

Diese TOMs haben lt. Art. 32 DSGVO folgende **Ziele**:

1. Personenbezogene Daten sollen verschlüsselt und nach Möglichkeit pseudonymisiert werden.
    - D.h.: Ihr solltet **digitale oder analoge Schlüssel** benutzen oder, falls das nicht möglich ist, personenbezogene Daten so vorhalten, dass man mit ihnen keine Person identifizieren kann (z.B. durch falsche Namen).
2. Personenbezogene Daten sollen vertraulich behandelt, integer (also unversehrt) und verfügbar sein; die Systeme und Dienste, mit denen ihr sie verarbeitet, sollen zudem belastbar sein.
    - **Vertraulichkeit** heißt, dass Menschen, die bestimmte Daten nichts angehen, zu diesen auch keinen Zugang haben.
        - Negativbeispiel: Im Raum von Sippe Taubsi hat Meutenführerin die ausgefüllten Anmeldungen zur Meutenfahrt liegen gelassen. Die Sipplinge amüsieren sich köstlich, dass die kleine Schwester ihres Sippenführers keine Milch verträgt.
    - **Integrität** heißt, dass die Daten davor geschützt werden sollen, von irgendwem verändert werden, der das nicht darf.
        - Negativbeispiel (dieselbe Geschichte): Plötzlich kommt der Sippenführer rein und sieht die Anmeldungen. Bevor er sie einsammelt, schreibt er noch "Nutella-Allergie" dazu, um seine Schwester zu ärgern.
    - **Verfügbarkeit** heißt, dass die Daten sofort genutzt werden können, wenn sie benötigt werden.
        - Negativbeispiel (dieselbe Geschichte): Währenddessen sitzt die Meutenführerin zu Hause und stellt fest, dass die Meutenfahrt 30 Euro teurer werden muss und dass sie die Eltern schnellstens darüber informieren muss, bevor die Zugtickets noch teurer werden! Nur leider findet sie die blöden Anmeldungen nicht und weiß nicht, wie sie die Eltern erreichen soll.
    - **Belastbarkeit** heißt, dass die "Systeme und Dienste", die ihr benutzt – also z.B. euer Computer oder nds.meinbdp –, es auch aushalten, dass auf ihnen Daten verarbeitet werden.
        - Negativbeispiel (dieselbe Geschichte): Natürlich hat die Meutenführerin auch die Telefonnummern der Eltern auf ihrem Computer gespeichert... oder sie wollte es zumindest. Aber wo sind sie? Hat sie sie neulich gelöscht, weil ihre Festplatte mal wieder voll war? Diese verdammte Festplatte! Ständig ist die voll und sie muss wichtige Dateien löschen!
3. Personenbezogene Daten sollen nach einem "physischen oder technischen Zwischenfall **rasch wiederherzustellen**" sein.
    - D.h.: Wenn mal irgendwas passiert (sei es ein Platzregen auf Fahrt oder ein technischer Defekt), solltet ihr Vorkehrungen getroffen haben, wie ihr die Daten wiedergewinnen könnt, ohne sie noch einmal neu zu erheben. Ziel ist, dass sie schnell wieder verfügbar sind!
        - Negativbeispiel (dieselbe Geschichte): Endlich ist der Meutenführerin eingefallen, dass sie die Anmeldungen im Sippenraum vergessen hat, und sie fährt sofort hin. Auf dem Rückweg fängt es plötzlich an, wie aus Eimern zu schütten, und als sie zu Hause ankommt, ist alles durchweicht – auch die Anmeldungen: Man kann nichts mehr entziffern, außer einem Wort mit Edding geschrieben: Nutella-Allergie!
4. Ihr solltet regelmäßig **überprüfen**, bewerten und evaluieren, ob die TOMs, die ihr getroffen habt, die Sicherheit wirksam gewährleisten.
    - D.h.: Ihr habt bestimmt mitbekommen, dass es immer mal wieder Updates gibt, z.B. von eurem Virenschutz. Aber ihr solltet auch selbst immer mal wieder schauen, ob noch alles auf einem guten Stand ist. Kennt mittlerweile jede*r das Versteck vom Schlüssel für den Schrank mit den Mitgliedsanträgen? Hat sich 1234 als WLAN-Passwort vielleicht doch nicht so bewährt? Und wer hat eigentlich die Mitgliederliste an die Küchentür gehängt?!
        - *Positiv*beispiel (dieselbe Geschichte): Die Meutenführerin hat gemerkt, dass sie ständig irgendwo Anmeldungen liegen lässt. Also hat sie damit angefangen, dass die Eltern ihr die Anmeldungen als PDF per E-Mail schicken und sie sie als verschlüsselte (!) zip-Datei in ihrer Dropbox speichert. So kann sie sogar von ihrem Handy darauf zugreifen! Wie praktisch doch alles geht in dieser schönen neuen Welt!

