Evangelische Kirche in Deutschland

DER BEAUFTRAGTE FÜR DEN DATENSCHUTZ DER EKD

Begriff des Risikos

Die Kurzpapiere des Beauftragten für den Datenschutz der EKD (BfD EKD) dienen als erste Orientierung für die praktische Anwendung des novellierten EKD-Datenschutzgesetzes (DSG-EKD). Die in den Kurzpapieren vertretene Auffassung des BfD EKD steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung, die sich im praktischen Vollzug des DSG-EKD entwickeln kann.

Einleitende Überlegungen

Eine der wesentlichen Neuerungen des novellierten EKD-Datenschutzgesetzes ist die Verwendung des Begriffs „Risiko“ (§§ 27, 32, 33, 34 und 49 DSG-EKD) in Verbindung mit Quantifizierungen wie „hohes“, „unerhebliches“ und „dem Schutzniveau angemessenes“ Risiko. In § 34 DSG-EKD (Datenschutz-Folgeabschätzung) wird darüber hinaus Bezug auf ein „voraussichtliches Risiko“ genommen. „Folgen“ lassen sich nur mit Wahrscheinlichkeit voraussagen, so verwendet § 27 DSG-EKD explizit die Formulierung „unterschiedliche Eintrittswahrscheinlichkeiten“. Das verlangt eine Bewertung dieser Risikobegriffe. Aussagen zu Risiken sind immer mit Wahrscheinlichkeiten verknüpft, da es für die Vergangenheit keine Risiken mehr gibt, - diese Ereignisse haben faktisch stattgefunden - , für die Gegenwart Risikoüberlegungen zu spät sind, - die Gegenwart findet gerade statt - , und sich Risiken somit nur noch auf zukünftige Ereignisse beziehen können. Das Eintreten künftiger Ereignisse kann jedoch immer nur mit Wahrscheinlichkeit angegeben werden.

Umgangssprachlich wird gerne etwas als „wahrscheinlich“ bezeichnet, aber meist im Sinne einer vermuteten Möglichkeit, die eintreten könnte oder auch nicht. Eine fundierte Einschätzung von Risiken bedeutet aber, dass Wahrscheinlichkeiten quantifiziert werden müssen. Wahrscheinlichkeiten lassen sich nur anhand einer konkreten Liste möglicher Ereignisse, etwa Datenschutzverstöße, quantifizieren. Dazu muss eine Häufigkeitsverteilung dieser Ereignisse bestimmt oder mindestens geschätzt werden. Es gibt etwa im Gesundheitsbereich viele Beispiele, wie nichtssagend bis irreführend Aussagen zur Wahrscheinlichkeit sein können, wenn die dahinterstehende Häufigkeitsverteilung intransparent ist.

Für verantwortliche Stellen bedeutet dies insofern eine Entlastung, als sie sich nunmehr auf eine bestimmte Anzahl konkret benannte risikobehaftete Ereignisse konzentrieren können und nicht wie bisher einer unüberschaubaren Vielfalt von vielleicht Möglichem oder Denkbaren gegenüberstehen. De facto haben verantwortliche Stellen sich auch jetzt schon auf eine Auswahl ihnen als relevant erscheinender Ereignisse beschränkt. Darin, dass dies nun auch rechtlich gefordert ist, dürfte einer der wesentlichen Fortschritte der EU-Gesetzgebung liegen. Hinzu kommt, dass eine verantwortliche Stelle auf diese Weise besser einzuschätzen lernt, was mögliche Ereignisse mit schädlichen Folgen beim Umgang mit Daten anbelangt.

Das DSG-EKD fokussiert den Begriff des Risikos auf „voraussichtliche Risiken für die Rechte natürlicher Personen“. Damit wird neben kritischen Ereignissen und deren Eintrittswahrscheinlichkeiten die zweite Komponente eines Risikos angesprochen, nämlich die Folgen für Betroffene, wenn diese Ereignisse faktisch eintreten. Auch diese Folgen müssen bewertet werden, da erst beides zusammen, Eintrittswahrscheinlichkeit und Schwere potenzieller Folgen, das Risiko eines Ereignisses quantifizieren.

