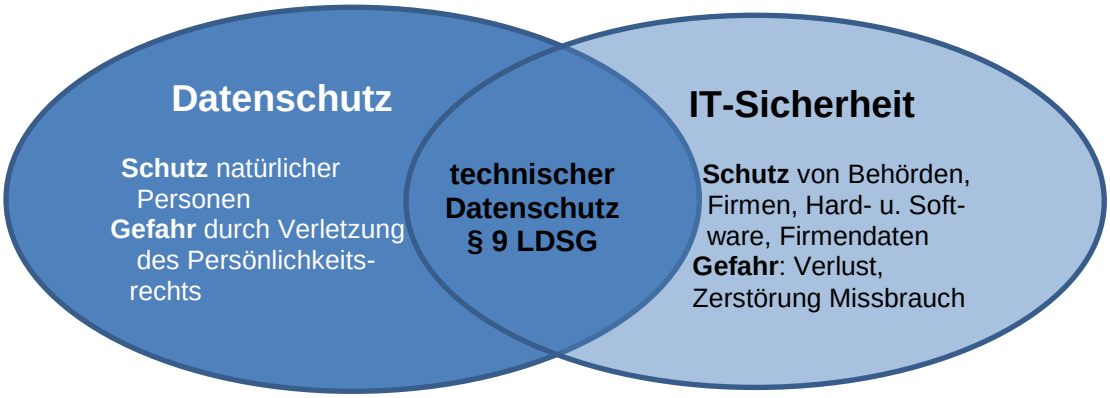
## Hinweise zur Zertifizierung bei einer Auftragsdatenverarbeitung

Erfolgt eine Auftragsdatenverarbeitung, so muss sich der Auftraggeber nach § 7 Abs. 2 Satz 6 LDSG davon überzeugen, dass der Auftragnehmer u.a. die notwendigen technischen und organisatorischen Maßnahmen trifft.

Aufgrund der Komplexität der modernen IT stellt es Schulen vor ein großes Problem, dies zu überprüfen. Selbst für erfahrene Informatiker ist dies schwierig, ganz besonders dann, wenn es sich beim Auftragnehmer um ein größeres Rechenzentrum handelt.

Die gesetzliche Pflicht kann man jedoch auch erfüllen, indem man sich vom Auftragnehmer ein Zertifikat vorlegen lässt. Dabei kommt es auf die Art und den Inhalt bzw. Umfang des Zertifikates an:
Zum einen muss ganz genau darauf geachtet werden, um welches Zertifikat es sich handelt, denn Zertifikate beziehen sich meist auf Aspekte der IT-Sicherheit, diese ist jedoch nur eine Teilmenge des Datenschutzes.




| | | |
|---|---|---|
| **Spezifische Maßnahmen des Datenschutzes:** Zweckbindung, Erforderlichkeitsprinzip, Datensparsamkeit, Wahrung der Betroffenen-Rechte, Verfahrensverzeichnis / ggf. Vorabkontrolle usw. | **Datenschutz und IT-Sicherheit:** Passwort, Protokollierung, Verschlüsselung, Zugriffsberechtigungen usw. | **IT-Sicherheitsmaßnahmen:** Blitzschutz, Hochwasserschutz, Datensicherung, Ausfallsicherheit, Zutrittsschutz, usw. |

Zum anderen muss auch noch der Umfang der Zertifizierung betrachtet werden. Das Zertifikat muss nämlich den gesamten Umfang der an den Auftragnehmer übertragenen IT umfassen. So genügt die alleinige Zertifizierung des Rechenzentrums nicht, wenn beispielsweise der Auftragnehmer mit dem Betrieb einer Anwendung in dem Rechenzentrum beauftragt wurde, und die Anwendung nicht in der Zertifizierung enthalten ist. Das Zertifikat muss also nicht nur das Rechenzentrum an sich, sondern alle vom Auftragnehmer wahrgenommenen Aspekte der Datenverarbeitung umfassen, also neben dem Rechenzentrum selbst auch die evtl. dort gehostete Anwendung. Ggf. muss der Dienstleister also seine vorhandene Zertifizierung auf das Verfahren erweitern lassen.

Das Kultusministerium empfiehlt daher eine Zertifizierung **nach BSI-Grundschutz. incl. des Bausteins Datenschutz sowie ggf. der einschlägigen Bausteine (z.B. "Baustein Cloud Nutzung")**

Alternativ kommt ein Zertifikat nach **ISO 27001** bzw. **ISO 27018** in Frage.
Die Zertifizierung nach **ISO 27001** umfasst im Wesentlichen den IT-Grundschutzkatalog des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) - jedoch nicht den Datenschutz wie oben dargestellt. Sie bezieht sich somit alleine auf die IT-Sicherheit. Die datenschutzrechtlichen Aspekte muss dann der Auftraggeber, also die Schule, selbst prüfen.
Die Zertifizierung nach **ISO 27018** ist eine Erweiterung der ISO 27001 und bezieht sich auf cloudbasierte Dienste. Diese ISO 27018 beinhalt die Vorgaben von ISO 27001 und zusätzlich weiterer cloudspezifischer Anforderungen und Anforderungen des Datenschutzes. Jedoch sind auch hier einige wenige Datenschutzspezifika selbst zu prüfen.

