200 JAHRE 1818 2018

UNIVERSITÄT HOHENHEIM

UNIVERSITÄT HOHENHEIM

Gesetzgebung als gemeinsame Basis für Datensicherheit und Datenschutz

Dr. Robert Formanek

UNIVERSITÄT HOHENHEIM

European Parliament

Ten issues to watch in 2018

IN-DEPTH ANALYSIS

EPRS | European Parliamentary Research Service
Author: Étienne Bassot
Members' Research Service
January 2018 — PE 614.650

UNIVERSITÄT HOHENHEIM

TABLE OF CONTENTS

UNIVERSITÄT HOHENHEIM

- EU steps to curb influence campaigns
- Growing international cooperation amid increased hybrid threats
- Cybersecurity: **a shift towards increased regulation**

  […] At the EU level, two key legal instruments will enter into force in May 2018: the **Network and information Security (NIS) Directive** and the **General Data Protection Regulation (GDPR)** […] In October 2017, **MEPs adopted a resolution** on the fight against cybercrime, urging Member States to invest more in cybersecurity to prevent […]

UNIVERSITÄT HOHENHEIM

Verfahren : 2017/2068(INI)

Werdegang im Plenum

Entwicklungsstadium in Bezug auf das Dokument : A8-0272/2017			
Eingereichte Texte : A8-0272/2017	Aussprachen : PV 02/10/2017 - 17 CRE 02/10/2017 - 17	Abstimmungen : PV 03/10/2017 - 4.6	Angenommene Texte : P8_TA(2017)0366

Angenommene Texte

253k

Dienstag, 3. Oktober 2017 - Straßburg — Vorläufige Ausgabe

Bekämpfung der Cyberkriminalität — P8_TA-PROV(2017)0366 — A8-0272/2017

Entschließung des Europäischen Parlaments vom 3. Oktober 2017 zur Bekämpfung der Cyberkriminalität (2017/2068(INI))

Das Europäische Parlament,

11. verurteilt aufs Schärfste jedweden Eingriff in Systeme, der von einem fremden Staat oder dessen Agenten vorgenommen oder gesteuert wird, um demokratische Prozesse in einem anderen Land zu stören;

12. betont, dass grenzübergreifende Aufforderungen zum Domänendiebstahl, zum Entfernen von Inhalten und zum Zugriff auf Nutzerdaten schwierige Herausforderungen darstellen, auf die umgehend reagiert werden Menschenrechte, die sowohl für die Online-Welt als auch im wirklichen Leben gelten, als wichtiger Maßstab auf globaler Ebene dienen;

13. fordert die Mitgliedstaaten auf, dafür zu sorgen, dass die Opfer von Cyberangriffen die in der Richtlinie 2012/29/EU verankerten Rechte in vollem Umfang in Anspruch nehmen können; fordert die Mitgliedstaaten au sie die Europol-Arbeitsgruppe zur Identifizierung von Opfern auch künftig unterstützen; fordert die Mitgliedstaaten auf, in Zusammenarbeit mit Europol umgehend entsprechende Plattformen einzurichten, damit alle Inter Kommission auf, auf der Grundlage der Richtlinie 2012/29/EU eine Studie zu den Auswirkungen der grenzübergreifenden Cyberkriminalität auszuarbeiten;

14. betont, dass im Europol-Bericht 2014 über die Bewertung der Bedrohungslage im Bereich der organisierten Kriminalität – unter Berücksichtigung der bestehenden Beschränkungen der Verfahren im Rahmen von R darin zudem eine weitergehende Harmonisierung der Rechtsvorschriften in der EU empfohlen wird, soweit hierfür Bedarf besteht;

15. hebt hervor, dass Cyberkriminalität das Funktionieren des digitalen Binnenmarkts gravierend beeinträchtigt, da sie das Vertrauen in die Anbieter digitaler Dienste schmälert, die Sicherheit grenzübergreifender Trans

16. betont, dass Strategien und Maßnahmen im Bereich Cybersicherheit nur dann tragfähig und wirksam sein können, wenn die Cybersicherheit auf den in der Charta der Grundrechte der Europäischen Union verankei

