1. Datenschutz ganz kurz

- Was ist Datenschutz?
- Es bleibt: Verhältnismäßigkeit („notwendig, geeignet, angemessen“)
- Beispiel(e)

2. Worum es nicht geht

Ein paar Dinge kann ich hier nicht sagen:

- „X ist in Ordnung“
- „Installiert dieses Programm oder nutzt diese Plattform (nicht), und es ist ok“
- „Schreibt Text Y dorthin oder lasst die Leute Z unterschreiben, und alles ist gut“

Wenn ihr nach diesem Kurs wisst, warum wir das nicht können, haben wir die halbe Miete.

3. Worum es geht

Euch einen Werkzeugkasten geben, mit dem ihr strukturiert (oder zur Not empathisch) beurteilen könnt, ob und wie ihr eine Datenverarbeitung angehen solltet.

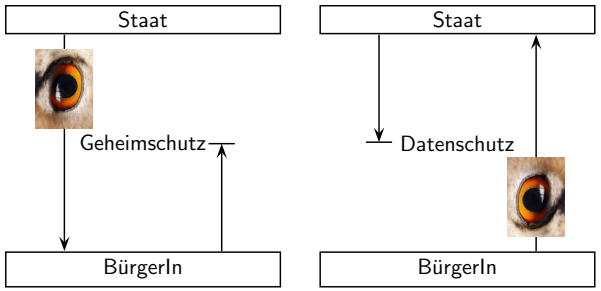

Fig. 1

4. Soziales Modell des Datenschutz

(cf. Fig. 1)

Im Modell des Volkszählungsurteils ist Datenschutz ein Schutzrecht des Individuums gegenüber dem Staat (das gilt, nebenbei, für die meisten Grundrechte – ein weiterer Grund, warum das imaginierte „Grundrecht auf Sicherheit“ ein autoritäres Phantasma ist). In Analogie ist er ein Schutzrecht gegenüber jeder Sorte von Autorität, in eurem Fall also etwa der Hochschule (HS).

Umgekehrt seid ihr selbst ein „oben“, wenn ihr die Daten von anderen verarbeitet oder verarbeiten lasst, und das ist besonders dann ernst, wenn damit wesentliche Vorteile für die Studis verbunden sind (oder diese gar keine Wahl haben), oder die Eingriffe in den Datenschutz regelmäßig besonders tief sind (davon ist etwa bei facebook auszugehen).

Eine Folge dieser Überlegungen ist, dass sich die HS nur in Ausnahmefällen auf Datenschutz berufen kann, wenn sie dem StuRa z.B. Angaben verweigert (das ist dann Geheimschutz, für den andere Regeln gelten). Im Gegenteil beinhaltet der Datenschutz ein Transparenzrecht gegenüber der Obrigkeit. In gewisserweise ist der Name unserer Aufsichtsbehörde, „Landesbeauftragter für Datenschutz und Informationsfreiheit“, ein Pleonasmus (und gleichzeitig eine steile Behauptung, den das hiesige Informationsfreiheitsgesetz verrät einen sehr autoritären Freiheitsbegriff).

Auch wenn Datenschutz im Machtgefälle immer „unten“ vor „oben“ schützt, ist es manchmal nützlich, auch dem „oben“ Eigeninteresse an Datenschutz klarzumachen; so ist z.B. eine Umfrage ohne hinreichende Anonymitätsgarantien wahrscheinlich wertlos, weil die Leute lügen werden.

5. Personenbezogen?

Datenschutz kommt aus Art. 1 GG („Menschenwürde“).

Daher: Datenschutz redet nur über Daten „zur Person“.

Aber: Viele Daten sind personenbezieh**bar**: IP-Adressen, IMSIs, TMSIs, Kamerabilder, Verbrauchsdaten, Zahlungstransaktionen, DNA-„Fingerabdrücke“...

BVerfGE 65, 1ff (1983): „[es gibt] unter den Bedingungen der automatischen Datenverarbeitung kein ‘belangloses’ Datum mehr“.

Eine Illustration zur Verknüpfbarkeit:

Viele Fachschaften binden auf ihren Seiten Webfonts ein, die direkt von Google gezogen werden. Unabhängig davon, dass es ohnehin schon eine Zumutung ist, Leuten den Font in ihrem Browser vorzuschreiben: Damit kann Google – so, wie die meisten Browser konfiguriert sind – mitlesen, was die Leute auf den Fachschafts-Webseiten lesen.

