Ibexa Agentic Marketing Platform

Mesures techniques et organisationnelles de sécurité de l'information et de protection des données (MTO)

Version :	1.0
Date de la version :	07/10/2026
Propriétaire du document :	Maxime Auvy (Responsable Sécurité IT & GRC)
Niveau de confidentialité :	Restreint

Historique des modifications

Date	Version	Créé par	Description de la modification
7/10/2026	1.0	Maxime Auvy	Version initiale

Table des matières

Ibexa Agentic Marketing Platform 1
Introduction 7
Qu'est-ce que l'« Ibexa Agentic Marketing Platform » ? 7
Pourquoi ce document ? 7
À qui s'adresse ce document ? 7
Comment utiliser ce document ? 7
Système de management de la sécurité de l'information (SMSI) 8
Organisation de la sécurité de l'information 8
Politiques et procédures 8
Rôles et responsabilités 8
Gestion des risques 9
Méthodologie de gestion des risques 9
Sécurité des ressources humaines 10
Sélection et vérification des candidats 10
Processus d'intégration 10
Sensibilisation et formation continue à la sécurité 10
Processus de départ 11
Clause de confidentialité dans les contrats de travail 11
Gestion des actifs 12
Inventaire des actifs 12
Classification de l'information 12
Contrôle d'accès 12
Politique de contrôle d'accès d'Ibexa 12
Politique de mots de passe d'Ibexa 13
Politique de mots de passe d'Ibexa – utilisateurs 13
Authentification unique (SSO) 14
MFA (authentification multifacteur) 15
Création d'utilisateur 15
Expiration de session 15
Séparation des tâches 16
Principe du moindre privilège 16
Arrivées, départs, changements de poste et revues périodiques 16
Architecture multi-tenant et cloisonnement des données 16
1. Authentification et identification du tenant 16
2. Rattachement des données au tenant 17
3. Accès aux données cloisonné 17
4. Autorisations au sein d'une organisation 17
5. Traitements en arrière-plan 18

6. Stockage des fichiers 18
7. Accès des agents d'IA aux connaissances des clients 18
8. Intégrations entrantes (webhooks) 19
9. Vérification 19
Cryptographie 20
Chiffrement des données au repos 21
Chiffrement des données en transit 21
Sécurité physique et environnementale 21
Centres de traitement de données 22
Les bureaux d'Ibexa 22
Les ordinateurs portables d'Ibexa 22
Chiffrement du disque dur 23
Protection antimalware 23
Écran vide, verrouillage et appareils laissés sans surveillance 23
Périphériques de stockage USB 24
Sécurité des opérations 24
Politique de sauvegarde 24
Sauvegarde des bases de données 24
Sauvegarde des contenus fournis par les utilisateurs et hébergés par Ibexa 25
Documentation et fichiers internes 25
E-mails 25
Code applicatif 25
Protection contre les attaques DDoS et pare-feu 26
Journalisation et supervision 26
Contrôle des accès à distance, détection et prévention des intrusions 26
Sécurité des communications 27
HTTPS et SSL 27
Acquisition, développement et maintenance des systèmes d'information 27
Cycle de développement sécurisé (SDLC) 27
Fonctionnalités 28
Bugs 28
Projets clients 28
Équipes 28
Pratiques de développement 29
Séparation des environnements 29
Accès aux environnements 29
Architecture générale 30
Revue de code et tests 30
Revue de code par les pairs 31
Tests 31

Gestion des mises en production 31
Qu'est-ce que la gestion des mises en production ? 31
Objectifs 32
Politiques 32
Processus de mise en production 33
Retour d'expérience 33
Données de production 34
Gestion des incidents de sécurité de l'information 34
Procédure de gestion des incidents 34
Support client 34
Page de statut 34
Assistance en ligne 34
Gestion des vulnérabilités techniques et politique de correctifs 35
Application des correctifs de vulnérabilités techniques 35
Autres correctifs et mises à jour 36
Changements de version majeure 36
Politique d'utilisation raisonnable 36
Continuité d'activité et reprise après sinistre 37
Redondance 37
Continuité d'activité 37
RTO 37
RPO 37
Reprise après sinistre 38
Conformité 38
Audits et rapports de sécurité 38
Audits externes 38
Test d'intrusion 38
Audits à la demande des clients 39
Audits internes 39
Analyse de vulnérabilités 39
Analyse statique de code 40
Assurances 40
Ibexa est-elle certifiée ISO 27001 ou ISO 27701 ? 40
Protection des données et vie privée 41
Ibexa en tant que « sous-traitant » 41
Politique de conservation des données personnelles 41
Adresses IP 41
Restitution des données à la fin du contrat 42
Documentation d'Ibexa sur les mesures de protection au titre du RGPD 42

Mesures organisationnelles pour garantir la sécurité et la protection des données personnelles 42
Délégués à la protection des données 42
Mesures relatives aux ressources humaines 43
Clause de confidentialité dans les contrats de travail 43
Sensibilisation et formation continue du personnel à la sécurité 43
Procédures en cas de violation de données 43
Réception de l'incident 43
Évaluation de l'incident 44
Traitement de l'incident 44
Traitement du volet « sécurité » de l'incident 44
Traitement du volet « vie privée » de l'incident 44
Clôture de l'incident 45
Transfert de données personnelles au client 45
Transmission automatique de données personnelles au système d'information du client 45
Transfert manuel de données personnelles au client 46
Mesures techniques pour garantir la sécurité et la protection des données personnelles 46
Protection des données dès la conception et par défaut 46
Gestion des cookies 47
Suppression des données personnelles 47
Accès restreint aux données personnelles de production 47
Accès physique à nos bureaux 47
Ordinateurs 47
Mesures de sécurité IT 47
Engagements contractuels avec les clients 48
Accords de traitement des données (DPA) 48
Registre des activités de traitement 48
Sous-traitants ultérieurs d'Ibexa 50
Intelligence artificielle et conformité 51
Annexe 1 : Définitions 52

Introduction

Qu'est-ce que l'« Ibexa Agentic Marketing Platform » ?

L'Ibexa Agentic Marketing Platform (« IAMP » en abrégé) est une plateforme multi-tenant d'opérations d'IA qui aide les organisations à créer, exécuter et gouverner des agents d'IA. Elle relie des modèles de langage à des outils externes approuvés et aux connaissances de l'entreprise, afin que les équipes puissent automatiser leurs tâches récurrentes, accompagner leurs utilisateurs grâce à un assistant IA et piloter l'usage dans un environnement organisationnel sécurisé.

Pourquoi ce document ?

Ce document présente une vue d'ensemble du système de management de la sécurité de l'information (SMSI) mis en place chez Ibexa. Il aide les prospects, clients et fournisseurs à évaluer la maturité d'Ibexa en matière de sécurité de l'information.

À qui s'adresse ce document ?

Ce document s'adresse aux évaluateurs du risque tiers, aux équipes sécurité, aux auditeurs en sécurité de l'information, aux RSSI et aux directions informatiques de nos prospects, clients et fournisseurs.

Comment utiliser ce document ?

Le document est structuré selon les domaines du référentiel ISO 27701 et reprend des extraits de nos politiques internes, déclassifiés pour pouvoir être communiqués à un public extérieur à l'organisation.

Il doit être lu avec ses annexes, qui contiennent les définitions et les références.

Système de management de la sécurité de l'information (SMSI)

Le CIO et le DPO assurent respectivement la gestion de la sécurité de l'information et de la protection des données chez Ibexa, en exploitant un SMSI (système de management de la sécurité de l'information) et un PIMS (système de management des informations personnelles) conformes à l'état de l'art, selon la norme internationale ISO 27701.

La norme ISO 27701 sert de cadre de référence pour gérer, de manière systématique et exhaustive, la sécurité de l'information tout au long de son cycle de vie chez Ibexa.

Organisation de la sécurité de l'information

Politiques et procédures

Le SMSI et le PIMS reposent sur un ensemble de politiques, de procédures et de documents d'appui, élaborés, revus et approuvés par la Direction d'Ibexa.

Le SMSI et le PIMS sont communiqués à l'ensemble des collaborateurs d'Ibexa et font explicitement partie de leur engagement contractuel. Celui-ci renvoie également au processus disciplinaire applicable en cas de non-respect du SMSI et du PIMS.

