Die DSGVO - Anwendungen in der Fachschaft

eNik, Konschdants, niklas.westermann@uni.kn

Unglaublich hässliche LaTeX-Präsentation weil die Standartvorlage genommen wurde

ZaPF in HD - SS 2018

Inhalt

Angaben in Klammern [Art. X, Nr Y] beziehen sich auf den Original-Text der DS-GVO auf Deutsch.
Auf Richtigkeit der Angaben gibt es keine Garantie!

Quellen

1. **Verordnung (EU) 2016/679 des Europäischen Parlamentes und des Rates**
   https://www.datenschutz-grundverordnung.eu/wp-content/uploads/2016/05/CELEX_32016R0679_DE_TXT.pdf
2. **Datenschutz im Verein - Der Landesbeauftragte für den Datenschutz Baden-Württemberg**
   https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/03/OH-Datenschutz-im-Verein-nach-der-DSGVO.pdf

Weitere interessante Links:

1. https://kif.fsinf.de/wiki/KIF460:DSGVO
2. https://www.heise.de/newsticker/meldung/Analyse-zur-DSGVO-von-Peter-Schaar-Die-notwendige-Zumutung-Datenschutz-40 html
3. https://www.heise.de/newsticker/meldung/DSGVO-Ende-der-Fotografie-oder-halb-so-schlimm-4052969.html

Definitionen

Personenbezogene Daten

- **Alle Informationen, die sich auf eine in sonstiger Weise identifizierte oder identifizierbare natürliche Personen beziehen** [Art. 4, Nr. 1]
- Name, Anschrift, Geburtsdatum
- Aber auch **IP-Adresse**, Familienstand, Beruf, Telefonnummer, E-Mail, persönliche Interessen
- Informationen jeder Art: Schrift, Bild, Ton

Definitionen

Verarbeitung

- **Jeder Vorgang im Zusammenhang mit personenbezogenen Daten** [Art. 4, Nr. 1]
- Erheben, Erfassen, Verwenden, Offenlegen, Verbreiten, Abgleichen, Löschen

Definitionen

Dateisystem

- **Jede Strukturierte Sammlung personenbezogener Daten** [Art. 4, Nr. 6]
- Muss nach bestimmten Kriterien zugänglich sein
- Auch Papier-Akten!

Definitionen

Auftragsverarbeiter

- Person oder Stelle, die Daten im Auftrag des Verantwortlichen verarbeitet [Art. 4, Nr. 8]
- Auslagerung der Daten in die (Uni-) Cloud

Zusammenfassung mit Schwerpunkt auf die FS-Arbeit

Was für Daten werden überhaupt gesammelt?

- **ZaPF-Anmeldung**: Name, Vorname, Essgewohnheiten, Uni, E-Mail, Weckwünsche, Getränkewünsche, Kleidergrößen Adresse und Geb. Datum und Ausweisnummer bei manchen Exkursionen nötig, viele weiter Punkte...
- **ZaPF-e.V.**: Namen, Uni, Adresse, E-Mail, Telefonnummer, Geburtsdatum
- **Div. FS-Veranstaltungen**: Namen, E-Mail, Telefonnummern, Geb.Datum
- Benötigt auch für Protokolle, Wikis, Ownclouds, Altklausuren
- **Homepages**: Cookies, Google Analytics, Statistiken

Wie müssen die Daten erhoben werden? Teil I

- Vorne weg: Das sind alles Daten, die unter die DSGVO fallen
- Für eine Rechtmäßige Verarbeitung (=Erhebung) müssen die **betroffenen Personen zustimmen**. Aber: es gehen auch **sonstige zulässige Rechtsgrundlagen**, die sich aus der DSGVO ergeben! [Art. 6, Nr. 1]
- "Die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich" [Art. 6, Nr. 1, lit. f)]: Wenn ohne die Daten die Veranstaltung/Ausleihe nicht stattfinden kann, ist die Verarbeitung ohne explizite Zustimmung rechtmäßig
- Elektronisch zustimmen ist möglich.

Wie müssen die Daten erhoben werden? Teil II

- Bei Erhebung bei der betroffenen Person muss man eine **Datenschutzrechtliche Unterrichtung** vornehmen [Art. 13, Nr. 1 & 2]
  - Name und Kontaktdaten des/der Verantwortlichen
  - (Kontakdaten des Datenschutzbeauftragten) $\rightarrow$ Geht das Uniweit??
  - Zwecke der Verarbeitung (einzeln Aufzählen)
  - Rechtsgrundlage der Verarbeitung, berechtigte Interessen nach Art. 6, Nr. 1, lit f)
  - Empfänger der Daten
  - Speicherdauer
  - Hinweis auf Speicherung in (Uni-) Cloud / auf Uni-Servern
  - Absicht über Drittlandtransfer
  - Belehrung über Betroffenenrechte (Auskunft, Berichtigung, Löschung, Widerspruchsrecht)
  - Hinweis auf Widerrufsrecht und Beschwerderecht bei Aufsichtsbehörde

Wie ist mit den Daten umzugehen?

