Mise à jour : 25 Mai 2018

indaïa

TRUST & SECURITY

Mise à jour : 25 Mai 2018

Mise à jour : 25 Mai 2018

NOTRE APPROCHE SUR LA SÉCURITÉ DES DONNÉES

La gestion des données constitue une part importante de notre activité principale et nous prenons très au sérieux la protection des données personnelles, la confidentialité et la sécurité. Ce document explique comment nous gérons les données collectées.

Nous nous sommes toujours engagés à investir dans un programme de sécurité continu et croissant depuis la création d'Indaïa, et nous nous efforçons d'aller au-delà des attentes.

Voici quelques exemples pratiques de contrôles de sécurité sur notre site Web:

- Lors de la synchronisation de périphériques avec notre application en ligne sécurisée, la communication est effectuée via HTTPS et cryptée à l'aide de TLS
- Toutes les données non essentielles sont stockées le plus rapidement possible et sont supprimées dès que possible tout en conservant toutes les fonctionnalités du site.
- L'accès des utilisateurs à Indaïa est sécurisé par un jeton d'authentification fort et complexe et les contrôles de complexité sont applicables.
- Nous investissons dans des tests de pénétration programmés à trois niveaux

GLOSSAIRE

Pour plus de clarté, voici quelques termes que nous utilisons dans notre document de sécurité, et ce qu'ils signifient:

Le Processeur	Nous, Indaïa
Le Contrôleur	Vous, votre entreprise
L'Application	Le site d'Indaïa

Mise à jour : 25 Mai 2018

PROPRIÉTÉ DES DONNÉES, UTILISATION ACCEPTABLE ET ACCÈS AUX DONNÉES COLLECTÉES

Sans ambiguïté, les données que vous collectez sont vos données et réservées uniquement à votre usage personnel.

Les données et les informations personnellement identifiables collectées via notre logiciel sont stockées pour l'usage exclusif du contrôleur.

Nous facilitons la collecte et le stockage fiables des données au nom de nos clients, et nos intentions seront toujours encadrées par ceci.

De temps à autre, certains membres du personnel technique d'Indaïa auront un accès restreint aux données que nous stockons pour votre compte afin que nous puissions effectuer les tâches de maintenance absolument nécessaires telles que le contrôle et l'amélioration de la qualité et de la performance de nos services. En aucun cas, aucun tiers ne peut accéder à vos données à d'autres fins, telles que le marketing ou la communication.

Les données ne seront jamais divulguées à des tiers, sauf en conformité avec notre politique de confidentialité. Les exceptions sont:

- Si nous, ou la quasi-totalité de nos actifs, sommes acquis ou sont en train d'être acquis par un tiers, auquel cas les Informations personnellement identifiables que nous détenons, concernant nos clients, seront l'un des actifs transférés.
- Si nous avons été légitimement invités à fournir des informations à des fins légales ou réglementaires ou dans le cadre de procédures judiciaires ou de poursuites judiciaires éventuelles.

Mise à jour : 25 Mai 2018

CONFORMITÉ ET ACCRÉDITATIONS

Travailler avec des organisations britanniques et européennes

Nous nous conformons pleinement et opérons dans le cadre de la législation britannique et européenne sur les données.

À la lumière du retrait potentiel du Royaume-Uni de l'Union européenne dans les années à venir, nous continuerons d'évaluer la situation et d'adopter la position la plus favorable à la sécurité des données que nous puissions atteindre.

Travailler avec les US, les EAU et d'autres organisations internationales

En tant qu'entreprise enregistrée en France et stockant des données au sein de l'EEE, nous sommes régis par des lois européennes qui sont généralement considérées comme plus strictes que beaucoup en dehors de la région.

Une grande partie de notre conformité couvre les exigences de base du droit des données à l'étranger, mais nous croyons que les lois européennes et la protection des droits de l'individu et la propriété des données offrent actuellement la meilleure protection des données internationalement.

