Die Datenschutzgrundverordnung

Digitalisierung und Datenschutz –

ewige Gegensätze

oder lediglich 2 Seiten einer Medaille?

Ltd. Ministerialrat Gregor Eisenhuth,
Bayer. Staatsministerium d. Justiz

Die Datenschutz-Grundverordnung (DSGVO)…
ist – für viele völlig überraschend – am 25. Mai 2018 in Kraft getreten:

- Dauer des Gesetzgebungsverfahrens: Sechs Jahre
- Inkrafttreten: Mai 2016
- Seit 25. Mai 2018 unmittelbar geltendes Recht in allen EU-Mitgliedstaaten
- 99 Artikel mit 173 Erwägungsgründen regeln insbesondere
  - Die Grundsätze der Verarbeitung personenbezogener Daten
  - Die Rechte der betroffenen Personen,
  - Die Verantwortlichkeit für die Datenverarbeitung (DV) und
  - Die Befugnisse der Aufsichtsbehörden und Sanktionsmöglichkeiten
- Grundlage ist das europäische Grundrecht auf Schutz personenbezogener Daten gem. Art. 8 der Charta der Grundrechte der EU (GRCh)
- Als **Grund**-Verordnung hat die DSGVO trotz ihrer unmittelbaren Geltung zum Teil richtlinienähnlichen Charakter in Form von **Öffnungsklauseln**, die es den Mitgliedstaaten gestatten, einzelne Bereiche zu konkretisieren; die für die Justiz wichtigsten finden sich in Art. 6 Abs. 2 i. V. m. Art. 6 Abs. 1 lit. c) und lit. e) DSGVO bzw. in Art. 23 Abs. 1 lit. f) DSGVO.

Ltd. Ministerialrat Gregor Eisenhuth,
Bayer. Staatsministerium d. Justiz

Betrifft uns das eigentlich alles bzw. ist die DSGVO auf die Justiz anwendbar?

- Grundlage: Erwägungsgrund 20 => auch die Datenverarbeitung im „Rahmen der justiziellen Tätigkeit“ wird erfasst.

- Im Rahmen der rechtsprechenden Tätigkeit sind lediglich die Befugnisse der Aufsichtsbehörden sowie des Datenschutzbeauftragten eingeschränkt.

- Sondersituation in der **Strafgerichtsbarkeit und** bei der **Strafverfolgung**:
  - Art. 2 Abs. 2 lit. d) DSGVO: Ausgenommen vom Anwendungsbereich
  - Art. 28 ff. BayDSG: Weit gehende Anwendung der DSGVO auch auf Strafgerichte und Staatsanwaltschaften, allerdings mit praktisch besonders relevanten Ausnahmen
  - Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/680 im Strafverfahren sowie zur Anpassung datenschutzrechtlicher Bestimmungen an die Verordnung (EU) 2016/679 (BR-Drs. 433/18):
    § 500 StPO-E => Umfassende Anwendung von Teil 3 des Bundesdatenschutzgesetzes (BDSG 2018)

Ltd. Ministerialrat Gregor Eisenhuth,
Bayer. Staatsministerium d. Justiz

Medienberichte und soziale Netzwerke:

In den Medien und den sozialen Netzwerken hat die DSGVO ein zwiespältiges Echo hervorgerufen:

- Einerseits werden die neuen Möglichkeiten der Aufsichtsbehörden betont, bei Verstößen künftig hohe Geldbußen (bis zu 20 Mio. € oder 4% des weltweit erzielten Jahresumsatzes eines Unternehmens verhängen zu können.

- Politisch wird der Datenschutz zum Teil neben Umweltschutzstandards als der mögliche Wettbewerbsvorteil europäischer Produkte betrachtet.

