Le grand filtre

Matrice de sécurité de l'IA en entreprise suisse : conformité LPD, secret d'affaires, souveraineté.

Le groupe de gauche évalue la conformité LPD. Le groupe de droite évalue la protection effective du secret d'affaires. Un outil peut satisfaire l'un sans l'autre. Les marqueurs (a), (b), (c) renvoient aux conditions de la page suivante.

Matrice des verdicts

OUTIL	RÉSIDENCE	DPA	NO-TRAIN	VERDICT LPD	CMK / CLÉS	CLOUD ACT	VERDICT SECRET
ChatGPT perso (Free / Plus)	US	Non	Non	Non conforme	Non	Élevé	Exposé
ChatGPT Team / Enterprise	US (UE option)	Oui	Oui	Conforme (a)	Non	Élevé	Risqué
API OpenAI (+ ZDR)	US	Oui	Oui	Conforme (a)	Non	Élevé	Risqué
Azure OpenAI (CH North)	CH	Oui	Oui	Conforme	Oui (+ HYOK)	Moyen	Bon (b)
AWS Bedrock (Zurich)	CH	Oui	Oui	Conforme	Oui (+ HYOK)	Moyen	Bon (b)
Infomaniak AI (API)	CH	Oui	Oui	Conforme	Chiffrement CH	Nul	Protégé
Self-host (Ollama / on-prem)	CH requis (c)	Sans objet	Oui	Conforme (c)	Total	Nul	Maximal (c)

conforme / risque faible sous conditions non / risque élevé

Réalité opérationnelle

OUTIL	POINT D'ATTENTION
ChatGPT perso	Cauchemar du Shadow IT. Aucun contrôle d'accès, aucune visibilité sur ce que les employés copient-collent.
ChatGPT Team / Enterprise	Faux sentiment de sécurité. Protège de l'entraînement, pas du Cloud Act. SSO strict requis.
API OpenAI (+ ZDR)	Nécessite un middleware pour filtrer ou pseudonymiser les requêtes avant le départ US.
Azure OpenAI (CH North)	Niveau "Bon" suppose HYOK + calcul confidentiel (TEE) + exemption de journalisation.

OUTIL	POINT D'ATTENTION
AWS Bedrock (Zurich)	Profil jumeau d'Azure. Souveraineté par empilement KMS externalisé + Nitro Enclaves.
Infomaniak AI (API)	Écart possible sur les raisonnements très complexes vs modèles frontière propriétaires.
Self-host (Ollama / on-prem)	Le risque se déplace vers la sécurité interne (accès, sauvegardes, durcissement). Coûts GPU souvent cachés.

Conditions

(a) Transfert vers les États-Unis. "Conforme" seulement si le mécanisme de transfert est en place : fournisseur certifié Swiss-US DPF (adéquation reconnue depuis septembre 2024, à vérifier sur la liste officielle *dataprivacyframework.gov/list*, certification annuelle) **ou** clauses contractuelles types + analyse d'impact (TIA). Le statut DPF d'OpenAI est ambigu selon les sources ; Microsoft est certifié.

(b) Niveau "Bon" Azure / Bedrock. Atteint uniquement en empilant : clé en HYOK (hors d'atteinte de l'hébergeur), calcul confidentiel (TEE) pour l'inférence, et exemption de journalisation. Sans ces couches, le verdict retombe à "Moyen".

(c) Self-host. Valable à deux conditions : serveur physiquement en Suisse (matériel propre ou hébergeur suisse type Infomaniak ; un VPS étranger ou un cloud américain fait retomber la résidence et peut réintroduire le Cloud Act par la couche infrastructure), **et** sécurité interne (accès, sauvegardes, durcissement) à la hauteur.

Avertissement

Aide à la décision, pas un avis juridique. La qualification précise des données et la conformité d'un déploiement donné doivent être validées par un conseil juridique spécialisé, en particulier sur le volet FINMA. Les caractéristiques des fournisseurs (résidence, options de chiffrement, statut DPF, conditions contractuelles) évoluent et doivent être vérifiées au moment de la contractualisation.

Mathieu, Survivant de l'IA · dernière révision 7 juin 2026 · version étendue + glossaire sur survivant-ia.ch/outils/le-grand-filtre