

Datenschutz

Allgemeines zum Datenschutz an der Berliner Schule und BOLLE-spezifische Einstellungsmöglichkeiten im Rahmen der DSGVO

- Allgemeines zum Datenschutz und dem Einsatz von BOLLE an der Berliner Schule
- Rollenkonzept
- Benutzerhinweise zur Informationssicherheit und zum Datenschutz
- Zwei-Faktor-Authentisierung in BOLLE
- FIDO2 als Login-Möglichkeit
- Verzeichnis der Sub-Auftragsverarbeiter

Allgemeines zum Datenschutz und dem Einsatz von BOLLE an der Berliner Schule

Auf dieser Seite wird sich bezogen auf
die Datenschutz-Grundverordnung in ihrer Fassung vom 4 März 2021,
das Berliner Schulgesetz in seiner Fassung vom 10. Juli 2024 und
die Berliner Schuldatenverordnung in ihrer Fassung vom 4. März 2024.

Auf dieser Seite möchten wir über unseren Kenntnisstand* bezüglich der Antworten auf datenschutzrechtliche Fragen im Einsatz von BOLLE an der Berliner Schule mit Ihnen teilen. Der Kenntnisstand speist sich aus unserer Korrespondenz mit regionalen Datenschutzbeauftragten der Berliner Schulen und einer intensiven Literaturrecherche über die Stadtgrenzen hinaus. Sobald uns neue Erkenntnisse vorliegen, aktualisieren wir diese Seite.

Machen Sie sich am besten erst einmal einen Tee. Lesen Sie dann die Punkte in Ruhe durch. Es sind doch eine Menge Informationen, die wir so nachvollziehbar wie möglich mit Ihnen teilen möchten.

Inhaltsverzeichnis

1. Allgemeines
2. Was muss die Schule vor der Einführung von BOLLE beachten?
 - 2.1. Verzeichnis der Verarbeitungstätigkeiten (VVT)
 - 2.2. Verarbeitung der Daten durch einen Auftragsverarbeiter
 - 2.3. Verarbeitung von Daten besonderer Kategorien
 - 2.4. Informationspflichten der Schule
 - 2.5. Rechte der betroffenen Personen
 - 2.6. Einwilligung in die Verarbeitung personenbezogener Daten
 - 2.7. Sensibilisierung der Beschäftigten

1. Allgemeines

Beim Thema Datenschutz ist innerhalb der EU die DSGVO von tragender Bedeutung. Die DSGVO schützt personenbezogene Daten natürlicher Personen. Sie unterscheidet dabei i.d.R. nicht in der Form der Speicherung (z.B. Papierform oder elektronische Datenspeicherung und -verarbeitung). Für die Benutzung von BOLLE werden mit Ausnahme von Metadaten keine zusätzlichen Daten erhoben, als jene, die Schulen ohnehin erfassen müssen, um z.B. in der Lage zu sein, Zeugnisse auszustellen. In BOLLE werden lediglich bereits schulintern sowieso zu erhebende Daten übersichtlicher organisiert. Das System speichert die oben erwähnten Metadaten (z.B. Loginzeiten, fehlgeschlagene Loginversuche). Diese dienen ausschließlich dazu, auffälliges Verhalten, wie z.B. einen Hack-Versuch zu verhindern und sind zu keinem Zeitpunkt vom Personal der Schule einzusehen.

Alle Schulen, die BOLLE als Schulorganisationssoftware an Ihrer Schule einsetzen möchten, schließen vorher einen Auftragsdatenverarbeitungsvertrag (AVV) mit uns ab. Dieser schließt eine Weitergabe jeglicher Daten an Dritte durch uns als Dienstleister kategorisch aus.

Neben der europaweit geltenden DSGVO gibt es für das Land Berlin das Schulgesetz und eine ganze Reihe von Verordnungen, die die Verarbeitung, Speicherung, Aufbewahrungsfristen und Archivierung von allen möglichen schulrelevanten Informationen und Dokumenten rechtlich regeln: GsVO, Sek-I-VO, VO-GO, SchulQualSiEvalVO und Schuldaten-VO.

Weil uns **Informationssicherheit und Datenschutz** besonders wichtig sind, haben wir uns als Firma einem Zertifizierungsprozess unterworfen. In solch einem Prozess werden alle internen Firmenabläufe auf Daten- und Informationssicherheit durch externe, unabhängige Expert:innen überprüfen. Mit diesem Audit wurde der Nachweis erbracht, dass unsere Firma die **Forderungen des international gültigen Regelwerks ISO 27001 : 2022 erfüllt**. Die Erfüllung der dort definierten Standards werden jährlich unabhängig überprüft. **Somit erfüllen nicht nur unsere Rechenzentren, sondern erfüllt auch unsere Firma die aktuell gültigen Standards für Daten- und Informationssicherheit.**



ZERTIFIKAT



Hiermit wird bescheinigt, dass

BOLLE

Bolle Software GmbH

Dürerstr. 37
12203 Berlin-Lichterfelde
Deutschland

ein **Informationssicherheits-Managementsystem** eingeführt hat und anwendet.

Geltungsbereich:

Design, Entwicklung und Vertrieb von Softwareprodukten im Verwaltungsbereich von Bildung und Schule sowie deren Einführung, Betrieb, laufende Kundenbetreuung und zugehörige Supportdienstleistung

Erklärung zur Anwendbarkeit: SOA Version V2, 21.08.2024

Durch ein Audit, dokumentiert in einem Bericht, wurde der Nachweis erbracht, dass das Managementsystem die Forderungen des folgenden Regelwerks erfüllt:

ISO / IEC 27001 : 2022

Zertifikat-Registrier-Nr. 31603183 ISMS22
Gültig ab 2024-08-30
Gültig bis 2027-08-29
Zertifizierungsdatum 2024-08-30



DQS GmbH

Christian Gerling
Geschäftsführer

DQS IS A MEMBER OF



Akkreditierte Stelle: DQS GmbH, August-Schanz-Straße 21, 60433 Frankfurt am Main
Die Gültigkeit der Zertifizierung kann nur durch den QR-Code verifiziert werden.

2. Was muss die Schule vor der Einführung von BOLLE beachten?

Neben der üblichen Einbindung der schulischen Gremien und Beschäftigtenvertretung vor Einführung einer solch umfangreichen Organisationssoftware, müssen Sie noch weitere datenschutzrechtliche Punkte in Kooperation mit Ihren regionalen Datenschutzbeauftragten beachten.

Ihre regionalen Datenschutzbeauftragten haben für die Berliner Schulen einen Leitfaden zum Umsetzen der DSGVO zur Verfügung gestellt. Hier finden Sie alle Datenschutzbriefe der regionalen Datenschutzbeauftragten. Der Leitfaden ist unter Datenschutzbrief Nummer 16 abrufbar. In diesem Leitfaden wird mitgeteilt, was alles zum Thema Datenschutz an Berliner Schulen zu beachten ist. **Diese im Leitfaden aufgeführten Punkte** (u.a. Verzeichnis der Verarbeitungstätigkeiten, Informationspflichten und -rechte) **sind auch ohne Einsatz von BOLLE seit 2018 zu beachten.** Wenn Sie BOLLE einführen möchten, müssen einige dieser Punkte noch ergänzt werden. Somit wird der Einsatz von BOLLE und Ihr mit uns abgeschlossener AVV transparent gemacht. Mit den folgenden Unterpunkten wollen wir Ihnen zeigen, welche zusätzlichen Angaben Sie vornehmen müssen.

Hier sehen Sie eine Checkliste mit Punkten, die Sie - auch unabhängig vom Einsatz von BOLLE - als Schule vorweisen können bzw. erfüllen müssen:

- ein Verzeichnis der Verarbeitungstätigkeiten (VVT) (siehe 2.1.)
- eine Datenschutzerklärung auf der Schulhomepage (siehe 2.4.)
- eine Einverständniserklärung, wenn Sie die E-Mailadressen von Eltern speichern (siehe 2.6.)
- eine Einverständniserklärung, wenn Schüler:innen Accounts nutzen (z.B. bei Schulcomputern) (siehe 2.6.)
- eine Genehmigung zur Nutzung privater Datenverarbeitungsgeräte des Personals durch die Schulleitung (siehe 2.7.)
- eine Datenschutz-Folgenabschätzung bei Nutzung bestimmter Software (siehe 2.8.)

