



Cette traduction est fournie à titre indicatif. Seule la version allemande fait foi. [Voir la version allemande](#)

La protection des données pour les écoles en une page

Offre scolaire secureIT · pour les délégués à la protection des données et les organismes gestionnaires · version du 03.10.2026 (version 1.0)

1. Qui est responsable ?

L'école est responsable du traitement au sens du RGPD pour les données de ses élèves et de ses enseignants. Elle décide si des cours sont utilisés et lesquels. **secureIT UG (haftungsbeschränkt)** (Patrick Ihle, Breisgau) exploite la plateforme et traite les données exclusivement pour le compte de l'école (art. 28 du RGPD). L'accord de sous-traitance (DPA) est conclu lors de l'enregistrement du compte de l'école et est disponible en PDF pour être archivé.

2. Quelles données sont enregistrées sur les élèves ?

Le moins possible. Il n'y a **ni compte élève, ni application, ni inscription par e-mail**.

- **Pour participer en classe** : le prénom (librement choisi, un surnom convient aussi) et un cookie de reconnaissance sur son propre appareil. Rien de plus. Les réponses aux questions de quiz, aux nuages de mots et aux jeux sont attribuées à la classe, ne sont pas notées et ne sont pas transmises à l'enseignant comme résultat individuel.
- **Entraînement au phishing uniquement dans le cours « Autodéfense numérique » et uniquement avec accord** : à la fin de ce cours (de la 8e à la 10e année), les élèves peuvent, avec l'accord de leurs parents (modèle dans la lettre aux parents), participer au scénario de test de phishing de secureIT : trois tentatives de fraude simulées par e-mail, réalisées de manière professionnelle, qui montrent si une tentative de fraude mise en scène est reconnue. Une adresse e-mail est enregistrée à cet effet ; elle n'est visible que dans le Cockpit de l'enseignant, jamais dans la vue du cours de la classe. Le certificat atteste la participation réussie à cet entraînement et n'est délivré qu'en cas de participation. Sans participation : participation en classe oui, données aucune, certificat aucun.
- **Lors du test de phishing** : seul est enregistré le fait qu'un e-mail a été distribué, ouvert, cliqué ou signalé. **Les mots de passe saisis ne sont jamais enregistrés**, seulement le fait que quelque chose a été saisi. Seule la personne concernée voit le résultat ; l'enseignant ne reçoit aucune liste de qui a cliqué.
- **Suppression** : les données des certificats sont supprimées automatiquement après 60 jours. L'école supprime elle-même à tout moment les données de cours et de test dans le Cockpit, ou sur simple demande auprès de moi, sans formulaire et sans délai.

3. Quelles données sont enregistrées sur les enseignants ?

- **Cockpit de l'école** : nom et adresse e-mail professionnelle de la direction de l'établissement et des enseignants inscrits, mot de passe uniquement sous forme de hachage, date et heure de la dernière connexion. Chaque enseignant ne voit que ses propres cours.
- **Formation pour l'équipe enseignante (facultative)** : nom, adresse e-mail professionnelle, achèvement du cours avec date, événements de la simulation comme ci-dessus. La direction de l'établissement voit la participation et l'achèvement du cours (pour l'attestation de formation), jamais le comportement de clic des personnes individuelles. Le conseil du personnel (Personalrat, instance représentative du personnel) doit être associé avant le lancement ; un modèle d'accord de service (Dienstvereinbarung) est disponible.

4. Où se trouvent les données ?

Sur des serveurs d'IONOS SE en Allemagne (centre de données certifié ISO 27001). Toutes les connexions sont chiffrées en TLS. Il n'y a **aucune transmission à des tiers**, aucune publicité, aucun traçage, aucun script ni police externe provenant de serveurs tiers. Les jeux pédagogiques fonctionnent eux aussi entièrement depuis la plateforme. Les statistiques de consultation internes sont sans cookies et sans données personnelles.





5. Base juridique

Pour l'école : accomplissement de la mission d'éducation et d'enseignement (art. 6, par. 1, point e) du RGPD en liaison avec la loi scolaire du Bade-Wurtemberg (Schulgesetz Baden-Württemberg)). Pour l'indication volontaire d'une adresse e-mail par les élèves : consentement (art. 6, par. 1, point a) du RGPD) ; pour les mineurs, il est recommandé d'informer les parents, la lettre aux parents prévue à cet effet est disponible. Pour les enseignants : relation de service (§ 15 LDSG BW, loi du Bade-Wurtemberg sur la protection des données) et, le cas échéant, l'accord de service conclu avec le conseil du personnel.

6. Coûts et intérêts

Pour les écoles, tout est gratuit : cours, Cockpit, jeux, certificats, formation pour l'équipe enseignante. Il n'y a ni licence, ni durée d'engagement, ni publicité en classe, ni intention de vente à l'égard des élèves, des parents ou des enseignants. L'offre est financée par les entreprises clientes de secureIT.

7. Interlocuteur

Patrick Ihle, secureIT UG (haftungsbeschränkt), info@secureit-online.de, +49 157 58278025. Je réponds directement aux questions du délégué à la protection des données (DPO) ou de l'organisme gestionnaire de l'école (Schulträger), en règle générale le jour même.

8. Documents à archiver

- Accord de sous-traitance (art. 28 du RGPD) : <https://secureit.icu/fr/auftragsverarbeitung.pdf>
- Modèle d'accord de service avec le conseil du personnel : <https://secureit.icu/fr/schulen/muster-dienstvereinbarung.pdf>
- Fiche d'information pour l'équipe enseignante : <https://secureit.icu/fr/schulen/infoblatt-kollegium.pdf>
- Fiche d'information sur l'intervenant et secureIT : <https://secureit.icu/fr/schulen/infoblatt-secureit.pdf>
- Lettre aux parents (modèle) : <https://secureit.icu/fr/schulen/elternbrief.pdf>
- Politique de confidentialité générale : <https://secureit.icu/fr/datenschutz>

Éditeur : secureIT UG (haftungsbeschränkt), Patrick Ihle. Cette fiche décrit le traitement effectif sur la plateforme secureit.icu et est mise à jour en cas de modification ; seule la version en vigueur sur secureit.icu/schulen/datenschutz fait foi.