- Andererseits werde nicht selten Fälle geschildert, in denen die DSGVO angeblich zu absurden Verhaltensweisen zwingt wie etwa…

Ltd. Ministerialrat Gregor Eisenhuth,
Bayer. Staatsministerium d. Justiz

Ltd. Ministerialrat Gregor Eisenhuth,
Bayer. Staatsministerium d. Justiz

Hinzu kommt…

- Der Umgang mit europäischen Rechtsvorschriften und die „Mehrebenen-Gesetzgebung“ (DSGVO – BayDSG – BDSG – Fachrecht) ist für viele Rechtsanwender ungewohnt und stellt sich relativ komplex dar.

- Der Bund und die Länder haben ihre Vorschriften teilweise erst kurz vor Inkrafttreten an die DSGVO angepasst – oder dies auch bis heute noch nicht vollständig geschafft.

Folgen:

- Verunsicherung bei Verantwortlichen und Datenschutzbeauftragten, ggf. auch noch bei den Aufsichtsbehörden?

- Großer Informationsbedarf

- Neigung zu Überreaktion

Ltd. Ministerialrat Gregor Eisenhuth,
Bayer. Staatsministerium d. Justiz

Alles neu macht die DSGVO?

- Vieles von dem, was bisher schon geltende Rechtslage war findet sich mindestens in ähnlicher Form, nicht selten sogar wortgleich, in der DSGVO wieder.

- Unverändert sind insbesondere die **elementaren Grundsätze der Datenverarbeitung**, **Art. 5 DSGVO**:

  - „Rechtmäßigkeit, Fairness und Transparenz“ -> Vorliegen einer Erlaubnis, mildestes Mittel, faire Information über Verarbeitung und Rechte
  - „Zweckbindung“ -> Daten werden nur für festgelegten, eindeutigen und legitimen Zweck erhoben
  - „Datenminimierung“ -> Datenverarbeitung muss auf das notwendige Maß beschränkt sein
  - „Richtigkeit“ -> Daten müssen sachlich richtig sein, unrichtige Daten gelöscht werden
  - „Speicherbegrenzung“ -> Datenspeicherung wird auf den Zeitraum der Verarbeitung beschränkt
  - „Integrität und Vertraulichkeit“ - > Gewährleistung angemessener Sicherheit bei der Verarbeitung personenbezogener Daten

Alles neu macht die DSGVO?

- Unverändert beruht die DSGVO auf einem (Verarbeitungs-)Verbot mit Regelungsvorbehalt, d. h. ein Gesetz muss Ausmaß, Grenzen und Zweck der DV regeln, zentrale Norm ist insoweit Art. 6 DSGVO:
  - Einwilligung (Art. 6 Abs. 1 lit. a) DSGVO)
  - Erforderlichkeit zur Vertragserfüllung (Art. 6 Abs. 1 lit. b) DSGVO)
  - Erfüllung einer rechtlichen Verpflichtung bzw. öffentlicher Aufgaben (Art. 6 Abs. 1 lit. c) bzw. lit. e) DSGVO).

Der Schwerpunkt des Umsetzungsbedarfs der DSGVO liegt folglich bei den Verfahrensvorschriften.

Was bis zum 25. Mai 2018 als Datenverarbeitung zulässig war, ist dies grundsätzlich noch immer.

…manches schon,
die wichtigsten Neuerungen der DSGVO:

- Ausgeweitete Transparenz- und Informationspflichten, Art. 12 – 15 DSGVO;
- Gemeinsame Verantwortlichkeit, Art. 26 DSGVO;
- Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung bei neuen oder besonders eingriffsintensiven Verfahren, Art. 35 DSGVO;
- Zertifizierung von Verfahren, Art. 42 DSGVO;
- Neue Befugnisse und Pflichten der Datenschutzaufsichtsbehörden, Art. 58 DSGVO

Ltd. Ministerialrat Gregor Eisenhuth,
Bayer. Staatsministerium d. Justiz

Die Informationspflichten des Verantwortlichen nach Art. 13 und 14 DSGVO
Lösung: Information in mehreren Stufen

- Eine vollständige Information auf jedem ausgehendem Schreiben ist weder rechtlich erforderlich noch sinnvoll.

