Informationsblatt für Ihre Datenschutzbeurteilung

Version 1.3, Fassung vom 7. November 2026.

Zweck, Datenflüsse, Risiken und Massnahmen von BYOD-Bot, vorausgefüllt als Grundlage für Ihre Risikoanalyse oder Datenschutz-Folgenabschätzung.

Dieses Blatt fasst für die Datenschutzverantwortlichen einer Schule zusammen, welche Daten BYOD-Bot bearbeitet, wohin sie fliessen, welche Risiken bestehen und wie sie begrenzt sind. Es folgt dem Aufbau, den kantonale Vorlagen für eine Datenschutz-Folgenabschätzung verwenden, und den Risikobereichen aus dem Merkblatt «Cloud-spezifische Risiken und Massnahmen» von privatim, der Konferenz der schweizerischen Datenschutzbeauftragten. Es beschreibt Sachverhalte; die Bewertung der Risiken und den Entscheid, ob eine Vorabkontrolle nötig ist, trifft die Schule. Massgebend sind der Auftragsbearbeitungsvertrag (AVV), die Liste der Unterauftragsbearbeiter und die Datenschutzerklärung.

1. Rechtlicher Rahmen

- **Öffentliche Schulen** unterstehen dem Datenschutzgesetz ihres Kantons. Die meisten Kantone verlangen vor einer neuen Bearbeitung von Personendaten eine Risikoanalyse oder eine Datenschutz-Folgenabschätzung. Ergeben sich besondere Risiken, ist das Vorhaben der kantonalen Datenschutzstelle zur Vorabkontrolle vorzulegen, im Kanton Zürich zum Beispiel nach § 10 IDG.
- **Private Schulen** unterstehen dem Bundesgesetz über den Datenschutz (DSG). Eine Datenschutz-Folgenabschätzung ist nötig, wenn eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringen kann (Art. 22 DSG).
- **Bearbeitung im Auftrag:** Die Schule bleibt für die Bearbeitung verantwortlich. Die digitalify GmbH, Euelstrasse 29, 8408 Winterthur, bearbeitet die Daten als Auftragsbearbeiterin nach dem AVV (Version 1.0).

2. Beschreibung der Bearbeitung

- **Zweck:** Ein Bot beantwortet Fragen der Lernenden zum BYOD-Konzept der Schule, ausschliesslich aus den Unterlagen, die die Schule hochlädt oder über einen Link angibt, und aus ihren eigenen Einträgen. Die Schule verwaltet, testet und wertet den Bot selbst aus.
- **Bearbeitungsvorgänge:** Erheben der Fragen im Chat; Weitergabe an das Sprachmodell, das die Antwort erzeugt; Aufbewahren der Angaben aus Abschnitt 3; Auswerten durch die Schule (Statistik, unbeantwortete Fragen, Export als CSV); Löschen nach Ablauf der Frist.
- **Umfang:** Hängt von der Zahl der Lernenden und ihrer Fragen ab. Lernende melden sich nicht an; die Plattform weiss nicht, wer eine Frage stellt, und bildet keine Profile.
- **Besonders schützenswerte Personendaten:** Nicht vorgesehen. Der Chat bittet die Lernenden, keine persönlichen Daten einzugeben.

3. Betroffene Personen und Daten

Lernende und andere Nutzende des Bots

Welche Daten: Die Frage (E-Mail-Adressen, Telefon- und AHV-Nummern vor dem Speichern unkenntlich gemacht; Namen erkennt das System nicht), der Tag der Frage ohne Uhrzeit, die zitierten Quellen, das Ergebnis (beantwortet, nicht beantwortet oder von der Prüfung der Antwort zurückgehalten) und die Bewertung (Daumen hoch oder runter). Keine Antworttexte, keine Anmeldung, keine IP-Adressen, keine Geräte-Kennungen.

