Bildung IN DER DIGITALEN WELT

Gewerkschaft Erziehung und Wissenschaft GEW

Arbeitsgruppe 1: Arbeit, Rechte und Arbeitsbedingungen im Bildungsbereich des GEW-Bundesforums „Bildung in der digitalen Welt“

Anforderungen an den Datenschutz in Schule

Grundlagen

1. Für den Datenschutz in Schule bilden die DSGVO, das Bundesdatenschutzgesetz sowie die Datenschutzgesetze der einzelnen Länder uneingeschränkt die rechtliche Grundlage.
2. Die Gesamtverantwortung für den Datenschutz liegt bei den Schulaufsichtsbehörden. Die Schulaufsichtsbehörden versetzen die Schulen in die Lage, rechtssicher zu agieren und ihren Teil der Verantwortung als datenverarbeitende Stelle nachkommen zu können.
3. Weitere Regelungen zum Schutz personenbezogener Daten an Schulen sollten in entsprechenden Verwaltungsvorschriften getroffen werden, um so auch die Besonderheiten von Schulen als Bildungseinrichtungen zu berücksichtigen.

Datenschutzbeauftragte

1. Für alle Dienststellen - auch in den Verwaltungsbehörden und Ministerien - sind Datenschutzbeauftragte unter Beteiligung der Personalvertretungen zu bestellen, die auch mit den Landesdatenschutzbeauftragten zusammenarbeiten. Sofern in Schulen Lehrkräfte diese Aufgabe übernehmen, sind entsprechende Anrechnungen zu gewähren.
2. Allen Personen, die personenbezogene Daten verarbeiten, müssen die Meldeketten bei Datenschutzverstößen oder Datenpannen transparent gemacht werden.

Beteiligung von Personalvertretungen

1. Bei der Einführung und Erweiterung der Nutzung von Software wie z.B. dem Digitalen Klassenbuch, Kommunikationsmodulen, Schulclouds etc. - die u. a. dazu geeignet sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen - sind die Personalräte gemäß BPersVG § 75 und den Landespersonvertretungsgesetzen in Form der Mitbestimmung zu beteiligen.
2. Die Personalvertretungen haben gemäß § 67 BPersVG und den Landespersonvertretungsgesetzen die Aufgabe, zu überwachen, dass alle in Schulen Beschäftigten nach Recht und Billigkeit behandelt werden. Dies beinhaltet, dass geltende Gesetze, Verordnungen, Verwaltungsvorschriften und weiteres zur Anwendung kommen und umgesetzt werden. Dies gilt auch für die Einhaltung der DSGVO!

Dienstvereinbarungen

1. Es ist notwendig, Dienstvereinbarungen wie sie im BPersVG § 73 und in den Landespersonalvertretungsgesetzen vorgesehen sind, zu schließen.
2. Diese sollten u.a. folgende Aspekte regeln:
   - Nutzung von Software durch Kolleg*innen
   - Art und Weise, wie die Kolleg*innen mit digitalen Arbeitsgeräten arbeiten
   - Begrenzung der Zeiträume, in denen Kolleg*innen erreichbar sein sollen
   - Nichtüberwachung der Kolleg*innen in ihrem Verhalten oder ihrer Arbeitsleistung
   - Schulungsangebote für Kolleg*innen
3. Rahmendienstvereinbarungen, die auf Landesebene geschlossen werden, sind dabei zu bevorzugen. In den Dienststellen kann ggf. durch ergänzende Dienstvereinbarungen nachgesteuert werden.

Schulungen für Kolleg*innen und Schüler*innen

1. Alle Beschäftigten in Schule, die mit personenbezogenen Daten arbeiten, sind in Bezug auf die Einhaltung des Datenschutzes umfassend zu schulen.
2. Speziell stehen Schulleitungen in besonderer Verantwortung, wenn es um den Datenschutz geht. Daher ist es erforderlich, gezielte Schulungen für Schulleiter*innen zum Thema anzubieten.

Sichere Kommunikation

1. Um eine gesicherte, pädagogische Kommunikation mit Schüler*innen und Erziehungsberechtigten sowie dienstliche Kommunikation mit Kolleg*innen zu ermöglichen, ist es erforderlich, allen in Schule Beschäftigten wie auch den Schüler*innen personalisierte Mailadressen sowie einen sicheren, webbasierten Messengerdienst zur Verfügung zu stellen. Nur so kann gewährleistet werden, dass die Beteiligten auf kommerzielle Angebote wie z. B. WhatsApp verzichten, die aufgrund des mangelnden Datenschutzes nicht nutzbar sind!
2. Sichere Kommunikation von Beschäftigten heißt u.a. sicher vor Zugriff von außen durch Verschlüsselung, die Abwicklung der Kommunikation (E-Mails, Messengernachrichten) über Server in Landesverantwortung und auf Boden der EU (damit die DSGVO auch gilt).