Bevor ihr anfangt, einfach TOMs umzusetzen, müsst ihr euch natürlich klar sein, **wer was wann warum wie** verarbeiten muss. Denn danach richten sich so Fragen wie: Für wen müssen die Daten denn auf dem Lager eigentlich verfügbar sein? Wann braucht die Schatzmeisterin die Namen und Anschriften und das Alter eigentlich für die Zuschussbeantragung? Usw. Diese Sachen müsst ihr bei vorübergehenden Verarbeitungstätigkeiten natürlich immer wieder neu entscheiden, aber einige Ähnlichkeiten zwischen zwei Lagern wird es ja wohl doch geben. Und bei Dauerbrennern wie die Aufbewahrung von Aufnahmeanträgen solltet ihr sowas auf jeden Fall vorher klären! **Es bietet sich an, solche Sachen schriftlich festzuhalten,** denn diese Antworten werdet ihr **die nächsten Jahre brauchen!**

Was ihr ebenfalls tun solltet, ist abzuwägen, welche **Risiken** in welchen Fällen auf euch zukommen können. Denn es macht durchaus einen Unterschied, welche Daten auf welche Weise vernichtet, verloren, verändert oder unbefugt offengelegt werden: Wenn plötzlich Kontodaten der Eltern auf Google zu finden sind, dann ist Polen offen. Wenn aber ein Wölfling auf der Zuschussliste seine große Schwester zwei Jahre jünger macht, ist das zwar auch eine unbefugte Offenlegung (und eine Veränderung der Daten), aber verkraftbar – ihr solltet es trotzdem tunlichst vermeiden, irgendwo Listen rumliegen zu lassen, denn eine solche Veränderung kann schon ziemlich Ärger geben mit der Zuschussbehörde!

Diese **Risikoabwägung** dürfte relativ leicht fallen, wenn ihr euer Verzeichnis der Verarbeitungstätigkeiten habt: Dann könnt ihr schauen, wer welche Daten wie wann warum verarbeitet und wo da potentielle Sicherheitslöcher bestehen könnten.

TOM analog

Ihr solltet versuchen, möglichst wenig personenbezogene Daten in Papierform zu haben. Wo es sich nicht umgehen lässt, solltet ihr sie so verwahren, dass sie nicht für jede*n zugänglich sind, sondern nur für die Personen, die mit diesen Daten umgehen müssen! Beispiele:

- Mitgliedsanträge solltet ihr in einem verschlossenen Schrank aufbewahren. Und nach Austritt des Mitglieds umgehend fachgerecht entsorgen (z.B. schreddern oder klein schnippeln).
- Buchhaltungsunterlagen (z.B. aus der Kassenführung) sollten ebenfalls in einem verschlossenen Schrank deponiert werden – bis zu ihrer gesetzlich vorgesehenen Vernichtungsfrist.
- Die Schlüssel zu diesen Schränken sollten natürlich nicht im Schloss stecken (dann könntet ihr die Sachen ja auch gleich offen ins Regal stellen), sondern an einem Ort verwahrt werden, den nur diejenigen kennen, die ihn kennen müssen.
- Diese Sachen gelten natürlich sowohl für euer Stammesheim als auch für Privaträume!
- Auf Lagern und Fahrten sollten Anmeldeformulare oder Teilnahmelisten nicht öffentlich und für alle einsehbar herumliegen, sondern von der verantwortlichen Person an einem möglichst sicheren und möglichst trockenen Ort verwahrt werden. Nach der Aktion sind sie selbstverständlich auch so zu vernichten, dass man keinen Inhalt mehr daraus ziehen kann.

Es kann Geld kosten, neue Schlösser einzubauen oder wasserdichte Zip-Bags für Anmeldungen zu kaufen. Das sollte es euch wert sein, denn: Denkt an euer Image und denkt an die möglichen Strafzahlungen.

TOM digital: IT-Sicherheit

Die meisten Daten, die wir verarbeiten, verarbeiten wir wahrscheinlich digital. Hier drohen auch die größten Risiken: Während man mit Daten von einer Veranstaltungsanmeldung auf Papier im ersten Moment nicht so viel anfangen kann (denn um sie auszuwerten, muss man sie erst abtippen), kann man aus Daten, die man von einem Computer abgeschöpft hat, sofort extrem viel machen. Häufig genug ist man übrigens selbst schuld, wenn man den Datenschutz verletzt! Einige Beispiele findet ihr unten (na, wer fühlt sich ertappt?).

"**Datenschutz ohne IT-Sicherheit kann es praktisch nicht geben.**" (Erste Hilfe zur Datenschutz-Grundverordnung, S. 25). Deshalb werden die Ziele Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit auch in der DSGVO erwähnt: Es sind die klassischen Schutzziele von IT-Sicherheit.

IT-Sicherheit kann Geld kosten! Ihr solltet euch also ggf. Gedanken darüber machen, wie viel Geld ihr zur Verfügung stellen wollt und könnt, um eure Daten sicher zu verwahren. Wir empfehlen, auf nds.meinbdp zu setzen, auch wenn ihr damit den LV als Auftragsverarbeiter einsetzt, aber hier könnt ihr euch relativ sicher sein, dass eure Daten sicher gelagert sind und oben genannte Ziele umgesetzt werden.

Hier nun einige Beispiele:

