ERNST MORITZ ARNDT
UNIVERSITÄT GREIFSWALD

Wissen
lockt.
Seit 1456

Merkblatt zur Verpflichtungserklärung gemäß § 6 DSG M-V (Unterrichtung und Belehrung zum Datenschutz)

Adressaten und Ziel dieser Belehrung

Alle Beschäftigten der Ernst-Moritz-Arndt-Universität, die aufgrund der ihnen übertragenen Aufgaben zwingend Zugang zu personenbezogenen Daten haben, sind über die bei ihrer Tätigkeit zu beachtenden Vorschriften über den Datenschutz in geeigneter Weise zu unterrichten und (regelmäßig bereits bei Aufnahme ihrer Tätigkeit) auf das Datengeheimnis zu verpflichten (vgl. § 6 Landesdatenschutzgesetz Mecklenburg-Vorpommern - DSG M-V). Ziel dieser Belehrung ist es daher, die betreffenden Beschäftigten im Hinblick auf die Erfordernisse des Datenschutzes zu sensibilisieren, auf die in diesem Zusammenhang anwendbaren Rechtsvorschriften hinzuweisen und über mögliche Konsequenzen der Verletzung dieser Rechtsvorschriften zu belehren.

Personenbezogene Daten

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (§ 3 Abs. 1 DSG M-V). Diese Definition erfasst *jede* Information, die einer bestimmten natürlichen Person zugeordnet werden kann, unabhängig von der Art ihrer Präsentation (z. B. auch Bild- und Tondaten). Einzelangaben sind beispielsweise: Name, Geburtsdatum, Geschlecht, Geburtsort, Matrikelnummer, Personalausweisnummer, Anschrift, Familienstand, Einkommen, Staatsangehörigkeit, Krankheiten, Zeugnisnoten, Berufsbezeichnung, Religionszugehörigkeit, Kfz-Kennzeichen, IP-Adresse und sonstige Protokolldaten der Internetnutzung u. v. m. Bestimmbar sind die Informationen über eine natürliche Person dann, wenn es möglich ist, die fraglichen Einzelangaben dieser konkreten Person zuzuordnen. Die Möglichkeit der Bestimmbarkeit ist sehr weit auszulegen. In Zweifelsfällen sollte stets der behördliche Datenschutzbeauftragte einbezogen werden.

Grundsätze des Datenschutzes

Generell ist eine Verarbeitung von personenbezogenen Daten (§ 3 Abs. 3 DSG M-V: Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen und Nutzen) nur dann zulässig, wenn die Vorschriften des DSG M-V sie zulassen, eine andere Rechtsvorschrift sie erlaubt oder zwingend voraussetzt oder der Betroffene (in der Regel schriftlich) eingewilligt hat (vgl. § 7 Abs. 1 DSG M-V). Man spricht insoweit von einem Verbot mit Erlaubnisvorbehalt.

Zweckbindung

Personenbezogene Daten dürfen grundsätzlich nur zu dem Zweck verarbeitet werden, zu dem sie erhoben worden sind (§ 10 Abs. 2 DSG M-V). Eine Nutzung zu einem anderen Zweck ist nur aufgrund einer Rechtsvorschrift zulässig, welche die Verarbeitung zu anderen Zwecken erlaubt oder zwingend voraussetzt oder wenn der Betroffene darin eingewilligt hat (§ 10 Abs. 3 Nr. 1 u. 2). Weitere Erlaubnistatbestände finden sich in § 10 Abs. 3 Nr. 3-9, Abs. 4-6). In Zweifelsfällen sollte stets der behördliche Datenschutzbeauftragte einbezogen werden.

