Law | Policy Concepts

PC.17 Riskbased Approach

Authors: Winfried Veil

Last update: 2021-11-27 20:51:15 | By: Winfried Veil

Created at: 2021-05-21 12:56:04

[Translation coming soon]

Idee des risikobasierten Ansatzes ist es, datenschutzrechtliche Pflichten an den Risiken für die Rechte des Betroffenen auszurichten.

Die ursprüngliche Idee des risikobasierten Ansatzes war es, zu einer stärkeren Ausdifferenzierung der datenschutzrechtlichen Pflichten zu gelangen, um ein vernünftiges Verhältnis zwischen dem Aufwand für den Verantwortlichen und dem Risiko für den Betroffenen herzustellen. Man hätte hierfür das Datenschutzrecht ohne völlige Aufgabe des bestehenden Regulierungsansatzes wie folgt ausgestalten können:

> *? Das Verbotsprinzip des Datenschutzrechts besagt, dass personenbezogene Daten nur verarbeitet werden dürfen, wenn ein gesetzlich vorgesehener Erlaubnistatbestand vorliegt **[Kachel PK.08]**. Man hätte das Verbotsprinzip für bestimmte, weniger riskante Datenverarbeitungen aufheben können (etwa für Datenverarbeitungen durch natürliche Personen zu nicht-kommerziellen Zwecken).*

> *? Der „one size fits all"-Ansatz des Datenschutzrechts besagt, dass für alle Verantwortlichen grundsätzlich dieselben Regeln gelten **[Kachel K.02]**. Man hätte dies dahingehend differenzieren können, dass bestimmte Pflichten für bestimmte Gruppen von Verantwortlichen, deren Datenverarbeitungen typischerweise weniger riskant sind (etwa bestimmte KMU oder Handwerksbetriebe), nicht gelten.*

> *? Der „all or nothing"-Ansatz des Datenschutzrechts besagt, dass das volle Datenschutzregime gilt, sobald ein Datum Personenbezug hat oder personenbeziehbar ist **[Kachel K.03]**. Man hätte dies dahingehend differenzieren können, dass bei geringem Verarbeitungsrisiko das Kriterium der „Personenbeziehbarkeit" nicht allein entscheidend für die Geltung aller Regelungen des Datenschutzrechts ist.*

? *Man hätte den Verantwortlichen bei geringem Verarbeitungsrisiko von einem Übermaß an datenschutzrechtlichen Pflichten - etwa von bestimmten Informationspflichten* ***[Kachel P.07]*** *und Dokumentationspflichten* ***[Kachel P.09]*** *freistellen können.*

? *Man hätte den Fokus der Regulierung weniger auf die Datenerhebung und -speicherung als auf die Datenverwendung* ***[Kachel L.13]*** *legen können und typischerweise besonders riskante Datenverarbeitungen (etwa das Kreditscoring) deutlich strenger regeln können als typischerweise weniger riskante Datenverarbeitungen (etwa Kundendatenbanken).*

? *Man hätte noch stärkere Anreize für die Vornahme risikominimierender Maßnahmen (jenseits der Datenminimierung) schaffen können - etwa für Pseudonymisierungen.*

Vergleicht man die letztendlich beschlossene Version des risikobasierten Ansatzes mit diesen Regelungsideen, muss man zu dem Ergebnis kommen, dass der Normgeber auf weniger als dem halben Weg stehen geblieben ist:

? *Verbotsprinzip, „one size fits all"-Ansatz und „all or nothing"-Ansatz bleiben unangetastet.*

? *Zu einem echten Pflichtenwegfall bei geringem Risiko kommt es nur in wenigen Fällen.*

? *Im Übrigen werden nur die zur Pflichtenerfüllung zu ergreifenden Maßnahmen risikoabhängig skaliert, nicht aber die Pflichten selbst.*

? *Die Art und Weise, wie der risikobasierte Ansatz in Kapitel IV der DS-GVO verankert wurde, führt sogar zu einer zusätzlichen Belastung des Verantwortlichen, weil dieser nunmehr „an sich" für die Erfüllung jeder einzelnen Pflicht der DS-GVO und vor der Ergreifung jeder einzelnen Maßnahme, die zur Sicherstellung der Erfüllung dieser Pflicht dient, eine Risikoanalyse vornehmen muss.*

Gleichwohl ist der risikobasierte Ansatz eine der wenigen echten Modernisierungen, die die DS-GVO hervorgebracht hat.

Von Verbraucherschützern wurde der risikobasierte Ansatz von Anfang an **kritisch beäugt**. Von Datenschützern wurde er auch schon als **Trojanisches Pferd** oder als **Täuschungsmanöver** bezeichnet. Die Art. 29-Gruppe warnte davor, den „risk-based approach" nicht im Sinne eines „harm-based approach" zu verstehen, der sich nur auf finanzielle Schäden konzentriere **[WP 218 (2014), S. 4 (Ziffer 11)]**. Die Grundsätze der Datenverarbeitung und die Betroffenenrechte müssten – so die Art. 29-Gruppe – vom risikobasierten Ansatz unberührt bleiben **[WP 218 (2014), S. 4 (Ziffern 2 und 4)]**. Zum Teil wird die Existenz eines risikobasierten Ansatzes in der DS-GVO sogar ganz geleugnet (*Rost*, **Risiken im Datenschutz, in: vorgänge 221/222, 79, 80**

).