

Wie geht's denn hier zum Datenschutz?

Erste Informationen für den Bereich Selbsthilfe zum Datenschutz und zur Datenschutz-Grundverordnung

Ab dem 25.05.2018 gilt in der europäischen Union ein einheitliches Datenschutzrecht. Dieses ist in der Datenschutzgrundverordnung (DS-GVO) niedergeschrieben. In ihr wird europaweit geregelt wie Organisationen mit personenbezogenen Daten umgehen müssen. Sie findet somit auch für den Bereich der Selbsthilfe Anwendung. Ergänzt wird die DS-GVO durch das neu gefasste deutsche Bundesdatenschutzgesetz.

Viele Organisationen/Einrichtungen sind mit dem Umsetzen der Anforderungen der DS-GVO zurzeit stark gefordert. Denn es ist nicht ganz einfach zu erkennen, an welcher Stelle in ihrer Arbeit diese zum Tragen kommt und welche Maßnahmen ergriffen werden müssen, um alle Regelungen einzuhalten.

Da noch viele Unklarheiten bestehen, sind alle folgenden Informationen unter Vorbehalt verfasst und erheben keinen Anspruch auf Vollständigkeit.

Es muss immer fallbezogen entschieden werden, welche Anforderungen der DS-GVO erfüllt werden müssen.

Selbsthilfe und DS-GVO

1. Wann findet die DS-GVO Anwendung? Art. 2, Abs. 1, DS-GVO

- Immer dann, wenn personenbezogene Daten automatisiert und nicht automatisiert verarbeitet werden und die Verarbeitung über reine Privatangelegenheiten (z.B. Einladung zum Geburtstag) hinausgehen.
 - Personenbezogene Daten: z.B. Name, Wohnort, Steuernummer...
 - automatisiert und nicht automatisiert: es werden bspw. Daten im PC gespeichert oder auch nur in Papierform abgelegt
 - verarbeiten: z.B. aufschreiben, speichern, ändern, verknüpfen, löschen....
- Die DS-GVO ist daher sowohl für Kontaktstellen wie für Selbsthilfegruppen und Selbsthilfeorganisationen zu beachten.

2. Wann dürfen Daten verarbeitet werden? Art. 6, DS-GVO

- Wenn eine Rechtsgrundlage besteht, z.B. eine **Einwilligung** nach Art. 7, DS-GVO vorliegt
 - Im Selbsthilfebereich ist die Einwilligung des Betroffenen die beste und sicherste Art auf rechtlich zulässige Weise Daten zu verarbeiten. Denn in der Regel geht es immer um Daten der „besonderer Kategorien“, also Gesundheitsdaten, die besonders streng geschützt werden sollen.
 - Eine Einwilligung sollte am besten schriftlich erfolgen, damit ein Dokument zum Nachweisen vorhanden ist. Folgende Bedingungen muss die Einwilligung erfüllen
 - Sie muss freiwillig abgegeben werden
 - Sie muss für konkrete Fallgestaltungen oder Verwendungszwecke abgegeben werden - es kann also **keine** einmalige „Generalvollmacht“ erstellt werden, die alle Eventualitäten abdeckt., Für unterschiedliche Zwecke wie z.B. „Veröffentlichung in der Verbandszeitschrift“ oder „Veröffentlichung auf der Homepage“ muss jeweils eine **eigenständige Einwilligung** eingeholt werden, die auch gesondert widerrufen werden kann. Möglich ist dies beispielsweise durch eine aktive Ankreuzmöglichkeit in einem Datenerhebungsbogen.
 - Sie muss für einen bestimmten Zweck abgegeben werden z.B. Vermittlung von Selbsthilfegruppen

- Hinweis, dass die Einwilligung ohne Angabe von Gründen widerrufen werden kann
 - Sie muss durch eindeutige, aktive und bestätigende Handlung des Betroffenen erfolgen (z.B. handschriftliches Ausfüllen, Ankreuzen in einem Onlineformular)
- Grundsätzlich sollte nach dem Prinzip der **Datensparsamkeit** gearbeitet werden. Es geht darum nur die tatsächlich notwendigen Daten zu speichern.