17. erachtet es als berechtigterweise und dringend geboten, die Kommunikation zwischen Privatpersonen sowie zwischen Privatpersonen und öffentlichen und privaten Organisationen zu schützen, um der Cyberkrimi betont außerdem, dass durch eine Einschränkung der Verwendung oder eine Schwächung der Leistung von Verschlüsselungswerkzeugen Schwachstellen, die zu kriminellen Zwecken ausgenutzt werden können, gesc gleichermaßen schadet;

UNIVERSITÄT HOHENHEIM

2017/0225 (COD)

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über die „EU-Cybersicherheitsagentur“ (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik („Rechtsakt zur Cybersicherheit“)

UNIVERSITÄT HOHENHEIM

Einführung

- Komplexe Gesetzgebung gestaltet Datenschutz und Datensicherheit zunehmend anspruchsvoller – werden juristische Kenntnisse für IT-Leiter, Datenschutzbeauftragte, IT-Sicherheitsbeauftragte und Administratoren „unabdingbar“?
- Datenschutz, IT-Sicherheit, IT-Leitung ➔ Wie kann oder soll mit unterschiedlicher Zielsetzung umgegangen werden?
- Welche konkreten Handlungen sind notwendig?
- Welche „pragmatischen“ Ansätze gewährleisten rechtliche Vorgaben?

UNIVERSITÄT HOHENHEIM

EU-Datenschutzgrundverordnung – EU-DSGVO

Die EU-DSGVO sieht ein Datenschutzkonzept sowie ein Risikomanagement vor und gilt ab 25. Mai 2018:

- http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679

Berichtigung der Artikel 28, 30, 33

- http://data.consilium.europa.eu/doc/document/ST-12399-2016-INIT/en/pdf

Ebenfalls ab 25. Mai 2018 gilt das Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU, welches spezifische Vorschriften (mit Kollisionsregelung) beinhaltet:

- https://dsgvo-gesetz.de/bdsg-neu/

UNIVERSITÄT HOHENHEIM

EU-DSGVO

Folgende Gesetze verlieren zum 25. Mai 2018 ihre Gültigkeit:

- §§ 11-15a Telemediengesetz
- §§ 22 und 23 Kunsturhebergesetz
- Abweichende Regelungen aus BDSG, LDSG, EKD, KDG

Folgende Gesetze gelten auch über den 25. Mai 2018 hinaus:

- Datenschutzregelungen Telekommunikation (Art. 95, RL 2002/58/EG und ePrivacy-VO)
- Datenschutzregelungen der Hochschulgesetze (Art. 6 Abs. 3 EU-DSGVO)

UNIVERSITÄT HOHENHEIM

EU-DSGVO

- Ziele der EU-DSGVO sind

  - Rechtmäßigkeit, Treu und Glauben, Transparenz (Abs. 1a);
  - Zweckbindung (Abs. 1b);
  - Datenminimierung (Abs. 1c);
  - **Richtigkeit** (1d);
  - Speicherbegrenzung (1e);
  - **Sicherheit**, Integrität, Vertraulichkeit (1f);
  - **Rechenschaftspflicht** (Abs. 2).

UNIVERSITÄT HOHENHEIM

EU-DSGVO

- Das Verhältnis von Datenschutz und IT-Sicherheit bringt Artikel 32 EU-DSGVO zum Ausdruck. Unternehmen werden demnach verpflichtet, geeignete IT-Sicherheitsmaßnahmen „unter Berücksichtigung des aktuellen Stands der Technik“ zu ergreifen, um so ein „dem Risiko angemessenes Schutzniveau“ zu gewährleisten.
- Die Vorgaben zur **Sicherheit der Verarbeitung** werden auch in anderen Artikeln (u. A. in Artikel 5, 6, 24, 25, 33, 35) festgelegt.
- Es gilt demnach einen „risikobasierten“ Ansatz zu etablieren, welcher eine regelmäßige Bewertung und Überprüfung der getroffenen Maßnahmen beinhaltet.

