GDD Erfa-Kreis Wuppertal

147. Erfa-Kreis-Sitzung am 08.06.2016, 14:00 – 16:40 Uhr

Teilnehmer:
Frau Guth
Herr Bittorf
Herr Däumer
Herr Dr. Voßbein
Herr Hilbert
Herr Hinz
Herr Pater
Herr Schumacher
Herr Thomas
Herr Tillmanns
Herr Karusseit

Protokoll

Herr Bittorf

EU-Datenschutz-Grundverordnung – Vortrag von Herrn Schumacher

Herr Schumacher stellte anhand einer Präsentation des GDD die Grundlagen der EU-Datenschutz-Grundverordnung (DS-GVO) dar. Herr Dr. Voßbein wird die Folien den Mitgliedern über das E-Forum zur Verfügung stellen.

Das Ziel der DS-GVO ist es europaweite Standards für den Datenschutz zu setzten und Regeln für den digitalen Binnenmarkt zu schaffen. Wichtige Grundsätze sind die Vermeidung von „Forum-Shopping" (Datenverarbeitung im Land mit den niedrigsten Datenschutzanforderungen in der EU, z.Zt. Irland) und „One-Stop-Shop" (eine zuständige Aufsichtsbehörde für ein Unternehmen). Die Kooperation der Datenschutzaufsichtsbehörden soll verbessert werden und das Datenschutzrecht EU-weit konsistent angewendet werden.

Die DS-GVO gilt unmittelbar und muss nicht, wie eine Richtlinie, in nationales Recht umgesetzt werden. Im Nicht-öffentlichen Bereich führt die Grundverordnung zu einer Vollharmonisierung, im öffentlichen Bereich hat sie Richtliniencharakter. In einigen Bereichen gibt es Öffnungsklauseln für nationale Gesetzgeber, so zum Beispiel beim Beschäftigtendatenschutz.

Anpassungsbedarf gibt es neben dem Beschäftigtendatenschutz (§ 32 Bundesdatenschutzgesetz BDSG) auch bei der Regelung zum

Datenschutzbeauftragten (§ 4f BDSG), der Datenschutzaufsicht (§ 38 BDSG) und bei den Sanktionen (§ 44 BDSG) sowie in weiteren Bereichen.

Die wesentlichen Inhalte der DS-GVO sind in den Artikeln 5 (Grundsätze für die Verarbeitung personenbezogener Daten) und 6 (Rechtmäßigkeit der Verarbeitung) zu finden. Wichtig ist insbesondere die Rechenschaftspflicht der für die Verarbeitung verantwortlichen Stelle, die in Artikel 5 Abs. 2 geregelt ist („Accountability").

Neue Regelungen finden sich unter anderem in den Artikeln 20 (Datenportabilität) und 17 Abs. 2 (Recht auf Vergessenwerden).

Die Datenschutz-Organisation ist in den folgenden Artikeln geregelt:

Technische Absicherung: Art. 25, 32

Organisatorische Absicherung Art. 24-31, 33-36

Überwachung durch den Datenschutzbeauftragten (DSB): Art 37-39

Die Schlagworte „Privacy by Design" und „Privacy by Default" sind in Artikel 25 zu finden. Ein Nachweis der Erfüllung dieser Anforderungen ist über Zertifikate (Artikel 42) möglich.

Unternehmen mit mehr als 250 Mitarbeitern müssen ein Verzeichnis der Verarbeitungstätigkeiten führen, das in etwa dem Verfahrensverzeichnis nach BDSG entspricht.

Diskussion im Kreis der Teilnehmer

Herr Thomas brachte das Thema „Treu und Glauben" zur Sprache, das seinen Weg in die DS-GVO gefunden hat. Der Begriff „Treu und Glauben" war schon in der Richtlinie 95/46/EG enthalten, ist aber vom deutschen Gesetzgeber nie in das BDSG übernommen worden. *„Treu und Glauben ist ein unbestimmter Rechtsbegriff der Rechtswissenschaft und bezeichnet das Verhalten eines redlich und anständig handelnden Menschen."* (Quelle deutsche Wikipedia). Herr Dr. Voßbein erläuterte, dass dieser Grundsatz insbesondere Rechtsmissbrauch verhindern kann.

Herr Tillmanns sprach das Themenbereich „Safe Harbor / Standardvertragsklauseln / EU-US-Privacy Shield" an. In der Diskussion herrschte Einigkeit darüber, dass die gleichen Argumente, die gegen Safe Harbor sprechen, auch gegen das EU-US-Privacy Shield gültig sind.

Herr Dr. Voßbein brachte eine Folie mit dem Titel „Was ist zu tun" in die Diskussion ein. Thema war die Umsetzung der DS-GVO in den Unternehmen.

- Erhebung Ist-Zustand
    - Prozesse, Rechtsgrundlagen, Organisation
    - Identifizierung von Lücken

- Aufbau/Überarbeitung/Dokumentation
- Anpassung von Prozessen und Verträgen
- Umsetzung der Anforderungen an die IT-Sicherheit
- Schulung der Mitarbeiter
- Anpassung interner Regelungen
- Umsetzung der Informationspflichten / Rechte der Betroffenen

Herr Dr. Voßbein betonte in der weiteren Diskussion, dass in der Liste keine zeitliche Reihenfolge vorgegeben ist.

Herr Tillmanns vertrat die These, dass durch die DS-GVO von jedermann ein Informations-Sicherheits-Management-System (ISMS) gefordert wird. Nach seiner Beobachtung war bisher der Datenschutz eher ein „Compliance Anhängsel" im Rahmen eines ISMS.