- **Berechtigungsmanagement**: Ihr müsst dafür sorgen, dass *nur die* Leute auf bestimmte Daten Zugriff haben, die sie *auch wirklich benötigen*.
  - Negativbeispiel: Alle Anmeldedaten zur Stammessommergroßfahrt liegen in der Stammesratsdropbox, sodass die Fahrtenleitung genauso zugreifen kann wie die Materialwartin, die gar nicht mitfährt und vielleicht höchstens wissen muss, wie viele Kohten sie rausgeben muss.
    - Lösung in Dropbox/ E-Mail o.ä.: Die Exceltabelle kommt weg und liegt nur nur auf dem PC der Fahrtenleiterin. Für die Küche gibt es eine Tabelle mit den Ernährungsgewohnheiten, Namen und Sippenzugehörigkeit. Für die Materialwartin eine Liste der Sippen mit Anzahl der Sipplingen. Und für Sippenführungen gibt es je eine eigene Exceltabelle, in denen alle (!) Daten ihrer Sipplinge (aber nur ihrer eigenen!) stehen. Diese Dateien können natürlich auch auf Dropbox abgelegt werden, sollten dann aber passwortgeschützt werden (s.u.)
    - Lösung in nds.meinbdp o.ä.: Die Exceltabelle kommt auf eine Unterseite, auf die nur die Fahrtenleitung Zugriff hat. Auf eine weitere Seite hat nur die Materialwartin und die Fahrtenleitung Zugriff (Inhalte wie oben), dasselbe gilt für die Küche und die einzelnen Sippen. Hier entfällt die Notwendigkeit zur Verschlüsselung, weil nds.meinbdp ausreichend sicher ist (sicherer als Dropbox).
  - Negativbeispiel: Obwohl Karlheinz seit drei Jahren nicht mehr im Stammesrat sitzt, hat er noch immer alle Zugriffsrechte.
    - Lösung: Zugriffsrechte entziehen, sobald jemand nicht mehr im Amt ist.
- **Verschlüsselung** lässt sich leichter umsetzen, als Du denkst!
  - Bei E-Mails reichen in der Regel die Einstellungen **STARTTLS** und **Perfect Forward Secrecy**. Die meisten deutschen E-Mail-Provider ermöglichen das – ihr müsst es nur einstellen, in eurem E-Mail-Programm. Wie das geht, erfahrt ihr ggf. auf den jeweiligen Hilfeseiten. Wir empfehlen, das einfach für alle E-Mail-Konten zu machen, auch wenn ihr eins von euren vier Konten nicht für die Pfadfinder*innen benutzt.
    - Der Versand von Dateien via E-Mail kann zusätzlich mit PGP oder S/MIME verschlüsselt werden (s.u. Datei-Verschlüsselung).
  - Eure Website benötigt **HTTPS**, wenn ihr z.B. einen Login oder ein Kontaktformular habt, also eine Möglichkeit, wo personenbezogene Daten angegeben werden. Hierbei solltet ihr euch über die korrekte Umsetzung informieren!
  - Dateien könnt ihr relativ zu einer **verschlüsselten ZIP-Datei** verpacken (z.B. mit der Verschlüsselungstechnik AES-256). Vorteilhaft ist natürlich, dass ihr mehrere Dateien in einem ZIP-Ordner zusammenfassen könnt. Diese Dateien könnt ihr dann auch per Mail verschicken.
    - ⚠️ Insbesondere wenn ihr externe Cloud-Dienste benutzt, die ihr nicht selbst hostet (z.B. Dropbox, iCloud, GoogleDrive), raten wir ganz entschieden zu einer Verschlüsselung von personenbezogenen Daten! Alternativ könnt ihr nds.meinbdp für euren Stamm benutzen, da ist eine Verschlüsselung nicht nötig.
  - Es ist selbstverständlich, dass ihr euer WLAN **sicher verschlüsselt**. Das Passwort, das auf der Rückseite eures Routers steht, solltet ihr nicht verwenden, sondern es ändern: Am besten sind hierbei WPA2 und ein 20-stelliges Passwort. Und auch das Passwort für die Konfiguration eures Routers (wer nicht weiß, wovon ich rede, sollte sich an dieser Stelle dringend informieren, denn: Dein Router ist gefährdet!) solltet ihr dringend ändern.
  - Wenn ihr Einwahllösungen nutzt, um von zu Hause auf den Stammesserver zuzugreifen, eignet sich **VPN**.
  - All eure Geräte (auch euer Smartphone) solltet ihr mit einem **Passwort** versehen! Und zwar nicht nur beim Hochfahren, sondern es sollte jedes Mal eingegeben werden, wenn ihr den Bildschirm aktiviert! Darüber hinaus kann eine **Datenträgerverschlüsselung** sinnvoll sein für den Datenträger, der besonders schützenswerte Daten enthält; empfehlenswert ist VeraCrypt (kostenfrei unter https://veracrypt.codeplex.com). Eine solche Datenträgerverschlüsselung bieten aber auch sowohl Computer- als Smartphone-Betriebssysteme heutzutage meist von sich aus an, sie sind integriert! Auch eure USB-Sticks und externen Festplatten solltet ihr verschlüsseln; es ist zu vermeiden, unbekannte Geräte an euer Device anzuschließen. Wie ihr **richtig verschlüsselt**, erklärt euch hier das BSI.
  - zu **WhatsApp** siehe unten.
- **Patch-Management** bedeutet, dass jede*r von euch darauf achtet, dass die Soft- und Hardware, die er*sie nutzt, möglichst auf dem neuesten Stand ist. Das heißt, dass ihr sofort in den Laden rennen müsst, wenn das neue iPhone Z rausgekommen ist, sondern: dass ihr

regelmäßig alle relevanten Programme und Dienste updatet. Wer also immer auf "Später" klickt, wenn Windows sagt: "Ich hab ein Update für dich!", der sollte sich dringend umgewöhnen. Das gleiche gilt auch für die Apps auf eurem Telefon.

