DSGVO

Information

TECHNISCHE UNIVERSITÄT DARMSTADT

Datenschutz

TECHNISCHE UNIVERSITÄT DARMSTADT

- Grundprinzipien DSGVO
- Konkrete Fragestellungen aus der TU
- Diskussion

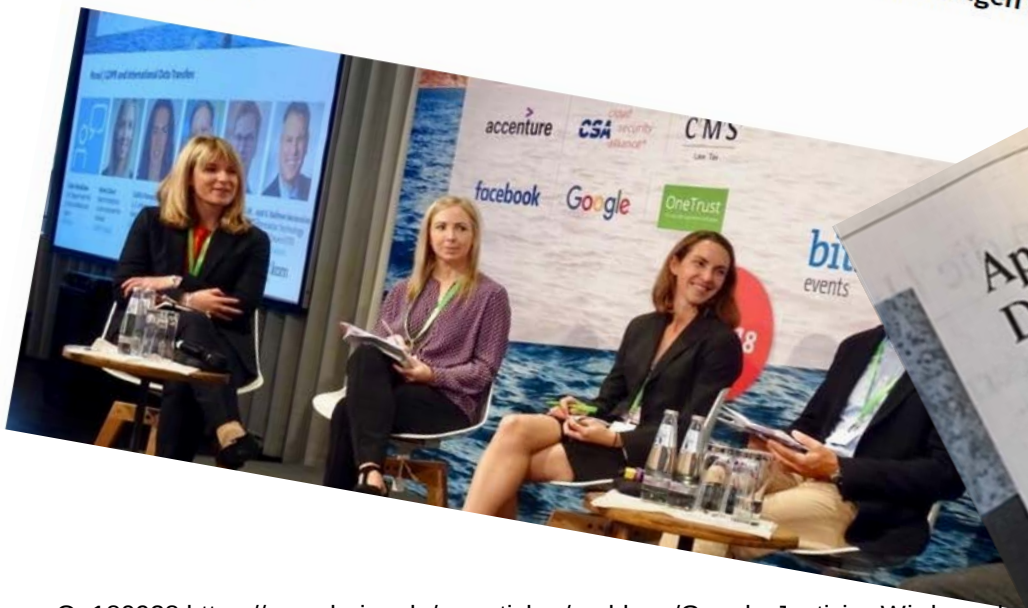
Datenschutzstandards

27.09.2018 18:52 Uhr

Google-Justiziar: "Wir brauchen weltweit die gleichen Datenschutzstandards"

Vertreter aus Wirtschaft und Politik werben für "pragmatische Lösungen", um Datentra
Zeitalter der DSGVO aufrecht zu erhalten.

Von Stefan Krempl



Apple-Chef: DSGVO Vorbild im Datenschutz

BERLIN, 21. Oktober (dpa). Der Chef des amerikanischen Technologieunternehmens Apple, Tim Cook, hat die Datenschutzgrundverordnung der Europäischen Union (DSGVO) als Basis für einen weltumspannenden Datenschutz gelobt. „Ich bin ein großer Fan der DSGVO. Sie stellt aber noch nicht alles dar, was gemacht werden muss", sagte er am Sonntag während einer Veranstaltung in Berlin. „Wir würden es gerne sehen, wenn nicht nur die Vereinigten Staaten, sondern auch viele andere Länder der Führungsrolle Europas folgen und vielleicht sogar darüber hinausgehen würden." Gerade in Deutschland gebe es bei den Bürgern ein prägtes Bewusstsein und ein ausgeprägtes Bedürfnis den Schutz der Privatsphäre. Auch weil

Q: 180928 https://www.heise.de/newsticker/meldung/Google-Justiziar-Wir-brauchen

Datenschutz

TECHNISCHE UNIVERSITÄT DARMSTADT

DSGVO

Die Entwicklung der DSGVO (2015 Regisseur David Bernet)

