

Grundsätze, Maßnahmen, Evaluation

1. Grundsätze bei der Verarbeitung von personenbezogenen Daten

- Personenbezogene Daten werden in dem Umfang erhoben, verarbeitet und so lange aufbewahrt, wie es für Ausbildungszwecke notwendig (und zulässig) ist (Datenminimierung, Begrenzung der Speicherdauer, Zweckbindung, Rechtmäßigkeit).
- Es wird für **Vertraulichkeit, Richtigkeit** sowie für Transparenz bezogen auf die personenbezogenen Daten der Betroffenen und deren Rechte gesorgt.

2. Maßnahmen zur Umsetzung der Grundsätze

Systeme werden – soweit möglich – technisch so eingestellt, dass analoge wie digitale Daten geschützt werden und gleichzeitig flüssig gearbeitet werden kann. Organisatorische Maßnahmen (Absprachen, Anweisungen) wirken ergänzend.

a) **Vertraulichkeit:** Der Zutritt zu Arbeitsräumen bzw. Zugang zu Daten wird so gesichert:

- Schlüsselvergabe erfolgt nach Funktion; eine Ausleihe des je eigenen Schlüssels ist nicht gestattet.
- Zugriff auf Aktenschränke im ZfsL erfolgt nur bezüglich eigener LAA.
- Im Falle der Aushändigung eines dienstlichen Rechners werden auf dem privaten Gerät keine personenbezogenen Daten mehr verarbeitet.
- Dienstrechner werden gemäß Nutzungsordnung und Administration durch ITD-ZfsL verwendet; wenn kein Dienstrechner zur Verfügung steht, kann ein privates Endgerät nur nach Genehmigung durch die ZfsL-Leitung für die Verarbeitung personenbezogener Daten genutzt werden.
- Email: Personenbezogenen Daten (Verhalten, Leistung) werden grundsätzlich verschlüsselt verschickt.
- Die dienstliche Kommunikation muss über die dienstlich bereitgestellten Kommunikationskanäle (Chatfunktion, dienstliche Email-Adresse) erfolgen. Weiterleitung auf private Emailadressen ist nicht statthaft.
- Organisationsdaten ohne Bezug zu Leistungs- und Verhaltensdaten (z. B. Terminabsprachen) können auch mit einem privaten digitalen Gerät (z. B. Handy) im dienstlichen Kontext verarbeitet werden.
- Es besteht Informationspflicht bezüglich der Kommunikationsregeln in digitalen Kommunikationsräumen (Email, Chat, Cloud: Wer sieht wann was? Z. B. bei Teams Zulassung von Gästen/Nutzung personalisierter Kanäle innerhalb der Ausbildungsgruppen etc.)
- Schriftliche Unterrichtsplanungen: vgl. Handreichung im Logineo-Datenschutz-Kurs
- Unterrichtsnachbesprechungen bzw. Beratungen: Bei Lösungen jenseits von Logineo muss im Vorfeld Einvernehmen hergestellt werden und an die Nutzungsregeln erinnert werden (Dienstrechner/genehmigtes privates Gerät, keine Aufzeichnung, keine Einsichtnahme Dritter; ausschließlich die dienstliche Online-Plattform bzw. ... nutzen (iServ , Teams ...).
- Offene Unterlagen, Bildschirme können von Dritten nicht eingesehen werden (z. B. Nutzung von Sichtschutzfolien bei Arbeit außerhalb des ZfsL oder unterwegs).

b) **Zweckbindung, Speicherdauer:** Nur dienstlich benötigte Daten werden vorgehalten:

- Dokumente, die als Vorlagen genutzt werden können, werden nach Ablauf der Aufbewahrungsfrist durch Löschen des Personenbezugs anonymisiert.
- Daten, deren Aufbewahrungsfrist abgelaufen ist, werden gemäß dienstlicher Anweisung
 - geschreddert (Aktenschredder in Raum x, Sicherheitsstufe 3, cross cut) bzw.
 - an einen zertifizierten Aktenvernichter übergeben und zu diesem Zweck *hier* (Ort) gesammelt.
- Digitale Daten unterliegen einem verabredeten Löschkonzept:
 - Automatische Löschung nach x Wochen
 - Digitale Aufbewahrung von ... für x Wochen/...Analoge Aufbewahrung ...

c) **Richtigkeit:** Die Daten sind und bleiben richtig:

- Die Wahrung bzw. Kontrolle von Authentizität /Richtigkeit unterliegt der Verantwortung der SAB. *Oder im Einzelnen:*
- Von Kolleg:innen bei der Erstellung von LZB übernommene Daten werden kontrolliert (z. B. durch Endkontrolle der digitalen LZB im Vieraugenprinzip).
- Für die Verschlüsselung personenbezogener Daten wird z.B. der folgende Mechanismus verabredet (Verschlüsselungstiefe/-programm, Passwort o. ä.): ...

d) **Datensicherung:** Die Daten sind vor technischen Störungen und Umwelteinflüssen geschützt bzw. nach einem Zwischenfall wiederherstellbar:

- Es wird eine regelmäßige Datensicherung durchgeführt (empfohlen wird z. B. ...).
- Vorgaben von ITD-NRW bzw. Nutzungsordnung für dienstliche Rechner werden eingehalten (z. B. regelmäßige Backups, Passwortschutz, ... einsehbar unter ...).

3. Kontrolle und Evaluation

Alle Maßnahmen werden regelmäßig auf Umsetzbarkeit bzw. Zweckmäßigkeit geprüft und ggfls. aktualisiert. Hierzu wird das Folgende vereinbart:

- Konkrete Anfragen können über die Seminar- und ZfsL-Leitung an den/die Datenschutzbeauftragten gerichtet werden.
- Datenschutzrechtliche Verdachtsfälle oder Vorfälle müssen unverzüglich an die ZfsL-Leitung gemeldet werden.
- Eine regelmäßige Auffrischung zum Thema Datenschutz (auch: Gelegenheit zum Austausch über die pädagogische Dimension des Themas) erfolgt anlässlich ...; als Rhythmus gilt z. B.: *1x pro Ausbildungszyklus*
- *Person/Name* informiert das Kollegium regelmäßig über Neuerungen im Bereich Datenschutz (über eine regelmäßige Sichtung des Kurses Datenschutz in Logineo, der durch die DS-Beauftragten der ZfsL gepflegt wird) und gibt Informationen an das Kollegium weiter bzw. zeigt Regelungsbedarf an (z. B. bei Notwendigkeit der Überarbeitung von Routinen): Jede:r informiert sich hier (Ort) und zeigt ggfls. Beratungs- oder Anpassungsbedarf an.
- Als Ansprechpartner:in für neue SAB (*Ausgabe dieses Konzepts – oder: über Verwaltung?, Aussprache u. Klärung von Fragen*) bezogen auf dieses Basiskonzept fungiert/ist beauftragt *Name*.