- Dass **Backups** sinnvoll sind, braucht euch wahrscheinlich niemand mehr zu erzählen. Trotzdem hier ein paar Takte dazu:
  - Backups schützen vor so genannter Ransomware. Das ist ein Schadcode, der alle Dateien verschlüsselt und euch damit erpressen möchte, dass ihr einen unzahlbaren Geldbetrag in Bitcoins bezahlt. Oftmals werden die Dateien nach Bezahlen des Lösegelds aber nicht einmal rück-entschlüsselt und man hat gleich den doppelten Salat: Tausend Milliarden ausgegeben und trotzdem alle Daten verloren.
  - Backups schützen, weil man im Fall eines Befalls mit Ransomware zumindest ältere Versionen seiner Dateien noch hat. Das geht aber nur, wenn man sie regelmäßig macht und längerfristig aufbewahrt, auch in mehreren Versionen, denn: Ransomware und Viren geben sich nicht immer sofort zu erkennen, sondern machen es sich erstmal gemütlich, um dann nach einer gewissen Seite auf einmal zuzuschlagen. So kann es geschehen, dass sie auch in eine eurer Datensicherungen gelangen und sie genauso unbrauchbar machen, wie alles andere. Dann hättet ihr quasi den dreifachen Salat: Kein Geld mehr, keine Daten mehr, kein Backup mehr.
  - Backups schützen am besten, wenn sie möglichst viele Dateien zentral sichern. Das heißt: Natürlich kann jede*r einzelne alle eigenen Dateien auf dem eigenen Computer speichern und regelmäßig auf eine von drei (!) externen Festplatten sichern. Aber sinnvoller wäre es, wenn ihr die Dateien gleich an einem gemeinsamen Speicherplatz speichert und sie dann regelmäßig von einer*m Backup-Beauftragte*n gesichert werden.
    - Tipp: Ihr könnt z.B. nds.meinbdp benutzen und müsst euch dann um die Dateien, die dort liegen, keine Sorgen mehr machen: nds.meinbdp wird regelmäßig in Gänze gesichert.
- **E-Mails richtig adressieren**:
  - Es war einmal eine Ratsfraktion, die wollte ihre Newsletter auch nach der neuen DSGVO korrekt versenden. Sie schrieb eine E-Mail an über 900 Personen und Institutionen, um darüber zu informieren und um ein schriftliches Einverständnis für den weiteren Newsletterversand zu geben. Leider hat sie dabei alle 900 Empfänger*innen in die An-Zeile geschrieben, also schön hunderte personenbezogene Daten (E-Mail-Adressen) mit hunderten von Menschen geteilt (Quelle NDR). **So macht man's nicht**.
  - **So geht's besser**: Wenn ihr an mehrere Empfänger*innen schreibt (z.B. an alle Eltern), dann packt ihre E-Mail-Adressen ins BCC, sodass die Empfänger*innen nicht sehen, wer die E-Mail noch bekommen hat. Alternativ könntet ihr auch einen Verteiler einrichten (alle-eltern@stamm-zuckerberg.de). So ist es z.B. datenschutzrechtlich unbedenklich, alle Stämme mit ihrer nds.pfadfinden-Adresse in der An-Zeile anzuschreiben (ataulf@nds.pfadfinden.de, parzival@nds.pfadfinden.de usw.), aber die privaten E-Mail-Adressen der Stammesführungen, auf die die nds.pfadfinden-Adressen weiterleiten (z.B. wollepetry@weissdergeier.de), sind schützenswerte Daten und gehören in's BCC.
  - **Noch ein Tipp**: Bevor ihr eine E-Mail versendet, guckt nochmal alles nach, ob alles richtig ist: Die richtigen Empfänger*innen? Im richtigen Adressfeld? Der richtige Text? Der richtige Anhang? Sonst passiert sowas: Statt einer Bewerbungsmappe schickt ihr eurem potentiellen neuen Chef ein Bild von Nicholas Cage.

typische Irrtümer der IT-Sicherheit

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat sich mal mit typischen Sicherheitsirrtümern beschäftigt. Na, wer von euch kennt Sätze wie diese:

- "Ich hab ne **Firewall**, bei mir kann nichts passieren."
- "Ich surfe eh nur auf **Seiten, die sicher sind**, von denen kann kein Angriff kommen."
- "Meine Daten sind in der **Cloud**, da brauch ich doch kein Backup"
- "**Öffentliches WLAN** ist doch ausreichend sicher!"
- "Wenn ich **automatische Updates** aktiviert habe, brauch ich mich um nichts weiter zu kümmern."
- "Ich hab keinen Virus! Das hätte ich schon längst **gemerkt**!"
- "Ich hab doch **nichts zu verbergen**! Für meine Daten interessiert sich doch niemand."
- "Wenn ich den **Papierkorb leere**, sind die Daten weg."
- "Schad-E-Mails sind nur gefährlich, wenn ich den **Anhang öffne**."
- "Eine E-Mail kommt immer von der Adresse, die im **Absenderfeld** steht."
- "Phishing-Mails **erkenne ich sofort**!"

Na, klingen solche Sätze bekannt? Schaut gerne mal rein auf die Seite des BSI und korrigiert euer Wissen über IT-Sicherheit.

Was tun, wenn Datenschutz verletzt wurde

Was ist das?

Und dann ist es passiert... Aber **wann ist es eigentlich passiert?**

Eine Verletzung des Schutzes personenbezogener Daten liegt vor, wenn die Datensicherheit verletzt wurde – egal ob absichtlich oder nicht, egal ob rechtmäßig oder nicht – und Daten so vernichtet, verloren, verändert oder für Unbefugte offengelegt oder zugänglich gemacht wurden. Dabei spielt es keine Rolle, ob es "normale" personenbezogene Daten (wie das Geburtsdatum) oder besonders schützenswerte Daten (wie Gesundheitsdaten) sind. Eine Verletzung kann auch dann vorliegen, wenn nicht davon auszugehen ist, dass es zu einem Schaden kommen wird oder kann.

