Hinweise zum Datenschutz im Rahmen von Online-Jugendarbeit

Grundsätzlich ist davon auszugehen, dass die EU-Datenschutz-Grundverordung (EU-DSGVO) im (Jugend-)Feuerwehrdienst verbindlich zu beachten ist, da es in diesem Fall nicht um eine rein private Verarbeitung von Daten im Sinne der EU-DSGVO handelt. Somit muss die EU-DSGVO und ggfs. mitgeltende Vorschriften beachtet werden.

Annahme für diese Betrachtung ist, dass (Jugend-)Feuerwehren im Rahmen von Online-Schulungen/Übungsdiensten entsprechende Angebote an Ihre Jugendlichen und/oder Betreuer machen. Dabei werden i.d.R. Videokonferenz-Tools (ggfs. auch mit der Möglichkeit für eine Einwahl ohne Video oder nur per Telefon) und parallel Online-Tools zur gemeinsamen Arbeit eingesetzt (Whiteboards, Screensharing, u.v.m.)

Zu Beginn der datenschutzrechtlichen Bewertung muss zunächst betrachtet werden, welche personenbezogenen Daten im Rahmen von Online-Jugendarbeit überhaupt erhoben und verarbeitet werden. Hier können üblicherweise folgende Kategorien auftauchen:

1. IP-Adressen von Jugendlichen bzw. deren Erziehungsberechtigen als Internet-Nutzer
2. Mailadressen und weitere personenbezogene Daten, z.B. im Rahmen von Registrierungen auf Webseiten und ähnlichem
3. Selbst erstellte Inhalte mit Fotos, auf denen Jugendliche identifizierbar sind
4. Bilder und Videomaterialien ohne erkennbaren Personenbezug

Des Weiteren ist zu unterscheiden zwischen den Anbietern (hier i.d.R. also Jugend-Feuerwehren) und den Nutzern der Dienste (hier also üblicherweise Jugendliche/Feuerwehrangehörige).

Grundsätzlich sind Online-Seminare und/oder Videokonferenzen möglichst datensparsam durchzuführen. Daraus und aus den Kategorien der vorgenannten Daten ergeben sich schon einige Handlungsempfehlungen:

1. Der Dienst (Videokonferenz-Tool, andere Tools) sollte idealerweise in der EU angeboten werden. Eine Unterscheidung zwischen Deutschland und einem anderen EU-Land ist für diese Betrachtung i.d.R. nicht relevant. Alternativ sind auch sogenannte sichere Drittländer möglich, dies umfasst derzeit z.B. die Schweiz und Kanada. Ebenfalls zulässig ist die Nutzung eines Dienstes aus den USA, sofern sich dieser dem sogenannten „PrivacyShield“ unterworfen hat. Letzteres kann man über die Nutzungsbedingungen bzw. auch per Google herausfinden. Auch wenn dies „gefühlt“ problematisch ist, so ist die rechtliche Betrachtung davon unbenommen und es ist grundsätzlich zulässig.

2. Eine sogenannte „Vereinbarung zur Auftragsdatenverarbeitung“ ist notwendig, wenn Daten der Kategorien 2 und 3 erhoben werden oder Ihr mit den Tools andere personenbezogene Daten verarbeitet (z.B. Speichern einer Namensliste in einer Dropbox, Anbieten von Videokonferenzen mit Zoom). Diese Vereinbarung kann auch Teil der allgemeinen Geschäftsbedingungen sein oder sie ist im Kundenbereich der Anbieter einsehbar und kann dort explizit abgeschlossen werden. Wichtig ist, dass kostenlose Dienste dies oftmals NICHT anbieten und diese Leistung erst in kostenpflichtigen Angeboten verfügbar ist (ein Beispiel dafür ist Dropbox, nicht aber Zoom – da ist der Vertrag auch in der kostenlosen Version in den AGBs enthalten).

Stand: 11. Mai 2020

3. Der Dienst sollte eine Verschlüsselung auf einem dem Stand der Technik entsprechenden Niveau bieten.
4. Idealerweise werden Dienste ohne Registrierungszwang für die Nutzer verwendet, da im Falle einer Registrierung oftmals weitreichende Zugeständnisse vom Nutzer verlangt werden, die aus Sicht des Datenschutzes und der Datensparsamkeit problematisch sind.
5. Kostenlose Dienste, die von Jugendlichen beim Spielen/Gaming häufig eingesetzt werden, wie zum Beispiel Twitch oder Discord sind nicht zu empfehlen.
6. Der Zugang zu den Videokonferenzen sollte passwortgeschützt (idealerweise je Meeting ein neues Passwort) erfolgen.
7. Das Meeting darf nicht aufgezeichnet werden. Hier wäre eine separate Einwilligung der Teilnehmer/Nutzer erforderlich