181003 Q: http://www.democracy-film.de/

Kriminelle Szene reagiert schnell

Warnung vor Datenschutzauskunft-Zentrale: Betrugsversuch mit Fax zur Erfassung gewerblicher Betriebe zum Basisdatenschutz nach DSG

Die sog. DAZ Datenschutzauskunft-Zentrale, Lehnitzstrasse 11, 16515 Oranienburg versendet aktuell "eilige Fax-Mitteilungen", mit denen Firmen dazu aufgerufen werden, ihre Daten auf einem Formular per Unterschrift zu bestätigen und dann per Fax zurückzusenden. Mit der Unterschrift wird gleichzeitig ein "Leistungspaket Basisdatenschutz" für 149 Euro erworben sowie ein jährlicher Beitrag von 498 Euro für eine dreijährige Mindestlaufzeit vereinbart.

» Informationen des Deutschen Schutzverbands gegen Wirtschaftskriminalität e.V. (DSW)

Q: 180928 https://www.heise.de/newsticker/meldung/Google-Justiziar-Wir-brauchen-weltweit-die-gleichen-Datenschutzstandards-4177379.html

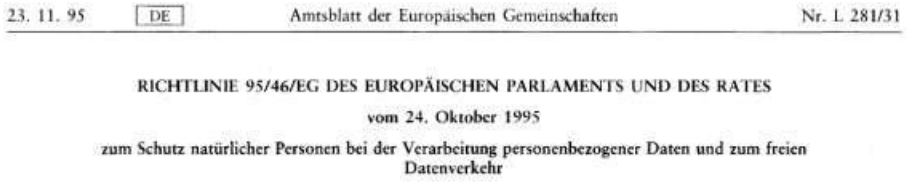
Hintergrund

TECHNISCHE UNIVERSITÄT DARMSTADT

- Die DSGVO (Datenschutzgrundverordnung) betrifft alle
- DSGVO -> HDSIG
- Einheitliche Regelung für EU
- TU als Universität nicht in der Form wie privatrechtliche Unternehmen betroffen
- Neues Hessisches Datenschutzgesetz (Hessisches Datenschutz- und Informationsfreiheitsgesetz (HDSIG)) ist in Kraft
- Für unsere wesentlichen Systeme (beispielsweise SAP; TUCaN) besteht eine Rechtsgrundlage für den Betrieb: Art. 6 Abs. 1 lit. e DSGVO

DSGVO - BDSG - HDSIG

- Die DSGVO (Datenschutzgrundverordnung) gilt unmittelbar
- DSGVO -> HDSIG
- HDSIG nur noch subsidiär
- DSGVO gilt für Verarbeitung personenbezogener Daten
  - automatisierte und
  - automatisiert erschlossene Akten



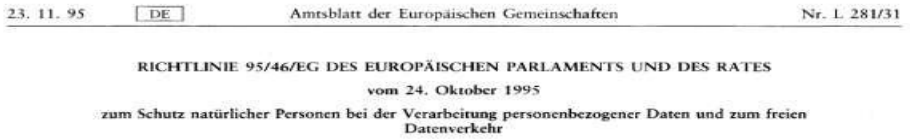
23. 11. 95 DE Amtsblatt der Europäischen Gemeinschaften Nr. L 281/31

RICHTLINIE 95/46/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 24. Oktober 1995

zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr

DSGVO 1


23. 11. 95 DE Amtsblatt der Europäischen Gemeinschaften Nr. L 281/31

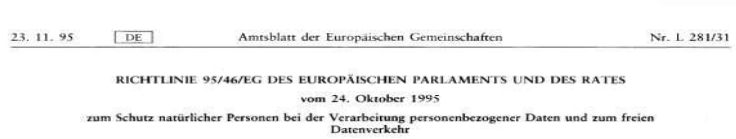
RICHTLINIE 95/46/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES
vom 24. Oktober 1995
zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr

TECHNISCHE UNIVERSITÄT DARMSTADT

- Datenverarbeitung ist verboten!
- Es sei denn,
- sie ist in der DSGVO selbst, in einem Spezialgesetz oder Dienst-Vereinbarung erlaubt
- oder
- … die betroffene Person hat eingewilligt.