Par ailleurs, le SMSI et le PIMS font partie du programme de sensibilisation dispensé à l'ensemble des collaborateurs d'Ibexa.

Rôles et responsabilités

La sécurité de l'information est pilotée chez Ibexa par le CIO (Chief Information Officer – directeur des systèmes d'information), qui rapporte directement au CEO (directeur général).

L'équipe Sécurité IT est composée de **deux rôles complémentaires** qui travaillent en étroite collaboration :

- un **Technical Security Lead (responsable sécurité technique) :** il pilote la mise en œuvre technique de la sécurité IT et produit, gère les outils de sécurité, l'analyse des risques, les programmes de sensibilisation et le suivi des indicateurs (KPI).
- un **GRC Lead (responsable gouvernance, risques et conformité) :** il est responsable de la gouvernance et de la conformité en matière de sécurité (y compris la feuille de route ISO 27001), tient à jour les politiques internes de sécurité IT et le registre des risques, et pilote les échanges avec les tiers, notamment les questionnaires de sécurité clients et la coordination avec les auditeurs externes.

Un DPO (délégué à la protection des données) a été nommé par Ibexa pour répondre aux questions relatives à la protection des données personnelles (PII – Personally Identifiable Information).

Ces responsabilités sont réparties entre plusieurs personnes afin d'assurer une séparation claire des tâches dans l'exploitation du SMSI et du PIMS.

Les politiques d'Ibexa sont approuvées par la Direction générale, qui s'assure de leur cohérence avec la stratégie de l'entreprise avant leur déploiement.

Gestion des risques

Méthodologie de gestion des risques

La méthodologie de gestion des risques appliquée par Ibexa évalue chaque risque selon son impact s'il se réalise et sa probabilité de survenance. L'impact comme la probabilité sont notés sur une échelle de 1 à 5. Le score final d'un risque est obtenu en multipliant son impact par sa probabilité.

Un appétit pour le risque est défini avec la Direction générale ; les risques qui dépassent ce seuil sont traités.

Les traitements possibles d'un risque sont :

- **Réduction** : sélection d'un ou plusieurs contrôles de sécurité issus de l'Annexe A de la norme ISO/IEC 27001 ou d'autres mesures de sécurité

- **Transfert** : transfert du risque à un tiers, par exemple en souscrivant une assurance ou en contractualisant avec des fournisseurs ou partenaires
- **Évitement** : suppression du risque en arrêtant l'activité qui en est à l'origine
- **Acceptation** : le risque est accepté ; cette option n'est permise que si les autres traitements coûteraient plus cher que l'impact potentiel du risque s'il se réalisait

Le registre des risques est placé sous la responsabilité du GRC Lead et revu chaque année. L'appétit pour le risque est abaissé à chaque nouvelle itération de l'évaluation des risques.

Sécurité des ressources humaines

Sélection et vérification des candidats

Les collaborateurs d'Ibexa sont recrutés à l'issue d'un processus de sélection qui évalue leurs compétences ainsi que leur adhésion à la culture de l'entreprise.

Processus d'intégration

Chaque nouveau collaborateur suit un parcours d'intégration comprenant une formation (jusqu'à 10 semaines) afin de s'assurer qu'il dispose des compétences nécessaires pour tenir son poste. La progression est évaluée chaque semaine avec son manager et un « Ibexa buddy » (mentor interne qui accompagne le nouvel arrivant dans sa montée en compétence), désigné dès l'embauche.

Une évaluation finale est réalisée à l'issue de l'intégration pour vérifier que la personne maîtrise le produit et les processus de l'entreprise.

Sensibilisation et formation continue à la sécurité

Ibexa a déployé un programme de formation et de sensibilisation à destination de ses collaborateurs.

Les sessions de formation et de sensibilisation sont organisées :

- En présentiel : lors de formations ponctuelles pour des publics restreints, ou lors de nos « réunions générales d'entreprise », organisées deux fois par an pour l'ensemble des équipes
- En ligne : via une plateforme d'e-learning permettant de déployer des campagnes de formation tout au long de l'année

Une attention particulière est portée à la protection des données et à la vie privée, grâce à :

- des sessions de formation récurrentes sur la sécurité et la vie privée, animées par l'équipe Sécurité IT, le DPO ou l'équipe juridique ;
- des ateliers spécifiques sur le RGPD et la sécurité pour les développeurs et les product managers ;

Processus de départ

Chaque collaborateur qui quitte l'entreprise suit un processus de départ rigoureux qui garantit, grâce aux inventaires des actifs et des accès utilisateurs, que tous les actifs sont restitués et tous les accès supprimés.

Clause de confidentialité dans les contrats de travail

Tous nos contrats de travail comportent une clause de confidentialité obligatoire, conformément au RGPD.

Gestion des actifs

Inventaire des actifs

Les actifs d'Ibexa, ainsi que ceux des tiers dont l'entreprise dépend, sont évalués une fois par an. Tous les actifs sont consignés dans un inventaire, avec l'attribution d'un propriétaire et une classification fondée sur leur criticité pour l'entreprise.

Le GRC Lead est responsable de l'inventaire des actifs et de sa revue annuelle.

Classification de l'information

Une politique formalise la classification de l'information : elle définit les niveaux de classification, le propriétaire de l'information, son traitement, les procédures de manipulation, ainsi que les modalités de mise au rebut et de destruction.

Les niveaux de classification actuellement utilisés par Ibexa sont :

- Public
- Usage professionnel uniquement (niveau par défaut)
- Confidentiel
- Restreint

Contrôle d'accès

Politique de contrôle d'accès d'Ibexa

Les administrateurs d'utilisateurs ont accès en temps réel à la liste de leurs utilisateurs et peuvent augmenter ou réduire leurs droits et accès. Le détail des droits des utilisateurs est présenté ci-dessous :

Rôle	Description
Propriétaire de	L'utilisateur qui est propriétaire de l'organisation. Il détient la plus

l'organisation (Organisation Owner)	haute autorité au sein de celle-ci, y compris pour les actions qui lui sont exclusivement réservées (par exemple certaines opérations de gestion au niveau de l'organisation), en plus de toutes les permissions de l'administrateur de l'organisation.
Administrateur de l'organisation (Organisation Admin)	Gère les utilisateurs, les paramètres, les intégrations (fournisseurs de LLM, serveurs MCP) et les ressources de sa propre organisation. Peut inviter et retirer des membres, attribuer des rôles et configurer les politiques au niveau de l'organisation.
Membre de l'organisation (Organisation Member)	Utilisateur final standard au sein d'une organisation. Peut utiliser les agents, les rapports, les conversations et les fonctionnalités de la base de connaissances selon les paramètres de l'organisation, mais ne peut pas gérer les utilisateurs, la facturation ni la configuration de l'organisation.

Les administrateurs conservent à tout moment la possibilité de désactiver des comptes.

Politique de mots de passe d'Ibexa

Politique de mots de passe d'Ibexa – utilisateurs

- Tous les mots de passe sont choisis par l'utilisateur, chiffrés en transit et stockés sous forme de hash au repos dans nos systèmes (voir Cryptographie).
- Complexité : le mot de passe doit répondre à toutes les exigences suivantes :
    - 12 caractères minimum
    - au moins 1 chiffre
    - au moins 1 majuscule
    - au moins 1 minuscule
    - au moins 1 caractère spécial
- Historique des mots de passe :
    - Les utilisateurs ne peuvent pas réutiliser leurs 100 derniers mots de passe (la version hachée de tous les mots de passe précédents est conservée en base de données)
- Expiration des mots de passe :
    - Le mot de passe expire au bout de 90 jours
- Protection contre la force brute :

    - Après 10 tentatives erronées, un délai d'une minute est imposé avant la tentative suivante
    - Chaque nouvelle tentative erronée allonge ce délai d'une minute
    - Le délai augmente jusqu'à un maximum de 15 minutes
    - Le compteur de tentatives erronées est réinitialisé au bout de 12 heures
- Création d'utilisateur :
    - Une invitation est envoyée par e-mail à l'utilisateur
    - Le lien est valable 7 jours
    - Si l'utilisateur ne s'est pas connecté avant l'expiration du lien, il doit lancer une procédure de réinitialisation de mot de passe
- Réinitialisation du mot de passe :
    - Le lien de réinitialisation est envoyé par e-mail
    - Lien temporaire : valable 1 heure
- Mot de passe temporaire :
    - Si l'utilisateur ne reçoit pas l'e-mail de réinitialisation ou d'invitation, l'équipe support peut générer un mot de passe temporaire et le lui transmettre
    - L'utilisateur devra créer un nouveau mot de passe dès sa première connexion
- La mise en cache des mots de passe n'est pas autorisée
- Expiration de session : les sessions du back-office durent 45 minutes (durée prolongée par toute action effectuée dans l'interface, par exemple un clic, un mouvement de souris ou une modification de contenu).