2.1. Verzeichnis der Verarbeitungstätigkeiten (VVT)

Auch ohne BOLLE müssen Sie ein Verzeichnis der Verarbeitungstätigkeiten (VVT) führen. Auf Seite 4 im oben verlinkten Leitfaden finden Sie entsprechende Hinweise. Hier finden Sie eine Vorlage zum VVT und ein Dokument mit Ausfüllhinweisen. In der Excel-Datei gibt es viele Reiter, die Sie ganz unten finden. Hier ein Bild zur Orientierungshilfe.

◀ ▶	Stammdaten	Übersicht	TOM	Schülerbögen	sonderpädagog. Förderbögen	Schülerkartei	Klassenbücher	Kursbücher
-----	------------	------------------	-----	--------------	----------------------------	---------------	---------------	------------

Bitte wählen Sie den Reiter *Übersicht*. Dort finden Sie in der grünen Spalte *Daten* und die Unterkategorie *mögliche Empfänger*. Wenn Sie weiter nach unten scrollen, sehen Sie hier auch Angaben wie *Untis-Support* oder *Winschule-Support*. Außerdem sehen Sie als weitere Unterkategorie *Verarbeitung außerhalb der Schule (Vertrag zur Auftragsverarbeitung AV mit...)*.

Daten					
Datenkategorie	Kategorien besonderer Daten	Verarbeitung außerhalb der Schule (Vertrag zur Auftragsverarbeitung AV mit...)	weitere Zugriffsberechtigte	mögliche Empfänger	technische und organisatorische Maßnahmen (TOM)

Für die Nutzung von BOLLE, müssen Sie zunächst eine weitere Zeile und einen Reiter hinzufügen sowie die TOMs ergänzen. Auf dieser Seite finden Sie eine Vorlage von uns. Suchen Sie nach der Datei: Vorlage zur VVT BOLLE. In der Datei sehen Sie unten die Reiter *Übersicht*, *TOM* und *BOLLE*.

Übersicht	TOM	BOLLE
------------------	-----	-------

In unserer Datei bleiben Sie zunächst beim Reiter *Übersicht*. Sie finden dort eine Vorlage für eine mögliche Zeilenergänzung in Ihrer VVT. Bitte sehen Sie sich alle Eingaben an und verändern die Angaben nach Bedarf.

Zum Schutz der personenbezogenen Daten müssen Sie für BOLLE auch die technischen und organisatorischen Maßnahmen (TOM) beschreiben. Sie brauchen hierfür Angaben von uns. Sie finden in unserer Datei zwar den Reiter *TOM* jedoch ohne weiteren Inhalt. **Eine Formulierungsvorlage erhalten Sie von uns auf Anfrage**, da diese sicherheitsrelevanten Angaben nicht für die Öffentlichkeit gedacht sind. Nach Durchsicht unserer Angaben fügen Sie diese Zeile den TOMs Ihrer eigenen VVT hinzu.

Zuletzt müssen Sie den Reiter *BOLLE* ebenfalls noch zu Ihrer VVT hinzufügen. Neben den Reitern Ihrer eigenen VVT finden Sie ganz am Ende ein Plus-Symbol. Klicken Sie darauf. Damit generieren Sie einen weiteren Reiter. Wenn Sie auf den Reiter mit einem Rechtsklick klicken, können Sie ihn in *BOLLE* umbenennen. Wir haben hier für Sie auch eine Formulierungshilfe zur Verfügung gestellt, die Sie noch ergänzen oder kürzen müssen.

Abschließend gehen Sie zurück zu Ihrer eigenen VVT zum Reiter *Übersicht*.

◀ ▶	Stammdaten	Übersicht	TOM	Schülerbögen	sonderpädagog. Förderbögen	Schülerkartei	Klassenbücher	Kursbücher
-----	------------	------------------	-----	--------------	----------------------------	---------------	---------------	------------

Daten					
Datenkategorie	Kategorien besonderer Daten	Verarbeitung außerhalb der Schule (Vertrag zur Auftragsverarbeitung AV mit...)	weitere Zugriffsberechtigte	mögliche Empfänger	technische und organisatorische Maßnahmen (TOM)

Gehen Sie nun alle Zeilen der VVT durch. An den Stellen, an denen Sie den Einsatz von BOLLE planen, machen Sie das in der Spalte *Verarbeitung außerhalb der Schule* den Bezug zu BOLLE transparent. Wenn Sie weiter unten in der von Ihnen hinzugefügten Zeile *BOLLE* bereits "Bolle Software GmbH (BOLLE)" geschrieben haben, reicht hier der jeweilige Vermerk: BOLLE. Außerdem müssen Sie ein *d* für digital beim Reiter *analog/digital* hinzufügen. Eventuell entfällt an einigen Stellen auch das *a* für *analog*.

Akte oder Verfahren			
laufende Nummer	Bezeichnung	Zweck	analog/ digital
1	Schülerbögen	Schüleraktenführung/ Dokumentation der Lern- und Leistungsentwicklung	a
2	sonderpädagogische Förderbögen	Ergänzung der Schülerbögen; gibt Auskunft über die sonderpädagogische Förderung	a
3	Schülerkartei	schnelles Ermitteln von Daten für laufende Verwaltungsgeschäfte	a
4	Klassenbücher	Informationen zum erteilten Unterricht und zu den teilnehmenden Schüler*innen	a
5	Kursbücher	Informationen zum erteilten Unterricht und zu den teilnehmenden Schüler*innen	a
6	Kurs- bzw. Anwesenheitsnachweise	Informationen zum erteilten Unterricht und zu den teilnehmenden Schüler*innen	a

Wichtig: Die VVT ist nicht für die Öffentlichkeit gedacht. Sie muss jedoch auf Verlangen der für den Datenschutz zuständigen Aufsichtsbehörde vorgelegt werden können. Sie dürfen das Verzeichnis elektronisch führen.

2.2. Verarbeitung der Daten durch einen Auftragsverarbeiter

Im Leitfaden informieren die regionalen Datenschutzbeauftragten, dass Sie eine Vereinbarung zur Auftragsverarbeitung mit Anbietern abschließen müssen, wenn personenbezogene Daten durch

diesen Anbieter verarbeitet werden. Wir legen Ihnen einen solchen Auftragsverarbeitungsvertrag unaufgefordert bei Vertragsunterzeichnung vor. Sie können BOLLE gar nicht ohne diesen Auftragsdatenverarbeitungsvertrag nutzen.

2.3. Verarbeitung von Daten besonderer Kategorien

Das Wichtigste ist hierbei, dass Sie die sonderpädagogischen Förderbögen "als einzige Schülerunterlage[] nicht automatisiert" führen dürfen (Leitfaden, Version 2.0, Regional Datenschutzbeauftragte für Berliner Schulen, 2018: 9). BOLLE wird Ihnen daher ein Führen sonderpädagogischer Förderbögen auch nicht ermöglichen. Statthaft sind jedoch gesundheitliche Rücksichten, wie z.B. individuelle Zeitverlängerungen aufgrund einer LRS. Dieses Recht leitet sich explizit aus Art. 9, Buchst. e DSGVO ab: Die Verarbeitung von Daten besonderer Kategorien ist erlaubt, wenn "die Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen" notwendig ist.

Das Schulgesetz konkretisiert im § 64 die Datenverarbeitung und Auskunftsrechte:

Die Schulen einschließlich der Einrichtungen des Zweiten Bildungswegs, die Schulbehörden und die Schulaufsichtsbehörde dürfen personenbezogene Daten von Schülerinnen und Schülern, Schulpflichtigen nach § 41 Absatz 3 und § 43, ihren Erziehungsberechtigten, Lehrkräften und sonstigen schulischen Mitarbeiterinnen und Mitarbeitern verarbeiten, soweit dies zur Erfüllung der ihnen durch Rechtsvorschriften zugewiesenen schulbezogenen Aufgaben erforderlich ist.

Von den besonderen Kategorien personenbezogener Daten im Sinne von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72 und L 127 vom 23.5.2018, S. 2) **dürfen nur solche verarbeitet werden, die sich auf die Familiensprache, die Religions- und Weltanschauungszugehörigkeit oder die Gesundheit der betroffenen Personen beziehen.**

Für die betroffenen Personen besteht Auskunftspflicht; deren Art und Umfang ist durch Rechtsverordnung nach § 66 Nr. 1 festzulegen.

Die Rechtsverordnung, die im zuletzt zitierten Absatz nach § 66 Nr. 1 Art und Umfang der Auskunftspflicht gegenüber Schüler:innen und deren Erziehungsberechtigten regeln soll, konnten wir bei unseren Recherchen bisher nicht finden. Wir freuen uns gerne über Hinweise, wenn Ihnen eine solche Rechtsverordnung vorliegt.