Wie lange: Nach der Frist der Schule: 7 bis 365 Tage, standardmässig 30

Lernende (technisch)

Welche Daten: Eine zufällige Kennung der Konversation, im Cookie des Chats oder, wenn der Browser es ablehnt, nur im Arbeitsspeicher der Seite. Sie begrenzt die Anzahl Fragen und zählt die Konversationen für das Kontingent der Schule. Gespeichert wird sie nur als Prüfwert, nie zusammen mit den Fragen. Den bisherigen Verlauf einer Konversation hält der Browser; der Server speichert ihn nicht.

Wie lange: Kennung höchstens 2 Stunden gültig; Prüfwerte nach höchstens rund einem Tag gelöscht; für das Kontingent bleibt pro Konversation nur der Zeitpunkt der Zählung, ohne Kennung

Admins der Schule

Welche Daten: Name, E-Mail-Adresse, Anmeldedaten (das Passwort nur als Hash, auf Wunsch ein zweiter Faktor), Änderungsverlauf des Bots, Zustimmungen zu AGB, Datenschutzerklärung und AVV mit Version und Datum; technisch notwendige Cookies der Anmeldung mit einer zufälligen Kennung; Angaben zu versendeten E-Mails

Wie lange: Bis zur Löschung des Kontos; Cookies höchstens 12 Stunden (Sitzung) und 10 Minuten (zweiter Faktor); Angaben zu E-Mails 90 Tage

Admins der Schule (Arbeit am Bot)

Welche Daten: Gespräche mit dem Coach, Testfragen und die Ergebnisse der Testläufe mit den Antworten des Bots

Wie lange: Coach-Gespräche 30 Tage nach der letzten Aktivität, eine Kopie einer Frage der Lernenden spätestens mit dieser; von den Testläufen die letzten 10

In den Unterlagen genannte Personen

Welche Daten: Was die Schule in ihre Unterlagen schreibt, zum Beispiel Kontaktangaben des Supports

Wie lange: Bis die Schule die Unterlagen löscht

Rechnungsempfänger

Welche Daten: Schulname, Rechnungsadresse, E-Mail-Adresse für die Rechnung, Zahlungsstatus

Wie lange: Gesetzliche Aufbewahrungsfrist, auch nach der Löschung der Schule

Personen im Betrieb (Support-Zugriff)

Welche Daten: Pro Zugriff des Supports Zeitpunkt, Name der Person und Art der Daten, ohne Inhalte; die Freigaben der Admins mit Dauer und Widerruf