Hierzu sollte das **Verfahrensverzeichnis** der Schule herangezogen werden, um folgende Punkte (Quelle: BSI-Grundschutz Baustein Datenschutz noch überprüfen:

| Prüfaspekt | Durch die Schule selbst zu prüfen bei Zertifizierung nach … | |
|---|---|---|
| | ISO 27001 | ISO 27018 |
| • **Fehlende Zulässigkeit der Verarbeitung personenbezogener Daten (**Nr. 3 des Verfahrensverzeichnisses).<br>Die Verarbeitung personenbezogener Daten ist nur dann zulässig, wenn ein Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder die betroffene Person eingewilligt hat. | x | x |
| • **Nichteinhaltung der Zweckbindung bei der Verarbeitung personenbezogener Daten** (Nr. 3 des Verfahrensverzeichnisses).<br>Personenbezogene Daten dürfen nur für den Zweck verarbeitet werden, für den sie erhoben oder erstmals gespeichert worden sind. | x | x |
| • **Überschreitung des Erforderlichkeitsgrundsatzes bei der Verarbeitung personenbezogener Daten** (Nr. 4 des Verfahrensverzeichnisses)<br>Personenbezogene Daten dürfen nur verarbeitet werden, wenn diese zur Erfüllung der rechtmäßigen Aufgaben der dafür zuständigen datenverarbeitenden Stelle erforderlich (in einem engen Sinne) sind. Es ist also zu prüfen, ob alle verarbeiteten Daten(-arten) tatsächlich erforderlich sind. Bei der Datenverarbeitung muss im Interesse des Betroffenen die sein Persönlichkeitsrecht am wenigsten beeinträchtigende Verarbeitung gewählt werden (Grundsatz der Verhältnismäßigkeit) | x | x |
| • **Missachtung oder ungenügende Beachtung des Grundsatzes der Datenvermeidung und Datensparsamkeit bei der Verarbeitung personenbezogener Daten** (Nr. 4 des Verfahrensverzeichnisses)<br>Datenvermeidung und Datensparsamkeit sind Grundanforderungen, die bei der Bestimmung der zu verarbeitenden Daten nach Art, Umfang und Dauer zu beachten sind. Sie sind gleichzeitig auch Vorgaben für die technische Gestaltung und ihre Auswahl. Eine Verletzung dieses Grundsatzes kann z.B. eintreten wenn mehr Daten erhoben werden, als für den Verarbeitungszweck benötigt werden oder durch die Verarbeitung von Daten in größerer Detaillierung als benötigt (z.B. Verarbeitung von Geburtsdatum, wenn nur die Bestätigung eines Alters von mehr als 18 Jahren benötigt wird). | x | x |
| • **Verletzung des Datengeheimnisses bei der Verarbeitung personenbezogener Daten** (Nr. 6 und Nr. 8 des Verfahrensverzeichnisses)<br>Das Datengeheimnis, d.h. der Schutz personenbezogener Daten, wird verletzt, wenn Personen, die Zugriff auf personenbezogene Daten haben, solche Daten unbefugt verarbeiten, z.B. durch Weitergabe von Adressdateien an Werbeunternehmen oder Weitergabe von personenbezogenen Daten innerhalb der Schule ohne dienstlichen Erforderlichkeit. | x | x |
| • **Gefährdung der Rechte Betroffener bei der Verarbeitung personenbezogener Daten**<br>Die Ausübung der aus dem Datenschutz herrührenden Rechte der Be- | x | |