§ 66 Nr. 1 SchulG verweist lediglich auf den oben zitierten § 64:

Die für das Schulwesen zuständige Senatsverwaltung wird ermächtigt, das Nähere über die Verarbeitung personenbezogener Daten durch Rechtsverordnung zu regeln, insbesondere

1. Art und Umfang der Daten, auf die sich die Auskunftspflicht nach § 64 Abs. 1 bezieht[.]

2.4. Informationspflichten der Schule

Ihre regionalen Datenschutzbeauftragten informieren Sie im Leitfaden auf S. 9 wie folgt:

Gemäß Artikel 12 bis 14 DSGVO muss die Schulleitung von sich aus den betroffenen Personen eine Reihe von Informationen geben. Über eine beabsichtigte Änderung des Verarbeitungszwecks personenbezogener Daten sind die betroffenen Personen vorab zu informieren (Artikel 13, Absatz 3 und Artikel 14 Absatz 4). Dies gilt auch, wenn die Zweckänderung in einer Rechtsvorschrift vorgesehen ist.

Ihnen wird an anderer Stelle eine Vorlage zur Verfügung gestellt, die die "betroffenen Personen" entsprechend dieser DSGVO-Vorschrift informiert. Sie finden diese Vorlage der regionalen Datenschutzbeauftragten hier. Dort finden Sie die Vorlage *5.2. Informationspflichten Sekundarschule (Januar 2019)*.

Bevor Sie BOLLE an der Schule einsetzen, müssen Sie darüber informieren. Die regionalen Datenschutzbeauftragten formulieren selbst, dass **Informationsschreiben nach Artikel 12 DSGVO nicht auf Papier als Ausdruck an jede Familie ausgeteilt werden müssen**. In der Vorlage heißt es auf Seite 1:

Die Informationen müssen den Betroffenen auf einfache Weise zur Verfügung gestellt werden. Sie können mit einem Hinweis bei der Anmeldung aus die Veröffentlichung aus Ihrer Homepage hinweisen ("Informationen über die Erhebung von personenbezogenen Daten gemäß Datenschutz-Grundverordnung finden Sie auf unserer Homepage unter [www... .](#)")

Sie müssen diese Vorlage jedoch ergänzen. Wir haben die Vorlage der Datenschutzbeauftragten vom Januar 2019 genommen um entsprechende Angaben ergänzt. **Sie finden unsere Vorlage in diesem Ordner.** Laden Sie die Datei *Vorlage zur Informationspflicht BOLLE* herunter. Sie finden unsere Vorschläge zur Ergänzung **rot markiert**.

2.5. Rechte der betroffenen Personen

Betroffene Personen haben nach Artikel 15 DSGVO ein Recht auf Auskunft, Berichtigung, Löschung und Widerspruch. BOLLE unterstützt die Schulleitung bei der Erfüllung möglicher Rechtsersuchen Betroffener (Admin > Datenschutz).

Vorab zitieren wir an dieser Stelle den Erwägungsgrund 63 "Auskunftsrecht" der DSGVO:

Verarbeitet der Verantwortliche eine große Menge von Informationen über die betroffene Person, so sollte er verlangen können, dass die betroffene Person präzisiert, auf welche Information oder welche Verarbeitungsvorgänge sich ihr Auskunftersuchen bezieht, bevor er ihr Auskunft erteilt.

Unabhängig davon kann die Schulleitung bei Vorliegen einer Auskunftsanfrage nach Art. 15 DSGVO einen Auszug aller in BOLLE von der Schule verarbeiteten Daten generieren. Dieser Auszug umfasst explizit nicht die individuellen Einzelnoten und eventuellen Stundenkommentare (Leistungsdaten) im Kursbuch der einzelnen Lehrkräfte. Das Recht auf Auskunft wird in Artikel 23 Abs. 1 Buchst. j beschränkt, wenn "Rechte und Freiheiten anderer Personen" vom Auskunftersuchen betroffen sind. Die Auskunft über Leistungsdaten wird durch § 47 Abs. 4 Schulgesetz näher definiert:

Die Schulleiterin oder der Schulleiter oder die Lehrkräfte informieren die Schülerinnen und Schüler sowie deren Erziehungsberechtigte individuell und in angemessenem Umfang

1. über die Lern-, Leistungs- und Kompetenzentwicklung sowie das Arbeits- und Sozialverhalten der Schülerin oder des Schülers,
2. über die Kriterien der Leistungsbeurteilung (Noten, Prüfungen, sonstige Beurteilungen), Versetzung und Kurseinstufung[.]

Im Schulgesetz wird also von den Lehrkräften verlangt, individuell und in angemessenem Umfang Auskunft über Leistungsdaten zu erteilen. Ein bloßes Zur-Verfügung-Stellen aller Einzelnoten und der Stundenkommentare aller Lehrkräfte einer Schüler:in würde gegen diese Vorschrift verstoßen. § 67 Abs. 2 Schulgesetz bestätigt die besondere Aufgabe und Stellung der Lehrkräfte:

Sie unterrichten, erziehen, beurteilen und bewerten, beraten und betreuen in eigener pädagogischer Verantwortung im Rahmen der Bildungs- und Erziehungsziele und der sonstigen Rechts- und Verwaltungsvorschriften sowie der Beschlüsse der schulischen Gremien.

Außerdem würde ein einfaches Auslesen und die vollumfängliche Übermittlung der persönlichen Notizen einer Lehrkraft innerhalb des eigenen digitalen Kursbuches gegen das Recht von Angestellten und Beamten verstoßen, dass sie lt. § 85 Abs. 13 Buchst. b Personalvertretungsgesetz vor Überwachung der Leistung und des Verhaltens schützen soll.

Sollten Erziehungsberechtigte oder Schüler:innen eine Auskunft über Leistungsdaten verlangen, so sollte dies nach den Grundsätzen des Schulgesetzes passieren: individuell und in angemessenem Umfang. Dies betrifft nicht die Auskunft darüber, zu welchem Zweck die Daten in einem digitalen Kursbuch wie BOLLE geführt werden (Transparenzgebot). Der Zweck des Führens von Leistungsdaten in BOLLE ist der oben erwähnte Grundsatz der Bewertung und Beurteilung durch Lehrkräfte in "eigener pädagogischer Verantwortung" (ebd.) und, weiterführend, der Erstellung von Zeugnissen gemäß der AV Zeugnisse.

Schüler:innen bzw. deren Erziehungsberechtigten haben also keinen Anspruch auf Herausgabe aller Daten. Sie haben einen Anspruch darauf, zu erfahren, was mit den Daten geschieht und wann sie z.B. wieder gelöscht werden. Zudem haben sie einen Anspruch darauf, die zusammengefassten Erkenntnisse über die eigene Leistungsentwicklung bzw. die des eigenen Kindes zu erfahren und von den Lehrkräften erklärt zu bekommen. Nicht mehr - aber auch nicht weniger.

Beachten Sie diesbezüglich auch die Antwort auf das letzte Praxisbeispiel im nächsten Punkt: "Eltern wollen nicht, dass Leistungsdaten des Kindes in BOLLE verarbeitet werden."

2.6. Einwilligung in die Verarbeitung personenbezogener Daten

Solange Sie nur Daten verarbeiten, die Sie ohnehin als Schule auf Grundlage des Schulgesetzes und den nachgeordneten Rechtsverordnungen erheben würden, benötigen Sie keine Einwilligung der Betroffenen. Wenn es für die Datenverarbeitung jedoch keine gesetzliche Grundlage gibt, müssen Sie sich eine Einwilligung holen. Dabei ist zwingend darauf zu achten, dass der Betroffene sich nicht verpflichtet fühlt einwilligen zu müssen und ihm keine konkret benennbaren Nachteile aus einem Einwilligungsverzicht entstehen.

Auf BOLLE bezogen, bedeutet das, dass sowohl Schüler:innen als auch Erziehungsberechtigte nicht dazu gezwungen werden dürfen, BOLLE selbst zu benutzen oder gar dort einen Account für sich anzulegen. Sie haben auch das Recht, ihre Einwilligung zu einem späteren Zeitpunkt zu entziehen, was eine Löschung der Daten dieser Person nach sich zöge.