3. Informationspflicht, Art. 13, DS-GVO

- immer, wenn die Daten bei der Person direkt erhoben werden, muss die betroffene Person zum Zeitpunkt der Erhebung über folgendes informiert werden (Art. 13, DS-GVO). Die folgenden Aufzählungen beziehen sich auf den Fall, dass eine Einwilligung nach Art. 7. DS-GVO als Rechtsgrundlage eingeholt wird.
 - Name und Kontaktdaten des für den Datenschutz **Verantwortlichen**
 - Name des **Datenschutzbeauftragten** (falls vorhanden)
 - **Zwecke**, für die personenbezogene Daten verarbeitet werden – z.B. Vermittlung von Selbsthilfegruppen
 - **Rechtsgrundlage** für die Verarbeitung – Einwilligung nach Art. 7 DS-GVO
 - Mitteilung, ob Daten **weitergegeben** werden und wenn ja den Empfänger der Daten – z.B. Weitergabe an Personen, die eine SHG suchen
 - Ggf. die Absicht des Verantwortlichen, die personenbezogenen Daten an ein **Drittland** oder eine internationale Organisation zu übermitteln.
 - **Dauer** der Speicherung oder Kriterien für die Löschung – z.B. bis die Einwilligung widerrufen wird
 - Betroffenenrechte, Hinweis auf...
 - Widerrufsrecht der Einwilligung
 - Auskunftsrecht über die verarbeiteten Daten sowie Recht auf Datenübertragbarkeit
 - Recht auf Löschung, Berichtigung und Einschränkung der Verarbeitung
 - Beschwerderecht bei der Aufsichtsbehörde
- **Sinnvoll ist es, diese Informationen direkt beim Versand des Einwilligungsformulars mitzuschicken**

4. Verarbeitungsverzeichnisse, Art. 30, DS-GVO

- Nach der DS-GVO ist es notwendig ein sogenanntes Verarbeitungsverzeichnis zu erstellen. Darin soll dokumentiert werden, wer welche Daten warum und auf welche Art und Weise verarbeitet und welche Schutzmechanismen gegen Missbrauch eingerichtet wurden. Der Mindestinhalt ist also:
 - Name, Kontaktdaten des **Verantwortlichen** (z.B. Gruppensprecher/in oder Geschäftsführer/in)
 - **Zweck** der Verarbeitung (z.B. Vermittlung von Selbsthilfegruppen, Übersendung von Infomaterial)
 - Kategorien **betroffener Personen** (z.B. Gruppenleiter von SHGs, Teilnehmende)
 - Kategorien **personenbezogener Daten** (z.B. Name, Vorname, Telefonnummer)
 - Kategorien von **Empfängern** von Daten (z.B. Personen, die eine SHG suchen oder Institutionen, die sich mit dem Gruppenthema befassen, bei Selbsthilfekontaktstellen bspw. auch Hinweis auf Weitergabe an externen Dienstleister)
 - **Drittlandtransfer** (Drittland meint nach DS-GVO alle Länder außerhalb der Europäischen Union)
 - **Löschfristen** (z.B. „bis zum Widerruf der Einwilligung“)
 - **Technisch/organisatorische** Maßnahmen (z.B. E-Mails werden verschlüsselt versandt)

5. Homepage und IT-Sicherheit

- Die Homepage sollte als erstes **überprüft** werden:
 - Fotos, Adressen, Namen etc.: sind hier Einwilligungen für eine Veröffentlichung vorhanden?
 - eventuell heikle Daten zunächst offline zu stellen und prüfen, ob und wie diese verwendet werden dürfen - ist aber nur ein Zwischenschritt und nicht ausreichend!

- **Datenschutzerklärung**

Da selbst bei dem Besuch einer Website, die nicht interaktiv ist, bestimmte Daten des Besuchers automatisch gespeichert werden, muss auch diese Website eine Datenschutzerklärung enthalten. Dies gilt umso mehr, wenn noch ein Kontaktformular ins Netz gestellt wird.

Die Datenschutzerklärung informiert über folgendes:

- Kontaktdaten des Seitenbetreibers
- Kontaktdaten des/der Datenschutzbeauftragten, wenn vorhanden
- Nennung aller Datenverarbeitungsvorgänge beim Besuch der Homepage
Hier muss mit dem Host der Homepage und ggf. dem Programmierer der Homepage geklärt werden welche Daten verarbeitet werden
- Dauer der Speicherung
- Betroffenenrechte, Hinweis auf...
 - Widerrufsrecht
 - Auskunftsrecht über die verarbeiteten Daten
 - Beschwerderecht bei der Aufsichtsbehörde
- IT-Sicherheit
 - Mit IT-Betreuern besprechen, ob ggf. die Sicherheit erhöht werden muss
 - Verschlüsselung von E-Mails besprechen und vornehmen

6. Auftragsdatenverarbeitung, Art. 28, DS-GVO

- Werden personenbezogene Daten an eine andere Stelle zur weiteren Verarbeitung gegeben – dies dürfte in der Regel höchstens bei Kontaktstellen oder Selbsthilfeorganisationen der Fall sein – ist ein Vertrag nach den Vorgaben der DS-GVO abzuschließen.
 - Auftragsverarbeitung liegt z.B. vor, wenn die eigene Adressdatenbank auf einem anderen Server liegt.