Es bietet sich an, für die Bewertung der Folgen mittels einer Punkte-Skala folgende Kriterien heranzuziehen:

a) Identitätsdiebstahl

b) Finanzieller Verlust

c) Diskriminierung

d) Profilbildung

e) Rufschädigung

f) Kontrollverlust.

Die Summe der an diese Kriterien geknüpften Punkte stellt ein Maß für die Schwere der Folgen eines faktischen Eintritts des zugrunde gelegten Ereignisses dar.

Möglichkeiten verantwortlicher Stellen zu Risikoabschätzungen zu gelangen

Der Begriff des „Risikos“ ist zwar schwierig, aber da es für verantwortliche Stellen genügt, das jeweils größte Risiko zu ermitteln, reicht es, die Risiken miteinander zu vergleichen (relatives Risiko). So muss beispielsweise die Eintrittswahrscheinlichkeit für das Ereignis, dass ein Notebook gestohlen wird, nicht absolut bestimmt werden, was wohl schwierig wenn nicht undurchführbar wäre, sondern es genügt festzustellen, ob sie größer, gleich oder kleiner als die Eintrittswahrscheinlichkeit für das Ereignis einer unbefugten Kenntnisnahme von Daten ist. Ein solches in sich stimmiges Gefüge von in Relation zueinander gesetzter Eintrittswahrscheinlichkeiten für eine Liste risikobehafteter Ereignisse ergibt sich aus den Gegebenheiten einer verantwortlichen Stelle und kann tabellarisch erfasst werden, indem man die relativen Eintrittswahrscheinlichkeiten anhand einer Punkte-Skala in Relation zueinander setzt. Auch die Schwere der aus solchen Ereignissen resultierenden Folgen können anhand einer Punkte-Skala in Relation zueinander gesetzt werden. Das Produkt aus den beiden Punktzahlen ergibt einen Wert für das relative Risiko des zugrunde gelegten Ereignisses. Über die Liste der als risikobehaftet eingeschätzten Ereignisse hinweg schält sich das Risikogefüge heraus, und die verantwortliche Stelle kann sich auf die Reduzierung der Risiken mit den höchsten Punkten konzentrieren. Das kann sie tun, indem sie Maßnahmen ergreift, die die Wahrscheinlichkeiten für das Eintreten der so identifizierten Ereignisse verringern oder dessen Folgen mildern oder die beides bewirken.

Wie groß absolut gesehen die Wahrscheinlichkeiten oder die Folgen sind, kann dann unbeachtlich bleiben, bis das eigentliche Ziel, dass die verantwortliche Stelle angemessene und wirkungsvolle Datenschutzmaßnahmen ergreift, erreicht ist.

Besonders effektiv ist diese Vorgehensweise, wenn sie etwa jährlich wiederholt wird, da die getroffenen Maßnahmen die Punkte für die Eintrittswahrscheinlichkeiten und auch für die Folgen und damit das Risikogefüge verändern werden. Im Ergebnis entsteht darauf ein kontinuierlicher Verbesserungsprozess.

Die Effektivität kann noch weiter gesteigert werden, indem sich bei der verantwortlichen Stelle mehrere Personen an der Vergabe der Punkte beteiligen. Zwar sind Menschen im Allgemeinen geübt darin, Relationen abzuschätzen. Es bleibt jedoch ein subjektives Element. Dieses kann reduziert werden, indem örtlich Beauftragte für den Datenschutz eine Vorlage mit ihren Einschätzungen erstellen und diese der IT, der Geschäftsführung und ggf. einem externen Dienstleister zur Zweit-, Dritt- oder Viertbewertung weitergeben. Eine dann vorgenommene Mittelung kann zu recht verlässlichen Risikogefügen führen.