Wie lange: Bis zur Löschung der Schule

4. Datenflüsse

1. **Frage:** Der Browser schickt die Frage verschlüsselt (TLS) an die Seite der Schule auf <kurzname>.byod-bot.ch oder an den eingebetteten Chat. Die Anwendung verwirft die Angaben zur Adresse des Geräts, bevor sie die Anfrage bearbeitet; die Protokolle des Webservers enthalten keine IP-Adressen.
2. **Antwort:** Die Anwendung gibt die Frage, den bisherigen Verlauf der Konversation und die passenden Abschnitte aus den Unterlagen der Schule an das Sprachmodell bei Infomaniak in der Schweiz. Prüfungen in der Anwendung halten Antworten zurück, die Anweisungen des Bots wiedergeben oder nicht lesbar sind, und entfernen Links auf Adressen, die nicht aus den Unterlagen oder den Angaben der Schule stammen. Die Antwort wird angezeigt und nicht gespeichert.
3. **Protokoll:** Gespeichert wird nur, was Abschnitt 3 nennt, in der Datenbank der Plattform, getrennt nach Schule.
4. **Auswertung:** Die Admins der Schule sehen die gespeicherten Fragen ihrer Schule und können Statistik und unbeantwortete Fragen als CSV exportieren. Öffnen sie eine unbeantwortete Frage im Coach, verarbeitet das Sprachmodell sie ein weiteres Mal, um einen Eintrag für die Unterlagen vorzuschlagen.
5. **Unterlagen über einen Link:** Gibt die Schule für ein Dokument eine Adresse an, ruft die Plattform das PDF dort ab und prüft es täglich auf eine neue Fassung. Der Server hinter der Adresse sieht dabei die Adresse unseres Servers und den Namen der Plattform; übermittelt werden keine Cookies und keine Daten von Lernenden. Wo dieser Server steht, bestimmt die Schule mit der Adresse.
6. **Betrieb:** Ohne Freigabe der Schule sehen die Betreiber der Plattform in ihrer Verwaltung keine Fragen und keine Unterlagen der Schulen. Sie sehen pro Schule Name und Kurzname, Abo, Rechnungen mit Rechnungsadresse, Zählungen (Fragen und Antworten, Konversationen für das Kontingent, verbrauchte Token und Kosten) und während 30 Tagen, auf welchen Seiten einer Website der Chat lief (nur die Adresse der Seite, keine Angaben zu Besuchenden). **Support-Zugriff:** Gibt ein Admin der Schule den Support frei (für 1, 7 oder 30 Tage; jeder Admin kann die Freigabe jederzeit mit sofortiger Wirkung widerrufen), können die Betreiber den Admin-Bereich der Schule ansehen, also Unterlagen, Einträge, Einstellungen, die gespeicherten Fragen, die Auswertung, Testfragen, den Änderungsverlauf, das Team mit Namen und Adressen der Admins sowie Abo und Rechnungen. Das geschieht nur lesend: Speichern, Hochladen, Testen und der Coach sind gesperrt, und die Datenbank lehnt jedes Schreiben ab. Nicht gezeigt werden die persönlichen Einstellungen eines Admins auf der Seite «Konto» (Passwort, zweiter Faktor) und die Coach-Gespräche der Admins. Voraussetzung ist ein Betreiberkonto mit zweitem Faktor. Die Ansicht endet nach 60 Minuten ohne Aktivität, spätestens nach 12 Stunden, mit dem Ablauf oder dem Widerruf der Freigabe, wenn die Schule gesperrt wird oder wenn sich die Person im Betrieb abmeldet. Jede aufgerufene Seite und jeder Download steht ohne Inhalte (Zeitpunkt, Name der Person im Betrieb, Art der Daten) im Protokoll, das die Admins auf der Seite «Support-Zugriff» sehen und das nur zusammen mit der Schule gelöscht wird (AVV, Ziffer 4.4). Jede neue Freigabe geht per E-Mail an alle bestätigten Admins. Zugang zu Server und Datenbank haben nur die Personen, die die Plattform betreiben; sie sind zur Verschwiegenheit verpflichtet (AVV, Ziffer 5).
7. **E-Mail:** Mails an die Admins (Anmeldung, Rechnungen, Hinweise) versendet Infomaniak in der Schweiz.
8. **Backups:** Datenbank und Dateien werden vor der Übertragung verschlüsselt und bei Exoscale (Akenes SA) im Rechenzentrum Zürich gesichert, höchstens 30 Tage. Den Schlüssel hat nur die Anbieterin.

9. **Passwortprüfung:** Wählt ein Admin ein Passwort, prüft die Anwendung es beim Dienst «Pwned Passwords» von Have I Been Pwned gegen bekannte geleakte Passwörter. Übermittelt werden nur die ersten 5 Zeichen eines Hashwerts des Passworts, weder das Passwort noch die E-Mail-Adresse. Der Dienst steht nicht in der Schweiz; die Anfrage enthält keine Personendaten.

5. Orte und Empfänger

Unterauftragsbearbeiter

Hosting von Anwendung und Datenbank

Unternehmen: Infomaniak Network SA, Genf

Standort: Schweiz

Daten: Alle Daten der Schule

Sprachmodell (Inferenz)

Unternehmen: Infomaniak Network SA, Genf

Standort: Schweiz

Daten: Unterlagen, Fragen und Antworten

E-Mail-Versand

Unternehmen: Infomaniak Network SA, Genf

Standort: Schweiz

Daten: E-Mail-Adressen der Admins, Systemnachrichten

Backups

Unternehmen: Akenes SA (Exoscale), Lausanne

Standort: Schweiz

Daten: Alle Daten der Schule, nur verschlüsselt

Stand: 7. November 2026

Infomaniak Network SA ist ein Schweizer Unternehmen in Schweizer Eigentum und untersteht nicht dem US CLOUD Act. Die Backups liegen bei Akenes SA (Marke Exoscale), Lausanne, einem Unternehmen der österreichischen A1-Gruppe, im Rechenzentrum Zürich; Exoscale erhält sie nur verschlüsselt und ohne Schlüssel. Neue oder geänderte Unterauftragsbearbeiter kündigt die Anbieterin mindestens 30 Tage im Voraus per E-Mail an; die Schule kann widersprechen (AVV, Ziffer 8). Die Daten werden nicht zum Training von KI-Modellen verwendet (AVV, Ziffer 4.2).

