Universität Vechta
University of Vechta

Arbeiten mit der Datenschutz-Grundverordnung



Universität Vechta
University of Vechta

DSGVO

1. Allgemeine datenschutzrechtliche Grundlagen
2. Erfordernisse nach der DSGVO
3. Umsetzung innerhalb der Universität

Allgemeine datenschutzrechtliche Grundlagen – Grundsätze des Schutzes personenbezogener Daten

Was sind personenbezogene Daten?

- Personenbezogene Daten sind alle Informationen, die sich auf eine bestimmte oder (ggf. mit Zusatzwissen) bestimmbare Person beziehen

- Beispiele: Name, Adresse, Geburtsdatum, Staatsangehörigkeit, Beruf, Titel, akademischer Grad, Zugehörigkeit zu einer Religionsgemeinsch., Identifikationsnummern, wie Personalnummer, Immatrikulationsnr., Sozialversicherungsnummer, Semesterzugehörigkeit

Allgemeine datenschutzrechtliche Grundlagen – Grundsätze des Schutzes personenbezogener Daten

Was fällt unter die Verarbeitung?

- jegliche Maßnahmen, die mit diesen personenbezogenen Daten durchgeführt werden (egal ob sie automatisiert sind oder nicht)
  - Erheben, Erfassen
  - Organisation, Ordnen, Speicherung
  - Anpassung, Veränderung, Auslesen
  - Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung
  - Löschen, Vernichtung

Allgemeine Datenschutzrechtliche Grundlagen
Grundsätze des Schutzes personenbezogener Daten

Wer ist Verantwortlicher?

- Verantwortlich für die Einhaltung der Regelungen sind natürliche oder juristische Personen, Behörden oder Einrichtungen, die über die Zwecke und Mittel entscheiden

  somit die Universität Vechta, vertreten durch den Präsidenten. Allerdings sind auch alle Mitarbeiterinnen und Mitarbeiter sowie alle Studierenden an die Regelungen der DSGVO gebunden, sofern sie im Rahmen ihrer Tätigkeit an der Universität Vechta personenbezogene Daten verarbeiten.

Allgemeine datenschutzrechtliche Grundlagen – Grundsätze des Schutzes personenbezogener Daten

Wann dürfen personenbezogene Daten verarbeitet werden?

- Grundsatz: Verbot mit Erlaubnisvorbehalt
- Verarbeitung personenbezogener Daten nur bei Vorliegen einer ausdrücklichen Berechtigung/Erlaubnis:
  a) Gesetz: DSGVO, NHG, HStatG, SGB, andere Rechtsvorschriften
  b) Einwilligung: i.d.R. Schriftform, Aufklärung über Verwendungszweck der Daten, Hinweis auf Widerrufsmöglichkeit, Freiwilligkeit, besondere Hinweispflichten

Allgemeine datenschutzrechtliche Grundlagen – Grundsätze des Schutzes personenbezogener Daten

Welche Grundsätze sind bei der Verarbeitung zu berücksichtigen?

- **Transparenz**
  - Information des Betroffenen
- **Zweckbindung**
  - Festlegung eindeutiger und legitimer Zwecke
- **Datensparsamkeit** (Datenminimierung)
  - Die personenbezogenen Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke notwendige Maß beschränkt sein.
- **Datensicherheit**
  - Schutz vor unbefugter Verarbeitung, Verlust, Schädigung

Erfordernisse nach der DSGVO

Sicherstellung der Betroffenenrechte

Auskunftspflicht:

- Kontaktdaten d. Verantwortlichen und d. Datenschutzbeauftragten
- Rechtsgrundlage und Zweck der Verarbeitung
- Kategorien verarbeiteter Daten
- Herkunft der Daten
- etwaige Empfänger (insb. in Drittländern)
- Speicherdauer, Löschfristen
- Bestehen von Auskunfts-, Berichtigungs- und Löschungsansprüchen
- Widerrufs-, Widerspruchs- und Beschwerderecht

Erfordernisse nach der DSGVO

Sonstige Betroffenenrechte:

