Hinweise zu technischen und organisatorischen Datenschutzmaßnahmen nach der EU-DSGVO

Ein Überblick

Die Schule als die datenschutzrechtlich verantwortliche Stelle ist für die Einhaltung des Datenschutzes verantwortlich. Die gilt auch für den Fall, dass die Verarbeitung durch einen Auftragsverarbeiter, also z. B. ein Rechenzentrum eines anderen Unternehmens, erfolgt.

Die Schule muss somit unter Berücksichtigung der Art, der Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen treffen.

Bereits bei der **Auswahl und ersten Installation und Konfiguration** einer Soft- und Hardware muss die Schule sich um den Datenschutz kümmern, denn schon durch die Gestaltung der Technik an sich müssen Datenschutzmaßnahmen realisiert sein.

- **privacy by design:**
  Die Software muss so gestaltet sein, dass die Einhaltung der Datenschutzgrundsätze nach Art. 5 EU-DSGVO eingehalten werden können. Dazu müssen technische aber auch organisatorische Datenschutzmaßnahmen überhaupt realisiert werden können. Beispielsweise muss eine Verschlüsselung möglich sein, wenn durch die Software Daten über das Internet übermittelt werden. Ferner muss die Software in der Lage sein, dass Daten überhaupt gelöscht werden können.
- **privacy by default:**
  Voreinstellungen sollten so gewählt sein, dass grundsätzlich nur personenbezogene Daten, die zur Aufgabenerfüllung erforderlich sind, verarbeitet werden können. Dies gilt im Hinblick auf die Menge der verarbeiteten Daten, den Umfang ihrer Verarbeitung, die Speicherfristen und auch deren Zugänglichkeit. Letztes bedeutet, dass Datenzugriffe durch ein vorkonfektioniertes Rechte- und Rollenkonzept so ausgestaltet sein müssen, dass nur ein Zugriff auf die Daten möglich ist, die zur Verarbeitung erforderlich sind. Es ist aber auch zu prüfen, ob sämtliche durch die Software einzugebenden personenbezogenen Daten überhaupt verarbeitet werden dürfen, d. h. ob dafür eine Rechtsgrundlage existiert, und ob diese Daten überhaupt zur Aufgabenerfüllung erforderlich sind.

Die Schule muss zudem gewährleisten, dass auch beim **Betrieb des Verfahrens** der Datenschutz gewährleistet ist. Hierzu sind insbesondere folgende Aspekte zu berücksichtigen:

- Pseudonymisierung und Verschlüsselung personenbezogener Daten, sofern dies zur Aufgabenerfüllung möglich ist.

- Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen.
  Dies umfasst - je nach Erforderlichkeit im Einzelfall - Maßnahmen der Zutrittskontrolle, der Zugriffskontrolle, der Benutzerkontrolle, der Eingabekontrolle, der Organisationskontrolle, ferner den Einsatz von Authentifizierungsverfahren und Verschlüsselungstechnologien (besonders wenn die Daten übermittelt werden).
- Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.
  Darunter sind insbesondere Maßnahmen der Verfügbarkeitskontrolle zu verstehen, wie eine Datensicherung durch Backups, aber auch die redundante Ausgestaltung verschiedener Komponenten wie z. B. Festplatten.
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.
- Maßnahmen, die die nachträgliche Überprüfung und Feststellung gewährleisten, ob und von wem personenbezogene Daten erfasst, verändert oder gelöscht worden sind.
- Die Sensibilisierung und Schulung der an Verarbeitungsvorgängen Beteiligten.
- Die Beteiligung der oder des Datenschutzbeauftragten der jeweiligen öffentlichen Stelle.
- Die Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der öffentlichen Stelle und von Auftragsverarbeitern.
- Spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung personenbezogener Daten für andere Zwecke die Einhaltung der datenschutzrechtlichen Vorgaben sicherstellen.

Die Schule ist für den Datenschutz bei der Verarbeitung personenbezogener Daten verantwortlich, auch dann, wenn eine Auftragsdatenverarbeitung erfolgt.

Dazu muss sie bereits bei der Auswahl der eingesetzten Technik den Datenschutz berücksichtigen und ferner während des Betriebes geeignete Maßnahmen treffen.