Si vous n'êtes pas sûr de la manière dont cela influence votre utilisation d'Indaïa, nous vous suggérons de demander un avis juridique supplémentaire. Nous constatons généralement que les équipes de conformité trouvent la parité même lorsque nous ne respectons pas une loi étrangère spécifique.

Accréditations et certifications

Nous travaillons continuellement avec des fournisseurs de données et des organisations qui travaillent déjà dans des cadres normalisés tels que ISO 27001, et nous comprenons que vous pourriez avoir besoin de voir des accréditation dans le cadre de votre évaluation, nous avons rassemblé tous les documents pertinents directement ici. section réservée.

Indaïa s'efforce de respecter ses propres premières normes internationales. Notre approche actuelle consiste donc à fournir notre propre corps de documents et de politiques qui répondent aux exigences des organisations qui respectent ces normes.

Nos données sont stockées dans des installations certifiées et notre infrastructure s'appuie sur des services certifiés.

Enregistrement auprès de la Commission nationale de l'information (CNIL)

Nous sommes membres du registre de la protection des données de la CNIL en France et notre numéro d'enregistrement est [2109824v0].

Mise à jour : 25 Mai 2018

La relation entre Vous et Nous

CE QUE LA CNIL DIT	EN FRANCAIS
Le contrôleur recueille et traite les données personnelles dans le cadre de ses activités commerciales ou personnelle.	Vous utilisez Indaïa avec vos propres données afin d'acheter un produit.
Le processeur traite les données personnelles pour le compte d'autres entreprises et organisations.	Nous gérons ces données pour vous.
L'article 17, paragraphe 2, de la directive 95/46 / CE sur la protection des données prévoit que, lorsque le traitement des données à caractère personnel est effectué par un sous-traitant pour le compte d'un contrôleur, celui-ci doit choisir un sous-traitant. les mesures et les mesures organisationnelles régissant le traitement à effectuer et doivent assurer le respect de ces mesures;	Il est de votre responsabilité de vous assurer que nos normes sont suffisantes pour répondre à vos obligations légales et aux normes de votre organisation. Nous sommes toujours prêts à essayer de vous aider à remplir toutes les obligations de données nécessaires pour utiliser notre logiciel.
L'article 17, paragraphe 3, et l'article 17, paragraphe 4, de la directive sur la protection des données exigent que le traitement effectué par un sous-traitant pour le compte d'un contrôleur soit régi par un contrat ou un acte juridique liant le sous-traitant au le processeur ne doit agir que sur instructions du contrôleur et doit se conformer aux mesures de sécurité techniques et organisationnelles requises par la législation nationale pour protéger les données personnelles contre la destruction accidentelle ou illicite ou la perte accidentelle, l'alternance, la divulgation ou l'accès non autorisé et contre toutes les autres formes illégales de traitement;	Nous gérons les données conformément aux accords que nous allons conclure avec vous. Ceux-ci sont décrits dans nos politiques de confidentialité et termes & conditions lorsque vous vous inscrivez ou commencez à utiliser nos produits. Il est de notre responsabilité de mettre en place des mesures pour sécuriser les données personnelles que vous stockez avec nous.
Le Processeur prend toutes les mesures pour protéger les Données Personnelles traitées par le Processeur au nom du Contrôleur contre un Incident de Sécurité et contre toutes les autres formes illégales de traitement, comme l'exige la législation nationale applicable.	Nous sommes tenus de mettre en place des mesures pour protéger les données que nous stockons en votre nom au niveau de l'organisation, du serveur et de l'application.

Mise à jour : 25 Mai 2018

VIE DES DONNÉES ET ÉLIMINATION

Vie des données, conservation et protection

Les données associées à votre compte Indaïa (y compris les informations personnelles et les données collectées) sont conservées tant que vous disposez d'un compte Indaïa et pour une durée plus longue que celle prévue par la loi.

Nous n'annulons pas les comptes pour inactivité.

