

Einige Schlaglichter und Erkenntnisse aus der Veranstaltung

„Datenschutz in der Selbsthilfe“!

- Die Datenschutzgrundverordnung „gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen“.
- Die Datenschutzgrundverordnung gilt für alle Bereiche der Gesellschaft in den Daten verarbeitet werden. Es gibt nur eine Ausnahme, wenn natürliche Personen Daten ausschließlich für persönliche oder familiäre Tätigkeiten verarbeiten, findet die DSGVO keine Anwendung.
- Es gelten für alle die gleichen Regeln. Ausnahmen für Vereine und/oder ehrenamtlich tätige Menschen gibt es nicht. Die DSGVO gilt im Verein, in der Selbsthilfekontaktstelle und in der Regel auch in der Selbsthilfegruppe.
- Die Maßnahmen zum Datenschutz müssen verhältnismäßig und angemessen sein. Die Datenschutzbeauftragten der Bundesländer beraten zur Umsetzung des Datenschutzes.
- Ob die Verpflichtung zur Bestellung eines Datenschutzbeauftragten besteht, hängt zum einen davon ab, wie viele Mitarbeiter in der Datenverarbeitung tätig sind (i. d. R. ab 10 MA).
- Einrichtungen/Institutionen (z.B. Vereine) müssen einen Datenschutzbeauftragten bestellen, wenn ihre Kerntätigkeit in der umfangreichen Verarbeitung sensibler Daten wie z.B. Gesundheitsdaten besteht. Dies trifft für alle Selbsthilfekontaktstellen und auf die meisten Vereine der Gesundheitsselbsthilfe zu.
- Aufgabe des/der Datenschutzbeauftragten ist die Beratung der Geschäftsführung bzw. des Vorstandes. Mitglieder der Geschäftsführung bzw. des geschäftsführenden Vorstandes können daher nicht als Datenschutzbeauftragte berufen werden.
- Datenschutzbeauftragte können Angestellte der Institution oder auch externe Mitarbeiter(-innen) sein. Sie müssen über besondere Fachkunde verfügen.
- Institutionen, die persönliche Daten verarbeiten wollen bzw. müssen, sollten sich die schriftliche Einwilligung der betroffenen Personen einholen. Bereits abgegebene Einwilligungen zur Datenverarbeitung bleiben i.d.R. gültig und müssen nicht komplett neu eingeholt werden. Eine Prüfung, ob die „alten“ Einwilligungen DSGVO-konform sind, ist gleichwohl zu empfehlen.
- Bereits vorhandene persönliche Daten (z.B. von Spendern), die rechtmäßig erhoben wurden, können weiterverwendet werden, sofern dafür ein „berechtigtes Interesse“ besteht. Auf Wunsch bzw. Widerspruch der betroffenen Person müssen die Daten, sofern keine gesetzlichen Aufbewahrungsfristen eingehalten werden müssen, gelöscht werden,
- Das Internet hat die Selbsthilfe bekannter gemacht und bietet vielfältige Möglichkeiten zum Austausch und zur Sammlung von Erfahrungswissen.

- Insbesondere der Austausch über persönliche Probleme sollte im Internet nur in vertrauensvollen und geschützten Bereichen erfolgen. Die Sozialen Netzwerke wie Facebook, Whats-App, Instagram bieten diese Sicherheit i.d.R. **nicht**.
- Da jede Aktivität im Internet eine Spur hinterlässt, lassen sich aus Suchanfragen und z. B. dem Besuch von bestimmten Internetseiten, Rückschlüsse auf die persönliche Situation von Nutzerinnen und Nutzern schließen. Diese unfreiwillige Abgabe von persönlichen Daten muss mehr in das Bewusstsein der Menschen dringen.
- Die EU plant die Verabschiedung einer ePrivacy Verordnung, die die Europäische Datenschutzgrundverordnung im Hinblick auf Vorgaben für datenschutzfreundliche Software-Technik spezifiziert. Die ePrivacy Verordnung sieht Neuregelungen zum Schutz der Verbraucher und ihrer Daten im Netz vor. Ziel ist es, europaweit die Vertraulichkeit in der elektronischen Kommunikation sicherzustellen und den Umgang mit personenbezogenen Daten im Online-Bereich zu regeln.
- Das Hauptproblem beim Datenschutz in der Digitalen Welt ist die „*Digitale Inkompetenz*“ der meisten Nutzerinnen und Nutzer.
- Die Erfassung und Verarbeitung personenbezogener Daten ist grundsätzlich verboten und nur erlaubt, wenn eine Einwilligung der Betroffenen vorliegt oder z.B. hoheitliche Aufgaben (Meldewesen) wahrgenommen werden. Dient die Datenverarbeitung einem Vertragsverhältnis (auch Mitgliedschaftsverhältnis im Verein) ist sie auch erlaubt.
- Emails sind kein sicheres Medium zur Versendung von persönlichen Daten. Nur verschlüsselte Emails z. B. über PGP (Pretty Good Privacy) bieten hier Sicherheit. Dies gilt auch für Kontaktformulare von Kontaktstellen, Selbsthilfeorganisationen und Selbsthilfegruppen.
- Wenn private Hardware z.B. für Vereinszwecke genutzt wird, muss der Zugang zumindest passwortgeschützt und die Daten verschlüsselt sein.
- Es empfiehlt sich dringend, für Zwecke des Vereines und der Selbsthilfegruppe, vereinseigene Hardware (Rechner, Smartphone) zu benutzen.
- Passwörter sollten grundsätzlich mindestens alle drei Monate verändert werden.
- Nur bezahlte Programme bieten Schutz vor Schadsoftware.
- Im Verfahren zur Umsetzung des Datenschutzes müssen Regelungen zu folgenden Bereichen getroffen werden: *Zugangskontrolle, Zugriffskontrolle, Übertragungskontrolle, Eingabekontrolle, Wiederherstellbarkeit, Verfügbarkeitskontrolle, Auftragskontrolle, Trennbarkeit, Datenträgerkontrolle, Speicherkontrolle, Benutzerkontrolle, Transportkontrolle, Zuverlässigkeit, Datenintegrität*