- konkrete Rechtsgrundlagen für den Betrieb; z.B. HHG + HImmaVO

DSGVO 2 – alles neu?

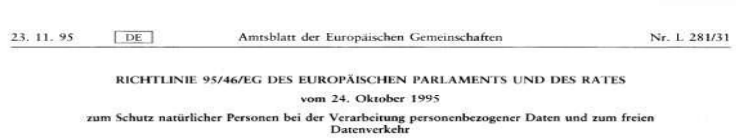

23. 11. 95 DE Amtsblatt der Europäischen Gemeinschaften Nr. L 281/31

RICHTLINIE 95/46/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES
vom 24. Oktober 1995
zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr

TECHNISCHE UNIVERSITÄT DARMSTADT

- **Transparenz (Art. 5 Abs. 1 lit. a DSGVO)**
- Datenverarbeitung muss nachvollziehbar erfolgen
- **Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO)**
- Auflösung der Bindung für besondere Zwecke, Art. 89 Abs. 1 DSGVO; z.B. Wissenschaft
- **Datensparsamkeit (Datenminimierung Art. 5 Abs. 1 lit. c DSGVO)**
- **Datensicherheit (Art. 5 Abs. 1 lit. f DSGVO)**

DSGVO 3 – neu!


23. 11. 95 DE Amtsblatt der Europäischen Gemeinschaften Nr. L 281/31

RICHTLINIE 95/46/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES
vom 24. Oktober 1995
zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr

TECHNISCHE UNIVERSITÄT DARMSTADT

- **Rechenschaftspflicht**
- **Datenschutzmanagement ->Art. 32 DSGVO**
- **Meldepflicht von Datenschutzverstößen**
- **Transparenz (Art. 5 Abs. 1 lit. a DSGVO)**
- Privacy by Design **Art. 25 DSGVO**
- Privacy by Default **Art. 25 DSGVO**

Synopse alt /neu

TECHNISCHE UNIVERSITÄT DARMSTADT

HDSG alt	DSGVO
• Verbot mit Erlaubnisvorbehalt: Die Verarbeitung der Daten ist zulässig, wenn der/die Betroffene zugestimmt hat oder eine Rechtsvorschrift dies gestattet.	• Verbot mit Erlaubnisvorbehalt Voraussetzungen der Einwilligung (Art. 7) präziser gefasst: Verständlich; Aufklärung über Verwendungszweck der Daten, Hinweis auf Widerrufsmöglichkeit, Freiwilligkeit, Schriftform fällt weg
• Zweckbindung	• Art. 5 Abs. 1 b
• Erforderlichkeitsprinzip	• Datensparsamkeit
• Technisch-organisatorische Maßnahmen	• Sicherheit der Verarbeitung Art. 32 **Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO)** • **„privacy by design“** • **„privacy by default“:**

Synopse alt /neu

TECHNISCHE UNIVERSITÄT DARMSTADT

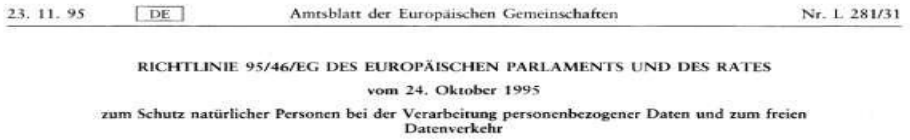
HDSG alt	DSGVO
• Verfahrensverzeichnis öffentlich	• Verzeichnis der Verarbeitungstätigkeiten (intern)
• Vorabkontrolle	• nur noch bei besonderem Risiko; Datenschutz-Folgeabschätzung
	• Rechenschafts- und Nachweispflicht Art. 5 Abs. 2 • Dokumentationspflichten
	• Meldepflichten bei Pannen Art. 33 Art. 34
• Anrufung HDSB	• Beschwerde bei Aufsichtsbehörde