Vous pouvez supprimer vos données du site à tout moment.

- Les données supprimées de cette manière seront rendues inaccessibles mais ne seront pas supprimées de manière permanente - une «suppression en douceur», tel que permis par la loi.
- Nous ne conservons vos données que pour nous permettre de les récupérer si vous les supprimez accidentellement.
- Nous finissons par effacer définitivement les anciennes données supprimées pour récupérer de l'espace de stockage, nous ne pouvons pas garantir que nous serons en mesure de restaurer les données supprimées.
- Nous n'utilisons les données supprimées que pour vous permettre de les restaurer. Parfois, nous pouvons conserver des données supprimées pour nous conformer à nos obligations légales, résoudre des litiges ou faire respecter nos accords. Dans ces cas, nous nous assurons que l'accès à ces données est bloqué, sauf aux fins pour lesquelles nous avons été tenus de conserver les informations.
- Il est de la responsabilité du client d'exporter et d'archiver les données avant la fin de la période de 12 mois car nous ne sommes pas un service d'archivage de données, mais cette période de 12 mois est conçue pour éviter toute mauvaise surprise.

Suppression permanente

Pour supprimer définitivement les données du site Web d'Indaïa, cliquez sur le bouton Supprimer et confirmez. Une fois supprimé de votre compte, vous pouvez nous contacter pour demander une suppression permanente des données supprimées.

Copies de sauvegarde

Les copies résiduelles des données supprimées de votre compte peuvent rester sur les supports de sauvegarde, comme le permet la loi. Ces données disparaissent généralement après 12 mois, car les anciens supports de sauvegarde sont remplacés par des sauvegardes plus récentes, ce qui entraîne une suppression totale, permanente et irrécupérable.

Gestion et élimination du matériel

Les équipements informatiques et les supports de stockage sont détruits sans aucune réparation en fin de vie. Notre fournisseur d'hébergement déchiquette le matériel en fin de vie (bien que nous ne soyons pas en mesure de fournir une certification pour chaque matériel), et nous utilisons un effacement sécurisé ou détruisons tout support de stockage que nous utilisons au sein de la société.

Tout le matériel informatique et les périphériques sont émis de manière centralisée et sont enregistrés dans notre système central de gestion des actifs.

Mise à jour : 25 Mai 2018

SERVEURS ET LIEU PHYSIQUE

Emplacement du centre de données

Le Data Center est situé à Roubaix en France et est exploité par OVH. OVH détient les accréditation liées à la sécurité suivantes.

ISO/IEC 27001 - Security Management
ISO 22301 - Business Continuity Management
ISO 9001 - Quality Management
ISO 27017 - Cloud security
ISO 27018 - Cloud confidentiality
SSAE16/ISAE 402 TypeII (SOC 1, SOC 2, SOC 3)

Physical security

Le centre de données implémente les contrôles d'accès suivants dans ses locaux et installations:

- Entrée sécurisée surveillée par présence humaine.
- Système d'accès par carte biométrique et uniquement pour employés accrédité d'OVH
- Sécurité humaine 24/7/365
- Des pare-feu et des listes de contrôle d'accès sont en place pour séparer le réseau sécurisé des réseaux non fiables externes
- L'accès administratif est limité aux seuls employés de OVH qui ont besoin de ce niveau d'accès et une séparation physique et logique est en place pour empêcher l'accès aux réseaux internes / de confiance.
- Les tiers, c'est-à-dire les sous-traitants ou les fournisseurs qui ne sont pas entièrement contrôlés par l'hôte, n'ont pas de niveau de système d'exploitation ou d'accès physique à l'infrastructure.
- IDS, IPS et la journalisation sont en place et surveillés 24h / 24 et 7j / 7 pour les alertes

Comment les données personnelles entrent dans notre site

Les données personnelles entrent dans Indaïa lorsqu'une personne entre volontiers ses coordonnées sur notre site internet.