Herr Dr. Voßbein betonte, dass durch die DS-GVO die Risiken für Unternehmen steigen und präsentierte in diesem Zusammenhang eine Folie zur Risikobetrachtung.

- Strafbarkeit
- Bußgeldrahmen
- Image
- Verstoß gegen Compliance
- gesamtschuldnerische Haftung
- erweiterter Aufgabenbereich der Behörden
- partiell persönliche Haftung
- sonstige Sanktionen

Datenschutzverstöße können laut Herrn Dr. Voßbein nicht ausgeschlossen werden und die Risiken müssen daher auch betrachtet werden.

Herr Thomas wies darauf hin, dass auch nach seiner Einschätzung das Risiko für Unternehmen steigen wird, weil Aufsichtsbehörden aufgrund des neuen europäischen Rechtsrahmens gezwungen werden Strafen auch tatsächlich zu verhängen.

Herr Tillmanns sprach das Thema BREXIT an. *Brexit ist ein Kunst- und Kofferwort aus „Britain" und „Exit"; es steht für einen möglichen Austritt Großbritanniens aus der Europäischen Union (EU).* (Quelle deutsche Wikipedia). Er betonte in diesem Zusammenhang die Risiken für Auftraggeber, die Dienstleister aus Großbritannien bei der Datenverarbeitung einsetzen.

Es wurde darüber diskutiert, ob die öffentliche Hand im Bereich Datenschutz/Compliance schlechter aufgestellt ist, als die freie Wirtschaft. Herr Dr. Voßbein vertrat diese These, Herr Hilbert konnte sie aus seiner praktischen Erfahrung bestätigen.

Herr Dr. Voßbein stellte heraus, dass IT Sicherheit ein Wert an sich ist. Die DS-GVO verweist indirekt auf die 27000er Normenfamilie. Die 27000er Normen skalieren deutlich besser als der IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Herr Thomas berichtete von seiner Beobachtung, dass die DS-GVO besser strukturiert ist, als das BDSG. Herr Dr. Voßbein relativierte diese Aussage und verwies darauf, dass zur DS-GVO im Rahmen von Öffnungsklauseln noch weitere Rechtsnormen hinzukommen werden.

Herr Dr. Voßbein führte aus, dass zwei Jahre ein Zeitrahmen sind, in dem man das Projekt „Umstellung auf die DS-GVO" auch in größeren Organisationen sinnvoll umsetzen kann. Eine Umsetzung ist nur mit Rückendeckung der Geschäftsführung möglich. Herr Dr. Voßbein stellte heraus, dass viele Themen, die in den Medien heiß diskutiert werden, für den Großteil der Unternehmen von geringer Bedeutung sind. Als Beispiele nannte er die Themen Datenportabilität und das Marktortprinzip.

Herr Thomas fragte nach, wie der Begriff „Dritter" im Rahmen der DS-GVO definiert ist. Insbesondere fragte er, ob Mitarbeiter, die nicht befugt sind personenbezogene Daten zu verarbeiten, als Dritte gelten. Als Beispiel für solche Fälle nannte er fehlgeleitete E-Mails. Herr Dr. Voßbein vertrat die Auffassung, dass unbefugte Mitarbeiter als Dritte zu betrachten sind. Herr Hilbert nannte als weiteres Beispiel in diesem Zusammenhang fehlgeleitete Briefe, z.B. wenn versehentlich zwei Anschreiben in einem Umschlag versendet werden.

Herr Thomas fragte, ob es eine Ausarbeitung zur DS-GVO gibt, in der die Erwägungsgründe den Artikeln zugeordnet sind. Herr Dr. Voßbein verwies auf eine entsprechende Dokumentation des GDD. Herr Bittorf wies auf die Ausarbeitung von Herrn Hülsmann hin, die man unter folgender URL herunterladen kann.

https://extdsb.wordpress.com/2016/05/23/dsgvo-synopse-mit-gegenueberstellung-der-artikel-und-erwaegungsgruende-sowie-vergleichbarer-bdsg-regelungen-erschienen/

Abschließend wies Herr Dr. Voßbein auf neue Veröffentlichungen von Datakontext hin.

- RDV: unter rdv-online.de gibt es eine umfangreiche Onlinepräsenz
- „Praxishilfe Datenschutz DS-GVO" wird allen GDD-Mitgliedern kostenlos zur Verfügung gestellt
- „Praxisfälle Datenschutz" in aktualisierter Fassung Mitte 2016
- „Handbuch Arbeitnehmerdatenschutz" (neue Fassung)
- „Handbuch Gesundheits- und Sozialpflege" (neue Fassung)
- „Handbuch Datenschutz am Arbeitsplatz" (neue Fassung)
- „Datenschutzaudit nach BSI-Grundschutz" (neue Fassung)

- „Projektbox zu § 42a BDSG“

Wer Interesse an Postern des GDD hat wendet sich bitte an Herrn Dr. Voßbein.

Wer Fragen an die Landesbeauftragte für Datenschutz und Informationsfreiheit hat, die in der Veranstaltung am 21.09.2016 gestellt werden sollen, wendet sich ebenfalls an Herrn Dr. Voßbein.

Am 21.09.2016 findet eine gemeinsame Veranstaltung der Erfa-Kreise Wuppertal, Dortmund, Essen und Düsseldorf-Krefeld statt.

Die nächste reguläre Sitzung findet am 23.11.2016 statt.

Protokoll
Georg Karl Bittorf