Evangelische Fachschulen für Sozialpädagogik

Stand: Mai 2019

Merkblatt über den Datenschutz für Mitarbeitende

Die sorgsame und vertrauliche Behandlung von Daten ist ein wichtiges Gebot im Rahmen der kirchlichen Arbeit. Die Mitarbeitenden sind für die datenschutzrechtlich korrekte Ausübung ihrer Tätigkeit verantwortlich. In diesem Merkblatt erhalten Sie Informationen über den wesentlichen Inhalt des Datengeheimnisses und den Sinn der Verpflichtungserklärung.

Warum ist Datenschutz wichtig?

Niemand darf durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt werden. Jeder hat das Recht, über den Umgang mit seinen personenbezogenen Daten grundsätzlich selbst zu bestimmen. Das Ziel des Datenschutzes ist es, den Einzelnen vor einer Beeinträchtigung zu schützen.

Welche rechtlichen Grundlagen gelten für den Datenschutz?

Für den Verein Evang. Ausbildungsstätten für Sozialpädagogik gilt das Datenschutzgesetz der Evangelischen Kirche in Deutschland (DSG-EKD). Bestimmungen aus dem Schulgesetz bzw. Regelungen des Kultusministeriums oder des Regierungspräsidiums haben Vorrang.

Was sind personenbezogene Daten?

Personenbezogene Daten sind alle Informationen, die sich auf natürliche Person beziehen, z. B. Geburtsdatum, Anschrift, Konfession, Beruf, Familienstand, Gesundheitszustand, Fotos, Videoaufzeichnungen, Grundbesitz, Einkommen oder Rechtsbeziehungen zu Dritten. Nach § 2 Absatz 2 DSG-EKD können personenbezogene Daten in Papierform (Akten, Notenlisten, Leitz-Ordner etc.) oder bei automatisierten Verarbeitungen anfallen (Word, Excel, PowerPoint, Outlook etc.) – auch auf mobilen Endgeräten oder privaten Computern.

Welche grundsätzlichen Regelungen gelten für den Datenschutz?

Für die Verarbeitung personenbezogener Daten gilt der Grundsatz des Verbots mit Erlaubnisvorbehalt, d. h. eine Verarbeitung ist nur rechtmäßig, a) wenn eine Rechtsvorschrift dies erlaubt, b) wenn es zur Erfüllung eines Vertrages notwendig ist oder c) wenn die betroffene Person eingewilligt hat.

Personenbezogene Daten sind gemäß § 5 DSG-EKD nach den folgenden Grundsätzen zu verarbeiten:

1. Rechtmäßigkeit, Verhältnismäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz;
2. Zweckbindung: Personenbezogene Daten werden für festgelegte, eindeutige und legitime Zwecke erhoben;
3. Datenminimierung: Die Verarbeitung personenbezogener Daten wird auf das dem Zweck angemessene und notwendige Maß beschränkt; personenbezogene Daten sind zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert;
4. Richtigkeit: Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein;
5. Speicherbegrenzung: Personenbezogene Daten werden in einer Form gespeichert, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Personenbezogene Daten dürfen länger gespeichert werden, soweit sie für die Zwecke des Archivs, der wissenschaftlichen und historischen Forschung sowie der Statistik verarbeitet werden;
6. Integrität und Vertraulichkeit: Personenbezogene Daten werden in einer Weise verarbeitet, die eine angemessene Sicherheit gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Zerstörung oder unbeabsichtigter Schädigung.

Alle Informationen, die Mitarbeitende auf Grund ihrer Arbeit an und mit Akten, Dateien und Listen erhalten, sind vertraulich zu behandeln. Diese Pflicht besteht auch nach Beendigung der Tätigkeit fort. Die Übermittlung der Daten an Personen, Behörden und sonstige öffentliche Stellen ist nur statthaft, soweit eine Rechtsgrundlage für die Offenlegung der Daten vorhanden ist und sie zur Erfüllung kirchlicher Aufgaben erforderlich sind (siehe auch § 8 DSG EKD).

Was ist aus Sicht des technischen und organisatorischen Datenschutzes zu beachten?