Mise à jour : 25 Mai 2018

SERVICES TIERS

Certaines de nos fonctionnalités facultatives premium ou personnalisées nécessitent l'utilisation de services tiers en dehors de l'EEE. Lorsque nous devons travailler avec des sous-traitants ou des services de données situés dans d'autres juridictions, nous préférons travailler avec des entreprises opérant dans le cadre de régimes soutenus par le gouvernement tels que le bouclier Privacy Shield (anciennement Safe Harbor).

Dans la mesure du possible, nous visons toujours à anonymiser les données (en les découplant de la source) lors du transfert de données à des tiers.

Nous travaillons continuellement et avec succès avec des tiers qui travaillent déjà dans des cadres normalisés et nous comprenons que vous pourriez avoir besoin de voir des accréditations dans le cadre de votre évaluation.

"Privacy Policy" - Stripe
"Privacy Policy" - Paypal
"Privacy Policy" - PrestaShop

Mise à jour : 25 Mai 2018

ÉCHEC DE SAUVEGARDE ET CATASTROPHES

Serveurs

- Les serveurs ont un onduleur avec des générateurs diesel de secours
- Des ingénieurs formés sur place 24/7/365 qui peuvent effectuer:
  - Échange de pièces
  - Diagnostic d'erreur
  - Résolution de problèmes logiciels - pour les serveurs, commutateurs, pare-feu et routeurs
  - Installation du serveur et racking

Calendrier de sauvegarde

- Nous effectuons des sauvegardes de données horaires qui sont archivées pendant une semaine
- Nous effectuons des sauvegardes de données quotidiennes qui sont archivées pendant un an
- Nous effectuons des sauvegardes hebdomadaires de données qui sont archivées pendant une semaine
- Les sauvegardes horaires, quotidiennes et hebdomadaires sont stockées de manière redondante sur nos serveurs OVH.
- Nous exécutons la réplication de base de données en continu en temps réel au sein du même réseau privé virtuel
- Les sauvegardes plus anciennes expirant sont remplacées cycliquement par des sauvegardes plus récentes

Veuillez noter que nos activités ne doivent pas servir de service de sauvegarde et d'archivage dédié. Nous encourageons donc nos clients à faire preuve de bon sens et à prendre des mesures raisonnables pour prendre leurs propres dispositions de sauvegarde en plus des mesures que nous prenons.

Récupération après sinistre et résilience

Notre programme de sauvegarde complet et notre sauvegarde redondante, versionnée et distribuée signifient qu'en cas de perturbation majeure, nous sommes en position de force pour récupérer les données les plus récentes et remettre les serveurs dans un état opérationnel.

Nos applications mobiles et tablettes fonctionnent en mode déconnecté lorsqu'il n'y a pas de bonne connexion avec notre serveur. Par conséquent, si les applications hébergées sur le serveur principal sont hors ligne, cela n'affectera pas les données non synchronisées sur les applications.

Mise à jour : 25 Mai 2018

POLITIQUES

Politique de violation de la confidentialité et d'assainissement

Tout incident de violation de la confidentialité entourant les données collectées est enregistré de manière centralisée et revu tous les trimestres. Des remédiations seront proposées et les délais de mise en œuvre seront convenus et consignés dans le journal.

Rôles du personnel et audit des privilèges

- Nous effectuons un programme annuel de certification programmée, enregistrée et signée des privilèges de l'utilisateur pour vérifier les autorisations correctes et corriger toute incohérence
- Nous effectuons un calendrier trimestriel des enquêtes enregistrées sur les privilèges des utilisateurs pour les personnes disposant de droits d'administrateur afin de vérifier les autorisations correctes et de corriger toute incohérence

Politique d'escalade du privilège du personnel des urgences

Si jamais nous devions accorder des privilèges d'urgence au personnel interne ou externe pour quelque raison que ce soit, cette action est enregistrée dans notre journal d'accès d'urgence avec un raisonnement complet. Nous enregistrons également lorsque ces privilèges sont révoqués.