Empfänger ausserhalb des Auftrags, ohne Personendaten der Lernenden:

- Have I Been Pwned, für die Passwortprüfung (Abschnitt 4, Punkt 9).
- Die Server hinter den Adressen, die die Schule für ihre Dokumente angibt (Abschnitt 4, Punkt 5).
- Der Programmcode liegt bei GitHub; dorthin gelangen keine Daten der Schulen. Neue Versionen stösst GitHub Actions über einen Schlüssel an, der auf dem Server nur das Skript für die Aktualisierung starten darf, ohne Zugriff auf Daten.

6. Cloud-spezifische Risikobereiche nach privatim

Vertragsgestaltung

Regelung im AVV: Verantwortung und Verfügungsmacht bei der Schule (Ziffer 2), Zweckbindung (Ziffer 4), Schweizer Recht und Gerichtsstand in der Schweiz (Ziffer 16); vereinbarte kantonale Vertragsbedingungen gehen vor (Ziffer 15.2)

Umsetzung: Der AVV ist öffentlich und im Konto abrufbar; die Zustimmung wird mit Version und Datum festgehalten. Kantonale Vertragsbedingungen prüfen wir gerne.

Orte der Bearbeitung und ausländische Behördenzugriffe

Regelung im AVV: Speicherung und Bearbeitung nur in der Schweiz, auch im Sprachmodell und in Backups; kein Zugriff aus dem Ausland, auch nicht zur Wartung (Ziffer 6); Herausgabe an Behörden nur nach Schweizer Recht, mit Information der Schule (Ziffer 12)

Umsetzung: Alle Unterauftragsbearbeiter in der Schweiz, kein CLOUD Act; neue Versionen stösst GitHub Actions an, ohne Zugriff auf Daten (Abschnitt 5)

Vertraulichkeit, Verschlüsselung und Schlüssel

Regelung im AVV: Verschwiegenheit, Amtsgeheimnis sinngemäss (Ziffer 5); Massnahmen nach Anhang B

Umsetzung: TLS für alle Verbindungen; Backups vor der Übertragung verschlüsselt; die Schlüssel verwaltet die Anbieterin. Während der Bearbeitung, etwa im Sprachmodell, liegen die Daten unverschlüsselt im Arbeitsspeicher. Der Bot ist nicht für Daten unter einem Amts- oder Berufsgeheimnis vorgesehen.

Daten über die Nutzenden (Rand- und Protokolldaten)

Regelung im AVV: Anhang A und Anhang B (Datensparsamkeit)

Umsetzung: Keine IP-Adressen, keine Fingerprints, keine Analyse- oder Werbedienste; technische Protokolle ohne Gesprächsinhalte; die Kennung der Konversation wie in Abschnitt 3

Unterauftragsverhältnisse

Regelung im AVV: Liste in Anhang C, Ankündigung 30 Tage im Voraus, Widerspruch und Kündigung (Ziffer 8)

Umsetzung: Liste öffentlich mit Datum der letzten Änderung

Meldepflichten

Regelung im AVV: Verletzungen der Datensicherheit spätestens innert 48 Stunden (Ziffer 10); Änderungen bei Unterauftragsbearbeitern (Ziffer 8.2)

Umsetzung: Dokumentierter Ablauf für Sicherheitsvorfälle (Anhang B)

Kontrollrecht

Regelung im AVV: Kontrolle durch die Schule, beauftragte Prüfstellen und Aufsichtsbehörden, insbesondere Datenschutzbeauftragte und Finanzkontrolle (Ziffer 11)