Nun nehmt an, dass ihr eine launige Anleitung zur Befreiung der Stadt von AfD-Wahlplakaten mithilfe von praktischen Wurfkrallen auf eurer Seite habt.

Wenig später findet die Polizei so ein Ding an einem “Tatort”. Der Staatsschutz hat euren Post bereits gesehen und fragt nun Google, wer den so gelesen hat. Google wird mit großer Wahrscheinlichkeit antworten, entweder gleich mit Namen, denn beim Ziehen der Fonts wird auch ein eventueller Google-Cookie übertragen, oder zumindest mit einer IP-Adresse, die die Polizei trotz ausgesetzter Vorratsdatenspeicherung meist zu Anschlüssen aufgelöst bekommt.

Die dreißig Leute, die auf diese Weise rauskommen, werden mit der Funkzellenabfrage für den Tatort abgegelichen und schwupps, die Person hat 40 Tage Knast (na gut, das Äquivalent, also 40 Tagessätze) und darf der AfD noch großzügig Schadensersatz zahlen. Nebenbei: in Heidelberg ist es nicht unwahrscheinlich, dass dieser Fall von der Schwiegertochter von Albrecht Glaser verhandelt würde, der wegen seiner islamophoben Ausfälle mehrfach als AfD-Bundestagsvize durchgefallen ist.

6. Prinzipien

Schon im Volkszählungsurteil werden die wesentlichen Punkte definiert, die für menschenrechtsachtende Datenverarbeitung einzuhalten sind. Tatsächliche Rechtsgrundlagen – für den StuRa vor allem die Datenschutzgrundverordnung und das LDSG, die allerdings gegenüber allen anderen Gesetzen subsidiär sind – gestalten das nur noch aus. Was konkret heißt: Höhlen das aus und sagen: „Jaja, das gilt schon, außer jemand hat was davon, es zu verletzen.“ In Wirklichkeit ist deshalb jeweils am Einzelfall zu prüfen („Datenschutz ist Gerichtsrecht“).

- Erlaubnisvorbehalt: PBD dürfen nur mit gesetzlicher Befugnis oder mit Einwilligung der Betroffenen verarbeitet werden. Die (schriftliche!) Einwilligung ist nur gültig, wenn sie tatsächlich auf einer freien Entscheidung des Betroffenen berüht. Kram, der bei der Immatrikulation unterschrieben wird, dürfte da nur in Ausnahmefällen gelten.
- Zweckbindung: DV muss einen klar bestimmten Zweck haben, der sich nicht mittendrin ändern kann. Das ist ein gutes Beispiel für die „Ja, aber“-Natur des Datenschutzes: §28 Abs. 2 BDSG erlaubt etwa sehr wohl eine Zweckänderung bei „für Geschäftszwecke“ gepeicherten Daten, z.B., wenn keine schutzwürdigen Interessen der Betroffenen berührt sind oder zur Strafverfolgung oder nach Interessenausgleich mit Dritten oder...“ – viel Platz für Gerichte. In der Rechtsprechung jedenfalls: Je weniger spezifisch der Zweck formuliert ist, desto tiefer ist der Eingriff in das Persönlichkeitsrecht.
- Datensparsamkeit: Es dürfen höchstens die zur Erfüllung des Zwecks nötigen Daten verwendet werden. Dies ist die Konkretisierung des Verhältnismäßigkeitsgebots der Notwendigkeit (s.u.) auf DV.

- Transparenz: Betroffene müssen von Speicherung und deren Inhalt wissen (können).
- Verhältnismäßigkeit: Das ist etwas komplizierter.

7. Verhältnismäßigkeit

Ein Eingriff ist *verhältnismäßig*, wenn er

- *geeignet* (Gegenbeispiel: Zwangsproxy gegen Viren)
- *erforderlich* (Gegenbeispiel: Logging bei elektronischen Schlössern gegen Diebstahl)
- *angemessen* ist (Gegenbeispiel: Logging aller Mails zur Mobbing-Prävention)
- und zum Erreichen eines *legitim*en Zwecks dient (Gegenbeispiel: Toilettenpausen erfassen)

Mit anderen Worten könnt ihr mit dem folgenden Vierschritt fast alle Datenschutzprobleme aufarbeiten: Welchen Zweck hat die DV? Taugt die DV überhaupt, den Zweck zu erreichen? Wenn ja, ginge es mit vertretbarem Aufwand auch ohne sie? Wenn ja, steht der Zweck in einem angemessenen Verhältnis zur Eingriffstiefe?