- **Berichtigungsanspruch**
- **Löschungsanspruch** „Recht auf Vergessenwerden“
  - wenn Daten für den Zweck nicht länger nötig sind
  - wenn Daten rechtswidrig erhoben wurden
  - wenn Einwilligung widerrufen wurde
- **Anspruch auf Einschränkung**
- **Widerspruchsrecht**
- **Beschwerderecht bei Aufsichtsbehörden**

Erfordernisse nach der DSGVO -Technischer Datenschutz

Technischer Datenschutz nach der DSGVO

- durch Umsetzung von technischen und organisatorischen Maßnahmen

Ziel der IT-Sicherheit:

- Verfügbarkeit
- Vertraulichkeit
- Integrität

➢ IT-Sicherheit ist Voraussetzung für effektiven Datenschutz

Erfordernisse nach der DSGVO -Technischer Datenschutz

Technische und organisatorische Maßnahmen bei der Verarbeitung personenbezogener Daten:

- Zutrittskontrollen
- Benutzerkontrolle
- Zugriffskontrolle
- Datenverarbeitungskontrolle
- Verantwortlichkeitskontrolle
- Auftragskontrolle
- Dokumentationskontrolle
- Organisationskontrolle

Erfordernisse nach der DSGVO - Technischer Datenschutz

Sicherheit der Verarbeitung

- angemessenes Schutzniveau durch geeignete technische und organisatorische Maßnahmen
- zu berücksichtigen sind: Stand der Technik, Implementierungskosten, Art, Umfang, Zweck der Verarbeitung sowie der Eintrittswahrscheinlichkeit und Schwere der Risiken für Rechte und Freiheiten natürlicher Personen
- Maßnahmenkatalog:

  Pseudonymisierung; Anonymisierung; Verschlüsselung; Fähigkeit zur Sicherstellung von Vertraulichkeit, Integrität, Belastbarkeit von Systemen u. Diensten; Wiederherstellung von Daten; regelmäßige Überprüfung d. Maßnahmen

Umsetzung innerhalb der Universität
Einwilligungserklärungen

- **Nachweis der Freiwilligkeit** der Erklärung: sie muss ausreichende Informationen über die geplante Datenverarbeitung erhalten, damit die betroffene Person verstehen kann, worin sie einwilligt.
- Mindesterfordernisse:
  - Zweck der Verarbeitung
  - Auflistung der Datenkategorien
  - Kontakt
- sog. **Opt-Out-Verfahren** bei elektronischer Erklärung nicht zulässig
- erteilte Einwilligung kann **jederzeit widerrufen** werden

Umsetzung innerhalb der Universität

Fotoaufnahmen im Rahmen universitärer Veranstaltungen

Zweck: Öffentlichkeitsarbeit, Veröffentlichung von Fotos auf der Uni-Webseite etc.:

- Hinweise auf Einladungen oder Anmeldeformularen, dass im Rahmen der Veranstaltung zu Zwecken der Öffentlichkeitsarbeit Fotoaufnahmen angefertigt werden und dass diese (und vor allem wo) veröffentlicht werden, Hinweis auf Möglichkeit der Abstimmung mit Fotograf, Kontaktdaten für weitere Fragen.
- Hinweis vor den Räumlichkeiten, in denen die Veranstaltung stattfindet
- bei Portrait-Aufnahmen (z.B. für Interviews) schriftliche Einwilligung für Aufnahmen und Veröffentlichung

Umsetzung innerhalb der Universität

Anfertigung und Veröffentlichung von Fotos von Mitarbeiter*innen

Veröffentlichung von Portrait-Fotos für die dienstliche Website oder Gruppenfotos zur Präsentation der eigenen Mitarbeiter*innen auf der Homepage

- Einwilligung zu Aufnahmen und Veröffentlichung im Vorfeld einholen
- sofern keine Einwilligung der auf dem Foto abgelichteten Person/en vorliegt, ist diese Anfertigung als auch die Veröffentlichung solcher Fotos unrechtmäßig. Die betroffenen Personen haben dann u.a. einen Anspruch auf Löschung dieser Fotos.

