IT-Sicherheitsrechtstag 2017

Gemeinsame Veranstaltung von TeleTrusT und BvD

Berlin, 07.11.2017

Wenn die Aufsichtsbehörde klingelt: Wie läuft eine Prüfung ab?

Dr. Philipp Stroh
Berliner Beauftragte für Datenschutz und Informationsfreiheit

Stichtag 25. Mai 2018

Hinweise zur (künftigen) Prüfpraxis der Aufsichtsbehörden

Dr. Philipp Stroh, Berliner Beauftragte für Datenschutz und Informationsfreiheit

IT-Sicherheitsrechtstag 2017

Agenda

- Aufgaben und Befugnisse der Aufsichtsbehörden
- Aus der Prüfpraxis (insbesondere Vor-Ort-Prüfung)
- Aus der Sanktionsstelle

AUFGABEN UND BEFUGNISSE DER AUFSICHTSBEHÖRDEN

Aufgaben und Befugnisse der Aufsichtsbehörden

BDSG

- Kontrolliert die Ausführungen von Datenschutzvorschriften, § 38 Abs. 1 Satz 1 BDSG
- Beratung DSB und verantwortlicher Stellen, § 38 Abs.1 Satz 2 BDSG

DSGVO

- Überwachung und Durchsetzung der DSGVO, Art. 57 Abs. 1 lit. a
- Sich mit Beschwerden befassen (lit. f)
- Sensibilisierung der verantw. Stellen (lit. d); Zusammenarbeit mit DSB (Art. 39 Abs. 1 lit.d)

Aufgaben und Befugnisse der Aufsichtsbehörden

BDSG

- Verhängung von Verwarnungen, Bußgeldern
- Bei Datenschutzverstoß: Unterrichtung Betroffener, Anzeige bei den für die Ahndung zuständigen Stellen bzw. bei der Gewerbeaufsicht, § 38 Abs. 1 Satz 6 BDSG
- Veröffentlichung des Tätigkeitsbericht, § 38 Abs. 1 Satz 7 BDSG

DSGVO

- Umfangreiche Abhilfebefugnisse in Art. 58 DSGVO
- Erstellung und Veröffentlichung des Tätigkeitsberichtes, Art. 59 DSGVO

Aufgaben und Befugnisse der Aufsichtsbehörden

BDSG

- Führt Register der meldepflichtigen automatisierten Verarbeitungen, § 38 Abs. 2 i. V. m. § 4d BDSG
- Vor-Ort-Prüfung und Einsichtnahme, § 38 Abs. 4 BDSG
- Anordnungen, § 38 Abs. 5 BDSG

DSGVO

- Klassifizierung von Verarbeitungsvorgängen hins. Datenschutz-Folgenabschätzung (lit. k)
- Zugangs- und Informationsrecht der AB, Art. 58 Abs. 1 lit. e)
- Anordnungsbefugnisse in Art. 58 Abs. 2 DSGVO

Und was macht die Aufsichtsbehörde noch?

BDSG

- Publikationen, Teilnahme an Seminaren, Workshops
- Beratung der Bürgerinnen und Bürger, Gesetzgeber (DSG Land)

- Amtshilfe (§ 38 Abs. 1 Satz 6 BDSG), Kooperation mit anderen Aufsichtsbehörden, u. a. Erstellung von Orientierungshilfen

DSGVO

- Öffentlichkeitsarbeit (Art. 57 lit. b)

- Beratung des Gesetzgebers (lit. c)
- Sensibilisierung verantw. Stelle und AN (lit. d)

- Zusammenarbeit mit anderen Aufsichtsbehörden und Amtshilfe (lit. g)

AUS DER PRÜFPRAXIS

Prüfung

⇒ Kunden beschweren sich

⇒ Mitarbeiter melden (oft anonym) Datenschutzverstöße

⇒ Betriebsräte/ Personalräte wenden sich an uns

⇒ Medien berichten über "Datenskandale"

⇒ Anlassfrei: keine einheitliche Auswahl von Branchen und Unternehmen (Behörde entscheidet selbst)

