Edith-Stein-Schulstiftung
des Bistums Magdeburg
Max-Josef-Metzger-Straße 1
39104 Magdeburg

Datenschutzkonzept der Edith-Stein-Schulstiftung des Bistums Magdeburg

1. Anwendungsbereich und Begriffsbestimmungen

Das Gesetz über den Kirchlichen Datenschutz in der jeweils gültigen Fassung ist Grundlade für die automatisierte und nichtautomatisierte Verarbeitung von Dateien und für Akten in der Verwaltung der Edith-Stein-Schulstiftung des Bistums Magdeburg (ESS) und in allen angeschlossenen Schulen der Stiftung. Eine automatisierte Datei ist jede Sammlung von Daten, die durch automatisierte Verfahren nach bestimmten Merkmalen ausgewertet werden kann (siehe § 4 KDG).

2. Datengeheimnis

Den bei der Verarbeitung personenbezogener Daten tätigen Personen ist untersagt, diese unbefugt zu verarbeiten (Datengeheimnis). Alle Mitarbeiter sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis und die Einhaltung der einschlägigen Datenschutzregelungen schriftlich zu verpflichten (§ 5 KDG). Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit.

3. Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten

Daten dürfen nur erhoben werden, wenn ihre Kenntnis notwendig ist, um die jeweilige konkrete und aktuelle satzungsgemäße Aufgabe vollständig und in angemessener Zeit erfüllen zu können. Eine Erhebung "auf Vorrat" ist unzulässig. Die Daten werden i. d. R. direkt bei den Betroffenen erhoben (§ 6 Abs. 1 KDO). Für die Erhebung und Verarbeitung muss eine rechtliche Verpflichtung oder die schriftliche Einwilligung der jeweiligen Person bzw. bei Schülern die Einwilligung der Erziehungsberechtigten vorliegen.

4. Zweckgebundene Nutzung der Daten

Personenbezogene Daten dürfen nur zweckgebunden verwendet werden. Gebunden sind sie an den Zweck, zu dem sie erhoben wurden. Eine Verwendung zu anderen Zwecken muss durch Gesetz oder Einwilligung der Betroffenen zulässig sein. Es muss gewährleistet sein, dass allen Beschäftigten in der Schule oder der ESS nur die Daten zugänglich sind, die sie zur Erledigung ihrer Aufgaben benötigen (siehe auch §§ 6 Abs. 2 und 7 KDG).

5. Einwilligung

Wird die Einwilligung bei der betroffenen Person eingeholt, ist diese auf den Zweck der Verarbeitung sowie bei Nachfrage auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung der betroffenen Person beruht. Die Einwilligung bedarf der Schriftform (Nachweis / siehe hierzu auch weitere Erläuterungen § 8 KDG). Personenbezogene Daten eines Minderjährigen, dem elektronisch eine Dienstleistung oder ein vergleichbares anderes Angebot von schulischer Seite gemacht wird, dürfen nur verarbeitet werden, wenn der Minderjährige das sechzehnte Lebensjahr vollendet hat. Hat der Minderjährige das sechzehnte Lebensjahr noch nicht vollendet, ist die Verarbeitung nur rechtmäßig, sofern und soweit diese Einwilligung durch den Personensorgeberechtigten erteilt wird.

6. Erstellung von eigenen Aufzeichnungen

Eigene Aufzeichnungen (von personenbezogenen Daten) dürfen nur angefertigt werden, wenn es zur Erfüllung einer konkreten und aktuellen arbeitsplatzbezogenen Aufgabe unumgänglich ist. Sie müssen auf das Notwendige beschränkt, auch im privaten Bereich an einem sicheren Ort aufbewahrt und sachgerecht vernichtet werden, sobald sie nicht mehr erforderlich sind.

7. Grundsätze für die Verarbeitung personenbezogener Daten

Es muss sichergestellt sein, dass die Daten sachlich richtig sind und erforderlichenfalls schnell auf den neuesten Stand gebracht werden. Daten die unrichtig sind, müssen unverzüglich gelöscht oder berichtigt werden. Die Daten müssen in einer Weise verarbeitet 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 (siehe auch § 7 KDG).

8. Aufbewahrung von Datenträgern

Daten und Datenträger (Akten, Karteikarten, Listen, Aufzeichnungen, USB-Sticks, beschriebene CD und DVD und sonstige Speichermedien) müssen so aufbewahrt werden, dass Unbefugte keinen Zugriff haben; ggf. müssen entsprechende Möglichkeiten (Verschlüsselung und/oder Passwortschutz) eingerichtet werden.

9. Erstellung von Kopien auf Datenträgern

Kopien von Daten und Datenträgern dürfen nur angefertigt werden, wenn es zur Durchführung einer konkreten dienstlichen Aufgabe erforderlich ist. Sicherungskopien sind verschlossen aufzubewahren und vor dem Zugriff von unberechtigten Personen zu schützen. Es ist zu prüfen, ob Verbleib und Rücklauf von kopierten oder weitergegebenen Daten geregelt werden müssen (z. B. bei Listen, Protokollen), um die Einhaltung der Datenschutzbestimmungen zu gewährleisten. Das Kopieren von Softwareprodukten ist nur mit Zustimmung der Eigentümer und unter Beachtung der Lizenzbestimmungen zulässig.

10. Umgang mit Passwörtern

Verwendete Pass- oder Kennworte sind geheim zu halten. Ggf. kommt zu einem späteren Zeitpunkt noch eine Anweisung zum Einsatz von Pass- oder Kennwort (Länge, Häufigkeit des Wechsels, Vermeidung bestimmter Wortarten, schriftliche Hinterlegung, Verwendung einer Bildschirmsperre), die dann beachtet werden muss.