- Die Informationen sollten daher wie folgt aufgeteilt werden:

  - Kurzhinweis auf dem Schreibwerk

  - Ausführliche Informationen auf der jeweiligen Homepage (s. insoweit mit JMS v. 16.05.2018 Gz. 1552 – VI – 3982/2016 übersandtes Muster)

  - Hinweis auf weiter gehende Informationen beim zuständigen Sachbearbeiter

Ltd. Ministerialrat Gregor Eisenhuth,
Bayer. Staatsministerium d. Justiz

Datenschutz-Folgenabschätzung

- Die DS-Folgenabschätzung **löst** in Bayern **das bisherige Freigabeverfahren nach Art. 26 BayDSG 1993 ab**.
- Der Verantwortliche hat vor einer Verarbeitung eine **Risikoanalyse** durchzuführen, in die der mögliche Schaden sowie die Eintrittswahrscheinlichkeit einzubeziehen sind (Risiko = Schadenshöhe x Eintrittswahrscheinlichkeit).
- Praktische Erfahrungen mit der Folgenabschätzung liegen derzeit noch nicht vor.
- Der Landesbeauftragte hat unter https://www.datenschutz-bayern.de/datenschutzreform2018/DSFA_Blacklist.pdf eine erste Fassung der **Liste von Verarbeitungstätigkeiten gem. Art. 35 Abs. 4 DSGVO (sog. „Blacklist“)** veröffentlicht.
  - Besondere Relevanz für die Justiz: Fallgruppe 15 „Rechtswesen“
  - Als Regelbeispiel genannt ist „Vorgangsverwaltungssysteme bei Betreuungsgerichten“
- Für laufende Verarbeitungen, die nach altem Recht datenschutzrechtlich freigegeben wurden, besteht eine **Übergangsfrist bis** zum **24. Mai 2021.**
- **Fachliche, technische** und **organisatorische** Fragen im Zusammenhang mit der Durchführung der Folgenabschätzung werden derzeit geprüft.

Ltd. Ministerialrat Gregor Eisenhuth,
Bayer. Staatsministerium d. Justiz

Datenschutz und Datensicherheit

- Grundsatz: Datenschutz ist enger als Datensicherheit.
  Gleichwohl ist eine trennscharfe Abgrenzung nicht immer möglich!

- Maßgeblich sind nach Art. 32 Abs. 1 DSGVO der „Stand der Technik“ und die „Implementierungskosten“ zu berücksichtigen. 3 wesentliche Schutzziele:
  - Vertraulichkeit (gewähren durch Zugriffsrechte)
  - Integrität (Unveränderbarkeit von Originaldokumenten gewährleisten)
  - Verfügbarkeit (Systemsicherheit und –stabilität)

- Für den Strafbereich definiert Art. 32 BayDSG folgende detaillierte Anforderungen an die Sicherheit:
  - Zugangskontrolle
  - Organisationskontrolle
  - Datenträgerkontrolle
  - Speicherkontrolle
  - Benutzerkontrolle
  - Transportkontrolle

Gutachten zu den Auswirkungen aktueller datenschutzrechtlicher Vorgaben auf die IT-Architektur der Justiz

- Ziel des Gutachtens ist die Ableitung IT-technischer Leitlinien aus den bestehenden datenschutzrechtlichen Vorgaben. Das Gutachten soll das BLK-Architekturbüro in die Lage versetzen, Leitlinien für die IT-Architektur der Justiz zu entwickeln, sodass bei Neuentwicklungen, Neubeschaffungen und wesentlichen Fortentwicklungen von IT-Verfahren der Gerichte und Staatsanwaltschaften die Anforderungen des Datenschutzes von Anfang an angemessen berücksichtigt werden können.

