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 Grundlage für die automatisierte und nichtautomatisierte Verarbeitung von personenbezogenen Daten 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). Weitere Begriffsbestimmungen finden Sie in Anlage 1.

2 Verantwortlicher und Datenschutzbeauftragte

Verantwortlicher ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Verantwortlicher i.S.d. § 4 Nr. 9 KDG ist die ESS und die jeweiligen Schulen selbst, vertreten durch den Vorstand bzw. die Schulleiter.

Für die ESS und die angehörigen Schulen wurde eine externe Datenschutzbeauftragte bestellt:

LGD Datenschutz GmbH
Frau Joelle Hirsch
Rogätzer Straße 8
39106 Magdeburg
Telefon: 0391 55686325
E-Mail: j.hirsch@lgd-data.de

3 Datengeheimnis

Den bei der Verarbeitung personenbezogener Daten tätigen Personen ist untersagt, diese unbefugt zu verarbeiten (Datengeheimnis). Alle Mitarbeiter*innen 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.

4 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. Für die Erhebung und Verarbeitung muss eine rechtliche Verpflichtung oder die schriftliche Einwilligung der jeweiligen Person bzw. bei minderjährigen Schülern die Einwilligung der Erziehungsberechtigten vorliegen (§ 6 Abs. 1 KDG).

5 Zweckgebundene Nutzung der Daten

Personenbezogene Daten dürfen nur zweckgebunden verwendet werden. Gebunden sind sie an den Zweck, zu dem sie erhoben werden. 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).

6 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 die/den Personensorgeberechtigten erteilt wird.

7 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.

8 Grundsätze für die Verarbeitung personenbezogener Daten

Es muss sichergestellt sein, dass

- die Daten auf eine rechtmäßige und nachvollziehbare Weise verarbeitet werden. Jede Verarbeitung bedarf einer Rechtsgrundlage und darf nicht ohne das Wissen des Betroffenen erfolgen,
- die Daten nur für die festgelegten Zwecke verarbeitet werden, für die sie erhoben wurden,
- 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 nur so lange wie für die jeweiligen Zwecke erforderlich verarbeitet und nach Wegfall des Zwecks anonymisiert oder gelöscht bzw. vernichtet 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.

9 Aufbewahrung von Daten

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 (Schloss, Verschlüsselung und/oder Passwortschutz) eingerichtet werden.

10 Einsatz von Drucker, Kopier- und Scangeräten

Bei der Auswahl eines Druckers bzw. Fax- oder Multifunktionsgerätes zum Druck von vertraulichen Unterlagen ist zu beachten, dass keine sensiblen Dokumente von Unbefugten gelesen werden können. Der Ausdruck ist sofort nach Fertigstellung aus dem Drucker bzw. Fax- oder Multifunktionsgerät zu entfernen, sodass ein unbefugtes Einsehen verhindert werden kann. Dies gilt insbesondere, wenn sich Fremdpersonen in den Räumlichkeiten aufhalten. Bei Kopier- und Scangeräten mit eigener Speichereinheit ist sicherzustellen, dass ein Zugriff auf personenbezogene Daten durch unberechtigte Mitarbeiter oder sonstige Dritte nicht möglich ist.

11 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.

12 Umgang mit Passwörtern

Standardpasswörter müssen durch ausreichend starke Passwörter ersetzt werden. Verwendete Pass- oder Kennwörter sind geheim zu halten. Es dürfen keine Notizen über die verwendeten Pass- oder Kennwörter aufbewahrt werden. Zudem darf die Eingabe nur unbeobachtet erfolgen. Wichtig ist, dass ein starkes Passwort verwendet wird. Für die Wahl eines starken Passwortes gelten folgende Regeln:

- mindestens 8 Zeichen
- Groß- und Kleinbuchstaben
- Ziffern
- Sonderzeichen
- kein persönlicher Bezug (Name, Geburtstag usw.)
- kein Wort, das in identischer Schreibweise in Wörterbüchern vorkommt

13 Vernichtung von Daten bzw. Datenträgern

Vertrauliche Unterlagen sind über Aktenvernichter zu entsorgen. Vertrauliche Unterlagen dürfen niemals im normalen Papiermüll entsorgt werden.

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.

14 Strafbare Handlungen im Zusammenhang mit der EDV-Nutzung

Bei der Nutzung von EDV sind strafbare Handlungen durch das Strafgesetzbuch mit entsprechenden Konsequenzen bedroht. So sind eine bewusst 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 Datenverarbeitungsvorgang verboten (vgl. insbes. §§ 202a, 263a, 269, 270, 303a, 303b StGB).
Soweit personenbezogene Daten verarbeitet werden, müssen diese vertraulich behandelt werden und dürfen nicht unbefugt erhoben, genutzt oder übermittelt sowie zu keinem anderen als dem zur Aufgabenerfüllung erforderlichen Zweck verarbeitet werden. Ein Verstoß gegen diese Verpflichtung kann nach § 51 KDG mit einem Bußgeld geahndet werden. Insbesondere können Verstöße zugleich arbeits- und dienstrechtliche Konsequenzen haben und zu einer Abmahnung, Kündigung oder auch zu einer Schadensersatzpflicht führen.