Bevor Sie den Schüler:innen die Logindaten für den jeweils eigenen Account herausgeben, benötigen Sie von Personen, die das 16. Lebensjahr noch nicht vollendet haben, eine

Einverständniserklärung einer erziehungsberechtigten Person. Dies ist der Fall, weil mit der Nutzung eines Accounts Daten erhoben werden, die über die im Schulgesetz und in den nachgeordneten Rechtsverordnungen erwähnten Daten und Zwecke hinausgehen. Da in BOLLE der Zeitpunkt des letzten Logins gespeichert wird, um mögliche Hackangriffe auf das System zu identifizieren und abwehren zu können, und weil eben dieses personenbezogene Datum (*Schüler X hat sich am 12.03.2021 zum letzten Mal um 13.42 Uhr eingeloggt*) nicht im Schulgesetz erwähnt wird, benötigen Sie ein Einverständnis. Dieses benötigen Sie im Übrigen auch, wenn sich Schüler:innen an den schuleigenen Computern mit einem persönlichen Zugang einloggen können. In beiden Fällen (auf BOLLE und bei Nutzung schuleigener Computer) werden Daten erhoben, die einen sicheren Login zu den Systemen erst ermöglichen.

Rein rechtlich dürfen Sie auch nicht ohne Weiteres die **E-Mailadresse von Eltern** und Erziehungsberechtigten speichern; egal wo. Das Datum *E-Mailadresse* wird bisher von der SchuldatenV nicht explizit im Zusammenhang aller Erziehungsberechtigten erwähnt. Es wird erwähnt, dass man die "E-Mail-Adressen der Klassenelternsprecherinnen und Klassenelternsprecher verarbeiten" darf (vgl. § 19, Abs. 1 SchuldatenV). Ansonsten ist nur von "Namen und Kontaktdaten der Erziehungsberechtigten sowie die Kontaktdaten einer zusätzlichen Person für den Notfall" (§ 7, Abs 2 SchuldatenV) die Rede.

Wollen Sie also die E-Mailadresse von Eltern nutzen, brauchen Sie auch hierfür immer am besten eine Einverständniserklärung.

Wir stellen Ihnen eine Vorlage für eine solche **Einverständniserklärung hier zur Verfügung**. Unsere Vorlage beachtet dabei die hier erwähnten Bereiche:

1. Nutzung der schuleigenen Computer durch das Kind
2. Nutzung eines BOLLE-Accounts durch das Kind
3. Speicherung der E-Mailadresse der Eltern und Erziehungsberechtigten durch Sie in BOLLE

Bitte ergänzen und streichen Sie die Angaben in der Vorlage je nach Ihren individuellen Voraussetzungen.

Durch Eingabe der E-Mailadressen der Eltern und Erziehungsberechtigten erhalten diese eine Mitteilung, dass sie sich einen **Eltern-Account auf BOLLE** anlegen können (sofern Ihre Schule das so voreingestellt hat). Das Einverständnis der Eltern und Erziehungsberechtigten hinsichtlich der Erstellung des Eltern-Accounts wird digital erfasst. Sie müssen hier keine schriftliche Einwilligung einholen.

Achtung: Sofern nicht eindeutig anders gekennzeichnet, geht es in diesem gesamten Bereich nicht um die Schuldaten, die die Schulen eh gesetzlich verpflichtend erheben müssen. **Hier ein paar Praxisbeispiele:**

Beispiel	Aktion
----------	--------

Eltern wollen für sich selbst keinen Account mehr auf BOLLE haben.	Sie müssen den Account löschen. Durch Accountlöschung werden auch etwaige Metadaten gelöscht (z.B. wann sich der Account eingeloggt hat, missglückte Anmeldeversuche bei falscher Passworteingabe)
Eltern wollen, dass Sie die Adressdaten löschen.	Die Anschrift der Erziehungsberechtigten sind Bestandteil des gesetzlich vorgeschriebenen Schülerbogens. Sie dürfen dieses Datum nicht vor der Löschfrist lt. SchuldatenV löschen. Die Eltern können die Daten aber natürlich jederzeit berichtigen.
Eltern wollen, dass ihr Kind keinen Zugang zu BOLLE erhält.	Sie müssen dem Wunsch entsprechen und dürfen das Kind nicht zwingen, einen Account anzulegen. Dem Kind darf daraus kein konkret benennbarer Nachteil erwachsen (siehe nächstes Beispiel).
Eine volljährige Schülerin möchte keinen BOLLE-Account haben, soll nun aber eine 5. PK in BOLLE eingeben. Sie weigert sich.	<p>Die Schülerin hat das Recht, die Eingabe auf BOLLE zu verweigern. Der Zweck, die personenbezogenen Daten <i>Name</i> und <i>Vorname</i> für die Accounterstellung zu einer Schulverwaltungssoftware zu nutzen, ist gesetzlich nicht beschrieben. Die Schülerin muss dennoch die Angaben zur 5. PK machen. Sie müssen der Schülerin die Gelegenheit geben, die erforderlichen Daten auf andere Weise zur Verfügung zu stellen (z.B. mit einem Vordruck).</p> <p>Wichtig dabei ist, dass zwar die Schülerin das Recht hat, sich nicht 'irgendwo' einloggen zu müssen, Sie aber auch das Recht haben, die gesetzlich notwendigen Daten der Schülerin in dieses System zu übertragen und dort weiter zu verarbeiten.</p> <p>In diesem konkreten Beispiel, kann die Oberstufenkoordination die Daten für die Schülerin in BOLLE eintragen.</p>

<p>Eltern wollen nicht, dass Leistungsdaten des Kindes in BOLLE verarbeitet werden.</p>	<p>Lehrkräfte erheben diese Daten auf Grundlage des Schulgesetzes. Eltern und Schüler:innen haben ein Recht auf Auskunft, aber kein Recht, den Lehrkräften vorzugeben, auf welche Weise sie diese Daten zu verarbeiten haben.</p> <p>Die SchuldatenV ermächtigt Lehrkräfte Leistungsdaten auch digital zu erfassen.</p> <p>§ 10 Abs. 4 SchuldatenV sagt aus: "Die Noten der mündlichen, schriftlichen und sonstigen Leistungen sind durch die Lehrkräfte in geeigneter Weise zu dokumentieren."</p> <p>In § 6 Abs. 3 wird außerdem eine Verarbeitung in Papierform und in digitaler Form genehmigt: "Schülerunterlagen können im Ermessen der Schule sowohl in Papierform nach Maßgabe des Absatzes 4 als auch in digitaler Form nach Maßgabe des Absatzes 5 geführt werden, sofern in den §§ 7 bis 14 nichts Abweichendes geregelt ist." Dies schließt den o.g. § 10 mit ein.</p> <p>Es bedarf keiner Zustimmung durch Schüler:innen oder Eltern; vgl. auch § 3 Abs. 1 Schuldaten V: "Die Einholung einer datenschutzrechtlichen Einwilligung kommt nur dann in Betracht, wenn die Datenverarbeitung nicht ohnehin durch Rechtsvorschrift erlaubt ist."</p> <p>Achtung: § 10 Abs. 4 SchuldatenV wurde ergänzt und nennt nun eine Einschränkung:</p> <p>"Sofern unterjährig erteilte Zwischennoten digital verarbeitet werden, darf dies nur lokal auf einem dienstlichen digitalen Endgerät im Sinne von § 17 Absatz 1 erfolgen" (ebd.).</p> <p>Zwischennoten werden sonst weder im Schulgesetz (Fassung vom 10. Juli 2024) noch in der SchuldatenV (Fassung vom 4. März 2024) erwähnt. Was genau als Zwischennote gilt, wird damit nicht weiter vom Schulgesetz oder der Schuldatenverordnung definiert.</p>
---	---

2.7. Sensibilisierung der Beschäftigten

Im Leitfaden finden Sie ein paar Angaben der regionalen Datenschutzbeauftragten zu dem Punkt, dass Sie Ihre Kolleg:innen regelmäßig auf die Grundsätze der rechtmäßigen Verarbeitung personenbezogener Daten hinweisen sollen. Dies gilt insbesondere auch bei der Nutzung von BOLLE. So sollten Sie regelmäßig darauf hinweisen, wie die Kolleg:innen BOLLE auf Geräten verwenden und welche **Sicherheitsvorschriften** dabei beachtet werden müssen.

Auch die **Schüler:innen** sollten regelmäßig über das Geheimhalten von Passwörtern und den sicheren Umgang mit eigenen Accounts informiert werden.

