

Befugnisse der Aufsichtsbehörden und Geldbußen

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.

Mit dem neuen EKD-Datenschutzgesetz (DSG-EKD) wird die Stellung der unabhängigen kirchlichen Aufsichtsbehörden durch ein erweitertes und differenziertes Instrumentarium von Untersuchungs- und Abhilfebefugnissen gestärkt (§ 44 DSG-EKD). Bei Datenschutzverstößen können die Aufsichtsbehörden zukünftig Geldbußen verhängen (§ 45 DSG-EKD).

Untersuchungs- und Abhilfebefugnisse

Im Rahmen ihrer Untersuchungsbefugnisse können die Aufsichtsbehörden verlangen, dass die verantwortlichen Stellen sie bei der Erfüllung ihrer Aufgaben unterstützen.

Verantwortliche Stellen sind in diesem Zusammenhang zur Mitwirkung an Untersuchungs- und Prüfungsaktivitäten der für sie zuständigen Aufsichtsbehörde verpflichtet. Hierzu zählt insbesondere, dass die verantwortliche Stelle der Aufsichtsbehörde Auskünfte zu erteilt, ihr Einsicht in Unterlagen und Akten über die Verarbeitung personenbezogener Daten gibt sowie alle diesbezüglichen Informationen bereitstellt.

Die aufsichtsbehördlichen Untersuchungs- und Prüfungsbefugnisse umfassen auch das Recht, jederzeit Zutritt zu den Diensträumen, Verarbeitungsanlagen und -geräten verantwortlicher Stellen zu erhalten.

Wenn die Aufsichtsbehörde feststellt, dass ein beabsichtigter Verarbeitungsvorgang voraussichtlich gegen das kirchliche Datenschutzrecht

verstößt, kann sie einen entsprechenden Hinweis geben.

Festgestellte Verstöße gegen Datenschutzbestimmungen oder sonstige Mängel der Verarbeitung personenbezogener Daten können die Aufsichtsbehörden gegenüber verantwortlichen Stellen in ihrem Zuständigkeitsbereich sowie den von diesen Stellen beauftragten Auftragsverarbeitern beanstanden. Die Beanstandung wird stets verbunden mit einer Aufforderung zur Stellungnahme innerhalb einer von der Aufsichtsbehörde gesetzten Frist. Diese Stellungnahme soll eine Darstellung der Maßnahmen enthalten, die von der verantwortlichen Stelle aufgrund der Mitteilung der Aufsichtsbehörde getroffen worden sind. Des Weiteren ist die Aufsichtsbehörde auch selbst befugt, Vorschläge zur Beseitigung der festgestellten Mängel oder zur sonstigen Verbesserung des Datenschutzes im Bereich der verantwortlichen Stelle zu machen.

Bei unerheblichen oder zwischenzeitlich beseitigten Mängeln kann die Aufsichtsbehörde von einer Beanstandung absehen.

Um einen rechtmäßigen Zustand herzustellen oder eine drohende Verletzung des Schutzes personenbezogener Daten abzuwenden, können die Aufsichtsbehörden gegenüber verantwortlichen Stellen auch Anordnungen erlassen. Anordnungen können darauf gerichtet sein, dass die verantwortliche Stelle

- 1) Verarbeitungsvorgänge mit dem Datenschutzrecht in Einklang bringt,

- 2) Verarbeitungsvorgänge beschränkt oder unterlässt,
- 3) Datenübermittlungen in ein Drittland oder an eine internationale Organisation aussetzt,
- 4) personenbezogene Daten berichtigt, sperrt oder löscht,
- 5) eine betroffene Person von einer sie betreffenden „Datenpanne“ benachrichtigt,
- 6) dem Antrag einer betroffenen Person entspricht.

Der Gebrauch der gesetzlich zur Verfügung stehenden Untersuchungs- und Abhilfebefugnissen im Einzelfall liegt im Ermessen der Aufsichtsbehörde.

Geldbußen

Zusätzlich zu Beanstandungen und Anordnungen oder anstelle von Beanstandungen und Anordnungen können Datenschutzverstöße verantwortlicher Stellen und kirchlicher Auftragsverarbeiter gemäß § 45 DSGVO künftig mit Geldbußen geahndet werden. Als milderer Sanktionsmittel besteht außerdem die Möglichkeit, Geldbußen für den Wiederholungsfall anzudrohen.

Das DSGVO ermöglicht eine Verhängung von Geldbußen nur, soweit verantwortliche Stellen oder der kirchliche Auftragsverarbeiter, in deren Verantwortungsbereich ein Datenschutzverstoß festgestellt wird, als Unternehmen am Wettbewerb teilnehmen. Unter den Unternehmensbegriff des DSGVO fallen natürliche oder juristische Personen, die eine wirtschaftliche Tätigkeit ausüben. Hierbei spielt die Rechtsform keine Rolle. Sowohl Personen- als auch Kapitalgesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen, gelten als Unternehmen.

Liegen diese Voraussetzungen vor, entscheidet die Aufsichtsbehörde jeweils unter Berücksichtigung der Umstände des Einzelfalles, ob eine Geldbuße verhängt wird oder nicht. Hierbei handelt es sich um eine Ermessensentscheidung, bei der insbesondere der Kriterienkatalog in § 45 Abs. 3 DSGVO Berücksichtigung findet. Er wird nicht nur der Entscheidung über die Verhängung einer Geldbuße („ob“), sondern auch der Entscheidung über

deren Höhe („wie“) zugrunde gelegt. Zu berücksichtigende Kriterien sind unter anderem

- 7) die Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der Verarbeitung, der Zahl der von ihr betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens,
- 8) die Schwere des Verschuldens (Vorsatz und Fahrlässigkeit),
- 9) Maßnahmen der verantwortlichen Stelle oder des Auftragsverarbeiters zur Minderung des bei den betroffenen Personen entstandenen Schadens,
- 10) einschlägige frühere Verstöße des Unternehmens,
- 11) die Kategorie der vom Verstoß betroffenen personenbezogenen Daten,
- 12) die Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde.

Diese Aufzählung ist nicht abschließend. Insbesondere sind auch im Gesetz nicht ausdrücklich benannte erschwerende oder mildernde Umstände zu berücksichtigen. So kann zum Beispiel auch die Ausgestaltung technischer und organisatorischer Maßnahmen der verantwortlichen Stelle oder des Auftragsverarbeiters Bedeutung erlangen. Sowohl Datenschutzmängel als auch besondere Vorkehrungen und Kontrollmechanismen zur Einhaltung der Anforderungen des Datenschutzes in den relevanten Betriebsstrukturen und Arbeitsprozessen des Unternehmens können hierbei – entweder erschwerend oder mildernd – in Rechnung gestellt werden.

- 13) Neben der Beachtung des Kriterienkatalogs in § 45 Abs. 3 DSGVO hat die Aufsichtsbehörde im Rahmen ihrer Ermessensentscheidung sicherzustellen, dass die Verhängung von Geldbußen in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist. Die maximale Höhe, die ein Bußgeld erreichen kann, beträgt 500.000 Euro. Bei Datenschutzverstößen gegen mehrere daten-

schutzrechtliche Bestimmungen durch gleiche oder miteinander verbundene Verarbeitungsvorgänge darf der Gesamtbetrag der Geldbuße den Betrag für den schwerwiegendsten Verstoß nicht übersteigen.