Synopse alt /neu

TECHNISCHE UNIVERSITÄT DARMSTADT

HDSG alt	DSGVO
• Das Speichern der Daten ist mitzuteilen.	• Informations- und Auskunftspflichten • Recht auf Kopie der Daten Aber: Gilt nicht für Daten, die nur noch aufgrund von Aufbewahrungspflichten oder für DV-Sicherheit usw. gespeichert § 33 I HDSiG
• Den Betroffenen muss Auskunft über ihre gespeicherten Daten erteilt werden.	
• Den Betroffenen muss mitgeteilt werden, an wen ihre Daten regelmäßig weitergegeben werden.	
• Unrichtige Daten sind zu berichtigen.	• Berichtigungsanspruch Art. 16
• Bestrittene Daten sind zu sperren. Überflüssige Daten oder unzulässige Daten sind zu löschen.	• Löschung Recht auf „Vergessen werden“ Art. 17
	• Widerspruchsrecht Art. 21
• Die Daten sind vor Missbrauch zu schützen.	• Datensicherheit

DSGVO 4


23. 11. 95 DE Amtsblatt der Europäischen Gemeinschaften Nr. L 281/31

RICHTLINIE 95/46/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES
vom 24. Oktober 1995
zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr

TECHNISCHE UNIVERSITÄT DARMSTADT

- **Rechenschaftspflicht** (Art. 5 Abs. 2) gegenüber der Aufsichtsbehörde (Hess. DSB), aber auch vor Gericht!
- Verantwortlicher muss nachweisen können:
  - Rechtmäßigkeit, Transparenz und Sicherheit der Verarbeitung,
  - Einhaltung der Zweckbindung,
  - Richtigkeit der Daten,
  - Datenminimierung auf das erforderliches Maß Speicherbegrenzung auf erforderliche Dauer
- → Beweislast beim Verantwortlichen
- **Entsprechende Prozesse müssen organisiert werden**

DSGVO 4

23. 11. 95 DE Amtsblatt der Europäischen Gemeinschaften Nr. L 281/31

RICHTLINIE 95/46/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES
vom 24. Oktober 1995
zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr

Meldepflichten bei Verletzungen:

- Pflicht zur Meldung an die Aufsichtsbehörde (Art. 33): im Falle einer Verletzung des Schutzes personenbezogener Daten (= Verlust, Veränderung oder Offenlegung von Daten) **72 Stunden Frist**
  - … es sei denn, es kommt voraussichtlich zu keinem Risiko für Rechte u. Freiheiten nat. Personen! → in diesem Fall dennoch **Pflicht zur Dokumentation**


Meldungen von Verletzungen des Schutzes personenbezogener Daten

Dieses Formular dient zur Übermittlung von Meldungen von Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 Abs. 1 Datenschutz-Grundverordnung (DS-GVO).

  - https://datenschutz.hessen.de/service/meldungen-von-verletzungen-des-schutzes-personenbezogener-daten

Pflicht zur Mitteilung an die betroffene Person (Art. 34) bei voraussichtlich hohem Risiko für deren Rechte und Freiheiten)

DSGVO 5


23. 11. 95 DE Amtsblatt der Europäischen Gemeinschaften Nr. L 281/31

RICHTLINIE 95/46/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES
vom 24. Oktober 1995
zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr

TECHNISCHE UNIVERSITÄT DARMSTADT

Sanktionen bei Verletzung?

Bußgelder (Art. 83): bis zu 10–20 Mio. Euro Geldbuße für fast jeden Verstoß

- Verantwortlicher muss Einhaltung der Verordnung nachweisen; Beweislastumkehr für Verschulden!

