PRESSEMITTEILUNG

EDPS/2016/08

Brüssel, den 21. März 2016

EDSB-Leitlinien zur Sicherung von Informationen und der Geschäftskontinuität

In seinen heute veröffentlichten **Leitlinien** zum *Informationssicherheitsrisikomanagement* erteilt der Europäische Datenschutzbeauftragte den EU-Organen Ratschläge im Hinblick auf die Gewährleistung einer sicheren und vertrauenswürdigen digitalen Umgebung, die eine Voraussetzung für das ordnungsgemäße Funktionieren ihrer Dienste bildet.

Wojciech Wiewiórowski, Stellvertretender Beauftragter, erklärte: *„Die Sicherheit personenbezogener Daten ist ein rechtliches Erfordernis, sie liegt aber auch im notwendigen Interesse von Organisationen, die sich in ihrem täglichen Dienstbetrieb auf die Nutzung von Informationen stützen. Diese müssen ein angemessenes Maß an Informationssicherheit wahren, da der Nutzen und die Effizienz ihrer Arbeit in so hohem Maße von Informationen abhängen. Ich rate den Vertretern der verschiedenen Führungsebenen in den EU-Organen dringend dazu, Verfahrensabläufe für das Informationssicherheitsrisikomanagement zu entwickeln und anzuwenden, die auf die jeweiligen Anforderungen ihrer Organisation zugeschnitten sind.“*

Verschiedene Organisationen sind in Bezug auf die organisationsintern genutzten Informationen unterschiedlichen Sicherheitsrisiken ausgesetzt. Dem aktuellen Stand entsprechende Risikobeurteilungsmethoden gestatten es, die geeigneten Lösungen für die bei einer Einrichtung jeweils bestehenden Risiken auf effiziente Weise zu ermitteln und den Einsatz von finanziellen und informationstechnischen Mitteln zur Entwicklung solcher Lösungen zu rechtfertigen.

Das Informationssicherheitsrisikomanagement für personenbezogene Daten erfordert spezialisiertes Fachwissen auf dem Gebiet der Informations- und IT-Sicherheit sowie auf dem des Datenschutzes. Behördliche Datenschutzbeauftragte sollten die Informations- und IT-Sicherheitsexperten bei der Entwicklung dieser Verfahrensabläufe unterstützen.

Allein mit technischen Sicherheitslösungen lässt sich das Problem der Informationssicherheit nicht bewältigen. Die Verantwortung für die Durchsetzung von Entscheidungen, die sich auf Anwendungen und die ihnen zugrunde liegenden IT-Infrastrukturen auswirken, liegt letztlich bei den Führungsebenen einer Organisation. Die Entwicklung und Umsetzung von strategischen Vorgehensweisen müssen von der Leitung unterstützt werden, die auch die erforderlichen Ressourcen mobilisieren muss, um den Informationsrisiken, denen eine Organisation ausgesetzt ist, entgegenzuwirken.

Wenngleich diese Leitlinien primär für die EU-Organe bestimmt sind, sind sie möglicherweise auch für alle anderen, die sich für Datenschutz interessieren, von Nutzen; die für die EU-Organe geltende Datenschutzverordnung (Verordnung (EG) Nr. 45/2001) entspricht in weiten Teilen der Datenschutzrichtlinie (EG) 95/46, die in

das nationale Recht der Mitgliedstaaten sowie jenes von Island, Liechtenstein und Norwegen umgesetzt wurde.

Diese Leitlinien werden auch nach dem Inkrafttreten der neuen Datenschutz-Grundverordnung weiterhin von Nutzen sein, die den Grundsatz des Sicherheitsrisikomanagements beibehält und die Gesamtverantwortung und Governance-Anforderungen durch die ausdrückliche Einführung des Grundsatzes der **Rechenschaftspflicht** bei der Wahrung von Datenschutzpflichten ausweitet.

Hintergrundinformationen

Die Datenschutzbestimmungen für die EU-Organe – sowie die Pflichten des Europäischen Datenschutzbeauftragten (EDSB) – sind in der **Verordnung (EG) Nr. 45/2001** geregelt. Der Europäische Datenschutzbeauftragte (EDSB) ist eine relativ neue, aber zunehmend einflussreiche unabhängige Aufsichtsbehörde, die die Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der EU überwacht, in Bezug auf politische Maßnahmen und Rechtsvorschriften, die sich auf die Privatsphäre auswirken, beratend tätig ist und mit vergleichbaren Behörden zusammenarbeitet, um einen kohärenten Datenschutz sicherzustellen.

