

Lignes directrices pour la protection des données dans l'ECAP

Sommaire

Introduction.....	1
Mesures générales.....	1
Sauvegarde, traitement et utilisation des données	2
Types de données.....	2
Types d'accès et rôles des employés.....	3
Divulgarion des données aux personnes tierces	4
Données simples sur les personnes	4
Données personnelles particulières.....	4
Données sans caractère personnel	5
Résumé des procédures opérationnelles	6

Introduction

Les présentes lignes directrices définissent les orientations générales pour le stockage, la gestion et l'archivage des données au sein d'ECAP. Elles tiennent compte de toutes les dispositions légales en vigueur¹ et doivent être appliquées dans les centres régionaux conformément aux réglementations des autorités compétentes, qui doivent être considérées comme un complément et une extension du présent document.

Les éventuelles adaptations régionales doivent être justifiées et garantir la même sécurité des données.

Les lignes directrices visent à atteindre les objectifs suivants :

- Assurer la protection des données personnelles "sensibles" contre les attaques et les abus internes et externes
- Assurer une gestion et une mise en œuvre efficace des cours
- Prendre en compte les besoins et les intérêts des participants
- Tenir compte des besoins des mandants et/ou des organismes de financement (par exemple, rapports, etc.)

Mesures générales

Ces mesures organisationnelles et techniques sont généralement appliquées à l'ECAP :

- Les employé(e)s ne sont pas autorisé(e)s à stocker des données personnelles sur des dispositifs qui n'appartiennent pas à ECAP

¹ Loi fédérale révisée sur la protection des données revLPD (valable dès le 1.09.2023), Ordonnance sur la protection des données OLPD (31.08.2022), éventuellement lois et ordonnances cantonales sur la protection des données, directives et ordonnances du SECO, du SEM et de la SEFRI.

- Tous les employés ont connaissance des présentes lignes directrices et de toute autre instruction relative à la protection des données émanant des mandants et s'engagent à les respecter
- Tous les serveurs de l'ECAP et de ses partenaires sont situés en Suisse
- Toutes les transactions sont protocolées
- L'accès aux données personnelles est personnalisé, différencié en fonction des rôles et protégé par des mots de passe
- Une évaluation des utilisateurs actifs et de leurs autorisations est disponible dans le système (audit des rôles)
- Les utilisateurs peuvent être obligés de réinitialiser leurs mots de passe
- Les mots de passe non sûrs ne sont pas autorisés par le système
- L'authentification à deux facteurs est disponible
- Les pages web mises en œuvre par ECAP comportent un avertissement avec un lien vers les politiques de protection des données et l'utilisation de cookies.

Sauvegarde, traitement et utilisation des données

Les données stockées et conservées par ECAP sont utilisées exclusivement pour l'organisation et la gestion de ses activités, sous réserve des obligations imposées par les mandants. Les données ne peuvent être collectées à l'insu des personnes concernées et ne peuvent être utilisées à d'autres fins. Tous les employé(e)s s'engagent à n'utiliser les données auxquelles ils ont accès que pour l'exercice de leurs fonctions.

La collection et le stockage des données sont basés sur trois principes :²

- Les personnes autorisées n'ont accès qu'aux données personnelles dont elles ont besoin pour exercer leurs fonctions (contrôle d'accès).
- Seules les personnes autorisées ont accès aux locaux et installations où sont traitées les données à caractère personnel (contrôle d'accès).
- Les personnes non autorisées n'ont pas accès aux données, aux systèmes de traitement ou aux moyens de transmission des données (contrôle des utilisateurs).

La non-observation de ces principes de base ou des instructions contenues dans le présent document sera considérée comme une faute, constituera un motif de résolution du rapport de travail conformément à l'article 12 de la CCT et, dans les cas les plus graves, peut conduire à la présentation d'une plainte auprès des autorités pénales.

Types de données

On distingue les types de données suivants :

Données du cours

- Dates de début et de fin
- Listes de présence
- Journaux de cours
- Projet, avis, groupe cible, objectifs, contenu, etc.