Was heißt das?

Ein paar Beispiele:

- Alle Stammesmitglieder haben in der Dropbox Zugriff auf die Handynummern aller Mitglieder. (= Sie haben *unbefugten Zugang*; das ist eine Verletzung, auch wenn sie sich die nicht angeschaut haben).
- Auf einem Stammeslager fallen die Anmeldebögen ins Feuer. Es gibt keine Kopien. (= Die Daten wurden *vernichtet*.)
- Ein Sippenführer hat die Excel-Tabelle mit den Anmeldungen aus Versehen durcheinander gebracht... zu allem Überfluss speichert er sie auch noch ab und lädt sie auf nds.meinBdP hoch. (= Die Daten wurden *verändert*).
- Der Schatzmeister lässt die Kassenunterlagen in der Bushaltestelle liegen (= Die Daten gingen *verloren*.)
- Ihr leitet eurer Bezirkssprecherin eine E-Mail von einer Mutter weiter; die E-Mail der Mutter war eine Antwort auf eine Mail von euch an alle Eltern, in der die E-Mail-Adressen aller Eltern in der An-Zeile hattet. (= Die Daten wurden gleich zweimal *für Unbefugte offengelegt*.)

Was mach ich dann?

1. Ruhe bewahren.
2. Wenn möglich, sofort den Schaden begrenzen (z.B. den Zugang sperren oder die noch nicht verbrannten Anmeldebögen aus dem Feuer retten.)
3. Sprich mit jemandem, der Ahnung hat, beispielsweise eurer*m Datenschutzbeauftragten oder der Aufsichtsbehörde.
4. Dokumentiere die Verletzung inklusive aller Fakten, die damit zu tun haben, sowie die Auswirkungen und, wie ihr Abhilfe geschaffen habt. Diese Dokumentation hilft der Aufsichtsbehörde dabei zu entscheiden, ob ihr alles richtig gemacht habt beim Lösen eures Problems. Was ihr dokumentieren solltet, seht ihr gleich unten in Punkt 5.
5. Informiere die Aufsichtsbehörde.
    - Dies muss "unverzüglich" geschehen, d.h. "ohne schuldhaftes Zögern". Das heißt: Ihr dürft erstmal versuchen, den Sachverhalt aufzuklären. Aber Achtung! Je komplizierter der Sachverhalt ist, desto gefährlicher ist die Lage! Wenn euch Informationen über den Sachverhalt nur schrittweise erreichen, dann stellt sie der Aufsichtsbehörde ebenso schrittweise zur Verfügung. Im 90 % der Fälle gilt eine Meldefrist von **72 Stunden!** Eine Verzögerungstaktik oder gar ein Verschweigen können Bußgelder nach sich ziehen!
    - Es ist davon auszugehen, dass die Landesbeauftragte für den Datenschutz ein entsprechendes Meldeformular zur Verfügung stellen wird. Was genau gemeldet werden muss, steht in Art. 33, Abs. 3 DSGVO:
        - Welche *Art der Verletzung* liegt vor?
        - Welche *Kategorie von Daten* wurde verletzt?
        - *Wie viele Personen* sind in etwa betroffen?
        - Wer ist der*die *Datenschutzbeauftragte* bzw. wo kann die Aufsichtsbehörde sich weiter informieren?
        - Welche *wahrscheinlichen Folgen* erwartet ihr?
        - Welche *Maßnahmen* habt ihr ergriffen oder werdet ihr ergreifen, um die Verletzung zu beheben und den Schaden zu begrenzen.
    - ℹ️ Ihr müsst die Behörde zwar nicht immer informieren, aber: lieber einmal zu viel als zu wenig. Die einzige Ausnahme lautet: Wenn voraussichtlich kein "Risiko für die persönlichen Rechte und Freiheiten" der Betroffenen besteht (Art. 33, Abs. 1 DSGVO).
        - Beispiel, wann ihr die Behörde informieren müsst: Du warst am Schulrechner in eurer Stammesdropbox und hast vergessen, dich anschließend auszuloggen; zwei Tage später stellst du fest, dass die Excel-Tabelle mit den Daten der Sommerfahrtsteilnehmer*innen weg ist und auch nicht wiederherstellbar. Die Daten sind noch da, die Frage ist nur bei wem und was der*diejenige damit vorhat Unbedingt melden!
        - Beispiel, wann ihr die Behörde nicht informieren müsst: Während eines Lagers brauchst du zwischendurch mal die Anmeldung einer Teilnehmerin. Du legst sie dann erstmal auf eine Kiste in der Jurte. Später denkt irgendwer, dass man dieses Stück Papier doch wunderbar zum Feuer anmachen verwenden kann. Zum Glück hat deine Stammesführung alle Anmeldungen auch digital auf dem Smartphone dabei, sodass im Notfall die Daten immer noch vorhanden sind Die Anmeldung ist unwiderbringlich verloren, niemand kann mehr etwas mit ihr anfangen; gleichzeitig habt ihr noch alle relevanten Daten an sicherer Stelle für den Notfall keine Gefahr für die "Rechte und Freiheiten" eurer Teilnehmerin keine Meldung nötig.
6. Findet heraus, ob ihr auch die Betroffenen informieren müsst.
    - ⚠️ Das ist nur dann notwendig, wenn durch die Verletzung "voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten" der Betroffenen besteht (Art. 34, Ab. 1 DSGVO) besteht. Davon gibt es aber auch noch Ausnahmen:
        a. wenn ihr die betroffenen personenbezogenen Daten ausreichenden TOMs unterzogen habt; dazu gehört insbesondere das Stichwort Verschlüsselung von Daten!
        b. wenn ihr nach der Entdeckung der Verletzung ausreichende Maßnahmen ergriffen habt, durch das "hohe Risiko für die persönlichen Rechte und Freiheiten" nicht mehr besteht.
        c. wenn eine solche Information einen "unverhältnismäßigen Aufwand" bedeuten würde – in diesem Fall ist aber eine öffentliche Information notwendig! Dieser letzte Fall dürfte allerdings eher ein Unternehmen wie Facebook betreffen, weniger unseren kleinen, süßen Laden hier.