8. Oder: Subjektiv

Um rauszukriegen, ob ihr Daten in einer bestimmten Weise verarbeiten wollt, versucht Folgendes:

1. A verarbeitet diese Daten *über euch*...
2. ... und verklügelt sie an B.
3. Nun sei B die andere Partei in der peinlichsten Trennung, die ihr je hattet.
4. Wie sauer wärt ihr auf A?

Wenn ihr richtig sauer auf A wärt, wollt ihr die Daten wohl gar nicht oder jedenfalls nicht so verarbeiten.

9. Beispiel I

„Die Fachschaften bescheißen bestimmt bei den Ersti-Abrechnungen – lass uns verlangen, dass sie Namenslisten der TeilnehmerInnen einreichen.“

Zweck: Prävention/Aufklärung von Betrug.

Eignung: Zweifelhaft. Es ist relativ einfach, solche Namenslisten zu füllen, auch ohne dass alle, die draufstehen, auch beim Erstifrühstück dabei waren. Schon um nachzuprüfen, dass die Namen alle wirklich immatrikulierten Studis entsprechen, bräuchte es einen Abgleich mit der Studidatenbank (was die Eingriffstiefe erheblich verschärfen würde), und selbst dann ist noch nicht klar, ob da nicht wer einfach nur Namen aus der Einführungsvorlesung abgeschrieben hat.

Notwendigkeit: Nein. Ein mindestens vergleichbarer präventiver Effekt wäre zu erreichen, wenn StuRa-Mitglieder halbwegs regelmäßig bei solchen Events auflaufen würden (was ja auch zur Vorstellung der Strukturen praktisch wäre) und einfach eine grobe Schätzung der Zahl der Anwesenden nennen würden.

Angemessenheit: Sehr zweifelhaft. Bei jeder Verarbeitung personenbezogener Daten gibts so viel, das schiefgehen kann – nehmt einfach mal an, die Polizei wüsste von solchen Listen und würde anfangen, Nichtdeutsche abzuschieben, weil sie nicht beim Erstifrühstück dabei waren und deshalb „ersichtlich ist“, dass sie gar nicht „wirklich“ studieren. Betrug zugunsten der Fachschaftskasse in Höhe von wohl idR unter 100 Euro ist eigentlich nie ein angemessener Grund, um sich so einen Schuh anzuzuziehen.

10. Beispiel II

„Wir verwalten alle Prüfungen, Anmeldungen dazu und sich ergebende Noten in einem Computersystem.“

Zweck: Verwaltung von zwingenden Anmeldungen zu Prüfungen, Fristüberwachung, Berechnung von Notendurchschnitten, Druck von Diploma Supplements,. . .

Eignung: Ja. Nun, jedenfalls, wenn der Kram halbwegs ordentlich geschrieben ist. Was er natürlich in der Regel nicht ist.

Notwendigkeit: Na ja. Der Bologna-Irrsinn ist natürlich schon so durchgeknallt, dass das mit Handarbeit wirklich keinen Spass mehr macht.

Angemessenheit: Ach ja. Wenn sichergestellt wird, dass der Rechner z.B. keine Gründe für Prüfungsverzögerungen speichert, sind die Eingriffe schon noch grenzwertig vertretbar. Aber der Kram ist schon immer noch recht intrusiv, vor allem auch für DozentInnen, z.B. weil deren Benotungspraxis einer maschinellen Beurteilung zugänglich werden könnte.

. . . was natürlich nicht ausschließt, dass der Zweck politisch angreifbar ist. Ich z.B. bin ohne Prüfungsverwaltung durchs Studium gegangen, weil ich halt einfach nur ein Dutzend Pass-/Fail-Scheine und acht mündliche Prüfungen brauchte – das ist leicht ohne EDV zu verwalten. Wenn wir den Bologna-Mist loswerden, brauchts auch keine DV mehr, und die menschenrechtsfreundlichste DV ist immer: keine DV.