Haben Sie als Schulleitung Ihren Lehrkräften die **Nutzung privater Datenverarbeitungsgeräte** zur Verarbeitung personenbezogener Daten genehmigt? Falls Sie Ihren Lehrkräften solch eine Zustimmung erteilen möchten, finden Sie hierzu eine Vorlage

auf dieser Seite unter 2. *Antrag zur Verarbeitung personenbezogener Daten auf privaten Geräten (September 2017)*.

Das Schulgesetz (§ 64, Abs. 2, Sätze 4 und 5) schränkt die Speicherung und Verarbeitung von personenbezogenen Daten zwar ein, genehmigt aber unter Auflagen die reine Verarbeitung dieser Daten dann doch wieder:

Bedienstete und die in Satz 3 genannten Personen dürfen personenbezogene Daten weder auf privateigene Datenverarbeitungsgeräte speichern noch diese Daten auf Datenverarbeitungsgeräten außerhalb der Schule verarbeiten.

Die **Schulleiterin oder der Schulleiter kann den Lehrkräften** und den sonstigen schulischen Mitarbeiterinnen und Mitarbeitern, die sich schriftlich zur Beachtung der datenschutzrechtlichen Vorschriften verpflichtet haben, **die Verarbeitung auf Datenverarbeitungsgeräten außerhalb der Schule gestatten**; sie unterliegen insoweit der Kontrolle der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit.

2.8. Datenschutz-Folgenabschätzung (DSFA)

Nach Art. 35 DSGVO muss bei einer

"systematische[n] und umfassende[n] Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung [...] gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten" (ebd., 3a)

eine sogenannte Datenschutz-Folgenabschätzung (DSFA) erfolgen. Dies ist unserer Ansicht nach bei der Verwendung von jeglicher Software im schulischen Bereich gegeben (auch bei Excel oder anderen reinen Notenverwaltungsprogrammen) - und damit auch bei der Nutzung von BOLLE.

Abs. 2 des Art. 35 DSGVO regelt, dass bei der Durchführung einer DSFA der Rat des Datenschutzbeauftragten einzuholen ist. Wir haben in Rücksprache mit regionalen Datenschutzbeauftragten der Berliner Schulen eine Vorlage für eine DSFA für den Einsatz von BOLLE erarbeitet. Unsere Vorlage muss durch Sie noch durchgesehen und in einigen Punkten ergänzt werden.

Die DSFA ist nicht für die Öffentlichkeit gedacht, da konkrete Risiken benannt werden und Angaben zu technischen und organisatorischen Maßnahmen getroffen werden, um denkbare Risiken maßgeblich zu minimieren. Sie erhalten eine derartige Vorlage von uns entweder im Zuge der Einrichtung oder gerne auch auf Anfrage über Ihre Schulleitung zugeschickt.

Die DSFA muss auf Verlangen Ihrer für Datenschutz zuständigen Behörde vorgelegt werden können. Darüber hinaus regelt der § 55 des Berliner Datenschutzgesetzes (BlnDSG) Folgendes:

Der Verantwortliche hat vor der Inbetriebnahme von neu anzulegenden Dateisystemen die Berliner Beauftragte oder den Berliner Beauftragten für Datenschutz und Informationsfreiheit anzuhören, wenn

1. aus einer Datenschutz-Folgenabschätzung nach § 53 hervorgeht, dass die Verarbeitung trotz Abhilfemaßnahmen **eine erhebliche Gefahr** für die Rechtsgüter der betroffenen Personen zur Folge hätte oder
2. die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, Mechanismen oder Verfahren, **eine erhebliche Gefahr** für die Rechtsgüter der betroffenen Personen zur Folge hat.

Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit kann eine Liste der Verarbeitungsvorgänge erstellen, die der Pflicht zur Anhörung nach Satz 1 unterliegen.

Wenn Ihre DSFA also **keine erhebliche Gefahr** feststellt, bleibt es dabei, dass Sie diese DSFA nur auf Verlangen vorlegen können müssen.

*Rechtlicher Hinweis zu dieser Informationsseite

Wir machen darauf aufmerksam, dass unsere Informationsseite lediglich dem **unverbindlichen Informationszweck** dient und **keine Rechtsberatung** im eigentlichen Sinne darstellt. Der Inhalt dieses Angebots und die zur Verfügung gestellten Dokumente zum Download können und sollen eine individuelle und verbindliche Rechtsberatung, die auf Ihre spezifische Situation eingeht, nicht ersetzen. **Insofern verstehen sich alle angebotenen Informationen ohne Gewähr auf Richtigkeit und Vollständigkeit.**

Rollenkonzept

Rollenkonzept von BOLLE

Den Nutzer:innen sind die Rollen Schulkind, Eltern oder Personal zugeordnet. Schulkinder haben nur auf ihre eigenen und Eltern nur auf ihre eigenen Daten und die ihrer Kinder Zugriff.

Innerhalb der Kategorie Personal gibt es die weiter unten beschriebenen Rollen. Diese können von Personen, die die Rolle *Admin* innehaben, vergeben werden.

Eltern

Lesender Zugriff

- Eltern besitzen ausschließlich lesenden Zugriff. Sie können die Fehlzeiten Ihres Kindes / Ihrer Kinder einsehen.
- Sie finden eine Übersicht der E-Mail-Adressen aller Lehrkräfte, sofern diese hinterlegt sind.
- Falls das Bibliotheksmodul genutzt wird, sehen sie die Ausleihen Ihrer Kinder.
- Falls das Dateiablagemodul verwendet wird, können sie dort für Eltern freigegebenen Dateien herunterladen.
- Falls das Materialmodul genutzt wird, sehen sie die Arbeitsaufträge mit Anhängen, die die Lehrkräfte in den Kursen
- Ihrer Kinder zur Verfügung stellen.
- Falls das Kalendermodul genutzt wird, haben sie die Möglichkeit, schulische Termine einzusehen.

Schulkind

Lesender Zugriff

- Schulkinder haben lesenden Zugriff auf die bei den Eltern genannten Daten.
- Falls das Nachschreibtermin-Verwaltungsmodul genutzt wird, haben sie lesenden Zugriff darauf, ob und wann sie für Nachschreibtermine angemeldet wurden.

Schreibender Zugriff

- Falls das Materialmodul genutzt wird, haben Sie die Möglichkeit, Kommentare und Anhänge als Antwort auf Arbeitsaufträge in ihren Kursen online zu stellen.
- Schüler:innen der E-Phase können, falls das entsprechende Modul genutzt wird, die Wahl ihrer Wahlpflichtkurse digital eintragen. Eine bindende Wahl der Wahlpflichtkurse erfolgt ausschließlich durch die Abgabe in Papierform, mit Unterschrift des Schulkindes und mindestens eines Erziehungsberechtigten.

- Schüler:innen der Q-Phase können, falls das entsprechende Modul genutzt wird, das Thema ihrer 5. Prüfungskomponente online eintragen.
- Schüler:innen der Q-Phase können, falls das entsprechende Modul genutzt wird, die Wahl ihre Kurse digital eintragen. Eine bindende Wahl der Wahlpflichtkurse erfolgt ausschließlich durch die Abgabe in Papierform, mit Unterschrift des Schulkindes - und mindestens eines Erziehungsberechtigten, falls das Schulkind das 18. Lebensjahr noch nicht vollendet hat.

Personal

Im Folgenden wird nicht jedes Mal erwähnt, dass das Recht nur besteht, falls eine bestimmte Funktion genutzt wird.

- Räume und Medien können gebucht werden.
- Der Kalender kann eingesehen werden.
- Dateien aus der Dateiablage können heruntergeladen werden.
- Stundenpläne, Aufsichtspläne und Vertretungspläne können eingesehen werden.

Die Rolle *Personal* berechtigt dazu, weitere Rollen innezuhaben, die im Folgenden beschrieben werden. Die Personen, die die Rolle *Admin* besitzen, können folgende Rollen berechtigten Personen zuweisen.

Verwaltungspersonal

Lesend und schreibend

- Fehlzeiten der Schüler:innen eintragen (morgens im Sekretariat).
- Neues Personal anlegen, bereits angelegtes Personal bearbeiten (Vor-, Nachname, E-Mail), Personal, das die Schule verlassen hat, deaktivieren.
- Lehrbefähigung des Personals bearbeiten.
- Stammdaten von Schüler:innen einsehen und bearbeiten.
- E-Mails an Gruppen verschicken (z.B. Schüler:innen Jahrgang 9).
- Klassen verwalten (neue Klassen anlegen, vorhandene bearbeiten, löschen).
- Fehlzeiten-Statistik erstellen, die an den Senat geschickt werden müssen.

