

Erläuterungen zur Freigabe und Vorabkontrolle i.S.d. § 19 DSG M.-V

I. Freigabe

Die Freigabe ist Voraussetzung dafür, dass die Verarbeitung personenbezogener Daten mit einem bestimmten automatisierten Verfahren begonnen oder ein wesentlich geändertes Verfahren weiterhin genutzt werden darf. Bei der Freigabe handelt es sich um eine materielle Zulässigkeitsvoraussetzung für die Rechtmäßigkeit der Datenverarbeitung.

Eine wesentliche Verfahrensänderung liegt vor, wenn die neue Version in einem oder mehreren Merkmalen der Verfahrensbeschreibung gemäß § 18 Abs. 1 DSG M.-V deutlich von dem bisherigen Stand abweicht. Dies ist beispielsweise der Fall, wenn der Kreis der Betroffenen oder der potentiellen Datenempfänger signifikant erweitert wird.

Grundsätzlich muss der Leiter der Daten verarbeitenden Stelle das automatisierte Verfahren freigeben. Es ist zwar möglich, diese Befugnis innerhalb der Daten verarbeitenden Stelle zu delegieren. Die Delegation wird jedoch als Ausnahme angesehen; sie muss ausdrücklich erfolgen.

Die Freigabe ist so zu dokumentieren, dass nachträglich festgestellt werden kann, wer für welche Verfahrensweise die Verantwortung trägt. Eine mündliche Freigabe mit anschließendem Aktenvermerk ist deshalb ausgeschlossen.

Die Freigabe erstreckt sich auf alle vier Grundbestandteile automatisierter Verfahren:

- die Hardware,
- die Software einschließlich der Betriebssysteme und der systemnahen Software,
- die Datenbestände und
- das aufbau- und ablauforganisatorische Regelwerk (Zuständigkeitsregelungen, Dienstanweisungen, Benutzerhandbücher und dergleichen).

Im Ergebnis darf in einer Daten verarbeitenden Stelle keine Hardware genutzt werden, die nicht mindestens einem automatisierten Verfahren zuzuordnen ist. In der Regel werden mit den einzelnen Hardware-Komponenten jeweils mehrere automatisierte Verfahren betrieben. Das Gleiche gilt für die Software und die Daten. Hardware, Software und Daten, die keinem freigegebenen Verfahren zugeordnet sind, müssen als überflüssig (richtiger: als von der Daten verarbeitenden Stelle nicht gewollt) angesehen und deshalb deaktiviert beziehungsweise gelöscht werden.

Den aufbau- und ablauforganisatorischen Regelungen kommt im Rahmen der Freigabe eine entscheidende Bedeutung zu, da in ihnen die sicherheitsrelevanten organisatorischen Maßnahmen festgelegt werden, die erforderlich sind, um technische Sicherheitsdefizite zu kompensieren.

Beispiele hierfür sind:

- Anweisungen zur Passwortgestaltung,
- Verbot der Datenspeicherung auf den Festplatten der Arbeitsplatzrechner,
- Lösungsfristen für Textdokumente,
- Anonymisierung von Musterbriefen und Textbausteinen,
- Deaktivierung von nicht benutzten Arbeitsplatzrechnern,
- Ausloggen vor Verlassen des Arbeitsplatzes,
- Überwachung von Administrations- und Wartungsarbeiten.

II. Vorabkontrolle

Die sogenannte Vorabkontrolle wird von Art. 20 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Abl. EG Nr. 281/31 vom 23. November 1995, S. 31 ff.) gefordert. Diese Richtlinie sieht vor, dass der Gesetzgeber in den Mitgliedstaaten festlegt, welche Datenverarbeitungen er für so gefährlich hält, dass vor ihrem Beginn zu prüfen ist, ob sie besondere Risiken für die Rechte der Betroffenen mit sich bringen.