15 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.

16 Versand sensibler Daten

Der Versand von E-Mails, deren Inhalt vertraulich ist, darf nur in verschlüsselter Form und ausschließlich an die vorab kommunizierte E-Mail-Adresse des Empfängers erfolgen. Unverschlüsselt dürfen E-Mails nur dann versendet werden, wenn ihr Inhalt nicht vertraulich ist. Erfolgt eine Übermittlung sensibler personenbezogener Daten an Postfächer, auf die mehr als eine Person Zugriff haben (Funktionspostfächer), muss vorher durch Abstimmung mit dem Empfänger sichergestellt werden, dass nur autorisierte Personen Zugriff auf dieses Postfach haben.

Sensible Daten dürfen nur unter Einhaltung von Sicherheitsvorkehrungen übertragen werden. So sind mit dem Empfänger Sendezeitpunkt und das Empfangsgerät abzustimmen, damit der Empfänger das Fax direkt entgegennehmen kann.

17 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 – 24 KDG entnehmen und sind Grundlage für dieses Konzept).

Um die gesetzlich geforderte Frist von einem Monat zur Beantwortung der Anfrage einhalten zu können, gibt der betroffene Mitarbeiter die Anfrage zügig an den Verantwortlichen und die Datenschutzbeauftragte weiter. Die Datenschutzbeauftragte prüft und beantwortet die Anfrage in Abstimmung mit dem Verantwortlichen innerhalb der gesetzlich vorgeschriebenen Frist und dokumentiert die Angelegenheit.

18 Verfahrensverzeichnisse

Jede*r 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 der/des Verantwortlichen und ggf. des gemeinsam mit ihm Verantwortlichen sowie des Datenschutzbeauftragten,
b) die Zwecke der Verarbeitung,
c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten,
d) die Kategorie von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden,
e) ggf. Übermittlung von personenbezogenen Daten in ein Drittland oder an eine internationale Organisation, einschl. Angabe des Drittlands bzw. der internationalen Organisation und der dort getroffenen geeigneten Garantien,
f) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien,
g) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen,
h) und zusätzlich eine detaillierte Beschreibung der gesamten Prozesse und aller beteiligten Personen, um nachvollziehen zu können, dass datenschutzkonform gearbeitet wird.

19 Auftragsverarbeitung

Ein Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

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 der/des Verantwortlichen.

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

20 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 personenbezogene 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 das 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 Übertragung 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.

21 Meldepflicht bei Verletzung des Datenschutzes

Dem Verantwortlichen obliegt die Meldung von Datenschutzverletzungen an die Datenschutzaufsicht und je nach Höhe des Risikos für die Rechte und Freiheiten betroffener Personen auch an die betroffene Person selbst. Um den gesetzlich geforderten Meldezeitraum von 72 Stunden einhalten zu können, informiert der betroffene Mitarbeiter bei einer erkannten Datenschutzverletzung umgehend den Verantwortlichen sowie den Datenschutzbeauftragten. Der Datenschutzbeauftragte nimmt nach Abstimmung mit dem Verantwortlichen und nach Prüfung des Sachverhalts und der etwaigen Risiken eine Meldung an die Datenschutzaufsicht und ggf. auch an die betroffene Person vor.

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

Anlage 1

Begriffsbestimmungen

- **Personenbezogene Daten**: Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Betroffener). Daten der Schüler oder Erziehungsberechtigten gehören dabei ebenso zu den personenbezogenen Daten wie Daten von Mitarbeitern. Es genügt, wenn die jeweilige Information mit dem Namen des Betroffenen verbunden ist oder unabhängig hiervon aus dem Zusammenhang hergestellt werden kann. Ebenso kann eine Person bestimmbar sein, wenn die Information mit einem Zusatzwissen erst verknüpft werden muss, so z. B. beim Autokennzeichen.
- **Besondere Kategorien personenbezogener Daten**: Informationen, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen sowie eine eventuelle Gewerkschaftszugehörigkeit hervorgehen kann sowie genetische Daten, biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben bzw. der sexuellen Orientierung einer natürlichen Person.
- **Verarbeitung:** Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten, wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.
- **Pseudonymisierung**: Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.
- **Anonymisierung**: Verarbeitung personenbezogener Daten in einer Weise, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.
- **Verantwortlicher**: Die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.
- **Datenschutzverletzung**: Verletzung der Sicherheit, die zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.