Umsetzung innerhalb der Universität

Einsatz von Social-Media-Accounts für Einrichtungen der Universität

Probleme:

- zwischen dem Betreiber einer "Fanpage" und dem Anbieter (Facebook, Twitter etc.) besteht für die Verarbeitung personenbezogener Daten eine "gemeinsamen Verantwortlichkeit"
- Ausübung der Betroffenenrechte mangels Zugriffsmöglichkeit des Betreibers schwierig
- Datenübertragung an Anbieter
  - ➢ Abstimmung mit Bereich Marketing und Kommunikation
  - ➢ Verlinkung mit der Datenschutzerklärung der Universität

Umsetzung innerhalb der Universität

Umgang mit E-Mail Adressen

E-Mail Adressen sind **immer** personenbezogene Daten. Auch dann, wenn die E-Mail nicht den Vor- und Nachnamen der betroffenen Person beinhaltet

- daher grundsätzlich immer einer Rechtsgrundlage erforderlich, um E-Mail Adressen im Sinne der DSGVO zu verarbeiten, also zu speichern, Inhalte an eine E-Mail zu senden etc.
- Anlegen von E-Mail Verteilern: Einwilligung der betroffenen Personen erforderlich
- Weitergabe nur mit Einwilligung der betroffenen Person
- Vermeidung offener E-Mail Verteiler

Umsetzung innerhalb der Universität

Datenschutzhinweise bei Kontaktformularen, Newslettern, E-MailVerteilern

Bei der Einrichtung von Newslettern und E-Mail-Verteilern über die Webseiten der Universität bestehen Informationspflichten:

- Nennung des Zwecks, der Rechtsgrundlage, der Dauer und Art der Datenverarbeitung sowie insbesondere der Art der Kategorien personenbezogener Daten
- zumeist reicht Verweis auf die Datenschutzerklärung der Universität
- bei Abfrage von Daten, die über die Datenschutzerklärung hinausgehen, ist eigene Datenschutzerklärung erforderlich
  - dringend erforderlich ist dabei die Abstimmung mit der Datenschutzbeauftragten und dem Bereich Marketing und Kommunikation

Umsetzung innerhalb der Universität

Ausübung des Auskunftsrechts der betroffenen Personen

Sicherstellung, dass Auskünfte über die Verarbeitung personenbezogener Daten nur an zur Auskunftserteilung berechtigte Personen erteilt werden. Die Identität der anfragenden Person muss also offengelegt werden.

- je sensibler die personenbezogenen Daten sind, desto sicherer muss die Identität der anfragenden Person durch geeignete Nachweise festgestellt werden:
  - Vorlage Personalausweis, Studierendenausweis
  - Bitte um schriftliche Anfrage
  - Erteilung der Auskunft möglichst ebenfalls schriftlich
  - telefonisch sollten nur organisatorische Auskünfte gegeben werden

Umsetzung innerhalb der Universität

Aushänge mit personenbezogenen Daten

Der öffentliche Aushang oder die öffentliche Auslegung von Listen oder Prüfungen mit Matrikelnummern und Namen der Studierenden stellt eine rechtswidrige Übermittlung personenbezogener Daten dar!

- Nutzung von StudIP: nur für die betroffene Person zugänglich
- analoge Aushänge für Noten nur unter Verwendung der Matrikelnummer (dahinterstehende Person darf nicht erkennbar sein)
- Teilnehmerlisten sollen lediglich Namen und gerade nicht (auch) die Matrikelnummer beinhalten

Umsetzung innerhalb der Universität

Arbeiten in Heimarbeit

- Daten und IT-Technik sind dem unmittelbaren Zugriff entzogen
- erhöhte Gefahr durch Zugriffsmöglichkeiten Dritter

daher:

- Zugriff auf Daten im Netzlaufwerk der Universität über Cloud/VPN
- sichere Aufbewahrung dienstlicher Unterlagen
- keine Weitergabe von Passwörtern
- sichere Übertragung von Daten
- Meldung sicherheitsrelevanter Vorkommnisse

Universität Vechta
University of Vechta

Vielen Dank für Ihre Aufmerksamkeit!