Hinweise zum Verfahren zur regelmäßigen Überprüfung, Bewertung, Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen nach Art. 32 EU-DSGVO

Nach Art. 32, Abs. 1, lit. d EU-DSGVO muss die Schule durch ein geregeltes Verfahren überprüfen, bewerten und evaluieren, ob die getroffenen technischen und organisatorischen Datenschutzmaßnahmen noch wirksam sind. Dies muss regelmäßig stattfinden.
Die Überprüfung, Bewertung und Evaluation ist allein schon deshalb erforderlich, weil bei Software-Produkten immer wieder Angriffsstellen (sog. Lecks) oder Fehler bekannt werden, die zu einem Datenschutz-Risiko führen könnten. Ferner ist dies auch aufgrund der technologischen Weiterentwicklung notwendig: so muss wegen der ständig steigenden Computerleistung die Verschlüsslung laufend angepasst werden, um eine mögliche Entschlüsselung zu verhindern. Eine Erforderlichkeit kann sich auch ergeben, wenn in einem Verfahren die Software ausgetauscht wird oder wenn eine funktionale Erweiterung eines bestehenden Verfahrens erfolgt und beispielsweise weitere Daten(-arten) verarbeitet werden.

<u>Vorgehen:</u>
Die Schule muss in regelmäßigen Zeitabstanden die Wirksamkeit der getroffenen technischen und organisatorischen Maßnahmen kontrollieren - auch bei bereits eingesetzten Verfahren.
Hierzu sollte sich die Schule für jedes einzelne Verfahren mit den folgenden Leitfragen befassen.

- Befindet sich die Software (Betriebssystem, Anwendungssoftware, evtl. Datenbank usw.) auf dem aktuellen Releasestand?
- Ist sichergestellt, dass die aktuellen, verfügbaren Patches eingespielt werden?
- Werden Firewall, Virenschutz und andere sicherheitsrelevante Software regelmäßig aktualisiert?
- Gab es in der Vergangenheit Sicherheitsvorfälle, Störungen, unbefugte Datenzugriffe oder wurde das System gehackt? Welche Maßnahmen wurden als Folge davon getroffen? Reichen diese Maßnahmen aus?
- Entsprechen die getroffenen technischen und organisatorischen Maßnahmen noch dem aktuellen Stand der Technik? Hinweise hierzu finden Sie auf der Seite des Bundesamtes für die Sicherheit in der Informationstechnik (BSI).
    - Ist die eingesetzte Verschlüsselungstechnologie ausreichend? Entspricht diese dem aktuellen Stand?
- Ist durch das realisierte Authentifizierungsverfahren bei einer Nutzeranmeldung sichergestellt, dass unbefugter Zugriff abgewehrt wird?
    - Genügen die Anforderungen an das Passwort (in Bezug auf Komplexität, Passwortlänge, Sperrung nach einer Anzahl von Fehlversuchen, usw.)?

        - Genügt eine Authentifizierung per User und Passwort oder ist eine zwei Faktoren-Authentifizierung erforderlich? -> Hinweise hierzu finden Sie im „Netzbrief“ des Kultusministeriums. Diesen finden Sie unter www.it.kultus-bw.de.
    - Sind die realisierten Protokollierungen ausreichend?
        - Kann nachvollzogen werden, welche Daten zu welcher Zeit von wem in das Datenverarbeitungssystem eingegeben wurden?
        - Werden die Protokollierungen tatsächlich regelmäßig überprüft?
    - Reichen die umgesetzten Datensicherungen (Backups) aus, um das System wiederherzustellen?
    - Werden die mit der Datenverarbeitung betrauten Personen regelmäßig sensibilisiert bzw. fortgebildet?

Hinweis für den Fall einer Auftragsdatenverarbeitung: Die oben erläuterte Pflicht hat die Schule auch für den Fall, dass die Datenverarbeitung durch einen Dienstleister als Auftragsverarbeiter erfolgt, wenn also eine sogenannte Auftragsdatenverarbeitung stattfindet. Sofern die Schule jedoch die vom Kultusministerium bereit gestellten Vertragsformulare verwendet, stellt sie sicher, dass diese Pflicht in Bezug auf die vom Auftragsverarbeiter betriebene Informationstechnik erfüllt wird, indem sie durch den Vertrag auf den Auftragsverarbeiter delegiert wird.

Getroffene technische und organisatorische Maßnahmen müssen regelmäßig im Hinblick auf deren Wirksamkeit verifiziert werden.
Dies muss schriftlich dokumentiert werden.