Die Wirksamkeit lässt sich noch weiter steigern, indem sich gleichartige verantwortliche Stellen zusammentun und voneinander lernen.

Möglichkeiten der Aufsichtsbehörden, Risikoabschätzungen verantwortlicher Stellen zu unterstützen

Den Aufsichtsbehörden kommt bei den Risikoabschätzungen eine besondere Verantwortung zu. Es ist unverzichtbar, dass sie die verantwortlichen Stellen bei der Erstellung der Liste mit risikobehafteten Ereignissen, die sie im Hinblick auf die Eintrittswahrscheinlichkeiten und die Folgen anhand ihrer Gegebenheiten bewerten, beratend unter-

stützen. Es bietet sich an, gleichartigen verantwortlichen Stellen Muster solcher Listen zur Verfügung zu stellen. Da Datenschutzvorfälle den Aufsichtsbehörden gemeldet werden müssen, sind sie am ehesten in der Lage, solche Listen zu erstellen und anhand der gemeldeten Datenschutzvorfälle zu Häufigkeitsverteilungen und damit echten Wahrscheinlichkeiten zu gelangen. Diese Wahrscheinlichkeiten kann die Aufsichtsbehörde an die verantwortlichen Stellen zurückspiegeln, die damit eine weitere Grundlage haben, ihre relativen Einschätzungen weiter zu optimieren.

Eine weitere Möglichkeit für die Aufsichtsbehörden besteht darin, risikobasiert anlasslose Begehungen verantwortlicher Stellen durchzuführen. Allerdings haben auch Aufsichtsbehörden das Problem zu bewerteten, bei welcher Art von Stellen das Risiko größer als bei anderen Stellen ist. Der Annahme, dass bei großen Stellen ein größeres Risiko besteht, weil dort mehr Daten verarbeitet werden, könnte entgegengehalten werden, dass deren örtlich Beauftragte für den Datenschutz größere Stellenumfänge haben und die IT-Sicherheit professioneller betrieben wird. Am ehesten könnte die Annahme zutreffen, dass bei kleineren Stellen, die besondere Kategorien von personenbezogenen Daten verarbeiten, das Risiko höher ist. Andererseits dürfte dort die Sensibilität größer sein. Diese Annahme wäre insofern anhand durchgeführter Begehungen zu überprüfen.

Zusammenfassende Betrachtung

Fundierte Risiko- und Folgeabschätzungen verlangen den Umgang mit Wahrscheinlichkeiten. Für verantwortliche Stellen bietet es sich an,

a) relative Wahrscheinlichkeiten subjektiv abzuschätzen und

b) subjektive Einschätzungen mehrerer Personen zu mitteln, um zu objektiveren Werten zu gelangen.

Das ist deshalb eine brauchbare Methode, weil Menschen in der Regel recht gut vergleichen können, auch in der Einschätzung von Risiken.

Aufsichtsbehörden sollten die Verantwortlichen Stellen dahingehend unterstützen, indem sie die Pflicht zur Meldung von Datenschutzvorfällen dazu verwenden, Häufigkeiten für Listen von risikobehafteten Ereignissen zu ermitteln und diese zu veröffentlichen. Die Listen sollten auf Typen datenverarbeitender Stellen abgestimmt sein. Mit solchen Angaben können die verantwortlichen Stellen ihre eigenen Risikoabschätzungen weiter objektivieren.

Ob sich der Gesetzgeber der Problematik des Begriffs eines „voraussichtlichen Risikos“ voll bewusst war, kann hinterfragt werden. Gleichwohl geht die dahinterstehende Intention in die richtige Richtung. Es kommt für die verantwortlichen Stellen und die Aufsichtsbehörden nun darf an, diese Intention in der Praxis sinnvoll umzusetzen.