UNIVERSITÄT HOHENHEIM

EU-DSGVO

- Art. 5 Abs. 2: „Der Verantwortliche ist für die Einhaltung des Abs. 1 [Datenschutzgrundsätze] verantwortlich und muss dessen Einhaltung nachweisen können.“

i. V. m.

- Art. 24 Abs. 1: „Der Verantwortliche setzt … geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt.“

➔ Erhöhte Anforderungen an Informationspflichten (Dokumentation) und Rechenschaftspflicht nebst Benachrichtigung der Aufsichtsbehörden und Betroffener bei „data breaches“.

UNIVERSITÄT HOHENHEIM

EU-DSGVO

- Art. 25 Abs. 1 – Privacy by design durch den Verantwortlichen (ErwGr. 78: „[….] *sollten* die Hersteller der Produkte, Dienste und Anwendungen *ermutigt* werden, das Recht auf Datenschutz bei der Entwicklung und Auslegung der Produkte, Dienste und Anwendungen zu berücksichtigen“.)
    - Festlegung der Mittel (z. B. Produktauswahl).
    - Eigentliche Verarbeitung (Customizing, Gestaltung).
    - Kriterien: Stand der Technik, Kosten, Art, Umfang, Umstände, Zwecke, Eintrittswahrscheinlichkeiten.

UNIVERSITÄT HOHENHEIM

EU-DSGVO

- Art. 25 Abs. 2 – Privacy by default
  - Verpflichtet ist auch in diesem Fall der Verantwortliche.
  - „Freundliche“ Voreinstellung der „unbedingt“ erforderlich personenbezogenen Daten (pbD).
  - Menge, Umfang der Verarbeitung, Speicherfrist, Zugänglichkeit.
  - Zugänglichkeit für Allgemeinheit nicht ohne Eingreifen des Betroffenen.

UNIVERSITÄT HOHENHEIM

EU-DSGVO

- Anmerkung zu ErwGr 78.
  - Der Verantwortliche legt interne Strategien fest um die Einhaltung der Verordnung nachweisen zu können und ergreift Maßnahmen, die insbesondere den Grundsätzen des Datenschutzes durch Technik und datenschutzfreundliche Voreinstellungen Genüge tun.

➔ Definition und Ansprechpartner aller Prozesse dokumentieren!

UNIVERSITÄT HOHENHEIM

EU-DSGVO

- Art. 32 – Sicherheit der Verarbeitung
  - Der „Verantwortliche und der Auftragsverarbeiter“ ist gefordert „geeignete technische und organisatorische Maßnahmen zu gewährleisten“.
  - Kriterien: Stand der Technik, Kosten, Art, Umfang, Umstände, Zwecke, Eintrittswahrscheinlichkeiten, ein „dem Risiko angemessenes Schutzniveau“.

UNIVERSITÄT HOHENHEIM

Exkurs: Stand der Technik (BSI-Gesetz)

Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit gesichert *erscheinen* lässt.

UNIVERSITÄT HOHENHEIM

Exkurs: Stand der Technik (BSI-Gesetz)

- Sie müssen sich selbst auf „dem Laufenden“ halten.
- Es gilt den Schutzbedarf im Detail zu erheben und zu entscheiden, welche Technologie umgesetzt werden muss.
- Zu den individuellen Details können das BSI, einschlägige Fachverbände und Aufsichtsbehörden herangezogen werden.

➔ Eine sinnvolle Kombination aus *bewährten* und *innovativen* Technologien erscheint angemessen und ist, vor allem im Eigeninteresse, umsetzbar.

UNIVERSITÄT HOHENHEIM

EU-DSGVO

- Art. 32 – Sicherheit der Verarbeitung
  - Pseudonymisierung & Verschlüsselung.
  - Sicherstellung der **Vertraulichkeit**, **Integrität**, **Verfügbarkeit** und **Belastbarkeit** (Resilienz) der Systeme und Dienste.
  - Wiederherstellung der Verfügbarkeit.