Erforderlichkeit, Vermeidbarkkeit, Sparsamkeit
Die Verarbeitung von personenbezogenen Daten muss das mildeste geeignete Mittel zur Erfüllung der Aufgaben der Universität (Zweck der Datenverarbeitung) darstellen. Ist dies der Fall, dürfen stets nur so viele personenbezogene Daten verarbeitet werden, wie zur Aufgabenerfüllung zwingend erforderlich sind. Die Daten sind zudem unverzüglich zu löschen, sobald sie zur Aufgabenerfüllung nicht mehr gebraucht werden.

Allgemeine Maßnahmen zur Datensicherheit (§ 21 DSG M-V)
Wenn personenbezogene Daten gespeichert und verarbeitet werden dürfen, stellt das DSG M-V hohe Sicherheitsanforderungen, die – durch nach dem Stand der Technik und nach der Schutzbedürftigkeit der zu verarbeitenden Daten erforderliche und angemessene – technische und organisatorische Maßnahmen sicherzustellen sind. Hierbei sind im Wesentlichen folgende Punkte zu beachten:

- *Vertraulichkeit:* Nur Befugte dürfen personenbezogene Daten zur Kenntnis nehmen können.
- *Integrität:* Personenbezogene Daten müssen während der Verarbeitung unversehrt, vollständig und aktuell bleiben.
- *Verfügbarkeit:* Personenbezogene Daten müssen zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können.
- *Authentizität:* Personenbezogene Daten müssen stets ihrem Ursprung zugeordnet werden können.
- *Revisionsfähigkeit:* Unter Beteiligung der Personalvertretung der Daten verarbeitenden Stelle ist ein Protokollierungsverfahren festzulegen, das die Feststellung erlaubt, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat.
- *Transparenz:* Die Verfahrensweisen bei der Verarbeitung personenbezogener Daten müssen vollständig und in zumutbarer Zeit nachvollzogen werden können.

Verfahrensbeschreibung, Sicherheitskonzept und Freigabe (§§ 18, 19, 22 DSG M-V)
Jedes Verfahren, welches personenbezogene Daten verarbeitet, ist nach Maßgabe des § 18 Abs. 1 DSG M-V in einer sog. Verfahrensbeschreibung zu dokumentieren. Sinnvoller Weise wird die Verfahrensbeschreibung von einem fachlichen Vorgesetzten des Verfahrensverantwortlichen erstellt. Bei automatisierten Verfahren, die an der Universität im Regelfall vorliegen, ist zudem in einem Sicherheitskonzept festzulegen, in welcher Form die allgemeinen (§ 21 DSG M-V) und die besonderen Anforderungen zur Datensicherheit (§ 22 DSG M-V) umgesetzt werden. Schließlich ist das Verfahren vom Kanzler *vor* der produktiven Inbetriebnahme freizugeben (§19 Abs. 1 DSG M-V). Die Federführung des gesamten Verfahrens zur Einrichtung, Kontrolle und Freigabe hat der behördliche Datenschutzbeauftragte.

Rechtsfolgen bei Verletzungen
Schuldhafte Verletzungen des Datengeheimnisses sowie sonstiger datenschutzrechtlicher Vorschriften können zum Teil erhebliche Folgen für den Verantwortlichen haben. Hinsichtlich des Beschäftigungsverhältnisses mit der Universität oder dem Land Mecklenburg-Vorpommen kommen arbeits- oder dienstrechtliche Sanktionen in Betracht (z. B. Abmahnung, verhaltensbedingte Kündigung, Verweis, Geldbuße, Kürzung der Dienstbezüge, Entfernung aus dem Dienst etc.). Denkbar sind ferner Ordnungswidrigkeiten (z. B. nach § 42 DSG M-V), die mit einer Geldbuße geahndet werden können, aber auch Straftaten nach dem Strafgesetzbuch, wie z. B. Abfangen von Daten (§ 202b), Verletzung des Post- und Fernmeldegeheimnisses (§ 206), Datenveränderung (§ 303a) und Computersabotage (§ 303b), die in schwerwiegenden Fällen auch mit Freiheitsentzug bestraft werden können.