Umsetzung: Auskünfte und Unterlagen über datenschutz@byod-bot.ch

Informationssicherheit

Regelung im AVV: Ziffer 7 und Anhang B

Umsetzung: Abschnitt 7 dieses Blatts

Pflichten bei Vertragsauflösung

Regelung im AVV: Export während 30 Tagen, danach Löschung; Backups spätestens innert 30 Tagen überschrieben; Bestätigung auf Verlangen (Ziffer 13)

Umsetzung: Die Unterlagen sind Dokumente der Schule und bleiben bei ihr.

7. Risiken und Massnahmen

Die Risiken folgen den Beispielen kantonaler Vorlagen für die Datenschutz-Folgenabschätzung, ergänzt um die Risiken eines Sprachmodells.

Falsche Auskünfte des Bots

Massnahmen: Der Bot ist angewiesen, nur aus den Unterlagen der Schule zu antworten, und zeigt die Quellen, aus denen er zitiert. Findet er keine Antwort, sagt er das und verweist an den Support der Schule, wenn sie einen hinterlegt hat. Prüfungen in der Anwendung halten Antworten zurück, die Anweisungen des Bots wiedergeben oder nicht lesbar sind. Die Schule testet den Bot vor der Veröffentlichung mit eigenen Testfragen. Über einzelne Lernende führt die Plattform keine Daten, die falsch sein könnten.

Manipulation des Bots durch Eingaben oder Dokumente

Massnahmen: Anweisungen in Fragen oder hochgeladenen Dokumenten übersteuern die Vorgaben des Bots nicht. Das wird vor jeder Änderung an diesen Vorgaben und vor jedem Wechsel des Sprachmodells mit Angriffsfällen gegen das echte Sprachmodell geprüft.

Intransparente Bearbeitung

Massnahmen: Der Chat weist auf die Speicherung hin und verlinkt die Datenschutzerklärung der Schule mit ihrer Frist. Dieses Blatt, der AVV und die Liste der Unterauftragsbearbeiter sind öffentlich.

Übermässige Erhebung

Massnahmen: Keine Anmeldung der Lernenden; keine Antworttexte, kein Verlauf, keine IP-Adressen, keine Uhrzeit; E-Mail-Adressen, Telefon- und AHV-Nummern werden vor dem Speichern unkenntlich gemacht.

Verwendung für andere Zwecke

Massnahmen: Bearbeitung nur für die vereinbarten Leistungen, keine eigenen Zwecke der Anbieterin, kein Training von KI-Modellen (AVV, Ziffer 4).

Verknüpfung von Daten oder Profilbildung

Massnahmen: Keine Kennung über eine Konversation hinaus, höchstens 2 Stunden; die Fragen werden nie mit dieser Kennung gespeichert.

Übermässig lange Aufbewahrung

Massnahmen: Frist der Schule von 7 bis 365 Tagen, stündlicher Löschlauf, eine kürzere Frist wirkt sofort; Coach-Gespräche 30 Tage; Backups höchstens 30 Tage. Nach einer Wiederherstellung wendet der Betrieb die Liste der Löschungen erneut an, damit Gelöschtes nicht zurückkehrt.

Unerlaubte Bekanntgabe

Massnahmen: Keine Weitergabe ausser an die Unterauftragsbearbeiter; Herausgabe an Behörden nur nach Schweizer Recht und mit Information der Schule (AVV, Ziffer 12).

Einsicht durch Unbefugte

Massnahmen: Die Daten jeder Schule sind in der Datenbank getrennt (Row-Level Security), abgesichert durch automatisierte Tests für jede Abfrage. Anmeldung mit Prüfung gegen geleakte Passwörter und Begrenzung der Anmeldeversuche; eine Sitzung endet nach 60 Minuten ohne Aktivität und spätestens nach 12 Stunden. Zweiter Faktor für die Betreiber Pflicht, für die Admins der Schule wählbar. Handlungen der Betreiber werden protokolliert. Einblick in den Admin-Bereich einer Schule hat der Support nur mit deren befristeter, jederzeit widerrufbarer Freigabe, nur lesend und mit einem Protokoll, das die Schule sieht (Punkt 6 in Abschnitt 4).