Auskunftspflicht

⇒ Erforderliche Auskünfte sind unverzüglich zu erteilen

⇒ Aussageverweigerungsrecht für Auskunftspflichtigen bzw. in §383 Abs. 1 Nr. 1-3 ZPO genannten Angehörigen bei Gefahr strafgerichtlicher Verfolgung oder eines OWi-Verfahrens

⇒ Aufsichtsbehörde muss einen entsprechenden Hinweis an den Auskunftspflichtigen geben (Belehrung)

⇒ Umfassende Auskunftsplicht bleibt bestehen: Art. 58 Art. 1 Abs. 1 a) und e) DSGVO

Anlassbezogene Prüfung

Anlassfreie Kontrolle

VOR-ORT-PRÜFUNG

Vor-Ort Prüfung

- Ankündigung Termin
- Mindestens zwei Referenten
- Prüfkonzept
- Protokollierung der Prüfung und Möglichkeit der anschließenden Stellungnahme

Ziel: je nach Einzelfall Datenverarbeitung im Unternehmen prüfen, insbesondere Einsichtnahme in datenschutzrelevante geschäftliche Unterlagen

Prüfkonzept

- Hinweise und Belehrung
- Fragen zum Unternehmen (Geschäftszweck, Struktur etc.)
- Verpflichtung aufs Datengeheimnis (Vorlage § 5-Erklärung)
- Fragen zum betrieblichen Datenschutzbeauftragten (ggf. Fachkundeprüfung)
- Vorabkontrollen, Schulungen/Fortbildung etc.
- Verfahrensverzeichnis
- Innerbetriebliche Organisation (Anweisungen etc.)
- Umgang mit Kundendaten, Mitarbeiterdaten (Erhebung, Verarbeitung)
- Notfallkonzept: § 42a BDSG-Meldepflichten
- Auftragsdatenverarbeitung
- Rechte Betroffener (standardisierte Verfahren?, Löschkonzept)
- t-o-Maßnahmen

Verpflichtung auf das Datengeheimnis

BDSG

- § 5 Satz 2 BDSG
- Schriftlichkeit empfohlen
- Erklärungen meist fehlerhaft: keine vollständige Aufklärung über Konsequenzen (auch Owi-Verfahren drohen)
- Hinweisblatt fehlt

DSGVO

- Keine ausdrückliche Pflicht in DSGVO
- Aber t-o Maßnahmen, vgl. Art. 24 EU-DSGVO
- Also: weiterhin empfehlenswert
- Arbeitsgruppe der AB zur Ausarbeitung geplant

Fragen zum Datenschutzbeauftragten

BDSG

- Bestellurkunde
- Unabhängigkeit, Fachkunde ? (ggf. Prüfung der Grundlagen)
- Überprüfung ob DSB Aufgaben wahrnimmt: Vorabkontrollen, Schulungen etc.
- Ausstattung
- Siehe: Beschluss DK 24./25.11.2010

DSGVO

- Art. 37 DSGVO i. V. m. § 38 DSAnpUG-EU
- Bestellpflicht wird beibehalten
- Ausr. Qualifikation und Fachkunde
- Verstärkte Publizität des DSB (Art. 37 Abs. 7 DSGVO)
- Wichtige Rolle bei RFA und vorherige Konsultation (Art. 35 bzw. 36 DSGVO)
- Beachte: WP 243

Datenschutzschulungen

BDSG

- Im Rahmen der Prüfung zum DSB wird nach Schulung, Fortbildung befragt
- Ggf. Vorlage der Schulungsunterlagen

DSGVO

- Artikel 39 Abs. 1 Nr. b DSGVO: Aufgabe des DSB
- Organisatorische Maßnahme, um Einhaltung der Datenschutzbestimmungen nachzuweisen (Art. 24 DSGVO)

Vorabkontrolle/DSFA

BDSG

- § 4d Abs. 5 DSGVO
  - Bei besonderen Arten pb Daten (§ 3 Abs. 9 BDSG)
  - Verarbeitung kann zu einer Bewertung des Betroffenen führen
  - Sofern Einwilligung u. §28 Abs. 1 S. 1 (-)
- Bisher in der Praxis kaum Vorabkontrollen feststellbar