² Art. 3.1 LPD

Données personnelles
- Données administratives relatives aux cours : réservations et assignations des enseignants, calendriers des cours et salaires - Données personnelles relatives au salaire et à l'assurance
Données des participants
- Données administratives relatives aux cours : données personnelles, inscriptions, etc. - Données personnelles liées au cours : CV, résultats d'examens, notes, certificats, etc.
Coordonnées de contact
Données personnelles des personnes de contact et des mandants
Comptabilité
- Comptabilité financière - Comptabilité du personnel - Débiteurs et créditeurs
Correspondance
- Courriels entrants et sortants - Correspondance entrants et sortants
Documents de travail sans référence à la personne
- Concept du cours - Programmes de cours - Modules - Etc.

Types d'accès et rôles des employés

Il existe différents types d'accès aux données en fonction de sept catégories différentes d'employé(e)s :

1. DN – Direction nationale
2. DC – Directeur/Directrice du centre
3. RS – Responsable de secteur
4. S – Personnel de secrétariat
5. E – Enseignant.e.s
6. Adm. - Administration
7. IT-Support

Catégorie	Tâches
DN	- Approuve les lignes directrices et surveille leur mise en œuvre - Détermine la personne responsable de la protection des données - Attribue et gère les droits d'accès aux bases de données Tocco et Abacus - Décide en cas de doute
DC	- Ils sont chargés d'assurer les conditions organisationnelles, logistiques et infrastructurelles nécessaires à l'application des lignes directrices dans leur domaine de compétence - Ils contrôlent l'application des lignes directrices par leurs collaborateurs et collaboratrices

	• Ils assignent des tâches aux techniciens de support informatique • Ils signalent les problèmes et les difficultés • Ils rendent compte à la DN
RS, S et E	• Ils appliquent les lignes directrices dans leur domaine de compétence • Ils signalent les problèmes et les difficultés • Ils rendent compte aux DC
Adm.	• Appliquent les lignes directrices dans leur domaine de compétence
IT-Support	• Il est chargé de fournir l'infrastructure informatique nécessaire, y compris la plateforme ECAP et les licences • Prépare les logins d'accès, les profils et les espaces de travail collectifs et individuels en accord avec les DC et assure la confidentialité des informations • Contrôle l'application des lignes directrices et informe le DC et la ND en cas d'irrégularité • Aide les collaborateurs et les collaboratrices à résoudre les problèmes • Assure la suppression des données à la fin de la période d'archivage établie • Rend compte à la DN
Responsable de la protection des données	• Contrôle l'application des présentes lignes directrices et des directives du mandant • Est le point de contact pour toute personne souhaitant obtenir des informations sur les données stockées et leur utilisation.

Divulgaration des données aux personnes tierces

Données simples sur les personnes

En principe, les données ne sont collectées qu'aux fins de ses propres activités et ne sont pas divulguées à des tiers.

Les données simples sur les personnes (informations administratives et relatives aux cours) peuvent être divulguées aux institutions ou aux organismes mandataires dans les cas suivants :

- Si une disposition légale ou contractuelle s'applique
- Si cela est nécessaire pour remplir une obligation légale ou contractuelle.
Dans ce cas, les personnes concernées doivent être informées en temps utile qu'une communication de données est possible ou envisagée.
- Cela est explicitement convenu à l'avance avec les personnes concernées et les données sont rendues anonymes.

Données personnelles particulières

Les données personnelles particulières sont divulguées aux autorités uniquement si elles sont demandées par écrit et

- si une loi l'exige expressément
- si cela n'est pas explicitement exclu dans le mandat spécifique ou le contrat de prestation
- si cela est absolument nécessaire à l'accomplissement d'une tâche clairement définie par la loi

- dans des cas particuliers, la personne concernée a expressément donné son consentement ou, si elle n'est pas en mesure de le faire, il est considéré qu'il est dans son intérêt de divulguer ses données et son consentement est présumé de bonne foi.

La liste de contrôle du délégué à la protection des données du canton de Bâle-Ville³ est l'outil utilisé pour décider si et dans quels cas des données à caractère personnel doivent ou peuvent être transférées. En cas de doute, la direction décide.