| | | |
|---|---|---|
| troffenen (z. B. das Recht auf Auskunft, Berichtigung, Sperrung, Löschung (Nr. 7 des Verfahrensverzeichnisses)) dürfen diesen von der datenverarbeitenden Stelle aus technischen oder organisatorischen Gründen nicht verwehrt werden. | | |
| • **Fehlende Transparenz für den Betroffenen und die Datenschutz-Kontrollinstanzen**<br>Werden personenbezogene Daten erhoben, ohne dass der Betroffene über die vorgesehene Verarbeitung und die Rechtsgrundlage unterrichtet wird, ist die Transparenz in Frage gestellt. Dies gilt auch dann, wenn ihm Angaben über Herkunft und Empfänger dieser Daten sowie Löschungsfristen vorenthalten werden.<br>Datenschutz-Kontrollinstanzen (behördl. Datenschutzbeauftragter oder LfD) sind ggf. rechtzeitig vor<br>- Einführung neuer Verfahren (Verfahrensverzeichnis),<br>- Freigabe von Verfahren (z.B. bei einer Vorabkontrolle),<br>- Einrichtung von automatisierten Abrufverfahren oder<br>- Vergabe einer Auftragsdatenverarbeitung<br>zu informieren, damit Vorschläge zur Verbesserung des Datenschutzes gemacht werden können. | X | |
| • **Fehlende oder unzureichende Absicherung der Datenverarbeitung im Auftrag bei der Verarbeitung personenbezogener Daten** (Nr. 6c und 10 des Verfahrensverzeichnisses)<br>Bei einer Auftragsdatenverarbeitung durch Dritte ist der Auftraggeber für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich. Die Vergabe des Auftrags hat unter besonderer Berücksichtigung der technischen und organisatorischen Eignung des Auftragnehmers zu erfolgen. Der Auftrag hat schriftlich zu erfolgen, wobei die Datenverarbeitung selber sowie die zugehörigen technischen und organisatorischen Maßnahmen zu beschreiben sind. Zu diesen Maßnahmen gehört insbesondere auch die Gewährleistung der Auftragskontrolle. Der Auftragnehmer bleibt bezogen auf die Datenverarbeitung weisungsgebunden. Das Kultusministerium hat für den Auftrag Vorlagen zur Verfügung gestellt. | X | |
| • **Fehlende oder unzureichende Absicherung der Verarbeitung personenbezogener Daten im Ausland** (Nr. 6c des Verfahrensverzeichnisses)<br>Bei der Übermittlung personenbezogener Daten ins Ausland sind besondere gesetzliche Bestimmungen zu beachten. Personenbezogene Daten dürfen in die Mitgliedstaaten der Europäischen Union unter den gleichen Voraussetzungen übermittelt werden wie innerhalb der Bundesrepublik Deutschland. Von einer Datenverarbeitung in weitere Länder wird derzeit abgeraten. | X | |
| • **Gefährdung vorgegebener Kontrollziele bei der Verarbeitung personenbezogener Daten und fehlende oder unzureichende Datenschutzkontrolle** (Nr. 10 des Verfahrensverzeichnisses)<br>Durch unzureichende technische und organisatorische Maßnahmen bei der Verarbeitung personenbezogener Daten besteht Gefahr für das Recht auf Informationelle Selbstbestimmung. Daher müssen für jede einzelne der Kontrollen nach § 9 Abs. 3 Nr.1 bis 10 LDSG Maßnahmen getroffen werden.<br>Die Kontrolle der Einhaltung der Datenschutz-Bestimmungen ist dann unzureichend, wenn in ihr nur ein unproduktiver Kostenfaktor gesehen wird. Die datenschutzrechtliche Kontrolle kann erschwert werden, wenn versäumt wird, ihre Anforderungen schon bei der Entwicklung und Erprobung von Verfahren einzubeziehen. Ferner sollte ein behördlicher Datenschutzbeauftragter bestellt oder datenschutzrechtlich geschultes Personal vorhanden sein. | X | |
| • **Fehlende oder nicht ausreichende Vorabkontrolle**<br>Ist eine Verarbeitung personenbezogener Daten mit besonderen Gefahren für das Persönlichkeitsrecht verbunden, wie z. B. die Verarbeitung besonderer Datenarten (Angaben über rassische und ethnische Herkunft, politische Meinung, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben) oder soll damit die Persönlichkeit des Betroffenen einschließlich Fähigkeiten, Leistungen oder Verhalten bewertet werden, ist vor dem Beginn der Verarbeitung eine Vorabkontrolle nach § 12 LDSG durchzuführen. | X<br>(falls Vorabkontrolle vorgeschrieben) | X<br>(falls Vorabkontrolle vorgeschrieben) |
| • **Unzulässige automatisierte Einzelfallentscheidungen oder Abrufe bei der Verarbeitung personenbezogener Daten (falss erforderlich)** | X<br>(falls automatisierte Entscheidungen | X<br>(falls automatisierte Entschei- |

| | | |
|---|---|---|
| Niemand darf einer automatisierten Entscheidung unterworfen werden, die für ihn eine negative rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen kann. Dies gilt nur dann, wenn sich die Entscheidung ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten stützt, die der Bewertung einzelner Persönlichkeitsmerkmale dient. Das Verbot gilt nicht, wenn dem Begehren des Betroffenen stattgegeben wurde; ferner wenn der Betroffene über die automatisierte Einzelfallentscheidung unterrichtet wurde und seine schutzwürdigen Interessen durch geeignete Maßnahmen gewährleistet werden, hierzu zählt die Möglichkeit, seinen Standpunkt geltend zu machen. Die verantwortliche Stelle muss dann ihre Entscheidung erneut zu überprüfen. | erfolgen) | dungen erfolgen) |

**Fazit:** Mit einer **Zertifizierung nach BSI-Grundschutz incl. Baustein Datenschutz** liegt die Schule datenschutzrechtlich auf der sicheren Seite.
Liegt eine Zertifizierung nach **ISO 27001** bzw. **ISO 27018** vor, bleibt immer noch eine Prüfungsaufgabe bei der Schule, die zwar im Umfang deutlich geringer ist als ohne Zertifizierung - jedoch durchaus aufwändig sein kann.