Authentification unique (SSO)

L'authentification unique est disponible avec les principaux fournisseurs d'identité :

- Google (SSO social)
- Microsoft (Azure Active Directory)

Nous prenons également en charge les protocoles d'authentification unique suivants :

- OAuth (aujourd'hui, plus précisément OAuth 2.0)
- OpenID Connect (OIDC)
- SAML (Security Assertion Markup Language)

Cette solution offre à nos clients la souplesse nécessaire pour respecter facilement leurs propres exigences et politiques d'authentification sécurisée.

MFA (authentification multifacteur)

Ibexa propose une méthode d'authentification à deux facteurs (2FA) reposant sur un mot de passe à usage unique basé sur le temps (TOTP). Cette couche de sécurité est désactivée par défaut et peut être activée pour renforcer la sécurité.

Les administrateurs peuvent rendre l'usage de la 2FA obligatoire.

Les applications d'authentification TOTP prises en charge sont FreeOTP et Google Authenticator. Les administrateurs peuvent réinitialiser, depuis le back-office, le lien entre l'appareil et le compte. Une fois la 2FA activée, elle est obligatoire à chaque connexion.

La 2FA peut être utilisée aussi bien avec la connexion par e-mail et mot de passe qu'avec le SSO.

Ibexa recommande vivement à ses utilisateurs d'utiliser l'authentification multifacteur fournie par l'intégration avec leur fournisseur d'identité (voir Authentification unique).

Création d'utilisateur

Les nouveaux utilisateurs reçoivent par e-mail un lien d'invitation valable 72 heures et doivent définir un nouveau mot de passe lors de leur première connexion.

Les nouveaux utilisateurs sont créés à l'état inactif et reçoivent par e-mail un lien d'invitation à usage unique et à durée limitée (72 heures). Le système valide le lien avant d'afficher le formulaire d'activation, dans lequel l'utilisateur définit son mot de passe et peut, s'il le souhaite, compléter son profil.

Une fois l'activation réussie, le compte devient actif, le jeton d'invitation est consommé et l'utilisateur est automatiquement connecté. Les liens expirés, déjà utilisés ou invalides sont rejetés, et les administrateurs peuvent émettre une nouvelle invitation si nécessaire.

Expiration de session

Les sessions utilisateur expirent automatiquement après 60 minutes d'inactivité.

Séparation des tâches

Ibexa a mis en place des processus techniques internes pour empêcher les équipes commerciales d'accéder aux données et aux environnements des clients.

Principe du moindre privilège

Les collaborateurs d'Ibexa disposent uniquement des accès minimaux nécessaires à l'exercice de leurs fonctions.

Arrivées, départs, changements de poste et revues périodiques

Des processus organisationnels encadrent l'attribution et le retrait des accès lorsqu'un collaborateur arrive, quitte l'entreprise ou change de poste.

Les accès sont revus périodiquement par les propriétaires des actifs afin de vérifier qu'ils sont toujours justifiés.

Architecture multi-tenant et cloisonnement des données

1. Authentification et identification du tenant

- Les utilisateurs s'authentifient avec des jetons d'accès signés et à durée limitée (JWT).
- Le jeton identifie uniquement l'utilisateur. L'organisation de l'utilisateur est récupérée en base de données à chaque requête et n'est jamais déduite de données transmises par le client. Un utilisateur ne peut donc pas agir au nom d'une autre organisation en modifiant les paramètres d'une requête.

- À chaque requête, la plateforme vérifie que le compte utilisateur et son organisation sont tous deux actifs. Le blocage ou la désactivation d'un utilisateur ou d'une organisation prend effet immédiatement, sans attendre l'expiration du jeton.

2. Rattachement des données au tenant

- Toutes les données clients sont rattachées à l'organisation qui en est propriétaire, soit directement, soit via l'enregistrement auquel elles appartiennent. Cela couvre les agents, conversations, exécutions, messages, fichiers, documents de la base de connaissances, intégrations, rapports, crédits et notifications.
- Le contenu de la base de connaissances utilisé pour la recherche par l'IA (fragments de documents et leurs embeddings vectoriels) porte son propre identifiant d'organisation, vérifié à chaque recherche.

3. Accès aux données cloisonné

- Toutes les requêtes de base de données portant sur des données clients sont limitées à l'organisation de l'utilisateur à l'origine de la requête.
- Si un utilisateur demande une ressource appartenant à une autre organisation, la plateforme répond comme si elle n'existait pas (« introuvable »), sans révéler que la ressource existe ailleurs.
- Les ressources partagées de la plateforme, telles que le catalogue public d'agents et d'intégrations ou les définitions de modèles d'IA, ne contiennent aucune donnée client. Les fournisseurs de modèles d'IA partagés ne sont mis à la disposition d'une organisation que sur attribution explicite par un administrateur de la plateforme.

4. Autorisations au sein d'une organisation

- Une couche d'autorisation dédiée vérifie chaque opération au regard de règles fondées sur les rôles : propriétaire de l'organisation, administrateur de l'organisation, membre et créateur de la ressource.

- Par exemple, seuls le créateur, un propriétaire ou un administrateur peuvent modifier ou supprimer un agent. Les conversations ne sont visibles que de l'utilisateur qui les a créées. Les membres ne voient que les exécutions qu'ils ont lancées.
- Lorsque des ressources sont liées entre elles (par exemple un outil ou un sous-agent rattaché à un agent), la plateforme vérifie qu'elles appartiennent bien à la même organisation.

5. Traitements en arrière-plan

- Les tâches asynchrones, telles que les exécutions d'agents, le traitement de documents et les évaluations, portent l'identifiant de l'organisation. Chaque tâche recharge ses données avec la même restriction d'organisation que les requêtes interactives.
- Les flux en temps réel et les caches temporaires ne sont accessibles qu'après le passage des contrôles d'autorisation décrits ci-dessus. Les entrées de cache contenant des résultats propres à une organisation incluent l'organisation dans leur clé.

6. Stockage des fichiers

- Les fichiers téléversés et les documents de la base de connaissances sont stockés dans des chemins de stockage propres à chaque organisation.
- Les fichiers ne peuvent être téléchargés que via la plateforme. Les liens de téléchargement sont de courte durée et liés à un fichier, une conversation et une organisation précis.

7. Accès des agents d'IA aux connaissances des clients

- L'outil de base de connaissances intégré utilisé par les agents d'IA s'exécute avec les permissions de l'utilisateur au nom duquel l'agent agit. Le modèle d'IA ne reçoit jamais d'identifiants d'organisation ni d'utilisateur.
- Un agent peut en outre être limité à certains dossiers de la base de connaissances de son organisation.

8. Intégrations entrantes (webhooks)

- Les appels de webhook entrants sont rattachés à leur organisation par un jeton unique et impossible à deviner.
- Ils peuvent aussi être protégés par une liste blanche d'adresses IP, une signature HMAC avec validation de l'horodatage (protection contre le rejeu) et une limitation du débit. Les tentatives rejetées sont consignées dans un journal d'audit.

9. Vérification

Une suite de tests automatisés s'exécute dans la chaîne d'intégration continue. Elle comprend des tests qui vérifient que les données d'une organisation ne sont pas accessibles à une autre, tant au niveau de l'accès à la base de données qu'au niveau de l'API.