11. Technisch und Organisatorisch

Wenn mensch ein EDV-Verfahren nicht ganz abschießen kann – und ich würde behaupten, dass eigentlich alles, das wirklich von Rechnern profitiert, bereits mit Rechnern gemacht wird, und so das in aller Regel der wünschbarste Ausgang ist –, ist durch Details („technische und organisatorische Maßnahmen“) immer noch einiges zu retten:

- ein Verzeichnis der Verfahrenstätigkeiten; die sind nach Datenschutzrecht vorgesehen und sollen dokumentieren, wer wie warum welche PBZ verarbeitet. Sie müssen nicht öffentlich sein. Sie können es aber sein, und das macht m.E. schon ein gutes Statetment. Es gibt im Internet Vorlagen für sowas, die meist nicht hilfreich sind. Besser: schreibt auf, was ihr tut, warum ihr es tut und wer was macht. Und dann kommt damit zu uns.
- aggressive Löschpolitiken (nur Daten, die weg sind, sind gut geschützte Daten; und meist gibts außer „Statistik“ auch kaum gute Gründe, Daten über längere Zeit zu speichern)
- weitgehende Zugangsbeschränkungen (je weniger Leute PBZ sehen, desto geringer ist (normalerweise) der Eingriff)
- gegenseitige Isolation der verschiedenen Systeme (richtig übel werden Daten erst durch Kombination – z.B. Prüfungssystem und Ausländerzentralregister; Verbindungsnachweis und Subscriber-Datenbank bei Telefonfirmen)
- möglichst frühzeitige Aggregation/Anonymisierung (durch Bildung hinreichend großer Durchschnitte *mag* es sein, dass Daten ihren Personenbezug verlieren. In der Regel ist es aber besser, den Leuten diesen Statistikquatsch auszureden; in fast allen Fällen bringt Erbsenzählerei genau gar nichts, schadet aber, weil sie politische Auseinandersetzungen mit objektiv scheinenden Zahlen unterdrückt)
- Protokollierung von Abfragen (aber: Beschäftigtendatenschutz nicht vergessen, d.h. die sollten allenfalls pseudonym gespeichert werden)
- ordentliche Artikel 13-Aufklärung. Artikel 13 DSGVO sagt, dass ihr Leuten, wenn ihr ihre Daten erfasst, sagen müsst, was ihr mit den Daten macht. Das ist dann klasse, wenn das nicht in endlosem Legalesisch untergeht. Wieder: Lasst die Finger von Vorlagen aus dem Internet, sondern nehmt euer Verfahrensverzeichnis, macht es vielleicht noch etwas lesbarer, überlegt euch, auf welcher Grundlage ihr die Daten verarbeitet (Artikel 6 DSGVO) und dann kommt nochmal bei uns vorbei.
- . . . und natürlich den Kram technisch ordentlich machen.

Leider kommen wir hier in Bereiche, die tiefere technische Kenntnisse erfordern. Wir gucken da gerne auch mal drauf.

12. Ach: Die DSGVO

Die DSGVO ist ein relativ lesbares Gesetz; guckt einfach mal rein:

http://stura.uni-heidelberg.de/datenschutz/DSGVO.pdf

Darin u.a.: Artikel 6, Gründe für DV. Für euch als Verarbeiter_innen in Frage kommen:

- (1) a Einwilligung. Aber Vorsicht: Leute mit Vorteilen zu einer Einwilligung zu bewegen ist meist unwirksam. Und etwa in Web-Formularen Häkchen setzen geht auch nicht. Dafür muss die Einwilligung auch nicht zwingend schriftlich sein und archiviert werden; solange nachvollziehbar ist, dass die Leute gewusst haben, was sie getan haben, passt das schon.
- (1) b Antrag der Person. Das kommt z.B. in Frage, wenn ihr Kram verleiht und für eine Weile speichert, wer was hatte.
- (1) c rechtliche Verpflichtung. Das käme z.B. in Betracht bei der Abhaltung von Wahlen. Aber klar: hier sind strenge Maßstäbe der Verhältnismäßigkeit anzulegen.
- (1) f berechtigte Interessen des Verantwortlichen. Auf sowas *könntet* ihr euch stützen, wenn ihr auf eurer Webseite Nutzungsstatistiken macht oder sowas. Aber klar: bei 1(f) gucken wir nochmal besonderes genau hin.

13. Fragt jetzt. . .

oder später: datenschutz@stura.uni-heidelberg.de PGP-Fingerprint:
FF9A 7A3C 53D6 CC8A 054B 6DA6 F1A8 39BA 742A 2E08