- Vorgehen:

  - Identifizierung der Verarbeitungsvorgänge
  - Rechtliche Anforderungen an die jeweilige Datenverarbeitung
  - Gefährdungen/Risiken für die Daten
  - Anforderungen an die Entwicklung von IT-Anwendungen und die IT-Architektur (Art. 25 DSGVO => „Privacy by design“ und „Privacy by default“)

Auftragsverarbeitung und gemeinsame Verantwortlichkeit

- Verträge über Auftragsverarbeitungen (AV) sind ggf. an die Anforderungen des Art. 28 DSGVO anzupassen.
- Legaldefinition für AV in Art. 4 Nr. 8 DSGVO (abzugrenzen von gemeinsamer Verantwortlichkeit iSv Art. 26 DSGVO und selbständiger Erbringung von Dienstleistungen, wie etwa Post- oder TK-Leistungen, Banken, Versicherer, etc.).
- Im Grundsatz gilt: Die DSGVO behandelt Auftragsverarbeiter wie eine eigene Dienststelle. => Die Behörde bleibt alleine verantwortlich und die Auftragsverarbeiter müssen sich so behandeln lassen, als seien sie Teil der Behörde.
- Wichtige Anwendungsbeispiele:
  - Gutachtenerstellung
  - Fernwartung von IT-Systemen
  - Scannen von Papiervorgängen für die elektronische Akte
  - Papiervernichtung
  - Vernichtung sichergestellter Datenträger

Ltd. Ministerialrat Gregor Eisenhuth,
Bayer. Staatsministerium d. Justiz

Checkliste für die Auftragsverarbeitung

- Steht im Vertrag genau, wo die Verarbeitung stattfindet (nicht nur der Firmensitz)? Sind diese Orte für effektive Kontrollmaßnahmen für uns ausreichend erreichbar?
- Werden uns (ohne Zusatzkosten) wirksame Weisungsrechte eingeräumt?
- Werden uns (ohne Zusatzkosten) wirksame Kontrollrechte eingeräumt?
- Gelten für bereits benannte Subunternehmer entsprechende Anforderungen? Dürfen weitere Subunternehmer nur mit unserem Einverständnis beauftragt werden?
- Besteht eine vertragliche Verpflichtung die TOM zu beschreiben und kostenneutral fortzuschreiben („Stand der Technik“). Hat der AV einen Datenschutzbeauftragten? Führt der AV ein Verarbeitungsverzeichnis und stellt er uns dieses ggf. zur Verfügung?
- Bestehen Mitwirkungspflichten bei Auskunftserteilung, Datenpannenmeldungen und Datenschutzfolgeabschätzungen?
- Gibt es eine angemessene Haftungsregelung für Verstöße beim AV, die zumindest eine Haftpflichtversicherung mit angemessener Deckungssumme garantiert?

Fazit:

Perspektivwechsel bei der justiziellen Datenverarbeitung:

Spätestens mit der Einführung der elektronischen Akte und des elektronischen Rechtsverkehrs – nicht vorrangig durch die DSGVO und ihre Umsetzung im nationalen Recht – sollte sich die Justiz ihre eigene Rolle als datenverarbeitende Organisation bewusst machen.

Datenschutz im justiziellen Kontext ist nicht mehr nur im Hinblick auf die Ziele einer sicheren IT-Infrastruktur und der Abwehr von Eingriffen in die richterliche Unabhängigkeit zu sehen.

Vielmehr erhebt die Justiz selbst zahlreich (nicht selten sensible) personenbezogenen Daten von Beteiligten wie auch von Unbeteiligten. Die zunehmende Möglichkeit der strukturierten Durchsuchung und Analyse von elektronisch gespeicherten Daten steigert zugleich das Bedürfnis nach der Gewährleistung datenschutzrechtlicher Grundsätze.


Der Verhandlungsbeginn
verzögert sich um einige Minuten.
Wir haben noch ein kleines
Softwareproblem...
Ungültiges
Passwort.
Noch1Versuch
bexte

Herzlichen Dank

für

Ihre Aufmerksamkeit!

Ihr Ansprechpartner: Ltd. Ministerialrat Gregor Eisenhuth (Gregor.Eisenhuth@stmj.bayern.de)