P. b. b. Verlagspostamt 1030 Wien WoGZ 213U

BUNDESGESETZBLATT

FÜR DIE REPUBLIK ÖSTERREICH

Jahrgang 2001 Ausgegeben am 3. Mai 2001 Teil II

174. Verordnung des Bundesministers für Inneres über das Verwenden der Meldedaten zum Aufbau und Betrieb des Zentralen Melderegisters (Meldedatensicherheitsmaßnahmen-Verordnung – MeldeDS-VO)

Auf Grund der §§ 16 und 16b MeldeG 1991, BGBl. Nr. 9/1992, in der Fassung des Artikels I des Bundesgesetzes BGBl. I Nr. 28/2001 wird verordnet:

Anwendungsbereich

§ 1. (1) Die Verordnung regelt Datensicherheitsmaßnahmen beim Verwenden von Daten zum Aufbau und Betrieb bis zur Aufnahme des Echtbetriebes des Zentralen Melderegisters (§ 16 Meldegesetz 1991) durch die Meldebehörden.

(2) Soweit Bürgermeister gemäß § 16b Abs. 6 Meldegesetz 1991, in der Fassung des Art. I des Bundesgesetzes BGBl. I Nr. 28/2001, für Meldebehörden tätig werden, gilt diese Verordnung für sie, wie für die Meldebehörden.

Zugriffe auf Daten des Zentralen Melderegisters

§ 2. Jeglicher Zugriff der Meldebehörden auf die im Zentralen Melderegister (ZMR) verarbeiteten oder zu verarbeitenden Daten darf nur in Vollziehung des Meldegesetzes erfolgen.

Zugriffsberechtigte

§ 3. Die Meldebehörde hat sicherzustellen, dass Zugriff auf das ZMR nur eingeräumt wird, wenn die Zugriffsberechtigten über die Bestimmungen gemäß § 15 Datenschutzgesetz 2000, BGBl. I Nr. 165/1999, und den Inhalt dieser Verordnung belehrt wurden.

Datensicherheitsmaßnahmen

§ 4. (1) Jede Meldebehörde hat zumindest einen Verantwortlichen für die Datensicherheitsmaßnahmen im Rahmen der Datenverarbeitung für das ZMR zu benennen; dieser kann vom Bundesminister für Inneres ermächtigt werden, Zugriffsberechtigungen für den Betrieb des ZMR zu erteilen, sofern der Bundesminister für Inneres als Betreiber des ZMR (im Weiteren: Betreiber) die Berechtigungen nicht selbst vergibt.

(2) Der gemäß Abs. 1 Verantwortliche hat nach Maßgabe des jeweiligen Standes der Technik und der organisatorischen Möglichkeiten den Zugriffsschutz zu personenbezogenen Daten und die erforderlichen Datensicherheitsmaßnahmen zu organisieren und umzusetzen. Er hat insbesondere die Zuständigkeiten und Regeln für die Programmverwaltung in seinem Bereich festzulegen sowie die Voraussetzungen für den physischen Zugriff auf die Daten des ZMR in seinem Zuständigkeitsbereich zu schaffen. Sofern er zur Erteilung von Zugriffsberechtigungen gemäß Abs. 1 ermächtigt worden ist, hat er für seinen Zuständigkeitsbereich die Zugriffsberechtigungen für das ZMR für die einzelnen Benutzer individuell zuzuweisen.

(3) Über Datensicherheitsmaßnahmen gemäß Abs. 2 hat der Verantwortliche Aufzeichnungen zu führen, die mindestens drei und höchstens sechs Jahre aufzubewahren sind.

(4) Die Meldebehörden haben dafür zu sorgen, dass für den Bereich der Systeme, über die der Zugang zum ZMR erfolgen soll, eine nach den Vorgaben des Betreibers zu gestaltende Datensicherheitsvorschrift, in der sämtliche für den Betrieb des ZMR erforderlichen Datensicherheitsmaßnahmen anzuordnen sind, erlassen wird.

Entzug der Zugriffsberechtigung

§ 5. (1) Benutzer sind vom gemäß § 4 Abs. 1 Verantwortlichen von der weiteren Benutzung für immer oder für eine bestimmte Zeit von der Ausübung ihrer Zugriffsberechtigung auszuschließen, wenn

1. sie diese zur weiteren Erfüllung der ihnen übertragenen Aufgaben nicht mehr benötigen oder
2. sie die Daten nicht entsprechend den für den Betrieb des ZMR maßgeblichen Bestimmungen verwenden.

(2) Unter den in Abs. 2 genannten Voraussetzungen kann auch der Betreiber einen Benutzer von der weiteren Benutzung ausschließen oder dies anordnen.

