BayLDA

Bayerisches Landesamt für Datenschutzaufsicht

Verhaltensregeln (Codes of Conduct) nach Art. 40 DS-GVO

BvD Herbsttagung

Stuttgart, den 25. Oktober 2018

Mirka Möldner

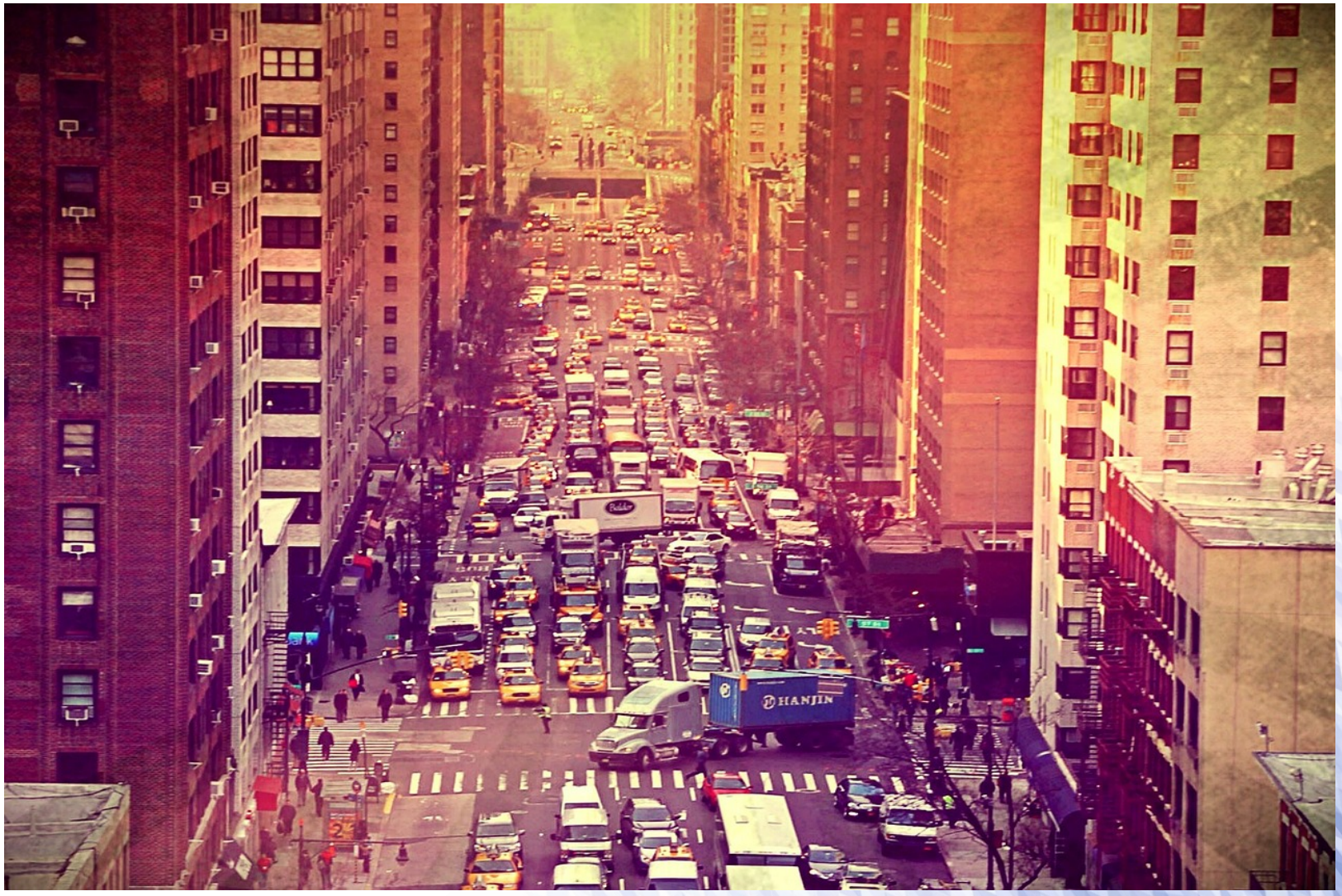
Bayer. Landesamt für Datenschutzaufsicht

Agenda

1. Begriff
2. Sachlicher Anwendungsbereich
3. Funktion
4. Nutzen
5. Rechtliche Grundlagen
6. Verfahren / Inhalt
7. Rechtsfolgen / Rechtliche Auswirkungen
8. Die Kontrollstelle
9. Ausblick

Agenda

Agenda



Agenda

1. Begriff

- Verhaltensregeln im Sinne des Art. 40 DS-GVO sind Normen, auf die sich Verantwortliche oder Auftragsverarbeiter verständigt haben, um in einem bestimmten Bereich zu klären wie eine DS-GVO konforme Verarbeitung auszusehen hat
- Instrument der Selbstregulierung

2. Sachlicher Anwendungsbereich

Was kann in einem CoC konkret geregelt werden?