Hessen: Behörden ausgenommen (§ 36 II HDSIG) vom Bußgeld

Meldepflicht (s. o.): Verantwortlicher muss sich selbst bezichtigen

- → öffentl. Verwaltung wird ausgenommen, Bußgeld trifft nur Private (Art. 83 Abs. 7, § 36 Abs. 2 HDSIG)

Schadensersatz Art. 82 auch für den sog. immateriellen Schaden

VVT

23. 11. 95 DE Amtsblatt der Europäischen Gemeinschaften Nr. L 281/31

RICHTLINIE 95/46/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 24. Oktober 1995

zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr

TECHNISCHE UNIVERSITÄT DARMSTADT

Vorabkontrolle als Standard entfällt

Nur noch DS-Folgeabschätzung bei Hochrisikoanwendungen

(Profiling, Gesundheitsdaten … Forschung!)

Verzeichnis ist nicht mehr öffentlich – dafür haben Betroffene Auskunftsrechte

Sicherheit der Verarbeitung (Art. 32 DSGVO)

TECHNISCHE UNIVERSITÄT DARMSTADT

Sicherheit der Verarbeitung (Art. 32 DSGVO)

- Geeignete technische und organisatorischen Maßnahmen („TOM“), um ein dem Risiko angemessenes Schutzniveau zu gewährleisten
- Kriterien: Stand der Technik, Implementierungskosten, Art, Umfang, Umstände, Zweck der Verarbeitung sowie der Eintrittswahrscheinlichkeit und Schwere der Risiken für Rechte und Freiheiten natürlicher Personen
- Maßnahmen nach DSGVO (siehe Katalog in Art. 32 DSGVO) z.B.:
- Pseudonymisierung, Verschlüsselung
- Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit von Systemen und Diensten
- Wiederherstellung der Daten und des Zugangs bei Zwischenfällen möglich
- Regelmäßige Prüfung der Wirksamkeit der Maßnahmen

Datenschutz durch Technikgestaltung

TECHNISCHE UNIVERSITÄT DARMSTADT

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO)

„privacy by design“:

- Treffen geeigneter technischer und organisatorischer Maßnahmen zur Umsetzung von Datenschutzgrundsätzen -> sog. „TOM“
- Einhaltung der Anforderungen der DSGVO und zum Schutz der Rechte der Betroffenen
- Kriterien: Stand der Technik, Implementierungskosten, Art, Umfang, Umstände, Zweck der Verarbeitung sowie der Eintrittswahrscheinlichkeit und Schwere der Risiken für Rechte und Freiheiten natürlicher Personen
- Bereits bei der Konzeption der Verarbeitung personenbezogener Daten mit berücksichtigen ; siehe Erwägungsgrund 78

Datenschutz durch „privacy by default“:

TECHNISCHE UNIVERSITÄT DARMSTADT

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO)

„privacy by default“:

- Konfiguration der DV, damit nur die personenbezogenen Daten verarbeiten, die für den jeweiligen Zweck erforderlich sind. Erforderlichkeitsgrundsatz
- Kriterien: Menge der erhobenen Daten, Umfang der Verarbeitung, Speicherfrist, Zugänglichkeit.
- Voreinstellungen müssen so sein, dass Zugänglichkeit personenbezogener Daten für die Allgemeinheit nicht ohne Eingreifen des Betroffenen möglich ist
- Adressiert vor allem Hersteller
- Berücksichtigung bei Ausschreibungen geboten!

Informations- und Auskunftspflichten

Informations- und Auskunftspflichten (Artt. 13–15) bei Erhebung der Daten sowie jederzeit auf Anfrage (→ Datenschutzerklärung)

- Kontaktdaten: Verantwortliche; Datenschutzbeauftragte
- Rechtsgrundlage und Zweck der Verarbeitung,
- Kategorien verarbeiteter Daten ,
- Herkunft der Daten (sofern durch Betroffenen genannt),
- etwaige Empfänger, insbes. in Drittländern,
- Speicherdauer, Löschfristen
- Bestehen von Auskunfts-, Berichtigungs-, Löschungsanspruch, Anspruch auf Einschränkung der Verarbeitung, Widerrufs-, Widerspruchs- u. Beschwerderecht
- Datenauszug, Kopie (in der Regel)