Daten (z. B. Belege, EDV-Listen), Datenträger (z. B. Festplatten, USB-Sticks, DVDs) und Zubehör (z. B. Schlüssel) sind stets sicher und verschlossen zu verwahren und vor jeder Einsicht oder sonstigen Nutzung durch Unbefugte zu schützen. Es ist untersagt, Passwörter und Hardwaretoken (z. B. USB-Stick und Chipkarten) sowie Benutzerkennungen weiterzugeben.

Eigenmächtige Änderungen der dienstlichen Hardware und deren Konfiguration – insbesondere der Einbau von Karten und der Anschluss von Druckern oder anderen Zusatzgeräten – sind ebenso wie das unbefugte Einspielen von privater Software nicht gestattet.

Soweit aus Gründen der Aufgabenerfüllung Daten mittels eines Datenträgers auf einen PC übertragen werden, ist durch geeignete Maßnahmen sicherzustellen, dass die auf dem Datenträger enthaltenen Daten nicht mit Schadsoftware befallen sind.

Analoge und digitale Daten, die nicht mehr benötigt werden, müssen in einer Weise vernichtet oder gelöscht werden, die jeden Missbrauch der Daten ausschließt. Mängel, die bei der Datenverarbeitung auffallen, müssen den Vorgesetzten gemeldet werden.

Welche Regelung gilt für den Umgang mit personenbezogenen Daten von Schülerinnen und Schülern auf privaten Datenverarbeitungsgeräten?

Auf privaten Datenverarbeitungsgeräten dürfen lediglich die personenbezogenen Daten jener Schülerinnen und Schüler verarbeitet werden, die von der jeweiligen Lehrkraft selbst unterrichtet werden bzw. deren Klassenlehrerin/Klassenlehrer sie/er ist. Die personenbezogenen Daten müssen verschlüsselt gespeichert werden und dürfen nur verschlüsselt über Internet übermittelt werden. Diese Daten sind gegen unbefugten Zugriff zu schützen. Das Kultusministerium empfiehlt eine Speicherung dienstlicher personenbezogener Daten auf einem verschlüsselten USB-Stick. Die Daten müssen spätestens nach dem Ende des nächsten Schuljahres gelöscht werden.

Folgende technischen und organisatorischen Maßnahmen sind laut Anlage 1 der Verwaltungsvorschrift „Datenschutz an öffentlichen Schulen“ zu beachten:

- Zutrittskontrolle: kein unbefugter Zugang zum Gerät
- Benutzerkontrolle: kein unbefugtes Starten des Geräts
- Zugriffskontrolle: kein unbefugter Zugriff auf Dateiordner
- Datenträger und Speicherkontrolle: verschlüsselte Ablage
- Transportkontrolle: falls Daten übermittelt werden, geschieht dies verschlüsselt
- Datenlöschung mittels geeignetem Verfahren
- Einsatz eines Betriebssystems, für das der Hersteller weiterhin Sicherheitsupdates anbietet
- Einsatz einer Firewall, sofern das Gerät eine Verbindung zum Internet hat
- Einsatz eines Virenschutzprogramms auf aktuellem Stand

Welche Vereinbarung gilt zur dienstlichen Nutzung privater Smartphones?

Der Trägerverein hat großes Vertrauen in das Verantwortungsbewusstsein seiner Mitarbeiterinnen und Mitarbeiter. Private Endgerät können für den dienstlichen Gebrauch genutzt werden. Die Mitarbeitenden sichern zu, dass auf den Endgeräten

- aktuelle Virenschutz-Programme (soweit verfügbar) eingesetzt werden
- alle Sicherheitspatches zeitnah eingespielt werden
- der Zugriff auf die Endgeräte angemessen geschützt ist, z. B. durch starke Passwörter
- so wenig wie möglich personenbezogene Daten verarbeitet werden
- die Nutzung unsicherer Software aus unbekannten Quellen unterlassen wird

Die Mitarbeitenden sichern zu, dass sie bei einem Wechsel des Endgeräts oder bei Beendigung ihrer Tätigkeit alle dienstlichen Daten vollständig löschen.

Bei Fragen zum Datenschutz wenden Sie sich bitte an die Schulleitung oder an die Geschäftsstelle des Trägervereins: info@ev-fs.de

Dieses Merkblatt basiert auf dem Musterformular der EKD vom Mai 2018: https://datenschutz.ekd.de