Siehe Art. 40 Abs. 2 DS-GVO, „beispielsweise“ Präzisierung hinsichtlich

- Faire und transparente Verarbeitung
- Berechtigte Interessen des Verantwortlichen in bestimmten Zusammenhängen
- Pseudonymisierung personenbezogener Daten

2. Sachlicher Anwendungsbereich

- Ausübung der Rechte betroffener Personen
- Maßnahmen / Verfahren gem. Art. 24 und 25
  Maßnahmen für die Sicherheit der Verarbeitung gem. Art. 32
- Datenpannenmeldungen nach Art. 33

…

3. Funktion

- Konkretisierung von Vorschriften (insb. der DS-GVO)
- Detaillierte Regelung wie Verarbeitung in bestimmten Bereich ausgestaltet sein soll
- Instrument der Harmonisierung der Auslegung zwischen den Mitgliedstaaten

4. Nutzen

- Instrument um DS-GVO-compliance zu demonstrieren (siehe z.B. Erwgr. 81 für Zuverlässigkeit d. Auftragsverarbeiters)
- Rechtssicherheit durch feststellenden Verwaltungsakt / Auslegung unbestimmter Rechtsbegriffe
- Möglichkeit auf technische Entwicklungen zeitnah einzugehen
- Kostenreduzierung durch gemeinsames Vorgehen im jeweiligen Sektor (statt Einzellösungen in Unternehmen)
- Erhöhung der Einhaltung des Datenschutzrechts
- Verringerung des Vollzugsdefizits des Datenschutzrechts

5. Rechtliche Grundlagen

- Art. 40, 41 DS-GVO
- Guidelines on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 des Europäischen Datenschutzausschusses (noch nicht verabschiedet)

6. Verfahren

„Das Verfahren der Genehmigung ist unklar, unvollständig, widersprüchlich und äußerst kompliziert geregelt.“

Kühling/Buchner, Kommentar zu DS-GVO / BDSG, 2. Auflage (2018) zu Art. 40, Rn. 23.

Die weiteren Ausführungen beziehen sich auf den Diskussionsstand des heutigen Tages!

6. Verfahren

6. Verfahren

a) Initiativrecht

Gem. Art. 40 DS-GVO

- Verbände
- Andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten

→ Nachweisbarkeit der Vertretungsbefugnis / Repräsentativität

→ Legitimation

Initiativrecht für Konzerne?

6. Verfahren

b) Inhalt(liche Ausgestaltung)

- Klare Bestimmung welche Verarbeitungstätigkeiten geregelt werden
- Klärung: räumlicher Anwendungsbereich

→ Kein grenzüberschreitende Verarbeitung: Abs. 5, 6

→ Grenzüberschreitende Verarbeitung: Abs. 7-11

- Benennung der Kategorien von Verantwortlichen / Auftragsverarbeiter

6. Verfahren

b) Inhalt

- Hintergrund: Beschreibung des betreffenden Sektors
- Spezifizierung des Gegenstands des CoC (Art. 40 Abs. 2 DS-GVO)
- Erklärung Notwendigkeit des CoC („Welches Problem löst der CoC?“)
- Darlegung wie der CoC eine wirksame Anwendung der DS-GVO erleichtert (EG 98)
- Bezugnahme auf / Auseinandersetzung mit anwendbaren Working Papers des EDSA
- Abgleich mit anwendbarem nationalen Recht
- Hinweis auf Vorgänger-CoC