DSGVO

- Art. 35 DSGVO: Verfahren auf Liste der AB, bei hohem Risiko, bei Verarbeitung bes. Kategorien pb Daten, bes. Verfahren
- Beschreibung des Verf., Zwecke, berechtigte Interessen, Bewertung der Notwendigkeit der DV, VHM, Risiken für Betroffenen
- Beschreibung der geplanten Schutzmaßnahmen (und Nachweise)
- WP 248 und Kurzpapier DSK Nr. 5

Verzeichnis der Verarbeitungstätigkeiten

BDSG

- § 4 g Abs. 2 iVm § 4 e S. 1 BDSG
- Jedermann-Verzeichnis, Meldepflicht
- Mängel: nicht alle Personengruppen aufgeschlüsselt; Zuordnung der jeweiligen Daten; Zuordnung Empfänger
- Angaben zu Löschfristen unpräzise
- Drittstaatentransfer nicht erwähnt
- t-o-Maßnahmen unzureichend

DSGVO

- Kein öffentliches Verzeichnis und keine Meldepflicht mehr
- Art. 30 Abs. 5 DSGVO: nicht bei < 250 Mitarbeiter, es sei denn Ausnahme
- Auch Auftragsverarbeiter
- Art. 30 Abs. 1 f) und g): "wenn möglich" (Fristen und t-o-Maßnahmen)
- Muster-Vorlage geplant; Ausfüllhinweise schon online, Kurzpapier DSK Nr. 1

Auftragsdatenverarbeitungsver-träge

BDSG

- Kein ADV geschlossen oder nur minimale Inhalte im Hauptvertrag
- Nicht alle Dienstleistungen erfasst: mangelnde Konkretisierung
- Fehlende Inhalte nach § 11 Abs. 2 BDSG

DSGVO

- Vertragliche Anforderungen, Art. 28 Abs. 3 DSGVO => inhaltliche Vorgaben des § 11 Abs. 2 BDSG finden sich weitgehend wieder (allerdings leichte Abweichungen)
- Konkretisierung der Dienstleistungen
- Neuer Mustervertrag in Arbeit

Meldepflichten bei Datenlecks

BDSG

- Prüfung eines Notfallkonzeptes für rechtswidrige Datenübermittlungen bzw. Prozess zu § 42a BDSG
- Dokumentation § 42a-Fälle (Risikoabwägung)
- In der Praxis relativ wenig Meldefälle
- FAQ zu § 42a BDSG

DSGVO

- Art. 33 DSGVO: deutlich erweiterte Meldepflichten bei Datenschutzverletzung (Art. 4 Nr. 12 DSGVO), aber auch Risikoabwägung
- Knappe Frist (72h)
- Kontrolle ds Notfallkonzepts wird voraussichtlich mehr Bedeutung bekommen
- WP 250

Rechte Betroffener (insbesondere Auskunfts- und Löschprozesse)

BDSG

- Behandlung von Auskunfts- und Löschersuchen: standardisiertes Verfahren?
- Lösch- bzw. Sperrkonzept häufig unzureichend
- Löschfristen werden nicht eingehalten

DSGVO

- §§ 34 bzw. 35 DSAnpUG-EU
- Standardisierte Verfahren zu empfehlen (insb. Bereitstellung)
- Ggf. zentrale Stelle
- Bei Lösch- und Sperrkonzept: präzise Abbildung der Löschregelungen
- Recht auf Vergessenwerden
- Zu Auskunft: DSK Kurzpapier Nr. 6

Mehr Aufmerksamkeit mit Inkrafttreten der DSGVO auf…

- Erweiterte Dokumentations- und Nachweispflichten
  - Rechenschaftspflicht in Art.5 Abs. 2 DSGVO
  - Weitere Dokumentationspflichten u.a. in Art. 28 Abs. 3 lit. a, Art. 33 Abs. 5, 35 DSGVO

- Erweiterte Transparenz- und Informationspflichten
  - Art. 12ff: Informationen sind präzise, leicht zugänglich, leicht verständlich Betroffenen zur Verfügung stellen => Überarbeitung der Datenschutzerklärung
  - Informationspflichten nach Art. 13 und 14 DSGVO (WP "Transparenz" in Arbeit)
  - Kurzpapier DSK Nr. 10

- Recht auf Datenübertragbarkeit (Art. 20 DSGVO)
  - Welche Prozesse sind ggf. vorhanden?
  - WP 242, Kurzpapier DSK Nr. 11