Données sans caractère personnel

En principe, seules des informations statistiques sur les activités de l'ECAP et des données techniques sur les rapports financiers sont divulguées. Les informations ou la documentation soumises à des droits d'auteur et/ou qui ont été collectées et sauvegardées dans le cadre du travail à l'ECAP ou en son nom ne peuvent être transmises à des tiers sans le consentement de la direction. Les informations qui nuisent directement ou indirectement à l'ECAP ne peuvent être divulguées à des tiers.

³ Voir <https://www.dsb.bs.ch/handreichungen/checkliste-bekanntgabe.html>

Résumé des procédures opérationnelles

Description	Support et lieu de stockage des données	Durée du sauvegarde ⁴	Qui a accès	Protection des données
1. Données du cours				
1.1 Listes de présence	1.1.1 Les listes de présence sont généralement compilées électroniquement et les informations restent enregistrées dans la base de données tocco	Illimitée	➤ DN, Adm: illimité ➤ S, RS, DC: filtre sur ses propres cours ➤ E: uniquement pour leurs cours actuels	Accès individuel protégé par mot de passe avec différents rôles
	1.1.2 Les documents imprimés sont archivés dans les centres régionaux. Après 10 ans, ils doivent être transférés à l'archive ECAP	Illimitée	➤ S, RS, DC: illimité ➤ E: uniquement pour leurs cours actuels	Salles ou casiers fermés dont l'accès est réservé aux personnes autorisées
1.2 Journal des cours ⁵	1.2.1 Il est sauvegardé en format électronique sur les serveurs de l'ECAP ⁶	10 ans	➤ S, RS, DC: limité à son centre régional	Accès individuel protégé par mot de passe
	1.2.2 Les éventuels documents imprimés sont conservés dans les archives des centres régionaux. Après 10 ans, ils doivent être transférés à l'archive ECAP	Illimitée	➤ S, RS, DC: illimité ➤ E: uniquement pour leurs cours actuels	Salles ou casiers fermés dont l'accès est réservé aux personnes autorisées
1.3 Projets	1.3.1 Ils sont sauvegardés sur les serveurs ECAP	Illimitée	➤ RS, DC, DN: illimité	Accès individuel protégé par mot de passe

⁴ Les informations sur la période de stockage des données sont des indications générales valables en absence d'instructions spécifiques de la part des commanditaires ou des autorités de subvention.

⁵ Les journaux de cours ne contiennent pas de données à caractère personnel.

⁶ Tous les serveurs de l'ECAP et de ses partenaires sont situés en Suisse.

2. Données personnelles				
2.1 Données administratives sur les cours ➤ Données personnelles ➤ Pourcentage d'emploi ➤ Durée du contrat ➤ Horaire de travail ➤ Qualifications	2.1.1 Les informations sont enregistrées exclusivement dans les bases de données Tocco et Abacus	Illimitée	➤ DN, Amm: illimité ➤ S, RS, DC: limité à son centre régional et à ses domaines de compétence	Accès individuel protégé par mot de passe avec différents rôles
	2.1.2 Les documents imprimés sont stockés dans les archives des centres régionaux. Après 10 ans, toutes les informations sont supprimées	10 ans	➤ S, RS, DC: limité à son centre régional et à ses domaines de compétence	Salles ou casiers fermés dont l'accès est réservé aux personnes autorisées
2.2 Données personnelles liées au salaire et à l'assurance ➤ Coordonnées bancaires ➤ Toutes les informations requises pour le paiement des salaires ➤ Toutes les informations requises pour les assurances sociales	2.2.1 Les informations sont stockées exclusivement dans la base de données Abacus et sur le serveur d'administration	Illimitée	➤ DN, Adm	Accès individuel protégé par mot de passe avec différents rôles
	2.2.2 Les documents imprimés sont stockés dans les archives de l'Adm.	10 ans après la fin des rapports de travail	➤ DN, Adm	Salles fermés dont l'accès est réservé aux personnes autorisées
2.3 Dossier personnel ➤ Documents de candidature ➤ Contrats de travail ➤ Entretiens avec les employés, avertissements, etc. ➤ Certificats ➤ Entretiens avec les employés	2.3.1 Les documents électroniques sont stockés dans le dossier de travail de la direction régionale et sur le serveur de l'administration	Fichier de travail de la DC : jusqu'à la fin du rapport de travail Serveur de l'administration : 10 ans après la fin des rapports de travail	➤ DC: limité à son centre régional ➤ DN, Adm: illimité	Accès individuel protégé par mot de passe
	2.3.2 Les documents imprimés sont stockés dans des armoires fermées dans le bureau de la direction régionale et dans les archives de l'administration	Bureau de la DC : jusqu'à la fin du rapport de travail Archives de l'administration : 10 ans après la fin des rapports de travail	➤ DC: limité à son centre régional ➤ DN, Adm: illimité	Salles ou casiers fermés dont l'accès est réservé aux personnes autorisées