6. Verfahren

b) Inhalt

Spezifische Beschreibung der DS-GVO konformen Verarbeitung

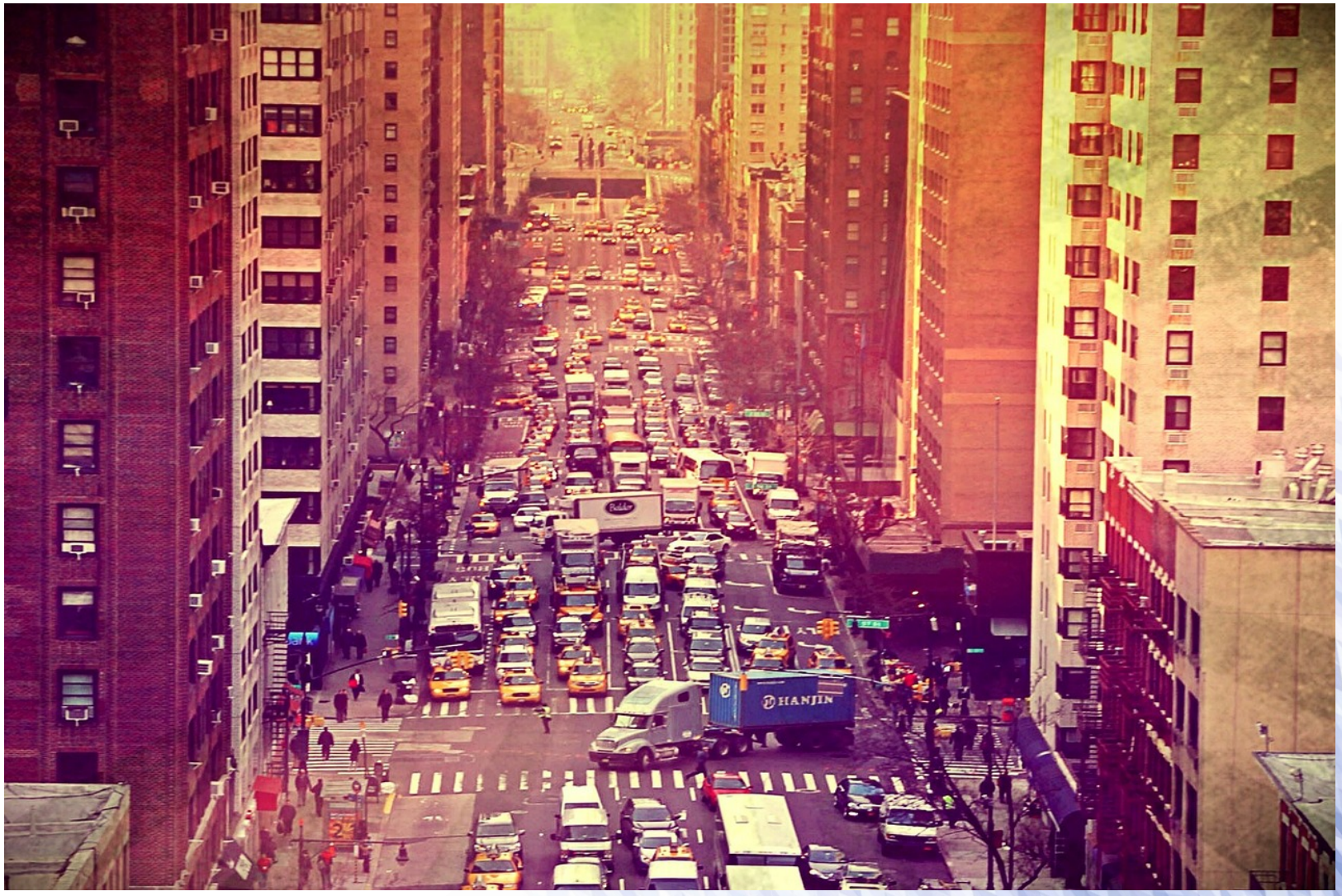
- Keine bloße Wiederholung der DS-GVO
- eindeutige, konkrete, einhaltbare und vollziehbare Standards
- Darstellung von best practices / und umgekehrt von DS-GVO-widrigem Verhalten
- ausreichend geeignete Garantien zur Minderung des Risikos in Bezug auf Verarbeitungen personenbezogener Daten / für die Rechte von Betroffenen
- Auch hier risikobasierter Ansatz: je höher das Risiko desto höher die Anforderungen an die Standards

6. Verfahren

b) Weiterer Inhalt

- Kontrollstelle, Art. 40 Abs. 4 DS-GVO / Art. 41 DS-GVO
  - Nach wie vor höchst streitig: interne oder externe, akkreditierte oder nicht akkreditierte Stelle erforderlich?
  - Unabhängigkeit
  - Fachkompetenz
  - Mechanismen zur effektiven Überwachung: effektives Monitoring, Berichtspflichten des Verantwortlichen, Aufklärungsbefugnisse, Sanktionsmöglichkeiten (z.B. temporärer Ausschluss des Verstoßenden aus dem CoC)
- Ausführungen dazu, wie mit Beschwerden umgegangen wird

Angekommen…



6. Verfahren

c) Konsultation

- Konsultation der maßgeblichen Interessenträger / betroffenen Personen und Berücksichtigung deren Stellungnahmen (EG 99)
- Anforderungen an die Ausgestaltung dieser Konsultation?
- Dokumentation dieser Konsultation
  - Wer wurde konsultiert?
  - Welchen Input lieferten die konsultierten Stakeholder?
  - Berücksichtigung?