Auftragsdatenverarbeitung

TECHNISCHE UNIVERSITÄT DARMSTADT

- Auftragsverarbeiter benötigt eigenes VVT
- Neue Verträge mit Auftragsverarbeitern sind anzupassen
- Auftragsverarbeiter
  - können mit Bußgeldern belegt werden
  - haften, wenn sie sich nicht an die DSGVO oder die Anweisungen des Auftraggebers halten

Tagung organisieren

TECHNISCHE UNIVERSITÄT DARMSTADT

Verarbeitung personenbezogener Daten:

- Einladung
- Durchführung der Tagung
- Fotos der teilnehmenden Menschen
- Nachbereitung
- Aufbau von Mailinglisten

Auftragsdatenverarbeitung prüfen?

……

Rechtsgrundlage?

Einwilligung?

Einwilligung

TECHNISCHE UNIVERSITÄT DARMSTADT

Wesentliche Punkte einer wirksamen Einwilligung nach Art. 7 DSGVO sind:

Freiwilligkeit der Einwilligung; kein Zusammenhang mit Leistungen der Technischen Universität Darmstadt . **Deshalb problematisch bei Uni-Mitgliedern!**

- Art der Daten benannt?
- Zweck der Datenverarbeitung?
- Zweckbindung der Daten
- (einfache) Möglichkeit, die Einwilligung jederzeit zu widerrufen, ist vorhanden
- Speicherdauer ist angegeben
- Wer ist Verantwortlicher?

Form: nicht vorgeschrieben! Keine Schriftform mehr erforderlich!

Aktives Handeln der Betroffenen ist notwendig.

Negativ-Beispiel: ein voreingestelltes Häkchen auf einer WWW-Seite reicht nicht!

Wichtig: die Einwilligung muss dokumentiert werden, damit im Zweifel nachgewiesen werden kann, dass die betroffene Person ihre Zustimmung zur Verarbeitung gegeben hat.

Mindestanforderungen an eine informierte Einwilligung -1

TECHNISCHE UNIVERSITÄT DARMSTADT

Koppelungsverbot

Eine Gegenleistung darf nicht an die Einwilligung in die Verarbeitung von Daten gekoppelt werden, die für die Rolle als Studierende (oder sonstige Rolle in der Universität) erforderlich sind.

Freiwilligkeit; Widerrufsmöglichkeit:

„Die Einwilligung ist freiwillig und kann jederzeit widerrufen werden. Ein Widerruf berührt die bis dahin erfolgte Verarbeitung nicht. Aus der Verweigerung der Einwilligung oder ihrem Widerruf entstehen keine Nachteile. Allerdings ist es dann nicht möglich am Programm X teilzunehmen."

Speicherdauer angeben

Speicherung der Einwilligung selbst:

„Die Einwilligung wird bis zum Ende der Datenverarbeitung / der Speicherdauer durch die Technische Universität Darmstadt aufbewahrt. Auch hiermit bin ich einverstanden."

Mindestanforderungen an eine informierte Einwilligung -2

Widerruf der Einwilligung:

berührt die bereits erfolgte Verarbeitung nicht.

Folge ansonsten: keine weitere Verarbeitung = Löschung der Daten

Form der Einwilligung: Textform (auch elektronisch) Wenn die Einwilligung zusammen mit anderen Erklärungen verlangt wird, muss sie besonders hervorgehoben sein (z.B. Drucktechnisch, oder als Kasten).

Die Einwilligung ist zu protokollieren (siehe 8.).

Die Erwägungsgründe 32, 43 und 171 bieten eine gute Orientierung zur Einwilligung.

https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L:2016:119:FULL&from=DE

VVT

TECHNISCHE UNIVERSITÄT DARMSTADT

DSGVO – Anforderungen gelten ab sofort

Sukzessive Anpassung geduldet

Bei Änderung

- der Gesetzesgrundlage
- der angewandten Technologien
- Art, Umfang oder Umstände der Verarbeitung
- Zweck der Verarbeitung

oder

- Wenn anhand der vorherigen 3 Punkte das Risiko deutlich steigt.