      Da das manchmal schwer zu sagen ist, solltet ihr euch hier mit eurer*m Datenschutzbeauftragten und ggf. der Aufsichtsbehörde absprechen. In richtig extremen Fällen könnt ihr euch auch anwaltlich beraten lassen (⚠️ Vorher unbedingt in der LGS melden!).
7. Informiert die betroffenen Personen
    - Hierzu braucht ihr natürlich erstmal deren Namen und Kontaktdaten. Hilfreich ist hierbei das Verzeichnis von Verarbeitungstätigkeiten, da hier verzeichnet ist, Daten welcher Betroffenen in diesem Verarbeitungsvorgang verarbeitet wurden.
    - Was muss in die Information rein? Sie muss zunächst "in klarer und einfacher Sprache" formuliert sein. Also: Kein Juristendeutsch, sondern Pfadfinderdeutsch.
        - *Was ist passiert und wie konnte das passieren?*
        - Wer ist *Datenschutzbeauftragte*r* und wie kann man den erreichen?
        - Was könnten *Folgen* sein?
        - Was habt ihr für *Maßnahmen* ergriffen oder werdet ihr ergreifen, um den Schaden zu beheben bzw. die Folgen abzumildern.
    - ⚠️ Wenn ihr Menschen benachrichtigt, können diese ggf. **Haftungsansprüche** stellen. Deshalb solltet ihr euch vor der Benachrichtigung unbedingt rechtlich beraten lassen – eure erste Anlaufstelle sind dazu der*die Datenschutzbeauftragte und die LGS! Da es zum Teil von einzelnen Formulierungen abhängt, ob jemand Haftungsansprüche stellen kann, solltet ihr hier besonders umsichtig formulieren.

Datenschutzfolgenabschätzung

...

Besonderheit: Bilder

Abbildungen von Personen sind personenbezogene Daten, denn anhand ihres Aussehens kann ich eine Person identifizieren. Im wesentlichen gilt hier also (neben den allgemeinen Regeln für personenbezogene Daten aus der DSGVO) das alte KUG weiter: **Keine Bilder verwenden, auf denen Menschen zu sehen sind, die darin nicht eingewilligt haben!** Was ihr genau dabei beachten müsst, wie eine solche Einwilligung aussehen kann, in welchen Fällen keine Einwilligung nötig ist, das findet ihr hier:

Nach § 22 KUG dürft ihr ein Bildnis nur mit der Einwilligung der abgebildeten Person veröffentlichen. Eine **Einwilligung muss vor der Veröffentlichung** erfolgen. Es gibt zwar Ausnahmen (s.u.), aber die sind genau das: Ausnahmen. In der Regel benötigt ihr also **immer** eine Einwilligung. Wie ihr das machen könnt, seht ihr Datenschutz & Bildrechte im Anmeldeformular. Hier erstmal ein paar Grundlagen:

- Es ist egal, ob ihr im Internet veröffentlicht oder auf Papier!
- Betroffen sind auch Verbreitungen über **Fileshare-Plattformen** wie GoogleDrive oder Dropbox! Sogar das Teilen eines Fotos mit auch nur einer anderen Person bei **WhatsApp und anderen Messengern** ist betroffen, denn ihr gebt das Bildnis an jemanden weiter und ihr erlaubt der App Zugriff auf das Foto. Also ⚠️ Wenn ihr mit einem Smartphone aufnehmt, von wo das Bild direkt in einer Cloud geladen wird, dann **ver öffentlicht ihr sogar schon im Moment der Aufnahme!**
- **Auch Bilder mit mehr als sieben Personen** unterliegen dem KUG! Dieses Gerücht ist reiner Blödsinn!
- **Personen kann man auch von hinten erkennen** oder mit verpixeltem Gesicht: Es genügt, dass die Mitschüler*innen, Nachbar*innen oder Bekannte diese Person identifizieren könnten.
- Bei Filmen ist es **egal, wie lange** die Person **zu sehen** ist!
- Ein **öffentlicher Hinweis**, dass Foto- und Videoaufnahmen gemacht werden, **ist nicht ausreichend!**

Minderjährige

Insbesondere bei Minderjährigen sollte **die Einwilligung schriftlich vorliegen**. Ihr könnt sie im Anmeldeformular unterbringen.