In Mecklenburg-Vorpommern wurden gemäß dieser Vorgabe folgende Arten der Datenverarbeitung als potentiell gefährlich eingestuft:

- Verbund- und Abrufverfahren nach § 17 Abs. 1 DSG M-V und
- Verfahren, bei denen die in § 7 Abs. 2 DSG M-V aufgeführten, so genannten sensiblen Daten automatisiert verarbeitet werden.

Ist eine Vorabkontrolle erforderlich, so muss vor der Einrichtung oder wesentlichen Änderung des Verfahrens geprüft werden, ob die Datenverarbeitung insgesamt zulässig ist und ob die vorgesehenen technischen und organisatorischen Maßnahmen ausreichen, die vermuteten Gefährdungen des Rechts auf informationelle Selbstbestimmung in vertretbaren Grenzen zu halten.

Vorabkontrolle ist ein Teil des so genannten vorgezogenen Datenschutzes; schon vor dem Einsatz oder der Änderung eines ADV-Verfahrens hat sich die Daten verarbeitende Stelle bewusst zu machen, welche Risiken für den Datenschutz mit einem bestimmten Verfahren verbunden sind und wie diese beherrscht werden können. Die Prüfung hat deshalb zu erfolgen, bevor ein neues Verfahren seinen Wirkbetrieb aufnimmt.

Die Vorabkontrolle ist anhand der vorhandenen Unterlagen zum Konzept des Verfahrens oder eines eventuell vorhandenen Prototypen durchzuführen.

Die Stelle, die den Einsatz des Verfahrens plant, hat die erforderlichen Informationen zur Verfügung zu stellen.

Vor wesentlichen Änderungen an Verfahren, für die die Voraussetzungen des § 19 Abs. 1 DSG M-V zutreffen, ist erneut zu prüfen. Dabei kommt es nicht darauf an, ob schon vor der Einführung des Verfahrens eine Vorabkontrolle erfolgte.

Vorabkontrolle ist gemäß § 20 Abs. 3 Satz 5 Nr. 5 und § 19 Abs. 2 Satz 1 DSGVO Aufgabe des behördlichen Datenschutzbeauftragten. Die Vorabkontrolle kann sich im Einzelfall technisch sehr anspruchsvoll darstellen. Sieht sich der behördliche Datenschutzbeauftragte nicht in der Lage, diese Aufgabe zu erfüllen, weil ihm z. B. die fachspezifischen Kenntnisse über bestimmte informationstechnische Verfahren fehlen, so kann er den Landesdatenschutzbeauftragten bitten, ihn zu unterstützen.

Die Prüfung hat innerhalb einer angemessenen Frist zu erfolgen. Die Länge dieser Frist lässt sich nicht pauschal festlegen. Sie hängt von den Gegebenheiten des Einzelfalls und damit vom jeweils erforderlichen Umfang der Prüfung ab. Bei komplexeren Verfahren kann eine Dauer von drei Monaten durchaus angemessen sein. Form und Tiefe der Prüfung haben sich an der Sensibilität der zu verarbeitenden Daten und an den technischen und organisatorischen Rahmenbedingungen der geplanten Datenverarbeitung zu orientieren. Ein formalisiertes Prüfverfahren ist nicht vorgeschrieben.

Für Verfahren, bei denen Daten zum Abruf bereitgestellt werden, die jedermann zur Benutzung offen stehen, muss keine Vorabkontrolle durchgeführt werden. Der geringe Schutzbedarf dieser Daten rechtfertigt die in § 19 Abs. 2 Satz 2 DSGVO formulierte Ausnahme. Bei allgemein zugänglichen Abrufverfahren sind Risiken für den Datenschutz nicht zu erwarten, so dass in der Regel keine besonders zu prüfenden Sicherheitsmaßnahmen erforderlich sind. Im Allgemeinen findet bei diesen Verfahren schon § 17 und damit auch § 19 Abs. 2 Satz 1 DSGVO keine Anwendung.