Cryptographie

Les exigences suivantes en matière de cryptographie ont été définies :

- Serveurs de production
    - En transit : chiffré
        - Algorithme de chiffrement : AES-256 au minimum (voir la suite de chiffrement)
        - Cet algorithme de chiffrement est reconnu par la NIST Special Publication 800-52
    - Au repos :
        - Systèmes de fichiers : tout serveur contenant des données personnelles a son système de fichiers chiffré (BitLocker pour les serveurs Windows, AES-XTS pour les serveurs Linux)
- Lieux de sauvegarde
    - En transit : AES-256 au minimum (voir la suite de chiffrement)
    - Au repos : les systèmes de fichiers sont chiffrés avec AES-XTS
- Données sensibles (clés d'API, configuration SSO, variables, etc.) : elles sont chiffrées en AES-256 avec une clé fournie à l'application au moment de l'exécution.
- Accès aux serveurs de production : une clé privée SSH est obligatoire pour accéder aux serveurs de production. Ces accès sont réservés à un nombre limité de collaborateurs d'Ibexa, selon les principes du « besoin d'en connaître » et du « moindre privilège ».
- Seules des autorités de certification (CA) de confiance et non compromises sont utilisées en production.
- La création, la distribution, le stockage et la suppression des certificats sont strictement encadrés par le CTO, ou automatisés (par programmation) sous sa supervision.

Chiffrement des données au repos

Le tableau suivant résume le chiffrement au repos au sein de notre infrastructure ainsi que la gestion des clés :

Nom	Siège social	Localisation du datacenter	Données personnelles transférées	Chiffrement au repos	Propriétaire de la clé de chiffrement
OVH	France	UE	Données des agents Journaux système, d'accès et applicatifs	Oui (niveau disque) Oui (niveau disque)	Ibexa Ibexa
AWS	États-Unis	UE	Journaux système, d'accès et applicatifs	Oui (niveau applicatif)	Ibexa

Chiffrement des données en transit

De Vers	OVH	AWS	CDN77
OVH		TLS	TLS
AWS	TLS		TLS
CDN77	TLS	TLS	

Sécurité physique et environnementale

Grâce à l'inventaire des actifs tenu par Ibexa, l'emplacement de chaque information et de chaque actif informatique critique est connu. Une politique est en cours de déploiement afin que ces actifs soient hébergés dans des centres de traitement de données conformes aux normes ISO 27001 et/ou SOC 2.

Centres de traitement de données

Nos applications cœur de métier sont hébergées dans des datacenters du groupe OVH, certifiés ISO 27001 et SOC 2, qui garantissent :

- Une politique stricte d'accueil des visiteurs
- Un système d'alarme
- Des équipements de vidéosurveillance (CCTV)
- Des dispositifs de prévention incendie
- Des systèmes de climatisation
- La redondance de l'alimentation électrique et des télécommunications
- ...

Notre empreinte géographique actuelle s'étend sur 700 km à travers l'Europe.

Plus d'informations sur la sécurité physique et environnementale figurent dans la section consacrée aux sous-traitants.

Les bureaux d'Ibexa

- L'accès à nos bureaux est sécurisé.
- Les bureaux sont verrouillés en dehors des heures d'ouverture.
- Aucune donnée n'est hébergée dans nos bureaux.

Les ordinateurs portables d'Ibexa

Les ordinateurs portables d'Ibexa sont régis par une « politique de sécurité des terminaux » (Secure EndPoint Device Policy) qui impose des mesures techniques et opérationnelles pour protéger l'appareil et son contenu. La conformité des ordinateurs portables à cette politique est vérifiée périodiquement.

La politique définit notamment les mesures suivantes :

Chiffrement du disque dur

Pour éviter toute fuite de données en cas de vol d'un ordinateur portable d'Ibexa, le chiffrement des disques durs est obligatoire. La liste complète des clés de chiffrement est conservée par Ibexa ; lorsqu'un collaborateur quitte l'entreprise, le disque dur est effacé par destruction de la clé de chiffrement (crypto-effacement).

Protection antimalware

Les ordinateurs portables d'Ibexa sont protégés par une solution antimalware toujours active, administrée de manière centralisée pour l'ensemble du parc.

Mises à jour logicielles

Les ordinateurs portables doivent toujours être à jour de la dernière version stable des logiciels (applications et système d'exploitation) fournie par l'éditeur.

Écran vide, verrouillage et appareils laissés sans surveillance

Lorsque la personne autorisée n'a pas le contrôle direct de l'appareil, aucune information sensible ne doit rester affichée à l'écran.

En cas d'absence brève, la règle de l'écran vide s'applique en verrouillant tous les systèmes ou en verrouillant l'écran par mot de passe ou par biométrie (empreinte digitale). Une règle de verrouillage automatique doit être configurée pour verrouiller l'appareil mobile après un délai défini.

En cas d'absence plus longue (par exemple pendant des congés), l'utilisateur doit fermer sa session.

La politique prévoit également que les ordinateurs portables ne doivent jamais être laissés sans surveillance en dehors d'une zone sécurisée.

Si l'appareil est laissé au bureau en dehors des heures de travail, il doit être rangé dans un meuble fermé à clé.

Périphériques de stockage USB

L'utilisation de tout périphérique de stockage USB sur un actif de l'organisation est strictement interdite. Veuillez vous référer à la politique de classification des données pour connaître les plateformes autorisées pour stocker ou partager (en interne comme en externe) les données d'Ibexa.

Sécurité des opérations

Politique de sauvegarde

Les types de données suivants entrent dans le périmètre de notre politique de sauvegarde :

- Bases de données
- Contenus fournis par les utilisateurs et hébergés par Ibexa
- Documentation
- Fichiers internes
- E-mails
- Code applicatif

Sauvegarde des bases de données

Les bases de données d'Ibexa hébergent les informations les plus sensibles et les plus critiques de l'entreprise.

C'est pourquoi toutes les bases de données contenant des données personnelles sont :

- Répliquées :
    - Les enregistrements sont répliqués en temps réel sur au moins deux nœuds de base de données situés dans des datacenters distincts.
    - La réplication s'effectue via un canal chiffré.
- Sauvegardées :
    - Toutes les sauvegardes de bases de données sont chiffrées
    - Le stockage est réalisé dans l'un des datacenters d'Ibexa situés dans l'UE

    - La durée de conservation est de 180 jours.
- Test des sauvegardes :
    - L'intégrité des sauvegardes est testée. Comme nous utilisons plusieurs technologies de bases de données selon le type de données à stocker, les tests de restauration sont effectués à tour de rôle (« round robin ») sur les différentes bases lors des exercices successifs.
- Fréquence des sauvegardes :
    - Les sauvegardes sont réalisées sur chacune des technologies de bases de données de manière à respecter les objectifs définis de RPO (Recovery Point Objective – perte de données maximale admissible) et de RTO (Recovery Time Objective – délai maximal de rétablissement).

Sauvegarde des contenus fournis par les utilisateurs et hébergés par Ibexa

Les contenus fournis par nos clients sont stockés sur plusieurs datacenters d'Ibexa situés dans l'UE (stockage objet). Les contenus sont versionnés et répliqués afin de respecter nos objectifs de RTO et de RPO.

Documentation et fichiers internes

La documentation et les fichiers internes sont hébergés sur Google Drive (région de données activée : Europe). La sauvegarde de ces données est assurée par Google, dans le cadre de sa politique de régions de données (https://support.google.com/a/answer/9223653).

E-mails

Nos e-mails sont hébergés par Google Mail (serveurs situés dans l'UE) ; leur sauvegarde est assurée par Google.

Code applicatif

Le code applicatif est versionné avec Git ; la sauvegarde des dépôts Git est assurée par des clones réguliers. Nous utilisons à la fois GitHub et des instances GitLab internes.

Protection contre les attaques DDoS et pare-feu

L'ensemble de l'infrastructure applicative d'Ibexa est protégé contre les attaques DDoS (déni de service distribué) par l'infrastructure Anti-DDoS d'OVH. Au-delà de cette première ligne de défense, notre infrastructure est protégée par des équipements réseau assurant la répartition de charge et la limitation de débit, ainsi que par un pare-feu qui interdit l'accès aux services non publics et protège contre les attaques courantes.

Journalisation et supervision

Ibexa a mis en place des outils adaptés pour journaliser, superviser et alerter les équipes en temps réel en cas de comportement suspect.

Tous les journaux (applicatifs et système) sont déjà collectés et agrégés dans un cluster Elasticsearch. Les plateformes suivantes répondent à nos besoins de journalisation, de supervision et d'alerte :

- Monit : supervision réactive, alertes et mise en œuvre de mesures de sauvegarde ou d'urgence pour gagner de précieuses minutes en cas d'incident.
- Stack ELK : agrégation des journaux pour centraliser tous les événements de la plateforme.
- Uptime et FreshPing : supervision externe de nos services
- Prometheus avec Alertmanager
- Scanner de ports externe pour détecter toute évolution de la surface d'attaque de l'infrastructure

Contrôle des accès à distance, détection et prévention des intrusions

Tous nos serveurs sont protégés contre les intrusions : l'accès se fait exclusivement via un VPN d'administration, associé à une protection contre les attaques par force brute. Les accès SSH reposent toujours sur une authentification par clé privée.