Lehrkraft

Lesend und schreibend

- Erstellen eigener Kurse, zuordnen von Schulkindern zu diesen. Führung des Kursbuches, inklusive Notenverwaltung. Eintragen von Unterrichtsterminen.
- Erstellen eigener AGs mit Führung eines Kursbuches.
- Schüler:innen der eigenen Kurse können zu Nachschreibterminen angemeldet werden.
- Bücher können für Lerngruppen angefragt werden (Ausleihe erfolgt über die Rolle Bibliothek).

Lesend

- Nachteilsausgleiche, die Schüler:innen der eigenen Kurse in ihrem Fach zustehen, können eingesehen werden.

Klassenleitung (KL)

Schreibend und lesend

- Die Fehlzeiten der Schüler:innen der eigenen Klasse können eingesehen und bearbeitet werden.
- Die Logindaten der Schüler:innen können zurückgesetzt werden, falls ein Schulkind seine Zugangsdaten zu BOLLE vergessen hat.
- KL können Eltern mit deren Einverständnis dazu einladen, ein Profil in BOLLE zu erstellen.
- KL können eine Beurteilung des Arbeits- und Sozialverhaltens der Kinder ihrer eigenen Klasse vornehmen.
- KL können Nachteilsausgleiche, die den Kindern ihrer Klasse zustehen, eintragen.

Lesend

- Daten zu Praktika, Wandertagen und Projekten können eingesehen werden.
- Die Kurszuordnungen und Noten der Schüler:innen der eigenen Klasse können kurz vor den Zeugnissen eingesehen werden, insofern die Fachlehrkräfte das Notenmodul nutzen.
- Daten zur Mittelstufenlaufbahn (d.h. Fremdsprachenfolge und Wahlpflichtfächer) können eingesehen werden.
- Zeugnisbemerkungen können eingetragen und Zeugnisse heruntergeladen und ausgedruckt werden.

Fachbereichsleitung (auch Fachleitung / Fachkoordination / FBL)

Schreibend und lesend

- An ISS können die Kurswechsel und Niveauzuordnungen vorgenommen werden (ER / GR).
- Es können Kursbücher des Fachbereichs zur Kenntnisnahme angefordert werden. Wenn eine Fachlehrkraft das Kursbuch abgibt, kann diese von der FBL eingesehen und zur Kenntnis genommen werden.

Bibliothek und Bibliothekshilfe

- *Schreibend und lesend*
- Bücher können ausgeliehen werden.
- Weiterhin können übliche Tätigkeiten einer Bibliothekssoftware (Pflege des Bestandes etc.) vorgenommen werden.

Dateiablage

Schreibend

- Es dürfen Dateien in die Dateiablage hochgeladen werden. Die Dateiablage ein ein Sammelort für nicht personenbezogene Daten wie z.B. allgemeine Formulare für den Arbeitsalltag.

Mittelstufenkoordination

Schreibend und lesend

- Kurszugehörigkeiten (und an der ISS Niveauwechsel) aller Fächer können bearbeitet werden.
- Noten aller Kurse der Mittelstufe können eingesehen und bearbeitet werden (z.B. während der Notenkonferenz).
- Die Mittelstufenlaufbahn aller Kinder der Mittelstufe kann bearbeitet werden (d.h. Fremdsprachenfolge und Wahlpflichtfächer).
- Die Fehlzeiten aller Kinder der Mittelstufe können bearbeitet werden.
- Die Zeugnisse aller Kinder der Mittelstufe können bearbeitet werden.
- Abgangs- und Abschlusszeugnisse können erstellt werden.

Oberstufenkoordination

Schreibend und lesend

- Die Wahlen der E-Phase und der Q-Phase können verwaltet werden.
- Die Themen der 5. Prüfungskomponente können verwaltet werden.
- Die Fehlzeiten aller Kinder der Oberstufe können bearbeitet werden.
- Die Zeugnisse aller Kinder der Oberstufe können bearbeitet werden.
- Abgangs- und Abschlusszeugnisse können erstellt werden.

Schulleitung

Lesend

- Alle Klassenbucheinträge können gelesen werden.
- Erbt die Schreib- und Leserechte der Mittel- und Oberstufenkoordination.

Nachschreibtermine

Schreibend und lesend

- Nachschreibtermine können angelegt und gelöscht werden.

Praktikumsorganisation

Schreibend und lesend

- Daten zu Schulpraktika (Schulkind + Betrieb, kein Praktikumsbericht o.Ä.) können verwaltet werden.

Projektverwaltung

Schreibend und lesend

- Daten zu einer Projektwoche (Projekte und Teilnahmen) können verwaltet werden.

Raum- und Medienbuchung

Schreibend und lesend

- Räume und Medien können eingepflegt und zur Buchung freigegeben werden.

Wandertag

Schreibend und lesend

- Wandertage können angelegt und verwaltet werden.

Benutzerhinweise zur Informationssicherheit und zum Datenschutz

Teil der technisch-organisatorischen Maßnahmen im Rahmen des Betriebs von BOLLE (oder ähnlichen Systemen) sind **regelmäßige Sensibilisierungsmaßnahmen des Personals**. Das Schulpersonal muss darüber informiert werden, wie es sich im Falle des Verlustes von Zugangsdaten zu verhalten hat. Die Schulleitungen oder die schulischen Beauftragten für Datenschutz geben jährlich Hinweise zur Informationssicherheit und zum Datenschutz. Die Benutzerhinweise auf dieser Seite können dabei behilflich sein.

Inhalt

1. Allgemeines
2. Passwort
3. Key-Datei
4. Verwaltungskey-Datei
5. Zeitlich limitiertes Einmalkennwort (TOTP)
6. FIDO2
7. Vertrauenswürdige Geräte (FIDO)

1. Allgemeines

Sie verwalten über BOLLE personenbezogene Daten der Schüler:innen. Seien Sie sich stets der Tatsache bewusst, dass die Vertraulichkeit der Daten und ihr Schutz vor unbefugter Veränderung höchste Priorität hat und in Ihrer Verantwortung liegt.

Der Zugang zu BOLLE wird daher durch eine Zwei-Faktor-Authentisierung besonders gesichert. Ihr Benutzerkonto wird sowohl durch ein persönliches Passwort als auch einen weiteren Faktor geschützt. Der weitere Faktor kann

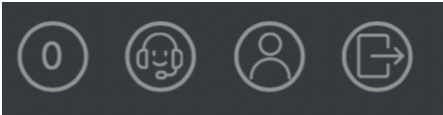
- die Key-Datei bzw.
- die Verwaltungskey-Datei,
- ein zusätzliches zeitlich limitiertes Einmalkennwort (TOTP) oder

- die Identifikation mit einem bestimmten, bereits als vertrauenswürdig definierten Gerät sein.

Sowohl beim Passwort als auch bei den zweiten Faktoren sollen folgende sicherheitsrelevante Aspekte beachtet werden.

Die wichtigste Regel: **Immer ordentlich ausloggen!**

Klicken Sie dafür auf das Logout-Symbol ganz oben rechts.



Ähnlich wie bei anderen sensiblen Bereichen im Internet (z.B. Online-Banking) erfolgt bei BOLLE ein automatischer Logout. Sollten Nutzer:innen aus welchen Gründen auch immer den oben beschriebenen ordentlichen Logout vergessen, werden sie innerhalb eines kurzen Zeitfensters automatisch ausgeloggt. Vor einem **automatischen Logout** wird man in der Menüleiste mit einem roten Countdown informiert. Wenn man auf den Countdown klickt oder eine andere Aktion innerhalb von BOLLE ausführt, wird das Zeitfenster zum automatischen Logout zurückgesetzt.

2. Passwort

- je länger, desto besser: Passwortlänge von **mindestens zehn Zeichen** wählen
- es **müssen** Groß- **und** Kleinbuchstaben verwendet werden
- das **Passwort muss eine Zahl oder ein Sonderzeichen** enthalten
- **erlaubte Sonderzeichen sind: !\$%&=+ #-_.:,@**
- mehrere Ziffern hinzufügen, wird empfohlen
- keine Passwort-Kombinationen, die Geburtstage (o.Ä.) enthalten
- keine Wiederholungs- und Tastaturmuster (asdf, 1234, 777)
- kein simples Passwort, das nur um ein Sonderzeichen am Wortanfang oder -ende ergänzt ist (z.B.: "!Passwort")
- nicht an andere Personen weitergeben
- nie per E-Mail versenden
- nicht auf PCs speichern, auf denen sich auch andere Menschen einloggen können
- nicht unverschlüsselt auf dem PC ablegen
- falls gespeichert, darf sich das Passwort nicht kontrolllos automatisch ausfüllen lassen
- nicht auf dem berühmten Notizzettel am Bildschirm schreiben

Weitere Informationen finden Sie beim [Bundesamt für Sicherheit und Informationstechnik](#)

bei Verlust oder Diebstahl:

Melden Sie sich bei Ihrem schulinternen Admin. Falls Sie sich noch einloggen können, gehen Sie auf Ihr Profil (ganz oben rechts, Profilicon) und klicken links auf *Sicherheit*. Hier können

Sie Ihr Passwort selbst verändern.

