Datenschutz-Folgenabschätzung

Waltraut Kotschy
Ludwig Boltzmann Institut für Menschenrechte

Tagung „Das Neue Datenschutzrecht“
Universität Salzburg
1. Februar 2018

Risikobestimmter Datenschutz?

- In der europäischen Diskussion ist „risikobasierter Datenschutz“ schon länger ein Thema
  - Unterschiedliche Schutzerfordernisse bei unterschiedlichem Risiko
  - Kann es dagegen einen vernünftigen Einwand geben?
- Das hängt davon ab, was die Konsequenzen sind:
  - Vom „EU-Nordwesten“ wurde lange propagiert, dass Datenschutz **überhaupt nur** dann **erforderlich** sei, wenn „ein Risiko“ besteht
  - Die gegenteilige Sicht verlangt, dass **erhöhter** Datenschutz angewendet werden muss, wenn ein Risiko wahrscheinlich ist

Von der DS-RL zur DSGVO

- Nach der DS-RL hatte der nationale Gesetzgeber eine Risiko-Folgenabschätzung vorzunehmen, indem er festzulegen hatte, wann ein VORABKONTROLLVERFAHREN durchzuführen ist.
- Einschätzung ist sehr unterschiedlich ausgefallen

  → mit ein Grund, warum es in der DSGVO keine Öffnungsklausel für diesen Punkt gibt
- Allerdings: „weiße“ und „schwarze Listen“ der Datenschutz-Aufsichtsbehörden vorgesehen → führt zu unterschiedlicher Interpretation von „Risiko“ → Vereinheitlichung wird durch die Vorlagepflicht an den EDSA gefördert

Festlegungen für einen Teilbereich

- Die Listen der Aufsichtsbehörden betreffend

  Verarbeitungsvorgänge, für die Datenschutz-Folgenabschätzung durchzuführen ist (obligatorisch)

  Verarbeitungsvorgänge, für die keine Datenschutz-Folgenabschätzung erforderlich ist (fakultativ)

- Für die in keiner der beiden Listen enthaltenen Verarbeitungsvorgänge muss die Notwendigkeit einer Risikofolgenabschätzung vom Verantwortlichen eigenverantwortlich entschieden werden

Welche Fragen muss man stellen?

- wodurch bestimmte sich das Risiko (Risikoelemente)?
- was wird vom Verantwortlichen als geeignete Maßnahme zur Risikovermeidung vorgesehen?
- wer entscheidet, ob die Maßnahmen zur Risikovermeidung voraussichtlich geeignet sind?

Die Risikoelemente

- Bisher war das eine leicht zu beantwortende Frage:

  Nach § 18 Abs. 2 DSG 2000 war eine besondere Prüfung von Datenverarbeitungen erforderlich, wenn sie

  - 1. sensible Daten enthalten oder
  - 2. strafrechtlich relevante Daten im Sinne des § 8 Abs. 4 enthalten oder
  - 3. die Auskunftserteilung über die Kreditwürdigkeit der Betroffenen zum Zweck haben oder
  - 4. in Form eines Informationsverbundsystems durchgeführt werden sollen.

- Nach Art. 37 DSGVO? Nur einige Anhaltspunkte:
  - Systematische umfangreiche Überwachung öff. zugänglicher Bereiche
  - Umfangreiche Verarbeitung von sensiblen und strafbezogenen Daten
  - Systematische und umfassende Bewertung persönlicher Aspekte

Weitere Orientierungshilfen

- Art. 29 Gruppe: Leitlinien zur Risikofolgenabschätzung, WP 248 , zählen folgende Gründe für erhöhtes Risiko von Verarbeitungen auf:
    - Verarbeitung von sensiblen Daten oder Daten über höchstpersönliche Umstände
    - Datenverarbeitung über besonders schutzwürdigen Betroffenenkreise

    - Bewertung und Scoring,
    - besonders wenn dadurch ein Recht oder Dienst nicht ausgeübt/erlangt werden kann
    - Automatisierte Entscheidungsfindung mit rechtlichen oder ähnlich signifikanten Folgen

    - Systematische Überwachung

    - Datenverarbeitung in sehr großen Ausmaßen
    - Abgleichen oder Zusammenführen von Datenmengen

    - Neuartige Technologien oder Organisationslösungen

Systematik der Risikoelemente?

- Alle wesentlichen Faktoren einer Datenverarbeitung können Risikoelemente enthalten:
  - Der Zweck: z.B. Überwachung, autom. Entscheidung…..
  - Die verarbeiteten Daten: sensible Daten, Bonitätsdaten….
  - Die Betroffenenkreise: Kinder, Personen mit Behinderungen…
  - Die Weitergabe von Daten: ins Dritt-Ausland
  - Die technische Umsetzung
  - ……..
- Eine Datenverarbeitung muss daher relativ genau beschrieben werden, wenn sie als „risikoarm“ eingestuft werden soll

  → bloße Benennung des Zwecks wird nicht genügen

  → könnte man auf die ö „Standardverarbeitungen“ zurückgreifen?