- Es müssen Grundzüge der Datenerhebung, -verarbeitung und -nutzung schriftlich festgelegt werden. Das sollte ein gesondertes Regelwerk sein (Name: Datenschutzordnung etc.) [??]
- Festlegen welche Daten für was nötig sind, welcher Zweck dahinter steht. Begründen, was wofür nötig ist und war!!
- Wer darf Zugriff auf die Daten haben? Wer darf die Daten auf seinem Rechner speichern?

Was bedeutet das jetzt für die FS-Arbeit?

Was bedeutet das jetzt für die FS-Arbeit?

- Wir sammeln eigentlich immer die Daten direkt bei den Betroffenen und müssen uns über die Erhebung der Daten durch und von Dritten keine Gedanken machen.
- Die Angaben die zur Durchführung der Veranstaltung/ Protkollausleihe/ Tutorien nötig sind, müssen gemacht werden (man muss nicht aktiv zustimmen). Trotzdem ist auf die Rechte der Betroffenen hinzuweisen[1].
- Bei nicht unbedingt benötigten Daten muss der Verarbeitung aktiv zugestimmt werden (Opt-In). *Reicht hier schon das alleinige Eingeben der Daten in ein Feld, das als nicht benötigt gekennzeichnet ist?*
- Daten dürfen nicht zu anderen Zwecken als den Angegebenen verarbeitet werden.
- Datenschutzbeauftragter erst ab 10 Leuten, die mit der Datenverarbeitung beschäftigt sind. Kann man auch bei der Uni mal nachfragen, der sollte wissen wo was verarbeitet wird.
- Bei verfassten Studierendenschaften müsste der AStA so etwas haben, anders sieht es bei Vereinen aus
- Bei Wahlen müsste eigentlich die Uni für alles zuständig sein (?)
- siehe auch Folie 11.

[1] Siehe auch 1.3.4 in `https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/03/OH-Datenschutz-im-Verein-nach-der-DSGVO.pdf`

Was noch Unklar ist

- Namensnennung in Protokollen
- Namensnennungen auf Websites (Ämter dürfen ohne Nachfrage genannt werden, dabei nur der Kontakt, nicht die Adresse)
- Websites mit GIT-Repos. Dort werden die Namen quasi auf Ewigkeiten gespeichert
- Für existierende Daten muss *eigentlich* bei nicht sofortiger Löschung nun eine Erlaubnis eingeholt werden. D.h. bei einem Mailman muss nochmal eine Mail an alle rumgeschrieben werden, in der gefragt wird.

Konkrete technische Umsetzung

Konkrete technische Umsetzung - Generelles

- Technische Maßnahmen treffen um ein dem Risiko angemessenes Schutzniveau zu schaffen [Art. 32]
- Backups machen und verschlüsseln (SSL dürfte reichen)!
- Zugangsbeschränkungen einrichten und nur die Leute die wirklich an die Daten kommen müssen, zulassen.
- Daten regelmäßig und sicher Löschen
- `https://datenschutz-generator.de/` zu Rate ziehen und etwas Ähnliches auf der eigenen Website veröffentlichen falls man Daten Verarbeitet
- Cookie-Erlaubnis abfragen
- Keine Like-Dinger einsetzen, bei Wordpress mit den Plugins aufpassen

Konkrete technische Umsetzung - Technik

- SSL einrichten - Gibt es genug Anleitungen, für Zertifikate siehe die eigene Uni oder "Let's Encrypt"
- IP-Adressen sind Personenbezogene Daten. Damit der Server, auf dem die Website läuft, funktioniert (bei Angriffen die IP nachvollziehen, Fehlermeldungen...) müssen diese für kurze Zeit gespeichert werden. Blacklisten um SSH-Angriffe abzuwehren sind auch OK. Es ist jedoch sinnvoll, die Daten nach einer bestimmten Zeit (z.B. zwei Wochen) zu löschen.
- Unter Linux übernimmt das `logrotate`. Unter `/etc/logrotate.d` und `/etc/logrotate.conf` kann das Verhalten eingestellt werden

Fragen und Diskussion