Les services exposés sur Internet ne le sont qu'en HTTP et sont protégés par un proxy HTTP de filtrage de niveau 7.

La détection d'intrusion (IDS) repose sur les événements d'audit Unix, collectés et centralisés sur un serveur distinct de celui qui est surveillé.

Sécurité des communications

HTTPS et SSL

Le trafic entre les serveurs d'Ibexa et le navigateur des utilisateurs finaux est chiffré uniquement en TLS 1.2 et 1.3.

La suite de chiffrement utilisée est `EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH`

Acquisition, développement et maintenance des systèmes d'information

Cycle de développement sécurisé (SDLC)

Les méthodes Scrum et Kanban sont utilisées pour piloter et gérer nos développements.

Chaque demande se voit attribuer l'un des types suivants :

- Fonctionnalité : une nouvelle fonctionnalité du produit, disponible pour tous nos clients
- Bug : une correction apportée à une fonctionnalité existante du produit. Les bugs incluent également les incidents.
- Projet client : une demande spécifique à un client, par exemple une intégration sur mesure.

Fonctionnalités

Toutes les fonctionnalités sont définies sous forme de « User Stories », rédigées avec le Product Owner, un représentant des équipes de développement et de QA.

Les fonctionnalités sont analysées sous l'angle de la sécurité et de la vie privée afin de garantir la sécurité et la protection de la vie privée dès la conception et par défaut.

Les fonctionnalités sont planifiées dans des sprints dès qu'elles atteignent l'état « Ready » (prête à être développée).

Pour garantir la qualité des développements, Ibexa applique des définitions strictes pour déterminer qu'une User Story est « Ready » (prête à être développée) puis « Done » (terminée).

Bugs

Tous les bugs sont évalués par l'équipe Produit et, selon leur criticité, planifiés dans un sprint futur ou traités dans le sprint en cours.

Projets clients

Tous les projets clients sont pilotés par des chefs de projet qui font le lien entre le client et le processus de développement interne. Les User Stories des projets clients sont définies puis planifiées dans les sprints à venir.

Équipes

Plusieurs équipes travaillent ensemble pour développer, maintenir et faire évoluer le logiciel d'Ibexa :

- Équipe Produit (PT)
- Équipe Assurance qualité (QA)
- Équipe de développement agile (Dev)
- Équipe Infrastructure (IT)

Pratiques de développement

Ibexa maintient et exploite une base de code unique pour tous ses clients. Ce code est développé avec une forte exigence de qualité et de performance. Pour y parvenir, différentes techniques et normes de codage sont employées, notamment :

- Programmation en binôme (pair programming)
- Développement piloté par les tests (TDD)
- Revues de code (humaines et assistées par IA)
- Code généré par IA

Ibexa cherche à éviter les refontes « big bang » et à ne pas réinventer la roue. C'est pourquoi Ibexa :

- Recourt à l'intégration et au déploiement continus, par petites étapes incrémentales
- Utilise des frameworks et des composants chaque fois que c'est possible (principalement pour les nouvelles applications)
- Fait évoluer les applications existantes plutôt que de repartir de zéro

Séparation des environnements

Les environnements sont séparés : seuls les serveurs de production contiennent de véritables données personnelles (PII) et/ou des données clients réelles ; les développeurs et les testeurs travaillent sur des données de test fictives dans leurs environnements respectifs (développement, QA).

Accès aux environnements

Ibexa dispose de différents environnements : développement, QA, recette et production. L'accès aux bases de données est restreint par utilisateur selon un **rôle attribué**, et par application selon un **périmètre**. L'accès à la base de données de production est limité à un nombre très restreint d'utilisateurs.

L'équipe Sécurité IT est chargée d'attribuer, pour chaque environnement, un rôle à chaque membre de l'équipe IT.

Architecture générale

Plateforme SaaS multi-tenant (API backend + frontend web) dédiée à l'orchestration d'agents d'IA. Les tenants sont isolés logiquement sous forme d'organisations, et toutes les données métier sont rattachées à un identifiant d'organisation.

Composants principaux :

- **Frontend** : application web monopage pour configurer et utiliser l'Ibexa Agentic Marketing Platform.
- **API backend** : service sans état (stateless) et évolutif horizontalement ; conception pilotée par le domaine (DDD) couvrant les utilisateurs, organisations, agents, conversations, base de connaissances, crédits, etc.

- **Worker** : service de traitement asynchrone des tâches de fond et planifiées (par exemple les exécutions d'agents de longue durée, les notifications, les déclencheurs planifiés), découplé du cycle requête/réponse de l'API.
- **Base de données relationnelle** et **Vector Store** : stockage principal des données structurées et des embeddings.
- **Cache** : stockage en mémoire pour la mise en cache et les métadonnées de planification.
- **Message broker / file de messages** : assure l'intermédiation du travail asynchrone entre l'API et le Worker.
- **Stockage objet** : stocke les fichiers, avatars et images.

Revue de code et tests

Nous utilisons les technologies et composants logiciels les plus avancés : Redis, NodeJS et React.js.

Tous les composants d'Ibexa ont été développés en interne et sont mis à jour par notre équipe IT.

Revue de code par les pairs

Tout code prêt pour la production est validé par au moins 2 développeurs internes ainsi que par un agent IA / GitHub Copilot.

Tests

Les tests sont un élément essentiel du développement de notre produit ; c'est pourquoi nous disposons d'une équipe QA interne à temps plein. Les tests sont réalisés manuellement et de façon automatisée.

Ibexa combine :

- Des tests unitaires : automatisés, au niveau applicatif
- Des tests d'intégration
- Des tests de bout en bout
- Des tests de non-régression manuels
- Des simulations d'utilisation par l'utilisateur final en préproduction

Nous recourons aux tests automatisés dès que possible, via une plateforme de test (comme Postman pour tous les tests de non-régression d'API).

Ces tests sont déclenchés automatiquement par notre plateforme de livraison continue.

Gestion des mises en production

Qu'est-ce que la gestion des mises en production ?

La gestion des mises en production (Release Management) est le processus qui consiste à gérer, planifier, ordonnancer et contrôler la construction d'un logiciel à travers ses différentes étapes et environnements, y compris le test et le déploiement des versions logicielles

Elle permet de livrer de nouvelles fonctionnalités tout en préservant l'intégrité des services existants.

Objectifs

- Garantir un nombre élevé de mises en production réussies, c'est-à-dire réduire le nombre de mises en production aux résultats inattendus ou nécessitant un retour arrière.
- Maintenir un faible nombre d'incidents causés par les mises en production.
- Disposer d'un processus unique et documenté pour gérer toutes les mises en production.
- S'assurer que le processus est appliqué et que tout problème de conformité est remonté à la direction.
- Améliorer la productivité en établissant des processus et des outils standard de mise en production.
- Tirer les enseignements du processus de gestion des mises en production, qui pourront être appliqués à d'autres domaines de la gestion des services.

Politiques

- Tous les projets, les lots de changements sur un service existant (mises en production regroupant plusieurs évolutions ou correctifs) et les changements critiques sur un service existant doivent suivre le processus de gestion des mises en production, avec les validations appropriées (Head of Product ou équipe Produit / équipe Projets clients, DPO et CIO).
- Dans la mesure du possible, les changements apportés à un service existant sont regroupés et livrés de façon régulière (chaque semaine) via le processus de gestion des mises en production.
- Un unique « Release Manager » doit être désigné pour chaque mise en production. Il est responsable de la bonne coordination et exécution de la mise en production, et veille à ce que toute la documentation requise existe.
- Chaque mise en production doit être testée et vérifiée par notre équipe QA avant son déploiement.
- Tous les travaux de mise en œuvre de la mise en production doivent être terminés à la date et à l'heure de fin prévues.
- La réussite de la mise en production doit être confirmée par des tests post-déploiement.