→ Ziel: Bestätigung o.g. Repräsentativität / Legitimität des CoC

6. Verfahren

d) Einreichung bei Aufsichtsbehörde, Art. 40 Abs. 5 / 7 DS-GVO

Zuständige Aufsichtsbehörde (AB)?

Art. 40 Abs. 5 / 7 verweisen auf Art. 55 DS-GVO

→ Welche Aufsichtsbehörde ist nach Art. 55 DS-GVO zuständig?

Wahlrecht zwischen

- AB in deren Hoheitsgebiet die meiste in CoC geregelte Verarbeitung stattfindet?
- Niederlassung der Verantwortlichen / Auftragsverarbeiter?
- Niederlassung der Kontrollstelle (Art. 41 DS-GVO)?
- Niederlassung des Verbands / der Vereinigung?
- Wo befinden sich die meisten betroffenen Personen?
- Expertise der AB?
- Kapazitäten der AB?

6. Verfahren

e) Einreichung bei Aufsichtsbehörde, Art. 40 Abs. 5 / 7 DS-GVO

- In welcher Sprache?
  - Sprache der zuständigen Aufsichtsbehörde
  - Bei Verfahren nach Abs. 7 ff. (grenzüberschreitende Verarbeitungen) zusätzlich gemeinsame Sprachfassung erforderlich - Englisch
- Form
  - Schriftlich oder elektronisch

6. Verfahren

f) Prüfung durch und Entscheidung der Aufsichtsbehörde, Art. 40 Abs. 5 DS-GVO (nationale Sachverhalte)

- An Hand der o.g. Kriterien
- Str.: Bei Änderungsanregungen durch die AB – ablehnender Verwaltungsakt und Neubeginn des Verfahrens oder Möglichkeit, im Rahmen des Verfahrens Änderungen zu verlangen; Ermessen der AB
- Keine weitere Konsultationsphase: Aus Sicht des Regelerstellers sollte ein fertiges Regelwerk vorliegen
- Genehmigung bzw. negative Entscheidung
- Veröffentlichung, Art. 40 Abs. 6 DS-GVO

6. Verfahren

g) Verfahren im Falle des Art. 40 Abs. 7 DS-GVO

Vorverfahren:

- Einbindung weiterer betroffener AB, Finden von co-reviewern
- Entscheidung der federführenden AB, ob CoC mit DS-GVO vereinbar ist
- Bei ablehnender Entscheidung: ablehnender Bescheid plus Information an betroffene AB
- Bei positiver Entscheidung („bevor sie ihn genehmigt“) gem. Art. 40 Abs. 7 DS-GVO →

Kohärenzverfahren gemäß Art. 63 DS-GVO

6. Verfahren

g) Verfahren im Falle des Art. 40 Abs. 7 DS-GVO

→ Kohärenzverfahren gemäß Art. 63 DS-GVO

- Information an Antragsteller
- Information an betroffene AB
- Übermittlung an EDSA durch zuständige Aufsichtsbehörde (Berichterstatterin)
- Stellungnahme des EDSA, Art. 40 Abs. 7
- Übermittlung dieser an Kommission, Art. 40 Abs. 7
- Genehmigung durch die AB
- Art. 40 Abs. 9: Kommission kann genehmigten CoC für allgemein gültig erklären (dazu gleich)
- Veröffentlichung, Abs. 10 / 11

7. Rechtsfolgen / Rechtliche Auswirkungen

Weitere in der DS-GVO vorgesehene rechtliche Auswirkungen

- z.B. für Nachweis der Zuverlässigkeit des Auftragsverarbeiters (EG 81)
- Als Nachweis geeigneter Garantien für den Datenexport nach Art. 40 Abs. 3, Art. 46 Abs. 2 lit. e DS-GVO
- Berücksichtigung im Rahmen des Art. 83 Abs. 2 lit. j DS-GVO

8. Die Kontrollstelle

- Höchst streitig (s.o.): Anforderungen an die Kontrollstelle
- Befugnisse der AB bleiben unberührt
- Rechtsfolgen bei Verstößen durch die Kontrollstelle
  - Bußgeld bei Verstoß durch Kontrollstelle, Art. 83 Abs. 4 lit. c DS-GVO
  - Zurücknahme der Akkreditierung nach Art. 41 Abs. 5 DS-GVO

9. Wie geht es weiter?

Vielen Dank für Ihre Aufmerksamkeit!