ℹ️ Es ist ein "höchstpersönliches Recht" darüber zu entscheiden, was jemand mit meinem Gesicht macht. Bei diesen Rechten haben Kinder und Jugendliche bereits ein gewisses Mitspracherecht. Ab einem bestimmten Alter bzw. einer bestimmten Reife solltet ihr also zusätzlich zur Unterschrift der Eltern auf das Verhalten der*s Jugendlichen achten. Mit dem eigenen Verhalten drückt man nämlich stillschweigend aus, ob man einverstanden ist (s.u.). Also: Auch wenn Mutti und Vati unterschrieben haben, dass Bilder der 16-jährigen Sandy überall verwendet werden dürfen, kann sie selbst auf euch zukommen und sagen, dass sie das nicht will, oder sich einfach aus dem Bild drehen, wenn sie merkt, dass ein Bild gemacht wird.

stillschweigende Einwilligung

Eine stillschweigende Einwilligung liegt vor, wenn eine Person **in dem vollen Bewusstsein, dass das Foto zur Veröffentlichung bestimmt ist, sich abbilden lässt**. Die Crux ist hier das *volle Bewusstsein*. Um zu ermitteln, ob eine Person veröffentlicht werden will, die ihr auf einem Bild seht, das ihr veröffentlichen wollt, von der aber keine schriftliche Einwilligung vorliegt, stellt euch folgende Fragen:

Der große Dr. Winter-Test: Stillschweigende Einwilligung

Beantworte die Fragen **nur dann mit ja, wenn du dir 100 % sicher** bist! Dein Dr. Winter-Team.

- Ist die Person **mindestens 18 Jahre** alt?
  - ja (3 Punkte)
  - nein (0 Punkte)
  - weiß nicht (1 Punkt)
- Ist es dieser Person **höchstwahrscheinlich bekannt, wofür*** Fotoaufnahmen von dieser Veranstaltung genutzt werden?
  - ja (3 Punkte)
  - nein (0 Punkte)
  - weiß nicht (1 Punkt)
- Hat diese Person **mitbekommen, dass gerade ein Foto von ihr gemacht** wird?
  - ja (3 Punkte)
  - nein (0 Punkte)
  - weiß nicht (1 Punkt)

Auflösung		
9 Punkte	**4–8 Punkte**	**0–3 Punkte**
Herzlichen Glückwunsch! Die Person hat wahrscheinlich ihre stillschweigende Einwilligung gegeben!	**Knapp vorbei ist auch daneben!** Da musst du wohl nochmal nachfragen.	**Schade!** Das sieht gar nicht gut aus, da musst du wohl nochmal nachfragen.

---

*) Es geht dabei auch um **alle Plattformen**: Wenn ihr also gerade einen neuen Snapchat-Account habt, dann weiß die Person das vielleicht noch gar nicht. Und wenn die Person gar kein Facebook hat, kennt sie eure Seite vielleicht auch nicht. Jemand aus einem befreundeten Stamm weiß nicht, dass ihr der Zeitung schreiben wollt. Usw.usf.

Ein typisches Beispiel ist das **Posieren** für ein Foto: Wenn ihr z.B. nach der Stammesvollversammlung ein Foto der neuen Stammesführung macht. Das heißt aber **nicht**, dass du als Stammespressesprecherin dieses Bild jetzt für immer und auf allen Plattformen verwenden darfst! Zu welchem konkreten Zweck wurde dieses Foto gemacht? Für die Homepage vielleicht oder auch für Facebook, aber hattet ihr auch über die Zeitung gesprochen? Frage lieber nochmal nach. Bei **Minderjährigen** gilt das genauso!

Bei **Minderjährigen** gilt: Die Einwilligung der Erziehungsberechtigten muss in jedem Fall vorliegen. Ab 14 Jahren bzw. ab einer gewissen Reife sollte jedoch auch die abgebildete Person zustimmen.

Social Media: WhatsApp, Facebook, instagram & co.

Laut dem Merkblatt "WhatsApp im Unternehmen" von der Landesbeauftragten für Datenschutz Niedersachsen ist die Nutzung von WhatsApp **in keinem Fall DSGVO-konform zu gestalten**.

Was ist das Problem bei WhatsApp?