- Les changements introduits préservent la rétrocompatibilité, et toute dépréciation ou suppression est annoncée au moins 2 semaines à l'avance. Un journal des modifications détaillé est disponible sur la page des notes de version : https://docs.ibexa.ai/release-notes

Processus de mise en production

- Toutes les fonctionnalités et tickets sont disponibles dans les environnements de préproduction.
- Toutes les fonctionnalités et tickets sont revus par l'équipe QA dans les environnements de préproduction.
- Toutes les fonctionnalités et tickets sont marqués avec le label approprié : Production Ready.
- Le début de la maintenance liée à la mise en production est signalé sur la page de statut.
- Les environnements de préproduction sont fusionnés dans les environnements de production.
- La version est correctement taguée.
- Le lien vers les notes de version est ajouté au tag Git.
- Les notes de version sont entièrement renseignées (temps prévu et réel corrects, présences, tous les tests au vert).
- La maintenance liée à la mise en production est clôturée sur la page de statut.
- Communication de la mise en production (interne et externe).

Retour d'expérience

Chaque régression identifiée lors d'une mise en production fait l'objet d'une analyse a posteriori des problèmes rencontrés. Ces informations sont jointes aux notes de version internes :

- Description
- Gravité
- Impacts
- Solutions à mettre en œuvre pour les prochaines mises en production
- Détails

Données de production

Les données de production sont strictement réservées à l'environnement de production. Les développements et les tests sont réalisés sur des données de test fictives.

Gestion des incidents de sécurité de l'information

Procédure de gestion des incidents

Ibexa a mis en place une procédure de gestion des incidents. Elle définit les responsabilités pour répondre aux incidents de sécurité et de vie privée, les atténuer et y remédier. Cette politique est disponible sur demande.

Support client

Page de statut

Une page de statut est disponible à l'adresse : https://Ibexa.status.io/ ; il est possible de s'y abonner pour recevoir des notifications par e-mail, webhook, RSS, etc.

Assistance en ligne

Tous les utilisateurs d'Ibexa peuvent contacter le Helpdesk https://www.support.Ibexa.co ou écrire à l'adresse support.agentic@ibexa.ai.

Le support standard est disponible pendant les heures de bureau habituelles (du lundi au vendredi, de 9 h à 18 h, heure locale Royaume-Uni et France), jours fériés inclus.

Disponibilité du service

Composant	Disponibilité	Description

Agent Runtime	99,0 %	La couche d'infrastructure sous-jacente qui exécute, gère et sécurise les agents d'IA en production.
Agent Administration	95,0 %	L'environnement de back-office dans lequel les agents sont construits, configurés et gérés.

Temps de réponse

Les délais de première réponse et d'atténuation sont mesurés pendant les heures de bureau :

Priorité	Délai estimé de première réponse	Délai d'atténuation	Délai de correction
P1	2h	8h	2 semaines
P2	4h	72h	1 mois
P3	8h	1 semaine	6 mois
P4	Au mieux	Au mieux	Au mieux

Les délais d'atténuation sont des objectifs. Selon le volume et la priorité des demandes adressées au support, les délais de réponse et de résolution peuvent varier.

Gestion des vulnérabilités techniques et politique de correctifs

Application des correctifs de vulnérabilités techniques

L'application des correctifs de vulnérabilités techniques est priorisée selon le système CVSS (Common Vulnerability Scoring System), comme suit :

	Critique	Élevée	Moyenne	Faible

Délai d'application du correctif à compter de la notification	48 heures	48 heures	15 jours ouvrés	60 jours ouvrés

Autres correctifs et mises à jour

Les correctifs sont traités pendant la semaine de maintenance régulière inscrite dans la feuille de route de l'équipe. Au moins deux semaines de maintenance doivent être planifiées chaque trimestre.

Comment : tâche de maintenance planifiée lors de la prochaine semaine de maintenance

Changements de version majeure

Les changements de version majeure des dépendances de projet et des composants d'infrastructure doivent être planifiés et traités dans le cadre d'un projet inscrit dans la feuille de route de l'équipe.

Délai : 6 mois

Comment : projet détaillé inscrit dans la feuille de route

Politique d'utilisation raisonnable

- Les systèmes d'Ibexa fonctionnent comme une application distribuée : un répartiteur de charge oriente les utilisateurs vers un nœud de calcul.
- Les ressources de base sont mutualisées entre tous les clients ; les requêtes sont dirigées vers le serveur le moins sollicité, d'après l'historique d'activité récente.

- Ibexa peut prendre des mesures raisonnables pour préserver la stabilité du système. Ces mesures et leurs conditions sont décrites dans nos conditions d'utilisation.

Continuité d'activité et reprise après sinistre

Redondance

Pour garantir ses SLA élevés, Ibexa s'appuie sur 3 datacenters : Francfort (DE), Gravelines (FR) et Roubaix (FR), tous certifiés ISO 27001 et SOC 2 Type II.

Cette configuration assure une répartition géographique de 700 km à travers l'Europe.

Continuité d'activité

Ibexa a défini des scénarios de continuité d'activité répondant aux perturbations d'origine environnementale, technique ou humaine.

Ces scénarios ont été définis pour respecter le RTO et le RPO approuvés par la Direction.

RTO

Le RTO (Recovery Time Objective) est la durée maximale pendant laquelle les données peuvent être indisponibles.

Toutes les solutions de sauvegarde déployées chez Ibexa doivent garantir un RTO maximal de 24 h lorsqu'elles protègent des données clients d'Ibexa. Lorsque les données protégées sont des données internes d'Ibexa, ce RTO ne doit pas dépasser 48 h.

RPO

Le RPO (Recovery Point Objective) est le délai maximal écoulé depuis le dernier point de sauvegarde. Il quantifie la quantité maximale de données pouvant être perdues.

Le RPO est de 24 h maximum.

Toutes les mesures ci-dessus doivent être respectées 99 % du temps. Compte tenu du fonctionnement des sauvegardes et de la réplication, des dépassements ponctuels de ces délais sont acceptables.

Reprise après sinistre

Une procédure de reprise après sinistre a été définie par le CTO pour rétablir les systèmes de production en cas de sinistre (reconstruction complète). Elle s'applique à tous les systèmes de production nécessaires à la fourniture du service Ibexa à nos clients et est revue chaque année.

Conformité

Audits et rapports de sécurité

Ibexa réalise des évaluations périodiques de la sécurité du produit. Elles peuvent être menées par un tiers (audit externe) ou en interne (audit interne).

Audits externes

Test d'intrusion

Un test d'intrusion est une cyberattaque simulée et autorisée, menée sur l'infrastructure et l'application d'Ibexa afin d'évaluer la sécurité de sa plateforme. Il vise à identifier les vulnérabilités, notamment la possibilité pour des tiers non autorisés d'accéder aux fonctionnalités et aux données du système, ainsi que les points forts, afin de permettre une évaluation complète des risques.

Ibexa fait appel à des prestataires externes pour réaliser des tests d'intrusion une fois par an.

Une version déclassifiée du rapport de test d'intrusion est disponible sur demande pour nos clients actifs, en écrivant à security@ibexa.co.

Audits à la demande des clients

Ibexa travaille avec plus de 1 200 organisations clientes à travers l'Europe, dans des secteurs variés (médias, banque, distribution, grande consommation, etc.). Chacun de nos clients applique des exigences élevées en matière de sécurité et de protection des données. C'est pourquoi Ibexa partage avec eux les résultats d'audits menés par des auditeurs externes, afin de garantir l'existence, le suivi et l'amélioration continue de ses systèmes de management liés à la sécurité de l'information (SMSI) et aux données personnelles (PIMS).

Ce mécanisme a été mis en place pour démontrer notre conformité aux normes internationales et faciliter les évaluations de sécurité menées par les clients, qui sont chronophages pour les deux parties.

Comme la plupart des éditeurs SaaS dont le prix annuel de licence est comparable, nous n'autorisons pas nos clients à organiser leurs propres audits d'Ibexa, ces exercices mobilisant fortement nos équipes. En tant qu'entreprise en forte croissance, il n'est pas envisageable de suivre des audits personnalisés pour chaque client.

Les demandes d'audits de sécurité supplémentaires à la demande (évaluation de sécurité et tests d'intrusion) ou d'exigences spécifiques peuvent être étudiées par notre GRC Lead pour les clients Platinum uniquement. Veuillez vous référer à nos Conditions générales et contacter votre responsable de compte pour toute question relative aux audits à la demande.

Audits internes

Parallèlement, Ibexa mène des audits en interne. Ces audits comprennent :

Analyse de vulnérabilités

Ibexa analyse en continu son infrastructure afin de détecter les ports ouverts et les vulnérabilités connues.

