

Verpflichtung auf Beachtung der datenschutzrechtlichen Anforderungen nach der DSGVO (Administratorenverpflichtung)

Stand: 04.05.2020

1. Geltungsbereich und Zweck

Beschäftigte eines Verantwortlichen, z. B. einer Behörde, dürfen personenbezogene Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, eine gesetzliche Regelung schreibt eine Verarbeitung dieser Daten vor (Art. 29 DSGVO).

Der Verantwortliche hat Schritte zu unternehmen, um sicherzustellen, dass ihm unterstellte Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Weisung verarbeiten, es sei denn, eine gesetzliche Regelung schreibt eine Verarbeitung dieser Daten vor (Art. 32 Abs. 4 DSGVO).

Administratorinnen und Administratoren informationstechnischer Systeme besitzen eine privilegierte Rolle innerhalb der von ihnen betreuten Systeme. Zur Erfüllung ihrer administrativen Aufgaben, die der Sicherstellung der Funktionsfähigkeit der Systeme dienen, sind sie gegenüber Standardbenutzerinnen und -benutzern mit weitergehenden Rechten und Zugriffsmöglichkeiten auf Funktionen und verarbeitete Daten ausgestattet.

Die vorliegende Verpflichtung dient

- der Sensibilisierung von mit administrativen Rechten in informationstechnischen Systemen ausgestatteten Personen für ihre Tätigkeit,
- dem Schutz der Administratorinnen und Administratoren vor unrechtmäßigen Tätigkeiten sowie deren Rechtsfolgen,
- dem Schutz der von der automatisierten Verarbeitung ihrer personenbezogenen Daten betroffenen Personen sowie
- dem Schutz der verarbeiteten Daten vor Zweckentfremdung oder Missbrauch.

2. Administrative Tätigkeiten

Administrative Tätigkeiten beinhalten u. a.

- Benutzerverwaltung:
Anlegen, Aktualisieren, Sperren, Löschen etc. von Nutzerinnen und Nutzern mittels Eingabe oder Import der notwendigen Stammdaten
- Rechteverwaltung:
Pflege von Ordnerstrukturen und Zugriffsrechten
- Support:
Kommunikation von Störungen an den Second-Level-Support

3. Datenschutzrechtliche Vorgaben

Die Grundsätze für die Verarbeitung personenbezogener Daten sind in Art. 5 Abs. 1 DSGVO festgelegt und beinhalten im Wesentlichen folgende Bestimmungen:

Personenbezogene Daten müssen

- a) auf rechtmäßige Weise und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden;
- b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden;
- c) dem Zweck angemessen sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
- d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden;
- e) in einer Form gespeichert werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).

Konkret gelten für die Administratorinnen und Administratoren folgende Vorgaben:

Die Nutzung und Administration des jeweiligen Systems unterliegt den Nutzungsbedingungen in der jeweils gültigen Fassung.

Protokolldaten, die in informationstechnischen Systemen anfallen, sind personenbezogen, da sie Aufschluss über die Aktivitäten einer Benutzerin / eines Benutzers geben. Sie unterliegen einer strikten Zweckbindung und dürfen ausschließlich zu Zwecken der Gewährleistung der Datensicherheit sowie zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert, nicht jedoch für Zwecke der Verhaltens- oder Leistungskontrolle verwendet oder ausgewertet werden. Unter der gleichen Voraussetzung erfolgt eine Protokollierung der Nutzung administrativer Rechte.

Die Auswertung personenbezogener Protokolldaten muss immer im Vier-Augen-Prinzip, unter Beachtung der personalrechtlichen Beteiligungspflichten und unter Einbeziehung der organisationseigenen Datenschutzbeauftragten erfolgen.

Jede Übermittlung oder Weitergabe von Daten an Dritte ist nur zulässig, wenn sie ausdrücklich gestattet ist. Im Zweifelsfall ist eine Genehmigung der bzw. des Verantwortlichen einzuholen und/oder die behördlichen Datenschutzbeauftragten in eine Entscheidung einzubeziehen.

4. Verpflichtungserklärung

Ich bestätige diese Verpflichtung.

Verstöße gegen diese Verpflichtung können mit Geldbuße und/oder Freiheitsstrafe geahndet werden. Ein Verstoß kann zudem eine Verletzung arbeitsvertraglicher Pflichten oder Geheimhaltungspflichten darstellen. Auch (zivilrechtliche) Schadenersatzansprüche können sich aus schuldhaften Verstößen gegen diese Verpflichtung ergeben. Eine sich aus dem Arbeits- bzw. Dienstvertrag oder sonstigen Vereinbarungen ergebende Vertraulichkeitsverpflichtung wird durch diese Erklärung nicht berührt. Die Verpflichtung gilt auch nach Beendigung der Tätigkeit weiter.

Name der Administratorin / des Administrators

Datum, Unterschrift der Administratorin / des Administrators

5. Übergabe und Entzug des administrativen Systemzugangs

administrativer Systemzugang	
<hr style="width: 80%; margin: 0 auto;"/> <p>(Benutzerkennung des administrativen Systemzugangs)</p>	
übergeben	entzogen und Passwort geändert
<p>Datum:</p> <hr style="width: 80%; margin: 5px 0;"/> <p>Uhrzeit:</p> <hr style="width: 80%; margin: 5px 0;"/> <p>Unterschrift Administratorin/Administrator</p> <hr style="width: 80%; margin: 5px 0;"/>	<p>Datum:</p> <hr style="width: 80%; margin: 5px 0;"/> <p>Uhrzeit:</p> <hr style="width: 80%; margin: 5px 0;"/> <p>Unterschrift Verantwortlicher oder beauftragte Person:</p> <hr style="width: 80%; margin: 5px 0;"/>