Zutritt zu Räumen

§ 6. (1) Die Meldebehörden haben durch organisatorische und technische Vorkehrungen sicherzustellen, dass der Zutritt zu Räumen, in denen sich eine Zugriffsmöglichkeit auf das ZMR befindet, grundsätzlich nur Bediensteten der Behörde möglich ist.

(2) Ist es erforderlich, dass in Räumen mit einer Zugriffsmöglichkeit auf das ZMR Parteienverkehr stattfindet, ist jedenfalls sicherzustellen, dass eine Einsichtnahme in die Daten des ZMR durch Außenstehende nicht möglich ist.

(3) Mitgliedern der Datenschutzkommission und des Datenschutzrates ist nach erfolgter Ausweisleistung der Zutritt zu gewähren, sofern sie im dienstlichen Auftrag tätig werden. Auf Verlangen sind die für deren Aufgabenerfüllung erforderlichen Auskünfte zu erteilen.

(4) Nähere Bestimmungen über den Zutritt, insbesondere auch Regelungen über den Zutritt anderer als der in Abs. 1 bis 3 genannten Personen – wie zB Angehörigen von Wartungsfirmen – und dessen Dokumentation sind von der Meldebehörde in einer Datensicherheitsvorschrift (§ 4 Abs. 3) zu treffen.

Technische Vorkehrungen

§ 7. (1) Es ist sicherzustellen, dass geeignete, dem jeweiligen Stand der Technik entsprechende, Wirtschaftlichkeitsüberlegungen berücksichtigende Vorkehrungen getroffen werden, um eine Vernichtung oder Veränderung der Daten durch Programmstörungen (Viren) zu verhindern.

(2) Wird ein Gerät, das den Zugang zum ZMR ermöglicht, aus dem Behördenbereich oder einer Dienststelle entfernt, ist sicherzustellen, dass eine unberechtigte Verwendung ausgeschlossen ist.

(3) Es ist sicherzustellen, dass der Zugriff auf das ZMR nur nach Eingabe einer Benutzerkennung und eines Kennwortes möglich ist. Kennwörter sind jedenfalls geheim zu halten und müssen nach Maßgabe der technischen Möglichkeiten in periodischen Zeitabständen geändert werden.

(4) Für den Verbindungsaufbau zum ZMR sind vom Betreiber zur Verfügung gestellte Software-Zertifikate zu verwenden. Software-Zertifikate sind Schlüssel, die den Zugang zum ZMR über dezentrale Systeme eröffnen und jedes zugriffsberechtigte System eindeutig identifizieren. Anstelle von Arbeitsplatz-Systemen kann mit einem Zertifikat auch ein Gateway-System authentifiziert werden, das sich in der Verfügung des Anwenders oder eines von ihm beauftragten Dienstleisters befindet.

(5) Es ist sicherzustellen, dass nach den Vorgaben des Betreibers geeignete, dem jeweiligen Stand der Technik entsprechende Vorkehrungen getroffen werden, um eine Vernichtung, Veränderung oder Abfrage der Daten des ZMR durch unberechtigte Zugriffe durch Benutzer oder Systeme zu verhindern.

Kontrolle der Einhaltung datenschutzrechtlicher Bestimmungen und von Datensicherheitsmaßnahmen

§ 8. Der Betreiber überprüft im Zusammenwirken mit der Meldebehörde durch Stichproben, ob die Verwendung der Daten des ZMR den einschlägigen Bestimmungen entsprechend erfolgt und die erforderlichen Datensicherheitsmaßnahmen ergriffen worden sind.

Private Dienstleister

§ 9. Bedient sich die Meldebehörde für den Datenverkehr zwischen dem örtlichen Melderegister (§ 14 MeldeG) und dem Zentralen Melderegister eines privaten Dienstleisters, hat sie diesen zur Einhaltung aller datenschutzrechtlichen Bestimmungen und Ergreifung der in dieser Verordnung vorgesehenen Datensicherheitsmaßnahmen zu verpflichten.

Mitteilungen an den Betreiber

§ 10. Die Meldebehörden haben dem Betreiber unverzüglich mitzuteilen:

1. Veränderungen im Bereich des auf das ZMR zugriffsberechtigten Personals (einschließlich der Änderungen gemäß § 5), sofern ihr nicht die Datenerfassung für die Benutzerverwaltung des ZMR vom Betreiber übertragen wurde,
2. den Wechsel oder das Ausscheiden eines Dienstleisters (§ 9) oder
3. das Auftreten von Programmstörungen, die den Datenbestand gefährden können.

Dokumentation

§ 11. Es sind Aufzeichnungen nach den Vorgaben des Betreibers zu führen, die die Zulässigkeit der tatsächlich im Bereich des ZMR durchgeführten Verwendungsvorgänge im notwendigen Ausmaß nachvollziehbar machen, wie insbesondere Änderungen, Abfragen und Übermittlungen.

Strasser