7. Datenschutzbeauftragte/r, Art. 37, DS-GVO

- Nach Rücksprache mit dem bayerischen Landesamt für Datenschutzaufsicht in Ansbach, benötigen Selbsthilfekontaktstellen, Selbsthilfeorganisationen und Selbsthilfegruppen nach jetzigem Kenntnisstand **keine/n** Datenschutzbeauftragte/n, wenn weniger als 10 Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.
- Es werden zwar zum Teil sensible Daten verarbeitet, jedoch nicht in einem solchen Umfang, dass ein/e Datenschutzbeauftragte/r verpflichtend benannt werden muss.

8. Datenschutz-Folgenabschätzung, Art. 35 ff., DS-GVO

- Nach Rücksprache mit dem bayerischen Landesamt für Datenschutzaufsicht in Ansbach, benötigen Selbsthilfekontaktstellen, Selbsthilfeorganisationen und Selbsthilfegruppen nach jetzigem Kenntnisstand **keine** Datenschutz-Folgenabschätzung.

9. Recht auf Auskunft und Löschung, Art. 15, 16, 17, DS-GVO

- Betroffene Personen haben das **Recht Auskunft** zu erhalten, welche Daten explizit über sie gespeichert sind und wie diese verwendet werden. Da die betroffene Person Recht auf Löschung bzw. ein Recht auf Einschränkung der Verarbeitung ihrer Daten hat, sind am besten **Löschverzeichnisse** anzulegen.
- Daten, die schon jetzt nicht mehr notwendig sind am besten gleich löschen.

10. Datenunfall

- Datenunfall = z.B. verschwundener Laptop ohne Festplattenverschlüsselung nach dem neusten Stand mit persönlichen Daten von Einzelpersonen.
 - Meldung bei der zuständigen Aufsichtsbehörde innerhalb von 72 Stunden (Formular auf der Website der Aufsichtsbehörde)

11. Erste Schritte für Selbsthilfegruppen

- **Problembewusstsein** bei der Verwendung personenbezogener Daten entwickeln
- **Datenminimierung:** welche Daten brauchen wir überhaupt?
- **Vertraulichkeit und Verschwiegenheit** sich gegenseitig versichern
- Auf jeden Fall **Verantwortliche/n** für die Datenverarbeitung benennen und prüfen ob Datenschutzbeauftragte erforderlich ist (siehe oben)
- Falls **Homepage** vorhanden, siehe Informationen oben! Wichtig!
- **Mailverkehr:** sich über Verschlüsselungen informieren, auf jeden Fall immer Mails unter Blindkopie verschicken
- **Einwilligungserklärungen einholen** (siehe Adressliste mit Präambel)
- **Erster Umsetzungsvorschlag:** siehe „Präambel für Selbsthilfegruppen“
- Dann **alle weiteren Schritte** wie oben nach und nach abarbeiten

12. Zuständige Stellen

- Bayerisches Landesamt für Datenschutzaufsicht (BayLDA)
Promenade 27
91522 Ansbach
Telefon: +49 (0) 981 53 1300 E-Mail: poststelle@lda.bayern.de
Das bayerische Landesamt für Datenschutzaufsicht in Ansbach ist für den nichtöffentlichen Bereich die Aufsichtsbehörde. Es setzt in erster Linie auf Beratung, nicht auf Ahndung. Auf deren Internetseite gibt es viel Material und gute Vorlagen, zumindest für Vereine.
<https://www.lda.bayern.de>
- Für öffentliche Träger (z.B. Stadtverwaltungen) ist der bayerische Landesbeauftragte für den Datenschutz Prof. Dr. Petri in München zuständig.

13. Hilfreiche Broschüren

- Erste Hilfe zur Datenschutz-Grundverordnung ISBN: 978-2-406-71662-1 (Beckverlag, Kosten 5,50 €)
- Eine Handreichung für Selbsthilfegruppen soll im Auftrag von SeKo Bayern e.V. von der Juristin Renate Mitleger-Lehner erstellt werden und bis zum Sommer erscheinen. Es ist geplant, dass es Mitte - Ende Juli 2018 beim Verlag AG-Spak als Ergänzung zum Buch „Recht für Selbsthilfegruppen“ erscheint. Die Handreichung wäre dann für wenige Euro über den Verlag erhältlich.