Les images Docker sont signées et analysées à la recherche de vulnérabilités avant d'être déployées.

Analyse statique de code

- SonarQube et GitHub Copilot sont utilisés pour l'analyse statique du code.

S'y ajoutent des outils propres à chaque langage : Ruff, Mypy, Biome, compilateur TypeScript.

Assurances

Les activités d'Ibexa sont couvertes par les assurances suivantes :

- Responsabilité civile professionnelle et responsabilité civile générale
- Assurance cyber

Ibexa est-elle certifiée ISO 27001 ou ISO 27701 ?

Non, Ibexa ne détient pas de certification ISO pour le moment.

Nous avons mis en place un système de management de la sécurité de l'information (SMSI) et un système de management des informations de vie privée (PIMS), fondés respectivement sur les normes ISO 27001 et ISO 27701.

Ces systèmes de management sont régulièrement revus et améliorés. Le présent document, structuré selon les contrôles ISO, témoigne de notre engagement et de notre adhésion à ces normes.

Nous veillons également à ce que nos fournisseurs offrent le même niveau de sécurité que nous. Notre politique de sécurité des fournisseurs exige ainsi que tous nos sous-traitants ultérieurs qui traitent des informations de nos clients soient certifiés ISO 27001 ou fournissent un rapport SOC 2 Type 2.

Convaincue de l'importance d'un SMSI et d'un PIMS, la Direction soutient pleinement ces systèmes de management et leur amélioration continue. Toutefois, elle a décidé de ne pas engager de démarche de certification ISO 27001, compte tenu de la taille actuelle de l'entreprise et de son agilité (délai de mise sur le marché).

Protection des données et vie privée

Ibexa en tant que « sous-traitant »

De par sa nature générique, l'IAMP peut traiter de nombreux types de données différents. Les types de données traités par le système dépendent des décisions du client.

Lorsque des données personnelles sont traitées par la plateforme, Ibexa agit en qualité de « sous-traitant » (data processor), traitant les données pour le compte de ses clients (les « responsables de traitement »).

En conséquence, Ibexa n'entretient aucune relation directe avec les personnes dont elle reçoit les informations de la part de ses clients. Ibexa ne contrôle pas ces informations, ne choisit ni ne détermine les types de données qu'elle traite, et ne détermine pas les finalités pour lesquelles elles sont traitées.

Politique de conservation des données personnelles

Adresses IP

Les adresses IP sont des données personnelles qui font l'objet d'un traitement spécifique par nos systèmes.

Au sein de l'infrastructure technique sous-jacente, Ibexa peut conserver les adresses IP des visiteurs pendant une durée n'excédant pas six (6) mois, afin de disposer de la traçabilité nécessaire pour assurer la sécurité de son système d'information, de ses produits et de ses services. Ces journaux d'accès permettent à Ibexa d'analyser les accès à ses systèmes et plateformes et de déterminer l'origine d'éventuels incidents et alertes (accès frauduleux, usage abusif, etc.) en établissant des corrélations entre les données de journalisation. Ces journaux d'accès ne sont utilisés à aucune autre fin que la sécurité technique et organisationnelle.

Il s'agit d'une durée de conservation recommandée du point de vue de la sécurité (disposer d'un historique exploitable en cas d'incident) et d'un délai reconnu comme acceptable par les autorités de protection des données.

Restitution des données à la fin du contrat

Les clients peuvent à tout moment demander l'export et la suppression de leurs données. Les bases de données et les comptes des clients sont définitivement supprimés dans un délai d'un mois après la fin du contrat.

Documentation d'Ibexa sur les mesures de protection au titre du RGPD

Vous trouverez ici l'accord RGPD standard d'Ibexa ainsi que nos autres mesures de protection des données. Ces documents seront mis à jour au fil du temps pour refléter nos dernières mesures.

Mesures organisationnelles pour garantir la sécurité et la protection des données personnelles

Délégués à la protection des données

Afin de garantir l'indépendance du délégué à la protection des données, nous avons nommé un DPO joignable à l'adresse e-mail dpo@ibexa.co.

Nous veillons à ce que notre délégué à la protection des données :

- soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données personnelles ;
- ne reçoive aucune instruction en ce qui concerne l'exercice de ses missions ;
- soit tenu au secret ou à la confidentialité dans l'exercice de ses missions, conformément au droit de l'Union ou au droit des États membres ;
- ne soit ni relevé de ses fonctions ni pénalisé par le responsable de traitement ou le sous-traitant pour l'exercice de ses missions ;
- n'exerce aucune autre mission ou tâche susceptible de donner lieu à un conflit d'intérêts.

Ibexa aidera le délégué à la protection des données à exercer les missions visées à l'article 39 du RGPD, en fournissant les ressources nécessaires pour les exercer, l'accès aux données

personnelles et aux opérations de traitement, ainsi que les moyens d'entretenir ses connaissances spécialisées.

Mesures relatives aux ressources humaines

Clause de confidentialité dans les contrats de travail

Voir la section « Clause de confidentialité dans les contrats de travail »

Sensibilisation et formation continue du personnel à la sécurité

Voir la section « Sensibilisation et formation continue à la sécurité »

Procédures en cas de violation de données

Réception de l'incident

Toute personne peut signaler à Ibexa une violation de sécurité et/ou de données aux adresses e-mail suivantes : dpo@ibexa.co et/ou security@ibexa.co.

Les informations suivantes doivent être fournies :

- la nature de la violation de données
- les catégories de données concernées
- le nombre d'enregistrements
- le nombre de personnes concernées
- toute autre information qui vous a conduit à présumer la violation de données
- les coordonnées de contact (DPO ou autre point de contact)

Si les informations sont insuffisantes, la personne chargée d'instruire l'incident demandera des précisions à l'auteur du signalement.

L'équipe DPO et/ou l'équipe Sécurité accusera réception de votre demande, puis commencera immédiatement à instruire votre cas de violation potentielle de données. Un ticket d'incident sera créé dans l'outil de ticketing d'Ibexa.

Évaluation de l'incident

Le DPO et/ou l'équipe Sécurité évalue l'incident reçu. Cette analyse permet de classer l'incident dans l'un des cas suivants :

- Faux positif
- Violation de sécurité sans violation de données personnelles
- Violation de sécurité avec violation de données personnelles

En cas de « faux positif », l'incident est mis à jour dans l'outil de gestion des tickets d'Ibexa puis clôturé.

Traitement de l'incident

Traitement du volet « sécurité » de l'incident

L'équipe Sécurité mène les activités suivantes :

- Confinement : les systèmes touchés sont isolés de l'environnement opérationnel afin d'éviter que l'incident ne se propage à d'autres actifs
- Atténuation (facultative) : l'équipe Sécurité met en place une solution temporaire en attendant qu'une remédiation soit disponible
- Remédiation : l'équipe Sécurité apporte une solution définitive au problème

Traitement du volet « vie privée » de l'incident

L'équipe DPO mène les activités suivantes :

- Évaluer la violation : l'équipe DPO, avec les ressources nécessaires, évalue la violation. Cette évaluation doit conclure sur :
  - la catégorie de données concernée par la violation
  - le volume de données concerné par la violation
  - l'impact de la violation sur les personnes concernées
- Notification : en tant que sous-traitant, Ibexa informe le responsable de traitement dans les meilleurs délais, en lui communiquant :
  - la nature de la violation de données
  - les catégories de données concernées

    - le nombre d'enregistrements
    - le nombre de personnes concernées
    - les coordonnées de contact (DPO ou point de contact) auprès duquel des informations complémentaires peuvent être obtenues
    - les mesures prises ou proposées pour remédier à la violation de données personnelles (y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives)
- Documenter : Ibexa consigne également la violation de données détectée dans un registre des violations de données personnelles.

À tout stade d'un incident, et quelle que soit sa catégorie (sécurité et/ou vie privée), Ibexa peut faire appel à une expertise de forensique numérique afin de recueillir des preuves légales de la violation.

Clôture de l'incident

Une fois l'incident traité, une analyse « post mortem » est réalisée et documentée. Ce rapport comprend :

- L'analyse des causes profondes
- La chronologie de l'incident
- Les enseignements tirés
- Le plan d'actions

Le RSSI (CISO) s'assure que l'incident a été correctement documenté dans l'outil de ticketing. En cas de violation de données personnelles, le DPO s'assure que l'incident a été correctement consigné dans le registre des violations de données personnelles.