3. Données des participants

3.1 Données administratives des cours: ➤ Données personnelles ➤ Adresse (correspondance et facture) ➤ Téléphone et e-mail ➤ Nationalité ➤ Langues ➤ Év. permis de séjour ➤ Test d'entrée, certificats d'apprentissage et de participation ➤ Personnes de contact ➤ Év. correspondance avec les organismes mandatés ➤ Év. informations commerciales ➤ Év. documentation pour la réduction des coûts ➤ etc. Sont sauvegardées uniquement les données nécessaires pour ➤ la réalisation et la gestion du cours ➤ la délivrance et la reproduction éventuelle de certificats et d'attestations de présence ➤ les rapports et les déclarations destinés aux commanditaires et/ou aux organismes de financement ➤ la facilitation d'autres inscriptions futures. Il est strictement interdit de collecter et de sauvegarder des informations sur l'orientation religieuse et/ou politique.	3.1.1 Les informations sont stockées électroniquement uniquement dans la base de données Tocco	Illimitée	➤ DN, Adm: illimité ➤ S, RS, DC: limité à son centre régional et à ses domaines de compétence	Accès individuel protégé par mot de passe avec différents rôles
	3.1.2 Les documents imprimés sont stockés dans les archives des centres régionaux. Après 10 ans, toutes les informations sont supprimées	10 ans	➤ S, RS, DC: limité à son centre régional et à ses domaines de compétence	Salles ou casiers fermés dont l'accès est réservé aux personnes autorisées
	3.1.3 Tous les autres documents nécessaires à la préparation des rapports ou à la comptabilité sont enregistrés sur les serveurs des centres régionaux jusqu'à la fin de la procédure comptable.	Jusqu'à la fin du rapport financier. À la fin du processus de reporting financier, les données sont archivées, sans accès, et conservées pendant 5 ans.	➤ S, RS, DC: pendant la phase de rapport et de décompte, limités à leur propre centre régional et à leurs domaines de compétence ➤ Après l'archivage, les données ne peuvent être rendues accessibles que par les informaticiens	Accès individuel protégé par mot de passe avec différents rôles

3.2 Données personnelles relatives au cours Curricula et toute autre information personnelle traitée pendant le cours (par exemple, cours de placement, etc.). Les données personnelles sont généralement enregistrées uniquement sous format électronique. Toute la documentation imprimée est remise directement aux participants ou détruite à la fin du cours. Pendant la formation, les documents imprimés sont conservés sous clé dans les cases des formateurs/trices.	3.2.1 Variante 1 → Sensibilité faible à moyenne des données et pas de travail intensif sur PC pour les participants Les données sont stockées dans l'espace de travail du cours sur le cloud ECAP et/ou la plateforme ECAP	Jusqu'à la fin du cours. À la fin des cours, les données sont supprimées ou archivées sans possibilité d'accès ⁷	➤ E: pendant la durée du cours ➤ RS: pendant la phase de rapport et de décompte ➤ Après l'archivage, les données ne peuvent être rendues accessibles que par les informaticiens	Accès individuel protégé par mot de passe
	3.2.2 Variante 2 → Sensibilité moyenne ou élevée des données et travail intensif des participants au PC. Les données sont stockées dans l'espace de travail individuel réservé aux participants sur le cloud ECAP et/ou la plateforme ECAP	Jusqu'à la fin du cours. À la fin des cours, les données sont supprimées ou archivées sans possibilité d'accès	➤ E: pendant la durée du cours ➤ Après l'archivage, les données ne peuvent être rendues accessibles que par les informaticiens	Accès individuel protégé par mot de passe et profil individuel
	3.2.3 Variante 3 → Il n'y a pas de serveur. Les participants travaillent avec une clé USB personnelle	Jusqu'à la fin du cours	➤ E	Toutes les informations enregistrées sur un PC dans les classes ECAP sont automatiquement supprimées lorsque le dispositif est arrêté. À la fin de chaque journée de cours, l'enseignant.e doit s'assurer que les participants sauvegardent leurs fichiers sur leur clé USB.