Mehr Aufmerksamkeit mit Inkrafttreten der DSGVO auf…

- Internes Datenschutzmanagementsystem
- Dokumentation der technisch-organisatorischen Maßnahmen zur Datensicherheit (Art. 32 DSGVO)
- Datenschutz durch Technik und datenschutzrechtliche Voreinstellungen (Art. 25 DSGVO)
  - T-o Maßnahmen sowie Verfahren, die eine Einhaltung der datenschutzrechtlichen Vorschriften gewährleisten
  - Verantwortliche Stelle muss sicherstellen, dass Standardeinstellungen darauf ausgerichtet sind, nur die pb Daten zu verarbeiten, welche für den konkreten Zweck benötigt werden

Weitere Informationen

- Working Paper der Artikel 29 Gruppe sind hier abrufbar: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083
- Kurzpapier der DSK sind hier abrufbar: https://www.datenschutz-berlin.de/kurzpapiere.html
- u. a. Tipps zur Erstellung eines Maßnahmenplans (Kurzpapier DSK Nr. 8: Bestandaufnahme, Handlungsbedarf eruieren und Umsetzung bis zum 25. Mai 2018)

AUS DER SANKTIONSSTELLE

Aufsichtsrechtliche Maßnahmen

⇒ Ein Ordnungswidrigkeitenverfahren einleiten (Berlin 2016: insgesamt 24 Buß- und Verwarngelder, 24.020 € festgesetzt)

⇒ Anordnungen treffen (2016: drei Anordnungsverfahren eingeleitet)

⇒ Strafantrag bei der Staatsanwaltschaft stellen (2016: 4 Strafanträge)

Bußgeld

⇒ Formelle Verstöße: § 43 Abs. 1 (z. B. nicht erteilte Auskunft) => bis zu 50.000€

⇒ Materielle Verstöße: § 43 Abs. 2 (z. B. unbefugte Datenerhebung) => bis zu 300.000€

⇒ Grundlage im OWiG: Einspruch möglich, dann Weitergabe an die StA und Entscheidung durch das Amtsgericht

⇒ Unter Umständen: einvernehmliche Lösung mit der Aufsichtsbehörde

Anordnungen nach § 38 Abs. 5 BDSG

⇒ Maßnahmen zur Beseitigung, Satz 1
- ⇒ Festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung
- ⇒ Technischer und organisatorischer Mängel nach § 9 BDSG

⇒ Bei schwerwiegenden Verstößen oder Mängeln, insbesondere bei Gefährdung des Persönlichkeitsrechts, Satz 2
- ⇒ Untersagung der Erhebung, Verarbeitung oder Nutzung ODER Einsatz einzelner Verfahren
- ⇒ Wenn Verstöße oder Mängel trotz Anordnung und
- ⇒ Trotz Verhängung eines Zwangsgeldes in angemessener Zeit nicht behoben

⇒ Abberufung des bDSB verlangen bei mangelnder Fachkunde und Zuverlässigkeit, Satz 3

Rechtsmittel gegen eine Anordnung

⇒ In Berlin: nur Klageerhebung vor dem Verwaltungsgericht (ggf. einstweiliger Rechtsschutz)

⇒ In anderen Bundesländern: Widerspruch und dann Widerspruchsbescheid der Aufsichtsbehörde

⇒ Empfehlung: einvernehmliche Lösung mit der Aufsichtsbehörde

Was ändert sich mit der DSGVO?

- Neue sanktionsrechtliche Abhilfebefugnisse
- Auch gegen Auftragsdatenverarbeiter
- Bußgeldtatbestände ausgeweitet
- Höhe der Bußgelder bemisst sich nach einem deutlich größeren Rahmen (EG 150: funktionaler Unternehmensbegriff)
- Verantwortlichkeit für Datenschutzverstöße werden umgestaltet (EG 150: funktionaler Unternehmensbegriff)
- Pflicht der AB zur Dokumentation von Verstößen
- Leitlinien (WP 253)
- Ggf. Zwischenverfahren (vgl. § 41 Abs. 2 DSANpUG-EU)

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

(030) 13889 - 315
STROH@DATENSCHUTZ-BERLIN.DE