Einige hilfreiche Links finden sich hier:

- Mitteilung des Hessischen Datenschutzbeauftragten zur Nutzung von Videokonferenz-Tools an Schulen während der Corona-Krise: https://datenschutz.hessen.de/videokonferenzsysteme-schulen
- Hinweise des Datenschutzbeauftragten und Rechtsanwalts Stephan Hansen-Oest zur Nutzung von Zoom als Videokonferenz-Lösung: https://www.datenschutz-guru.de/zoom-ist-keine-datenschleuder/
- Weitere Hinweise zur Auswahl und Beurteilung von Videokonferenz-Lösungen (Hinweis: hier sollte man mit dem entsprechenden Fachvokabular und den Herangehensweisen vertraut sein): https://www.datenschutzbeauftragter-info.de/videokonferenz-tools-tipps-zur-auswahl-und-verwendung/ https://datenschutz-generator.de/dsgvo-video-konferenzen-online-meeting/

Die vorgenannten Hinweise beziehen sich auf die ersten beiden Kategorien von personenbezogenen Daten aus der Einleitung. Für die weiteren beiden Kategorien ergeben sich weitergehende Hinweise:

Viele, insbesondere kostenlose Online-Tools und auch die sozialen Netzwerke behalten sich das Recht vor, alle auf deren Plattformen eingestellten Daten uneingeschränkt nutzen zu dürfen. Bei kostenpflichtigen Diensten mit entsprechender Vereinbarung zur Auftragsdatenverarbeitung sieht das in der Regel völlig anders aus. Im Rahmen der Auftragsdatenverarbeitung wird i.d.R. die Weitergaben von Daten an Dritte ausgeschlossen (was allerdings im Einzelfall zu prüfen ist). Somit kommen hier nun neben datenschutzrechtlichen Aspekten (im Falle von Kategorie 3 der oben genannten Daten) auch urheberrechtliche Fragen auf (Kategorie 3 und insbesondere 4) der genannten Daten. Hier gelten die bekannten Grundsätze:

- Es ist sicherzustellen, dass die Jugendfeuerwehr über die Rechte an den Bildern/Grafiken/Musikstücken/… verfügt, wenn diese auf offen zugänglichen Plattformen veröffentlicht werden.
- Dies gilt im Besonderen für Bilder von Jugendlichen unter 14 Jahren auch wenn diese im Rahmen eines allgemeinen Interesses ggfs. veröffentlicht werden dürften (Beispiele: Gruppenfotos auf öffentlichen Veranstaltungen o.ä.).

- Bei (öffentlicher) Verwendung von Inhalten aus dem Internet sollten die Urheberrechtsfragen im Vorfeld geklärt werden
- Im Zweifel sollte auf die Veröffentlichung von Bildern / Videos verzichtet werden.

Wichtig ist es insbesondere bei Diensten / Webinaren der Jugendfeuerwehren, dass die Eltern der Jugendlichen im Vorfeld informiert werden. Ebenso ist zu beachten, dass möglichst alle Jugendlichen mit einbezogen werden können und nicht einzelne Jugendliche aufgrund von Einschränkungen / Verboten durch die Eltern ausgeschlossen werden. Dies kann auch der Fall sein, wenn die Nutzung von Videokonferenz-Diensten grundsätzlich rechtlich möglich wäre, aber die Eltern einem Jugendlichen die Nutzung untersagen.

Zusammenfassende Hinweise:

- Die Nutzung von Videokonferenz-Tools auch von Anbietern aus den USA ist in der Regel rechtlich zulässig
- Eltern/Erziehungsberechtigte/Feuerwehrkameraden sollten im Vorfeld einbezogen werden
- Kostenlose Dienste mit Registrierungspflicht sind üblicherweise kritisch bzw. dürfen nicht eingesetzt werden (Beispiel: Twitch, Discord, Skype in der Basis-Version)
- Dienste für eine gemeinsame Nutzung ohne Registrierungspflicht sind zu bevorzugen
- Prüft, ob den Diensten uneingeschränkte Nutzungsrechte eingeräumt werden und ob Daten an Dritte weitergeben werden
- In Online-Tools sollten ausschließlich nicht personenbezogene Daten gemeinsam erarbeitet werden (also keine Geburtstagsliste im Whiteboard erstellen o.ä.)
- ggfs. kann es eine Einschränkung durch die Kommune geben, wenn Dienstrechner benutzt werden oder die Kommune ermöglicht bzw. verbietet bestimmte Tools
- Meetings dürfen nicht aufgezeichnet werden

Diese Hinweise stellen keine verbindliche rechtliche Beratung oder Bewertung dar, sondern geben nur Handlungsempfehlungen. Im Zweifel sollte vor Ort eine entsprechende fachkundige Person für die Betrachtung des individuellen Einzelfalles hinzugezogen werden.