3. Key-Datei

- nie per E-Mail versenden
- nicht an andere Personen weitergeben
- nicht vervielfältigen
- auf einem verschlüsselten mobilen Datenträger aufbewahren

Die Key-Datei wird Ihnen von Ihrem Admin vor Ort ausgestellt.

bei Verlust oder Diebstahl:

Melden Sie sich bei Ihrem schulinternen Admin. Falls Sie sich noch einloggen können, gehen Sie auf Ihr Profil (ganz oben rechts, Profilicon) und klicken links auf *Sicherheit*. Hier können Sie Ihre Key-Datei invalidieren oder sogar den Account vorerst komplett sperren.

4. Verwaltungskey-Datei

- nie per E-Mail versenden
- nicht an andere Personen weitergeben
- nicht vervielfältigen
- getrennt von der Key-Datei aufbewahren
- im besten Fall nur auf dem passwortgeschützten und verschlossenen stationären Dienstrechner ablegen und verwenden

Die Verwaltungskey-Datei ist nötig, um besonders sensible und weitreichende Bereiche in BOLLE einzusehen. Ihr Admin informiert Sie darüber, ob Sie solch einen Verwaltungskey benötigen.

bei Verlust oder Diebstahl:

Melden Sie sich bei Ihrem schulinternen Admin. Falls Sie sich noch einloggen können, gehen Sie auf Ihr Profil (ganz oben rechts, Profilicon) und klicken links auf *Sicherheit*. Hier können Sie Ihre Key-Datei invalidieren oder sogar den Account vorerst komplett sperren.

5. Zeitlich limitiertes Einmalkennwort (TOTP)

- nur auf einem persönlichen Gerät verwenden, bei dem weitere Sicherheitsmerkmale den Zugriff kontrollieren (z.B. Kennwort am Smartphone)
- nur Sie sollten Zugriff auf das persönliche Gerät haben, auf dem das TOTP ausgegeben wird

Wie Sie ein TOTP einrichten, wird Ihnen [hier](#) erklärt.

bei Verlust oder Diebstahl:

Melden Sie sich bei Ihrem schulinternen Admin. Falls Sie sich noch einloggen können, gehen Sie auf Ihr Profil (ganz oben rechts, Profilicon) und klicken links auf *Sicherheit*. Hier können Sie Ihre Zwei-Faktor-Authentisierung mittels TOTP löschen oder sogar Ihren Account sperren.

6. FIDO2

Mehr zu FIDO2 erfahren Sie auf dieser Seite.

7. Vertrauenswürdige Geräte

- sind nur Geräte, die sich permanent in Ihrem Besitz bzw. sich in Ihrer dauerhaften Zugriffskontrolle befinden
- Computer, auf denen sich auch andere Personen einloggen könnten, sind keine vertrauenswürdigen Geräte (z.B. der PC im Klassenraum oder Kolleg:innenzimmer)
- der Zugang zu vertrauenswürdigen Geräten ist abermals passwortgesichert
- Bildschirmschoner mit Kennwort sichern
- nicht unbeaufsichtigt lassen; vor allem nicht nach einer Anmeldung am Gerät

Auf vertrauenswürdigen Geräten können Sie z.B. einen FIDO2-Zugang einrichten. Mehr zu FIDO erfahren Sie hier: [Allgemeines](#)

[Informationen für den Admin der Schule](#)

[Einstellungsmöglichkeiten für das Personal](#)

bei Verlust oder Diebstahl:

Melden Sie sich bei Ihrem schulinternen Admin. Die Admins können auch Ihre FIDO2-Zugänge deaktivieren. Sie selber können sich, falls Sie sich noch einloggen können, Ihren gesamten Account oder z.B. nur die Keydatei deaktivieren. Ihre Admins können dann Ihren Account wieder aktivieren oder Ihnen eine neue Keydatei ausstellen.

Zwei-Faktor-Authentisierung in BOLLE

Der Zugang zu BOLLE erfolgt für das schulische Personal zwingend über die sogenannte Zwei-Faktor-Authentisierung (2FA). Auf dieser Seite finden Sie Informationen über die technische Organisation des zweiten Faktors.

Inhalt

1. Key für Lehrkräfte
2. Verwaltungskey
3. TOTP
4. BOLLE App
5. FIDO
6. Weitere Verfahren

1. Key für Lehrkräfte

Lehrkräfte verwalten besonders sensible Daten in BOLLE. Der Einsatz der 2FA ist obligatorisch und wird bei der Einführung von BOLLE dem Personal erläutert. Jede Lehrkraft erhält eine individuelle Key-Datei, die beim ersten Login generiert wird. Ab diesem Zeitpunkt ist jeder weitere Login nur mit 2FA möglich.

Die Key-Datei ist eine html-Datei, die einen geheimen, persönlichen Schlüssel enthält. Beim Login des Personals wird das gehashte Passwort vom User und dieser geheime Schlüssel zum BOLLE-Server übertragen. Nur wenn beide Faktoren mit den gespeicherten Daten über den User übereinstimmen, wird dieser eingeloggt.

Der geheime Schlüssel ist eine Zeichenkette mit einer Länge von mindestens 50 Zeichen (Zahlen, Groß- und Kleinbuchstaben).

Die html-Datei kann vom Besitzer der Datei nach Belieben vervielfältigt werden. Ein effektiver Schutz dagegen existiert nicht. Es ist ratsam, das Personal regelmäßig darüber zu informieren und auf diesen Sicherheitsaspekt hinzuweisen.

BOLLE unterstützt die Schulen bei der Umsetzung z.B. mit Erinnerungen/Checklisten und Hinweise für Benutzer:innen.

2. Verwaltungskey

Einige Lehrkräfte nehmen besondere Rollen und Verwaltungsaufgaben in BOLLE wahr. Diese besonders sensiblen Bereiche sind durch eine zweite Key-Datei geschützt, dem Verwaltungskey. Dies ermöglicht den Lehrkräften, dass sie ihre Verwaltungsaufgaben von ihren unterrichtlichen Aufgaben trennen können.

Der Aufbau der Verwaltungskey entspricht dem der normalen Key-Dateien.

In der Regel haben solche Lehrkräfte ein eigenes Büro mit stationären Dienstrechnern im Schulgebäude. So kann der Verwaltungskey separat von der *normalen* Key-Datei aufbewahrt werden.

3. TOTP

Anstelle der Key-Datei kann jeder User das TOTP-Verfahren aktivieren. Dabei wird ein offener Standard zur Erzeugung von Einmalkennwörtern genutzt, die zusätzlich zum Benutzernamen und dem Passwort eingegeben werden müssen (siehe Wikipedia TOTP). Die Aktivierung des TOTP steht allen Nutzer:innen offen (Lehrkräften, Schüler:innen und Eltern).

Verwaltungsaufgaben können **nur** durchgeführt werden, wenn eine Authentisierung **mittels Verwaltungskey** erfolgt ist. TOTP genügt hierfür nicht.

4. BOLLE App

Die BOLLE App ermöglicht den Lehrkräften einen schnellen Zugriff auf eine eingeschränkte Funktionsauswahl. Der Login erfolgt nur, wenn man gleichzeitig im Browser bei BOLLE eingeloggt ist. Das Gerät wird dann mittels eines mindestens 200 Zeichen langen Tokens authentisiert, der via QR-Code direkt vom Smartphone eingelesen wird. Ein Login in die App ist somit nur möglich, wenn man korrekt in BOLLE im Browser eingeloggt ist.

Verwaltungsaufgaben können in der App generell nicht durchgeführt werden.

Schüler:innen und Eltern können sich mit den gleichen Logindaten wie im Browser (ggf. mit TOTP) einloggen.