UNIVERSITÄT HOHENHEIM

EU-DSGVO

- Gemäß Artikel 42 EU-DSGVO haben Einrichtungen die Möglichkeit die Einhaltung der datenschutzrechtlichen Vorgaben durch Zertifizierung nachzuweisen.
- Eine regelmäßige **Überprüfung**, **Bewertung** und **Evaluierung** der Wirksamkeit der technischen und organisatorischen Maßnahmen durch **Zertifizierung** zur Erfüllung der Anforderungen ergibt sich aus Art. 24 Abs. 2, Art. 25 Abs. 3, Art. 28 Abs. 5 und Art. 32 Abs. 3.

➔ Schwachstellenmanagement

UNIVERSITÄT HOHENHEIM

EU-DSGVO – Konkrete Beispiele

- Aktualisierungs-Kadenz: Wie viele Sicherheitslücken existieren in Ihrem System? Wie viele davon müssen noch gepatcht werden?
- WannaCry Ransomware ist ein Beispiel wie Social Engineering für Organisationen ein enormes Risiko darstellen kann.
- Notwendige Kenntnis zu Sicherheitseinstellungen und vorhandener Schwachstellen.
- Existiert *Hacker-Chatter* in einschlägigen Foren (Darknet)?

UNIVERSITÄT HOHENHEIM

EU-DSGVO – Konkrete Beispiele

Bedrohung	EU-DSGVO-Artikel	Anmerkung
Aktualisierungs-Kadenz	24, 25, 32, 35 und 39.	Laufende Überwachung und regelmäßige Bewertungen.
Endsysteme-Sicherheit	18, 24, 25, 32, 35 und 39.	IoT beachtet?
"Social Engineering"	18, 24, 25, 32, 35, 39 und 40.	Aufklärung, Schulung, etc.
Netzwerksicherheit	25, 32, 33 und 34.	z. B. Perimeter-Kontrolle, Schwachstellenanalyse, etc.
"Hacker-Chatter"	18, 24, 25, 32, 35, 39 und 40.	Ist Ihre Einrichtung in "gängigen" Foren Tagesgespräch?
Anwendungssicherheit	18, 24, 25, 32, 33, 34, 35 und 39.	Patchen, Patchen, Patchen, Patchen, …

UNIVERSITÄT HOHENHEIM

Fazit zur Umsetzung

- Pseudonymisierung und Verschlüsselung von pbD.
- Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste sicherstellen.
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM.

UNIVERSITÄT HOHENHEIM

Fazit zur Umsetzung

Die EU-DSGVO erfordert ein präventives und iteratives Vorgehen aufeinander abgestimmter Maßnahmen. Hierzu können die folgenden Maßnahmen-kataloge als Grundlage dienen:

- ISO/IEC FDIS 29151:2016: Leitfaden für den Schutz pbD
- DIN ISO/IEC 27001:2015: Anhang A
- DIN ISO/IEC 27002:2016 (als *Richtschnur* zur Auslegung von Maßnahmen)
- BSI IT-Grundschutz-Kompendium

UNIVERSITÄT HOHENHEIM

Protokollierung

Zur Erhebung und Verarbeitung von Protokolldateien gem. Art. 6 Abs. 1 lit. F EU-DSGVO i. V. m. ErwGr 49 (die Verarbeitung von (pbD) […] stellt in dem Maße ein berechtigtes Interesse […] dar, wie dies für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig ist, d. h., soweit dadurch die Fähigkeit eines Netzes oder Informations-systems gewährleistet wird […]).

➔ Eine Protokollierung (Verarbeitung pbD) ist demnach *(und nur dann)* rechtmäßig, wenn sie erforderlich ist.

UNIVERSITÄT HOHENHEIM

Protokollierung

Grundrechte, Interessen und „vernünftige Erwartung“ betroffener Personen:

- Angreifer: hat keine überwiegenden Interessen …
- Beschäftigte, Kunden, etc.:
  - Erwartung, dass Netzwerkverkehr auf Bedrohungen überprüft wird.
  - Interesse, dass Webseiten oder IP-Adressen nicht gespeichert werden.
  - Beschäftigte erwarten gem. § 87 Abs. 1 Nr. 6 BetrVG keine Überwachung des Verhaltens oder der Leistung.