Einsatz von Software

1. Kommt Software externer Anbieter (z.B. von Schulbuchverlagen) im Unterricht zum Einsatz, so ist darauf zu achten, dass zum Schutz der

Minderjährigen keine Schüler*innenergebnisse personenscharf extern zugeordnet werden können.
2. Hierzu ist es erforderlich, dass die Lernenden anonymisiert bzw. pseudonymisiert werden, somit also niemals Klarnamen übermittelt werden (z.B. bei der Anmeldung bei Lernplatt-formen oder der Freischaltung von Lern-Software).
3. Aggregierte Daten, aus denen Rückschlüsse auf konkrete Personen vorgenommen werden können, dürfen Dritten (u.a. Schulbuchverlagen) nicht zur Verfügung gestellt werden.
4. Grundsätzlich ist der Einsatz von „learning analytics“ aufgrund der damit verbundenen Datenerhebung abzulehnen!

Digitale Endgeräte

1. Den Kolleg*innen sind digitale Endgeräte bereitzustellen, wenn personenbezogen Daten erhoben oder verarbeitet werden, damit keine privaten Geräte genutzt werden müssen. Dies ist besonders wichtig für die Erstellung von Gutachten, das Führen von Notenlisten etc.
2. Die Geräte müssen den Datenschutzprinzipien „privacy by default“ (durch die Voreinstellungen ist geregelt, dass möglichst wenig Daten erhoben werden), und „privacy by design“ (die Geräte werden so gebaut, dass wenig Daten gesammelt werden können) entsprechen.
3. Die Geräte müssen vor Angriffen von außen abgesichert sein, durch entsprechende Schutzsoftware, Administration und ein professionell verantwortetes Mobile-Device-Management.
4. Die zur Aufgabenerfüllung erforderliche Software muss auf den Geräten vorhanden sein und den datenschutzrechtlichen Anforderungen entsprechen, um datenschutzkonformes Arbeiten ermöglichen.
5. Für die Sicherheit der Geräte müssen alle technischen, programmatischen und administrativen Möglichkeiten genutzt und in entsprechenden Kriterienkatalogen für Erwerb, strukturelle Einbindung und Administration festgeschrieben werden (z.B. Mobile-Device-Management, Firewalls, Sicherheitsupdates, Administrationsroutinen).

Administration und Ressourcen

1. Für die Administration der (personen-)datenverarbeitenden Systeme in Schule ist externes Personal bereitzustellen. Die betrifft nicht nur die Verwaltung, sondern auch die im Unterricht eingesetzten Systeme!
2. Ein bedarfsgerechter Support für die in den Schulen eingesetzte Software und (personen-)datenverarbeitenden Systeme durch den Anbieter ist zu gewährleisten (Hotlines, Problembearbeitungsdauer etc.).

3. Die notwendigen finanziellen und personellen Ressourcen für eine angemessene und ausreichende Umsetzung und Ausgestaltung der hier dargestellten Anforderungen sind bereitzustellen.
4. Der/Die Verantwortliche sollte über eine Administrator*innenverpflichtung sicherzustellen, dass ihm unterstellte Administrator*innen personenbezogene Daten nur auf seine/ihre Weisung verarbeiten.
   Die Administratorenverpflichtung sollte Administrator*innen
   - sensibilisieren für die Verarbeitung und den Schutz personenbezogener Daten,
   - vor unrechtmäßigen Tätigkeiten sowie deren Rechtsfolgen schützen,
   - helfen, die Rechte der von Verarbeitung betroffenen Personen zu wahren,
   - unterstützen, die verarbeiteten Daten vor Zweckentfremdung oder Missbrauch zu schützen.

Impressum
Herausgeber:
Gewerkschaft Erziehung und Wissenschaft
Hauptvorstand
Reifenberger Str. 21, 60489 Frankfurt a. M.
Tel.: (069) 78973-0, Fax: (069) 78973-201
E-Mail: info@gew.de
Internet: www.gew.de
Empfehlungen der AG 1 „Arbeit, Rechte und Arbeitsbedingungen im Bildungsbereich“ des Bundesforums „Bildung in der digitalen Welt“ vom 16.11.2021

Verantwortlich: Dr. Ansgar Klinger
Juli 2021