- Alte VVzs bleiben gültig. Wenn Änderungen gemacht werden, dann neue Verzeichnis der Verarbeitungstätigkeit. Muster kann vom HDSB genommen werden.

Online-Anmeldeformulare für Veranstaltungen

TECHNISCHE UNIVERSITÄT DARMSTADT

Zulässigkeit der Datenerhebung

- Einwilligung oder Rechtsgrundlage Art. 6 Abs. 1 lit. e DS-GVO
  - Erforderlichkeitsgrundsatz: es ist bei jedem Datum zu hinterfragen, ob dies für die Aufgabenerfüllung der Universität – und hier im Besonderen die Organisation der Veranstaltung – zwingend erforderlich ist.
- Kritisch: Abfrage von Allergien, Rollstuhlnutzung, bevorzugte Ernährung und vergleichbare Gesundheitsdaten: Es handelt sich dabei um **besondere Kategorien personenbezogener Daten**, deren Verarbeitung grundsätzlich untersagt ist.
- Besser: Hinweis aufnehmen, dass Personen sich aktiv melden sollen

Hinweispflichten bei formularmäßiger Erhebung

Werden in einem Online-Formular personenbezogene Daten erhoben, so bedarf es die nach Art. 13 DSGVO erforderlichen Informationen.

Anschließende Datenverarbeitung

alle Spielregeln gelten: VVT, TOM, Betroffenenrechte

Was ist mit Bildern ?

TECHNISCHE UNIVERSITÄT DARMSTADT

Allgemeines Persönlichkeitsrecht § 22 KunstUrhG

§ 22 [1] [Recht am eigenen Bilde]

[1]Bildnisse dürfen nur mit **Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden.** [2]…

Es gibt Ausnahmen, aber diese führen zu schwierigen Abgrenzungsfragen

Spezifische Einwilligung erforderlich!

Ergänzung aufgrund von Nachfragen:

- Erstellen von Fotos ist Erhebung personenbezogener Daten
- Besonders problematisch: Bildverarbeitung in den herkömmlichen Programmen (externe Speicherung durch Cloud-Dienste außerhalb EU)

Mailinglisten

Rechtsgrundlage?

- Für Mitglieder der Universität:
  - Rechtsgrundlage in Art. 6 Abs. 1 lit. e oder
  - § 23 HDSIG (Beschäftigte)

Alle Übrigen: Einwilligung

„Verantwortlich“ ist der Verantwortliche der jeweiligen Institution

Verfahren: Double opt – in

Wichtig: Dokumentation der Einwilligung und des Verfahrens (Rechenschaftspflicht (Art. 5 Abs. 2)

Datenschutz

TECHNISCHE UNIVERSITÄT DARMSTADT

Das Datenschutzteam der TU z.Zt.:

Behördlicher Datenschutzbeauftragter

Gerhard Schmitt

Vertreter des behördlichen Datenschutzbeauftragten

N.N.

Funktionsadresse für Datenschutz: datenschutz@tu-darmstadt.de

Infos unter: https://www.intern.tu-darmstadt.de/dez_ii/hochschulrecht/datenschutz_dez_ii/index.de.jsp

Infoseite

- Soweit Änderungsbedarf besteht, sind wir dabei, die konkreten Schritte auszuarbeiten.

- Informationen – insbesondere Hinweise zur DSGVO - werden wir sukzessive auf der WWW-Seite des Datenschutzes

  https://www.intern.tu-darmstadt.de/dez_ii/hochschulrecht/datenschutz_dez_ii/index.de.jsp

  zur Verfügung stellen.

- E-Mail-Adresse (unverändert): datenschutz@tu-darmstadt.de

.