Giovanni Buttarelli (EDSB) und **Wojciech Wiewiórowski** (stellvertretender EDSB) sind Mitglieder dieser Behörde und wurden durch eine gemeinsame Entscheidung des Europäischen Parlaments und des Rates ernannt. Sie traten ihre fünfjährige Amtszeit am 4. Dezember 2014 an.

Personenbezogene Daten bzw. Informationen: alle Informationen, die sich auf eine bestimmte oder bestimmbare (lebende) natürliche Person beziehen. Beispiele hierfür sind unter anderem Namen, Geburtsdaten, Fotos, Videoaufnahmen, E-Mail-Adressen und Telefonnummern. Weitere Angaben, wie z. B. IP-Adressen und Inhalte von Mitteilungen, die sich auf Endnutzer von Kommunikationsdiensten beziehen oder von ihnen zur Verfügung gestellt werden, gelten ebenfalls als personenbezogene Daten.

Privatsphäre: das Recht einer natürlichen Person, in Ruhe gelassen zu werden und die Kontrolle über die Informationen über sich selbst auszuüben. Das Recht auf Privatsphäre und auf ein Privatleben ist in der Allgemeinen Erklärung der Menschenrechte (Artikel 12), der Europäischen Menschenrechtskonvention (Artikel 8) und der Europäischen Charta der Grundrechte (Artikel 7) verankert. Die Charta umfasst auch ein ausdrückliches Recht auf den Schutz personenbezogener Daten (Artikel 8).

Verarbeitung personenbezogener Daten: Gemäß Artikel 2 Buchstabe b der Verordnung (EG) Nr. 45/2001 bezeichnet die Verarbeitung personenbezogener Daten „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Wiederauffinden, das Abfragen, die Nutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten.“ Siehe hierzu das Glossar auf der EDSB-Website.

Artikel 22 der Verordnung (EG) Nr. 45/2001: erlegt den EU-Organen die rechtliche Anforderung auf, die Risiken bei der Verarbeitung personenbezogener Daten zu mindern;

- bei ihrer Auswertung muss das Informationssicherheitsrisikomanagement auch Informationssicherheitsrisiken erfassen, die sich auf personenbezogene Daten auswirken;
- ausgehend von ihrer Auswertung kann eine Reihe von geeigneten Sicherheitsmaßnahmen festgelegt und umgesetzt werden.

Sicherheitsmaßnahmen zum Schutz personenbezogener Daten können nicht allgemeingültig festgelegt werden, sondern müssen vielmehr aus dem Verfahrensablauf des Informationssicherheitsrisikomanagements erwachsen, der dem spezifischen Umfeld, in dem die personenbezogenen Daten verarbeitet werden, Rechnung trägt.

Informationssicherheitsexperten sind auf die Entwicklung von Verfahren zum Schutz von Informationen und Informationssystemen gegen unbefugten Zugriff, unbefugte Nutzung, Offenlegung, Störung, Änderung oder Vernichtung spezialisiert.

IT-Sicherheitsexperten sind auf die Entwicklung von Verfahren zum Schutz von Informationen mittels verschiedener Technologien zur Erzeugung, Speicherung, Nutzung und zum Austausch solcher

Informationen gegen unbefugten Zugriff, Missbrauch, Funktionsstörung, Änderung, Vernichtung oder nicht ordnungsgemäße Offenlegung spezialisiert.

Der Europäische Datenschutzbeauftragte (EDSB) ist eine unabhängige Aufsichtsbehörde, deren Aufgabe es ist, dafür zu sorgen, dass der Schutz personenbezogener Daten und der Privatsphäre gewährleistet ist und bewährte Verfahren in den Organen und Einrichtungen der EU gefördert werden. Er erfüllt diese Aufgabe, indem er

- die Verarbeitung personenbezogener Daten durch die EU-Verwaltung beaufsichtigt;
- in Bezug auf politische Maßnahmen und Rechtsvorschriften, die sich auf den Schutz der Privatsphäre auswirken, beratend tätig ist;
- mit vergleichbaren Behörden zusammenarbeitet, um einen einheitlichen Datenschutz sicherzustellen.

Die Leitlinien des EDSB sind auf der Website des EDSB abrufbar.

Ansprechpartner für Fragen: press@edps.europa.eu

EDSB – Der europäische Hüter des Datenschutzes

www.edps.europa.eu

Folgen Sie uns auf Twitter:

@EU_EDPS