Einmal eingeloggt, bleibt die App authentisiert, bis der User sich ausloggt. Beim Öffnen der App

wird ein Entsperrmechanismus vom Telefon verlangt (z.B. Fingerabdruck, Gesichtsscan oder Entsperrcode).

Ist die App über mehrere Wochen inaktiv, wird die Authentisierung automatisch aufgehoben.

5. FIDO

BOLLE unterstützt eine der sichersten Login-Methoden für Webservices: Fast Identity Online 2.0 (FIDO2). Sichere Login-Verfahren nutzen neben Username und Passwort noch einen weiteren Faktor. Diese Zwei-Faktor-Authentisierung (2FA) funktioniert z.B. mittels der oben beschriebenen Key-Datei oder dem TOTP. Diese beiden Varianten sind softwaregestützt. Es gibt aber nun auch die Möglichkeit, eine hardwaregestützte 2FA einzurichten: FIDO2. Hardwaregestützte 2FA gelten als noch sicherer (vgl. Bundesamt für Sicherheit in der Informationstechnik).

Der Login mittels FIDO2 erfolgt geräte- und browsergenau. Dabei wird im Browser bzw. auf dem Gerät mittels der vorhandenen Technik des Geräts der zweite Faktor direkt gespeichert. Selbst wenn er ausgelesen werden könnte, funktioniert dieser nur auf dem Gerät, auf dem er eingerichtet wurde.

Beim Login mit FIDO für Personal mit Verwaltungsaufgaben kann außerdem entschieden werden, ob man sich mit vollen Verwaltungsrechten einloggen möchte. Somit ist auch bei der Nutzung von FIDO eine Unterscheidung ähnlich wie bei den Verwaltungskkeys gegeben (siehe oben).

6. Weitere Verfahren

Neuen Entwicklungen im Bereich der passwortlosen Anmeldung oder weiterer 2FA-Verfahren verfolgen wir interessiert. Neue Verfahren werden von uns dann implementiert, sobald sie sich ausreichend verbreitet und bewährt haben.

FIDO2 als Login-Möglichkeit

Es gibt eine neue Möglichkeit, die wir Ihnen zusätzlich zum Login mit Key-Datei und TOTP anbieten. **Sie heißt FIDO2.**

(Diese Technik wird u.a. auch Passkeys genannt.)

Diese wesentliche Neuerung bezüglich der Sicherheit für den Login bei BOLLE beruht auf der Einführung des Sicherheitsstandards FIDO, dem sich alle großen Webservices angeschlossen haben und diesen auch umsetzen werden und der somit demnächst auch in weiteren Bereichen im Internet immer wichtiger wird.

Doch zunächst zur Relevanz für den Login bei BOLLE:

Für das Personal gab es bisher drei Login-Möglichkeiten: Key-Datei, TOTP oder die Einrichtung eines vertrauenswürdigen Geräts.

Die meisten Ihrer Kolleg:innen benutzen eines der ersten beiden Verfahren (**Key-Datei oder TOTP**), an denen sich auch in Zukunft nichts ändern wird. **Für diese Kolleg:innen besteht also aktuell kein Handlungsbedarf.**

All diese Möglichkeiten haben gemeinsam, dass sie das Sicherheitskriterium einer sogenannten Zwei-Faktor-Authentisierung (2FA) erfüllen. Die bisherigen Login-Verfahren für BOLLE sind alle softwaregestützt.

Das Bundesamt für Sicherheit in der Informationstechnik stellt fest, dass „vor allem hardwaregestützte Verfahren ein hohes Maß an Sicherheit“ bieten (Quelle).

An solch einem hardwaregestützten Verfahren als zweiten Faktor haben wir in den vergangenen Monaten gearbeitet und wollen Ihnen die Möglichkeit geben, dieses Login-Verfahren einzusetzen. **Das neue Verfahren heißt FIDO2 (Fast Identity Online 2.0).**

Der Login mittels FIDO2 erfolgt geräte- und browsergenau. Dabei wird im Browser mittels der vorhandenen Technik des Geräts der zweite Faktor direkt gespeichert. Selbst wenn er ausgelesen werden könnte, funktioniert dieser nur auf dem Gerät und dem Browser, auf dem er eingerichtet wurde.

Die meisten aktuellen Geräte und Browser unterstützen solch eine FIDO2-Einrichtung. Auch die durch die Senatsverwaltung ausgegebenen Dienstablets könnten das theoretisch. Bisher hat die zuständige Stelle die Möglichkeit hierzu aber noch nicht aktiviert.

(NB: Auf den Dienstablets funktioniert für eine mögliche FIDO2-Nutzung nur ein sogenannter YubiKey, eine Art USB-Sicherheitskey. Der Login auf den Dienstablets funktioniert aber auch weiterhin mit Key-Datei oder TOTP.)

Auf diesen Hilfeseiten erklären wir ausführlich,

1. **wie Ihre Admins FIDO2 als Login-Verfahren für Ihre Kolleg:innen aktivieren können** und
2. **wie Sie FIDO2 auf Ihren Geräten einrichten und nutzen.**

Im Zuge dieser Umstellung und der Veränderung der Sicherheitsanforderungen mussten wir die bisherige Möglichkeit der Einrichtung vertrauenswürdiger Geräte mittels TOTP deaktivieren. Diese Form der 2FA konnte bis jetzt auf vertrauenswürdigen Geräten zeitweise übersprungen werden. Dies führt zu einer Verringerung der Sicherheit. Daher kann der Login mittels eines vertrauenswürdigen Gerätes ab sofort nicht mehr erfolgen. **Mit FIDO2 können die Kolleg:innen jedoch ebenfalls „vertrauenswürdige Geräte“ einrichten,** nur handelt es sich hierbei um eine vielfach sicherere Möglichkeit.

Wichtig: Für Kolleg:innen, die den Login mittels Key-Datei und TOTP nutzen, ändert sich nichts. Sie können sich weiterhin normal mit ihrer Key-Datei oder TOTP einloggen. Erst wenn ein persönlicher FIDO2-Key erstellt wurde, geht der Login nur noch über FIDO2 sowie zusätzlich auch weiterhin mit der Key-Datei. Ein Login mittels TOTP ist dann nicht mehr möglich. Weitere Informationen finden Sie auf den oben genannten Hilfeseiten.

Wir hoffen, wir konnten Ihnen die ziemlich technische Seite des neuen sicheren Loginverfahrens gut erläutern und hoffen vor allem, dass Sie unseren Anspruch an höchsten Datenschutz und Datensicherheit nachvollziehen und teilen.

Wie bereits erwähnt: **Die Login-Verfahren mit Key-Datei und TOTP bleiben bestehen.** Wenn Sie möchten, probieren Sie gerne einmal die neue FIDO2-Technik aus. Die Erst-Einrichtung wirkt vermutlich erst etwas abschreckend; wir versuchen den Prozess für Sie und Ihre Kolleg:innen so einfach wie möglich zu gestalten.

Wenn Sie das Verfahren ausprobieren möchten, sprechen Sie Ihren Admin an der Schule an.

Verzeichnis der Sub-Auftragsverarbeiter

Diese Seite enthält sämtliche von uns eingesetzten Sub-Auftragsverarbeiter und gibt Auskunft darüber, welche Teilleistungen durch die Sub-Auftragsverarbeiter ausgeführt werden.

Name und Anschrift des Subunternehmers	Beschreibung der Teilleistungen
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen	Server-Hosting der BOLLE-Instanzen Speicherung der verschlüsselten Backups
Strato AG, Pascalstr. 10, 10587 Berlin	Speicherung der verschlüsselten Backups
rapidmail GmbH, Wentzinger Str. 21, 79106 Freiburg i.Br.	Versand von Mails durch BOLLE (noreply@bolle.schule)
netcup GmbH, Daimlerstr. 25, 76185 Karlsruhe	E-Mail-Verkehr (...@bolle-software.de)

Im Rahmen der Auftragsverarbeitungsverträge sind weitere Subunternehmer, die durch die o.g. Unternehmen eingesetzt werden, mit der Verarbeitung der Daten beauftragt.

Name und Anschrift des Subunternehmers	Eingesetzt durch Subunternehmen	Beschreibung der Teilleistungen
MEGASPACE Internet Service GmbH, Max-von-Laue-Str. 2b, 76829 Landau	rapidmail GmbH	Hosting der Server an Standorten innerhalb Deutschlands.
uvensys GmbH, Robert-Bosch-Straße 4b, 35440 Linden	rapidmail GmbH	Hosting der Server an Standorten innerhalb Deutschlands.