Es gibt 3 Probleme

1. WhatsApp liest regelmäßig dein *Adressbuch* aus, um abzugleichen, welcher deiner Kontakte auch WhatsApp nutzt. Dabei werden potentiell alle Daten übermittelt, die du in dem Kontakt gespeichert hast (Name, Handynummer, E-Mail-Adresse, Kontaktfoto, Geburtstag, Adresse...).
    - Es kann zwar davon ausgegangen werden, dass die Personen, die bereits WhatsApp nutzen, dieser Verwendung zugestimmt haben bzw. diese Verwendung in ihrem Interesse liegt (Art. 6 Abs. 1 lit. f DSGVO). Aber es gibt genügend Menschen in deinem Adressbuch, die WhatsApp *nicht* nutzen. Von denen müsstest du eine entsprechende Erlaubnis einholen (Art. 6 Abs. 1 lit. a i.V.m. Art. 7 u. 8 DSGVO). Das wiederum ist weder zumutbar noch auf die Dauer umsetzbar, denn: Woher sollst du wissen, welcher deiner Kontakte WhatsApp nicht nutzt, wenn nicht vorher WhatsApp das durchcheckt?
    - Es gibt zwar die Möglichkeit, dieses Auslesen zu verbieten (direkt zwischen Installation und Erstnutzung), aber das macht WhatsApp fast unbrauchbar, denn: Du kannst dann niemanden anschreiben, weil du ja keine Kontakte hast; ein manuelles Eintippen einer Nummer oder ein manuelles Erstellen eines WhatsApp-Adressbuchs bietet WhatsApp nicht an. Das heißt: Damit du WhatsApp benutzen kannst, muss WhatsApp deine Kontakte auslesen. Das wiederum ist **nicht DSGVO-konform!**
    - Es gibt andere Messenger-Dienste, die das so nicht machen. Bei manchen kann man sich z.B. mithilfe eines QR-Codes verbinden statt über das Adressbuch, bei anderen wird das Adressbuch zwar ausgelesen, aber die Daten der Kontakte, die diesen Dienst nicht nutzen, werden gelöscht. Das ist zwar nicht optimal, aber ausreichend.
2. WhatsApp übermittelt alle diese Daten in die USA.
    - Da WhatsApp im PrivacyShield ist (s.o. Auftragsverarbeitung), ist hiergegen prinzipiell nichts einzuwenden.
3. WhatsApp nutzt alle personenbezogenen Daten, die sie kriegen können, für alles, worauf sie Bock haben. So sagen sie es in ihrer Datenschutzerklärung, wörtlich: Sie nutzen es beispielsweise für "Messungen, Analysen und *sonstige Unternehmensdienste*." Sonstige Unternehmensdienste kann ggf. alles sein, worauf sie gerade Bock haben. Vielleicht spielen sie Memory mit deinen Profilbildern als Teambuilding-Maßnahme – wer kann es ihnen verbieten?
    - Wer das tut, widerspricht ganz klar dem Prinzip der **Datensparsamkeit** (Art. 5 Abs. 1 lit. c DSGVO). Wenn WhatsApp das tun will, ist das aber nicht nur deren Bier, denn in dem Moment, in dem du WhatsApp nutzt, wird es auch zu deinem, d.h.: DU verstößt gegen das Prinzip der Datensparsamkeit.
    - Wir allem müssen ja auch **TOMs** ergreifen, die dem Prinzip der Datensparsamkeit (und anderen) genügen. Das heißt: Schon bei der Wahl der Mittel zur Datenverarbeitung, anders gesagt: Schon bei der Wahl deines Kommunikationstools, musst du auf diese Prinzipien achten. Ein Tool, das dir massenweise Daten für die eigene Verwendung abgreift, kann nicht mit deinen TOMs kompatibel sein (wenn doch, hast du ziemlich schlechte TOMs).

Aber bei WhatsApp ist doch alles verschlüsselt, oder? Naja, **nicht alles!** WhatsApp kann zwar nicht lesen, *was* du schreibst. Aber WhatsApp kann sehr wohl lesen, *wer mit wem wann wo auf welchem Gerät wie* schreibt. All das sind personenbezogene Daten: so genannte **Metadaten.** Das sind Daten wie z.B. IP-Adressen, über die man schon zu einem gewissen Grad nachvollziehen kann, wer das ist; also Daten, nach denen eine Person zwar *nicht eindeutig bestimmt* ist, *aber* mit der eine Person *bestimmbar* ist. Das heißt in diesem Beispiel: Wenn ich all diese Daten von dir über einen gewissen Zeitraum sammle und auswerte, kann ich herausfinden, wo in etwa du wohnst (= wo du dich abends aufhältst), zu welcher Schule du gehst (= wo du vormittags bist), wann du Unterricht und wann du Pause hast (= wann du weniger bzw. mehr chattest), was für ein Gerät du dir leisten kannst (= Huawei oder iPhone? aktuelles Modell oder gebraucht gekauft? ...), vielleicht sogar wie alt du bist (= anhand der Art zu tippen, wie Forschungen herausgefunden haben), was du für Freizeitaktivitäten hast (= wie deine Gruppen heißen), wer deine engsten Freund*innen sind und wer eher nicht (= mit wem du wie oft schreibst), deine Handynummer, deinen Namen, dein Bild ... und vor allem: die Handynummern, Namen, Bilder, Adressen, E-Mail-Adressen usw. deiner Freund*innen (über das Adressbuch).

Im privaten Bereich kann natürlich dir niemand vorschreiben, was du mit deinen Daten machst. Wenn es dir persönlich egal ist, dass WhatsApp all das von dir erfahren kann, dann sei es so. **Aber schon hier** bist du rechtlich seit längerem verpflichtet, deine Kontakte zu fragen, ob es okay ist, dass WhatsApp ihre Daten ausliest; das musst du ggf. nachweisen können. Und da sind wir noch nichtmal im Bereich der DSGVO!

Was wir hier machen, ist ja aber nicht deine Privatangelegenheit, auch wenn du dein privates Handy benutzt (Stichwort: Bring Your Own Device; dazu anderswo mehr). Das heißt: **Wenn du dein privates Handy für Pfadfinder*innenzwecke benutzt, musst du dich an die DSGVO halten!** Und das heißt: **Wenn du WhatsApp benutzt** (egal ob privat oder für die Pfadfinder*innen), **bist du schuld, dass dein Stamm gegen die DSGVO verstößt.** Wenn also irgendein Elternteil, das gar kein Smartphone hat, herausbekommt, dass ihr WhatsApp benutzt, und also seine Daten von WhatsApp ausgelesen werden – dieses Elternteil kann sich bei der Aufsichtsbehörde beschweren und die Aufsichtsbehörde kann euch ordentlich dran kriegen. Dann hilft euch nichts und niemand mehr...

Ja und was machen wir jetzt?

Am besten: **WhatsApp löschen!**

(... ja das geht ...)

Aber vielleicht gibt es da ja doch noch Möglichkeiten mit unterstützenden Apps ...

Alternativen zu WhatsApp

(...)

Richtlinien von Facebook selbst: https://www.facebook.com/policies/pages_groups_events/

Belehrung