Transfert de données personnelles au client

Transmission automatique de données personnelles au système d'information du client

Ibexa est en mesure de transmettre les données collectées de plusieurs manières :

- Push en temps réel (REST sur HTTPS)

- Push/export FTPS
- Export vers un bucket Amazon S3

Vous trouverez plus d'informations dans cette FAQ : https://Ibexa.zendesk.com/hc/en-us/articles/360019072914-Push-export-data-to-your-CRM-Marketing-Automation-Platforms-other-MarTech-softwares

Transfert manuel de données personnelles au client

Le transfert d'exports de données en dehors d'Ibexa n'est autorisé que via une procédure stricte garantissant que le bon fichier a été reçu par le bon destinataire. Selon la classification des données contenues dans le fichier, un ou plusieurs des contrôles suivants sont activés :

- Envoi à l'adresse e-mail du destinataire d'un lien temporaire vers le fichier
- Limitation du nombre de téléchargements du fichier
- Chiffrement du fichier, avec transmission de la clé de chiffrement par un second canal sécurisé

Tous les accès (export et consultation) aux données des clients par le personnel d'Ibexa sont journalisés dans la GDPR Toolbox.

Mesures techniques pour garantir la sécurité et la protection des données personnelles

Protection des données dès la conception et par défaut

Nous mettons également en œuvre une politique de « protection des données dès la conception et par défaut » afin d'examiner systématiquement l'impact potentiel de chaque projet ou initiative sur la vie privée des personnes. Cela concerne tout particulièrement les équipes Produit d'Ibexa (qui conçoivent les nouvelles fonctionnalités) et, bien sûr, l'équipe IT.

Gestion des cookies

Les cookies et leur utilisation sont décrits dans notre « Politique de cookies », disponible sur demande à dpo@ibexa.co.

Suppression des données personnelles

Lorsqu'une demande de suppression est déclenchée depuis la GDPR Toolbox, les données personnelles concernées sont anonymisées afin d'être conservées sous forme agrégée dans le module statistique.

Cette anonymisation est propagée à toutes les instances de bases de données. Les données personnelles présentes dans nos archives sont détruites à l'issue de la durée de conservation des sauvegardes.

Tout matériel contenant des données personnelles et destiné à être mis hors service suit une procédure d'effacement sécurisé de l'ensemble de ses disques durs (à l'aide de l'outil d'effacement sécurisé hdparm) avant de quitter notre infrastructure.

Accès restreint aux données personnelles de production

Voir la section « Données de production »

Accès physique à nos bureaux

Voir la section « Sécurité physique et environnementale »

Ordinateurs

Voir la section « Les ordinateurs portables d'Ibexa »

Mesures de sécurité IT

Veuillez vous référer aux sections suivantes :

- Gestion des actifs

- Contrôle d'accès
- Cryptographie
- Sécurité physique et environnementale
- Sécurité des opérations
- Sécurité des communications
- Acquisition, développement et maintenance des systèmes d'information
- Gestion des incidents de sécurité de l'information
- Continuité d'activité et reprise après sinistre
- Conformité

Engagements contractuels avec les clients

Dans le cadre de nos engagements contractuels avec les clients, les documents suivants relatifs au RGPD sont établis :

Accords de traitement des données (DPA)

Des engagements contractuels clairs avec les clients, conformes à l'article 28, interdisant notamment à Ibexa de divulguer, d'exploiter ou de revendre des données personnelles à des tiers ;

Registre des activités de traitement

Conformément à l'article 30, paragraphe 2, du Règlement, notre registre des activités de traitement comprend :

- Nos coordonnées, ainsi que celles du responsable de traitement pour le compte duquel nous agissons et, le cas échéant, du représentant du sous-traitant et du délégué à la protection des données.
- Les catégories de traitements effectués pour le compte des responsables de traitement.

- Le cas échéant, les transferts de données vers un pays tiers, accompagnés des documents attestant l'existence de garanties appropriées pour chaque transfert.
- Une description générale des mesures de sécurité techniques et organisationnelles.

Sous-traitants ultérieurs d'Ibexa

Des engagements contractuels clairs avec les sous-traitants ultérieurs, conformes à l'article 28, afin de s'assurer qu'ils présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées, de manière à ce que le traitement réponde aux exigences du Règlement et garantisse la protection des droits des personnes concernées.

Ibexa met en place des garanties adéquates lorsqu'elle transfère des données personnelles hors de l'Espace économique européen (EEE) ou vers tout pays ne bénéficiant pas d'une décision d'adéquation. Les clauses contractuelles types de la Commission européenne (ou les autres garanties prévues à l'article 46 du RGPD) sont contractualisées. En outre, Ibexa évalue (analyse d'impact du transfert, ou TIA) si le droit ou les pratiques du pays de destination sont susceptibles de nuire à l'efficacité des garanties appropriées prévues par les outils de transfert, et identifie et adopte des mesures supplémentaires lorsque cela est nécessaire (chiffrement avec gestion des clés par Ibexa, pseudonymisation, traitement fractionné, etc.).

Lorsque cet autre sous-traitant ne remplit pas ses obligations en matière de protection des données, nous demeurons pleinement responsables de l'exécution de ses obligations.

Ibexa fait appel à des sous-traitants ultérieurs pour réaliser les activités de traitement nécessaires à la fourniture des services au client. La liste de ces sous-traitants et des activités de traitement associées figure sur la page des sous-traitants d'Ibexa, accessible depuis la GDPR Toolbox ou à l'adresse suivante : https://gdpr.Ibexaapp.com/subprocessors.

Intelligence artificielle et conformité

Le comportement agentique de la plateforme repose sur l'utilisation d'une intelligence artificielle fondée sur des grands modèles de langage (LLM). Les fonctionnalités d'IA peuvent être fournies, selon le choix du client, de deux manières :

- Un accès à plusieurs fournisseurs de LLM, fourni par Ibexa
    - Ces modèles fournis par Ibexa peuvent être opérés soit par un sous-traitant ultérieur d'Ibexa
    - Soit par des modèles LLM exploités sur les serveurs et l'infrastructure d'Ibexa
- Des clés d'API et un accès aux modèles fournis par le client

Le fournisseur du modèle LLM est visible à tout moment dans l'application. Les clients peuvent restreindre l'accès à certains fournisseurs et/ou modèles.

Principales caractéristiques de l'intégration de l'IA chez Ibexa

1. Minimisation des données :
    - Les données envoyées au modèle d'IA sont déterminées par les instructions du client et la définition de l'agent. Ibexa veille à ce que le plus petit ensemble de données pertinent pour l'activité de l'agent soit transmis au sous-traitant ultérieur.
2. Aucune donnée utilisée pour l'entraînement :
    - La clé d'API et la configuration du compte sont paramétrées de sorte que les données partagées avec le sous-traitant LLM ne soient pas utilisées pour l'entraînement ni l'affinage (fine-tuning) des modèles d'IA, ce qui garantit que les données saisies par les utilisateurs restent confidentielles et ne sont pas conservées pour améliorer les modèles.

Annexe 1 : Définitions

- « Violation de données » : une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données personnelles transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données ;
- « Responsable de traitement » : la personne physique ou morale qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données personnelles ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable de traitement peut être désigné, ou les critères spécifiques applicables à sa désignation peuvent être prévus, par le droit de l'Union ou le droit d'un État membre ;
- « Sous-traitant » : la personne physique ou morale qui traite des données personnelles pour le compte du responsable de traitement ;
- « Délégué à la protection des données » (« DPO ») : la personne chargée de superviser la stratégie et la mise en œuvre de la protection des données afin d'assurer la conformité aux exigences du RGPD ;
- « Personne concernée » : une personne physique identifiable, c'est-à-dire une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ;
- « Mesures organisationnelles » : les mesures relatives à l'environnement du système, et en particulier aux personnes qui l'utilisent ;
- « Données personnelles » : toute information se rapportant à une personne physique identifiée ou identifiable (« personne concernée ») ;
- « Traitement » : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données personnelles ou des ensembles de données personnelles, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre

forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ;

- « Autorité de contrôle » : une autorité publique indépendante instituée par un État membre en vertu de l'article 51 ;
- « Mesures techniques » : les mesures qui concernent directement le système informatique.