11. Ausgediente Datenträger oder EDV-Geräte

Nicht mehr benötigte Datenträger oder EDV-Geräte (PC, Festplatten, Kopierer, USB-Sticks, Smartphone …) müssen in einer Weise vernichtet, gelöscht oder entsorgt werden, die jede unbefugte Kenntnisnahme von Daten ausschließt. Bis zu ihrer Vernichtung, Löschung oder Entsorgung müssen sie vor einem unbefugten Zugriff geschützt aufbewahrt werden.

12. Strafbare Handlungen im Zusammenhang mit der EDV-Nutzung

Bei der Nutzung von EDV sind bestimmte Handlungen durch das Strafgesetzbuch mit Strafe bedroht, so eine rechtswidrige Veränderung, Löschung oder Beseitigung von Daten, eine Zerstörung von Datenverarbeitungsanlagen oder Datenträgern, eine dadurch erfolgte Störung des Ablaufs der Datenverarbeitung einer Stelle, dass unbefugte sich Verschaffen von besonders gesicherten EDV-Daten oder das Schädigen fremden Vermögens durch unbefugtes Einwirken auf einen Daten-verarbeitungsvorgang (vgl. insbes. §§ 202a, 263a, 269, 270, 303a, 303b StGB).

13. Nutzung privater IT-Geräte

Die Nutzung privater PC oder anderer speicherfähiger Geräte zu dienstlichen Zwecken ist nur zulässig, wenn personenbezogene Daten nicht auf dem privaten Gerät gespeichert werden. Die Speicherung darf nur in dafür autorisierten Medien (derzeit verschlüsselter USB-Stick der ESS) und einem freigegebenen Bereich des Schulservers erfolgen. Für die Nutzung der USB-Sticks gibt es gesonderte Nutzungsbedingungen, die getrennt vereinbart werden. Die Daten der mobilen USB-Sticks sind regelmäßig auf dem Schulserver zu sichern. Bei Missbrauch oder bei Nichtbefolgung von Vorgaben kann die Nutzung privater IT-Geräte untersagt werden. In diesen Fällen müssen Geräte in der Schule genutzt werden.

14. Unabdingbare Rechte der betroffenen Person

Die Rechte der betroffenen Person auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit oder Widerspruch können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden (genauere Details kann man den §§ 17 – 25 KDG entnehmen und sind Grundlage für dieses Konzept).

15. Verfahrensverzeichnisse

Jeder Verantwortliche in der Verwaltung und in den Schulen führt ein Verzeichnis aller Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen. Dieses Verzeichnis hat folgende Angaben zu enthalten (siehe § 31 KDG):

a) den Namen und die Kontaktdaten des Verantwortlichen und ggf. des gemein-sam mit ihm Verantwortlichen sowie des betrieblichen Datenschutzbeauftragten,
b) die Zwecke der Verarbeitung,
c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten,
d) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien,
e) eine detaillierte Beschreibung des gesamten Prozesse und aller beteiligten Personen, um nachvollziehen zu können, dass datenschutzkonform gearbeitet wird.

16. Auftragsverarbeitung

Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so darf dieser nur mit Auftragsverarbeitern zusammenarbeiten, die den Vorgaben des KDG bzw. der EU-Datenschutzgrundverordnung entsprechen und die dies auch schriftlich in einem Vertrag bestätigen.

In diesem Vertrag sind folgende Inhalte festzulegen (siehe auch § 29 KDG):

a) Gegenstand der Verarbeitung,
b) Dauer der Verarbeitung,
c) Art und Zweck der Verarbeitung,
d) die Art der personenbezogenen Daten,
e) die Kategorien betroffener Personen und
f) die Pflichten und Rechte des Verantwortlichen.

Ein Auftragsverarbeiter darf die Daten nur innerhalb der Mitgliedstaaten der Europäischen Union oder des Europäischen Wirtschaftsraumes verarbeiten.

17. Allgemeine Grundsätze bei der Nutzung von personenbezogenen Daten, die automatisiert verarbeitet oder gespeichert werden

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind:

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbe-zogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Über-tragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten stattgefunden hat (Weitergabekontrolle),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle), zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
7. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Edith-Stein-Schulstiftung
des Bistums Magdeburg
Max-Josef-Metzger-Straße 1
39104 Magdeburg

Verpflichtungserklärung

Ich verpflichte mich,

1. das Gesetz über den Kirchlichen Datenschutz in der jeweils gültigen Fassung sowie die anderen für meine Tätigkeit geltenden Datenschutzregelungen einschließlich der zu ihrer Durchführung ergangenen Bestimmungen sorgfältig einzuhalten und bestätige, dass ich auf die wesentlichen Grundsätze der für meine Tätigkeit geltenden Bestimmungen hingewiesen wurde. Hierzu wurde mir das Datenschutzkonzept der Edith-Stein-Schulstiftung vorab zum Durchlesen und Durcharbeiten ausgehändigt. Ich wurde ferner darauf hingewiesen, dass die KDG und die Texte der übrigen für meine Tätigkeit geltenden Datenschutzvorschriften eingesehen werden können.
2. das Datengeheimnis auch nach Beendigung meiner Tätigkeit zu beachten.

Ich bin darüber belehrt worden, dass ein Verstoß gegen das Datengeheimnis gleichzeitig einen Verstoß gegen die Schweigepflicht darstellt, der disziplinarrechtliche beziehungsweise arbeitsrechtliche/strafrechtliche Folgen haben kann.

Vorname	
Name	
Ort, Datum	
Unterschrift (Mitarbeiter*in)	

Diese Erklärung wird in die Personalakte hinzugefügt.