Missbrauch und Überlastung des Bots

Massnahmen: Begrenzung der Fragen pro Konversation und Zeitraum, eine Rechenaufgabe im Browser beim Start einer Konversation, ein Kontingent pro Schule.

Verlust von Daten

Massnahmen: Die Datenbank wird fortlaufend gesichert (Wiederherstellung auf einen Zeitpunkt, höchstens rund 5 Minuten Verlust), die Dateien alle 15 Minuten, alles zusätzlich jede Nacht; die Wiederherstellung wird regelmässig geübt.

Doppelte Datenhaltung

Massnahmen: Ein Export als CSV liegt danach in der Verantwortung der Schule. Die Kopie einer Frage im Coach wird spätestens mit der Frage gelöscht.

8. Besondere Risikofaktoren

Die Faktoren folgen dem Merkblatt zur Datenschutz-Folgenabschätzung der Datenschutzbeauftragten des Kantons Zürich.

Automatisierte Einzelentscheidungen

Sachverhalt: Keine. Der Bot beantwortet Fragen zum BYOD-Konzept und entscheidet nichts über Lernende.

Systematische Überwachung

Sachverhalt: Keine. Keine Anmeldung, keine Wiedererkennung über eine Konversation hinaus.

Besonders schützenswerte Personendaten

Sachverhalt: Nicht vorgesehen. Lernende können sie trotz Hinweis in eine Frage schreiben; die Frist der Schule begrenzt, wie lange sie bleiben.

Bearbeitung in grossem Umfang

Sachverhalt: Hängt von der Zahl der Lernenden ab. Gespeichert werden pro Frage nur die Angaben aus Abschnitt 3, ohne Bezug zu einer Person.

Zusammenführen von Daten aus verschiedenen Prozessen

Sachverhalt: Keines. Die Plattform bezieht keine Daten aus anderen Systemen der Schule.

Einsatz neuer Technologien

Sachverhalt: Ja. Die Antworten erzeugt ein Sprachmodell (KI); Massnahmen in Abschnitt 7.

Zusammenarbeit mehrerer Stellen

Sachverhalt: Keine. Auf die Daten greifen die Admins der Schule zu und, nur mit deren befristeter Freigabe und nur lesend, der Support der Plattform (Abschnitt 4, Punkt 6).

Scoring oder Profiling

Sachverhalt: Keines.

Online-Zugriffe oder Abrufverfahren für andere Stellen

Sachverhalt: Keine.

Ob eine Vorabkontrolle nötig ist, entscheidet die Schule, im Zweifel zusammen mit ihrer kantonalen Datenschutzstelle.

9. Rechte der betroffenen Personen

Anfragen von Lernenden oder Admins richten sich an die Schule als Verantwortliche; die Anbieterin unterstützt sie dabei (AVV, Ziffer 9). Weil Fragen ohne Anmeldung und ohne Kennung gespeichert werden, lässt sich eine Frage in der Regel keiner Person zuordnen. Die Schule kann die Frist für gespeicherte Fragen jederzeit verkürzen.

10. Kontakt und Grundlagen

Fragen Ihrer Datenschutzstelle: datenschutz@byod-bot.ch

Unterlagen: Auftragsbearbeitungsvertrag, Unterauftragsbearbeiter, Datenschutzerklärung

Auftragsbearbeitungsvertrag: https://byod-bot.ch/avv

Unterauftragsbearbeiter: https://byod-bot.ch/unterauftragsbearbeiter

Datenschutzerklärung: https://byod-bot.ch/datenschutzerklaerung

Grundlagen: privatim, Merkblatt «Cloud-spezifische Risiken und Massnahmen» (Version 3.01, 3. Februar 2022); Datenschutzbeauftragte des Kantons Zürich, Merkblatt «Datenschutz-Folgenabschätzung DSFA» (Version 2.1, Oktober 2025)