Übergangslösung?

- Leitfaden der öDSBeh:

  Für bereits vor dem Inkrafttreten der GVO durchgeführte Datenverarbeitungen ist dann keine Risikofolgenabschätzung erforderlich, wenn diese Verarbeitung Gegenstand eines

  Vorab-Kontrollverfahren nach § 18 DSG 2000

  war.

  Dies gilt freilich nicht bei zwischenzeitigen Änderungen der Datenanwendung.

Ablauf der Risikobewertung

Bei **jeder** der in der „Befreiungsliste“ („white list“) der Aufsichtsbehörde *nicht* genannten Verarbeitungen muss geprüft werden, ob und welche Risikoelemente vorliegen („Schwellwertanalyse“),

- ⟶ Prüfpflicht besteht daher bei den allermeisten Verarbeitungen
- ⟶ Wenn Risikoelemente gefunden werden, muss der von der DSGVO vorgeschrieben Mechanismus der „Folgenabschätzung“ in Gang gesetzt werden

Mechanismus der Folgenabschätzung

1. Die **Risiken** müssen **definiert** werden
2. Die beabsichtigten **Maßnahmen** zur Risikoverminderung müssen **beschrieben** werden
3. Es muss eine **Bewertung** getroffen werden, ob
   - ⟶ die Maßnahmen die Risiken voraussichtlich neutralisieren können oder
   - ⟶ ob ein signifikantes Restrisiko bleibt
4. bei signifikantem Restrisiko ist die **Aufsichtsbehörde** zu **konsultieren**

Einbindung der Betroffenen?

- Art. 35 (9): „Der Verantwortliche holt gegebenenfalls den Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung *unbeschadet* des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungs-vorgänge ein.“
- Das macht wohl vor allem in arbeitsrechtlichen Zusammenhängen Sinn – sonst wird es eher schwer sein, maßgebliche „Vertreter“ zu finden

Restrisiko – was ist das ?

- Der Ausdruck stammt nicht aus der DSGVO, sondern aus dem WP248 der Art. 29 Gruppe
- Ausdrucksweise der DSGVO ist etwas „sperrig“:

  Konsultation soll erfolgen , wenn

  „die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft“
- Meist geht es nicht darum, dass KEINE Maßnahmen zur Risikoverminderung beabsichtigt sind, sondern darum, ob die beabsichtigten Maßnahmen ausreichen oder ob das verbleibende Restrisiko zu hoch ist und durch zur Verfügung stehende Maßnahmen voraussichtlich nicht abgefangen werden kann.

Konsultation der Aufsichtsbehörde

- Voraussetzung ist die Vorlage einer nachvollziehbaren Dokumentation der vorstehend dargelegten Überlegungen (Art. 36 (3), insbes. lit. e)
- Rolle der Aufsichtsbehörde bei der Konsultation? Art. 36 (2):
  - Wenn Beschreibung der beabsichtigten Risikovermeidung nicht überzeugt, hat die Aufsichtsbehörde innerhalb von 8 Wochen

    eine Empfehlung auszusprechen UND (?)

    „kann ihre Befugnisse nach Art. 58 ausüben“ , was insbesondere auch Anordnungen oder auch ein Verbot der Verarbeitung inkludiert

Ergebnisse der Konsultation

- Die Konsultation kann ergeben, dass
  - gar kein Restrisiko vorliegt, ODER
  - die beabsichtigten Schutzmaßnahmen ausreichen ODER
  - zusätzliche Schutzmaßnahmen vereinbart/angeordnet werden ODER
  - die Verarbeitung untersagt wird, weil
    - die Maßnahmen, die der Verantwortliche willens ist zu ergreifen, für die Neutralisierung des als wahrscheinlich festgestellten Risikos nicht ausreichen

RFA – ein einmaliger Prozess?

- Die Datenschutz-Folgenabschätzung

  ist „**ein iterativer Prozess stetiger Überprüfung und Anpassung durch ein interdisziplinäres DSFA-Team.**“

  (Kurzpapier Nr. 5 der deutschen Datenschutzkonferenz zur Datenschutz-Grundverordnung)

- Man wird also für eine gelegentliche Überprüfung Vorsorge treffen müssen, insbesondere um allfällige Änderungen der Verarbeitungsumwelt in die Beurteilung miteinzubeziehen.

Danke für Ihre Aufmerksamkeit