⁷ Selon les instructions du commanditaire.

4. Coordonnées de contact

4.1 Informations de contact non sensibles , c'est-à-dire sur les personnes et institutions externes avec lesquelles nous coopérons : ➤ Données personnelles ➤ Informations sur la communication ➤ Facturation ➤ etc.	4.1.1 L'information reste sauvegardée dans la base de données Tocco	Illimitée	➤ DN, Adm: illimité ➤ S, RS, RL: limité à son centre régional et à ses domaines de compétence	Accès individuel protégé par mot de passe avec différents rôles
--	---	-----------	--	---

5. Comptabilité

5.1 Comptabilité financière et salariale	5.1.1 Les informations sont enregistrées exclusivement dans la base de données Abacus sur le serveur de l'administration centrale	Illimitée	➤ DN, Adm	Accès individuel protégé par mot de passe
5.2 Comptes débiteurs	5.2.1 Les informations sont enregistrées exclusivement dans la base de données Abacus sur le serveur de l'administration centrale	Illimitée	➤ DN, Adm: illimité ➤ Responsable de visum : limité à son centre régional	Accès individuel protégé par mot de passe

6. Correspondance

6.1 Courriel	6.1.1 Les courriels contenant les données personnelles des participants ne peuvent être envoyés, reçus et stockés qu'avec les adresses électroniques ECAP des employés sur les serveurs Microsoft Exchange. Les courriels contenant des données personnelles et sensibles sont traités conformément	Illimitée. Les courriels privés doivent être supprimés à la fin de la relation de travail. Les courriels professionnels sont archivés. Les courriels électroniques contenant des données personnelles et sensibles des participants (voir 3.2) sont archivés	➤ Chaque employé/e n'a accès qu'aux adresses électroniques qui lui ont été attribuées. ➤ Après l'archivage, les données ne peuvent être rendues accessibles que par les informaticiens	Accès individuel protégé par mot de passe
---------------------	--	--	---	---

	ment aux instructions de l'organisme mandant ou assignant ⁸	pendant la période convenue avec le commanditaire.		
6.2 Correspondance	6.2.1 La correspondance imprimée est sauvegardée dans des armoires fermées et dans les archives des centres régionaux	10 ans Après 10 ans, il est transféré aux archives ECAP	➤ DN, Adm: illimité ➤ S, RS, DC: limité à son centre régional	Salles ou casiers fermés
7. Documents à caractère non personnel				
7.1 Documents de travail courants ➤ Documents de travail internes ➤ Rapports ➤ Drafts ➤ Documents relatifs aux réunions ➤ Protocoles ➤ etc.	7.1.1 Les versions électroniques partagées des documents de travail courants sont stockées sur les serveurs ECAP (ou dans Microsoft Teams) avec la structure appropriée	Illimitée	➤ Tous les employé(e)s n'ont accès qu'à la documentation relative à leur fonction	Accès individuel protégé par mot de passe avec différents rôles
	7.1.2 Les versions imprimées des documents partagés sont stockées dans les archives des centres régionaux	10 ans Après dix ans, ils doivent être transférés aux archives de la Fondation	➤ DN, Adm: illimité ➤ S, RS, DC: limité à son centre régional	Salles ou casiers fermés dont l'accès est réservé aux personnes autorisées
	7.1.3 Les documents de travail personnels au format électronique sont enregistrés dans les profils individuels des employé(e)s sur le serveur du centre régional (ou dans Microsoft Teams)	Durée du rapport de travail À la fin de la relation de travail, les documents sont archivés	➤ Chaque employé/e n'a accès qu'à ses propres données	Accès individuel protégé par mot de passe

La Direction

Guglielmo Bozzolini, Giuliana Tedesco-Manca

Zurich, en juillet 2023

⁸ Par exemple avec IncaMail