UNIVERSITÄT HOHENHEIM

Protokollierung

Abwehr von Sicherheitsrisiken wie z. B.:

- Verlust von Informationen durch Ausspähen und Übermittlung an nichtautorisierte Dritte (z. B. APT, Online-Skimming).
- Verletzung des Schutzes personenbezogener Daten (Art. 4 Nr. 12 EU-DSGVO).
- Erfüllung der Meldepflicht nach Art. 33 EU-DSGVO.
- Gefährdung der IT-Systeme (z. B. durch Command-and-Control-Server oder Bot-Malware).
- Gefährdung des Netzes (z. B. DoS-Attacken).
- Verbreitung von Spam oder Schadsoftware.

UNIVERSITÄT HOHENHEIM

Protokollierung

Interessenabwägung zugunsten von IT-Sicherheit bei gleichzeitiger Begrenzung der Datenerhebung und -verarbeitung auf das Erforderliche durch

- Anonymisierung / Pseudonymisierung.
- Automatisierte Überprüfung in Echtzeit.
- Speicherung für max. 7 Tage (Nur bei Bedrohungserkennung längere Speicherung und Verarbeitung zulässig).
- Unverzügliche Löschung pbD nach Abwehr oder Beseitigung der Störung.
- Information des Betroffenen.
- Einbindung des Datenschutzbeauftragten.

UNIVERSITÄT HOHENHEIM

Fazit zur Protokollierung

- Notwendig zur Gewährleistung von Netz- und Informationssicherheit.
- Abwehr von Angriffen, Störungen und widerrechtlichen Eingriffen.
- Schutz vor Beeinträchtigung der Belastbarkeit, Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit.
- Umsetzung der Verpflichtungen aus Art. 32 EU-DSGVO.

UNIVERSITÄT HOHENHEIM

Und wer macht was?

IT-Sicherheit

Datenschutz

IT-Leitung

UNIVERSITÄT HOHENHEIM

Und wer macht was?

Konzeptionelle Verantwortung von Leitung, DSB, SIB und IT-Leitung				
		DSB	**SIB**	**IT-Leitung**
1.	Einführung eines Sicherheitskonzeptes			
2.	Einführung eines Datenschutzkonzeptes			
6.	CIA-Maßnahmen			

UNIVERSITÄT HOHENHEIM

Und wer macht was?

Operative Verantwortung von Leitung, DSB, SIB und IT-Leitung				
		DSB	SIB	IT-Leitung
1	Datenschutzrechtliche Konformität			
2	SPAM- und Viren-Filtern beurteilen			
3	Generische Richtlinien			
4	Verhinderung von Schädigung Dritter durch "eigene IT"			
5	"Virenfreier" Datenaustausch			
6	Datensicherung			
7	Verwendung „legaler“ Software			
8	Beachtung von Urheberrechte			

UNIVERSITÄT HOHENHEIM

Fazit

- Datenschutz kann nicht allein durch normative Vorgaben gewährleistet werden.
- Datensicherheit ist daher von entscheidender Bedeutung, da sich die EU-DSGVO spezifisch an die CIA wendet und einen risikobasierten Ansatz für Sicherheit und Risikominimierung erfordert.

➔ Organisieren Sie die Umsetzung der EU-DSGVO als KVP-Initiative.

➔ Etablieren Sie ein **iDIMS** (integriertes Datenschutz und Informations-sicherheitsmanagementsystem).

UNIVERSITÄT HOHENHEIM

Fazit

Datenschutz = Qualitätsfaktor

IT-Sicherheit = Notwendiges Fundament für Datenschutz

➔ **Datenschutz & IT-Sicherheit = Gewichtiger Wettbewerbsfaktor** ➔

UNIVERSITÄT
HOHENHEIM

87

UNIVERSITÄT HOHENHEIM

Dr. Robert Formanek

robert.formanek@uni-hohenheim.de