Politique de JML (Joiners, Movers and Leavers) sur l'accès aux données

Les privilèges du personnel sont assignés à leurs rôles spécifiques par les cadres supérieurs, et revus lorsque l'emploi cesse ou quand ils changent de rôle.

Lorsqu'un collaborateur quitte son emploi chez Indaïa, nous désactivons l'accès aux comptes du personnel dès que nous le pouvons physiquement, ce qui est généralement immédiat. Cette désactivation se produit toujours dans les 48 heures suivant la fin de leur emploi. Les comptes sont supprimés dans les 30 jours. Tous les changements de rôle sont enregistrés.

Politique de sécurité réseau

Tous les nouveaux composants de niveau système installés avec les paramètres par défaut du fournisseur sont réinitialisés à l'avance pour supprimer le risque de valeurs par défaut non sécurisées.

Tous les composants, protocoles, services et fonctions redondants sont arrêtés et supprimés dès que cela est techniquement possible.

Les journaux d'audit sont établis pour une période d'au moins un an, les trois derniers mois devant rester immédiatement disponibles.

Mise à jour : 25 Mai 2018

Politique de gestion du changement et de changement

Change Control fournit une manière ordonnée de modifier les processus clés chez Indaïa. Cela signifie notifier toute personne affectée par le changement, et écouter la réponse si le changement affecte négativement les membres de l'équipe ou les clients. Cela signifie également concevoir des plans d'urgence raisonnables pour restaurer le système si un changement ne fonctionne pas.

En utilisant une série de procédures et d'actions standardisées et répétables, nous sommes en mesure d'introduire des changements dans l'infrastructure Indaïa de manière à minimiser tout impact négatif

Cette politique décrit le processus à utiliser pour demander et gérer ces changements. Les rôles clés spécifiques au processus de contrôle des modifications sont les suivants. Un individu peut être responsable de plusieurs rôles et plusieurs individus peuvent jouer un rôle unique.

ROLE	DESCRIPTION
Change Control Manager	Le gestionnaire de contrôle des modifications gère le processus pour toutes les demandes et examine chaque demande pour s'assurer qu'elle est complète. Change Control Manager vérifie que les objectifs déclarés de la demande peuvent être atteints et sont conformes aux meilleures pratiques de l'entreprise. Le gestionnaire de contrôle des modifications a la possibilité de refuser les demandes qui ne sont pas conformes aux règles de l'entreprise ou aux meilleures pratiques.
Change Requestor	Le demandeur de changement lance la demande en soumettant une modification au gestionnaire de contrôle des modifications.
Change Implementer	Le responsable de la mise en œuvre apporte les modifications nécessaires et informe les autres parties concernées si des modifications correspondantes doivent être apportées. Les modifications sont implémentées dans la production par le responsable de la mise en œuvre du changement.

Mise à jour : 25 Mai 2018

Politique de classification des données et informations

Tous les membres de l'équipe Indaïa partagent la responsabilité de s'assurer que les informations que nous gérons bénéficient d'un niveau de protection approprié en observant cette politique de classification des informations:

- Les gestionnaires ou les «propriétaires» des informations sont responsables du choix des classifications des informations selon le système de classification des informations ci-dessous.
- Dans la mesure du possible, la catégorie d'information doit être intégrée dans l'information elle-même
- Tous les membres de l'équipe doivent utiliser les catégories d'informations dans le traitement des informations sur la société liées à la sécurité

Toutes les informations appartenant à la société et les informations qui nous sont confiées par des tiers relèvent de l'une des quatre classifications suivantes:

CATEGORIE	DESCRIPTION	EXAMPLES
Public non classifié	L'information n'est pas confidentielle et peut être rendue publique sans aucune implication pour Indaïa, la perte de disponibilité due aux temps d'arrêt du système est un risque acceptable, l'intégrité est importante mais pas vitale.	• L'information de marketing produit largement distribué • Informations largement disponibles dans le domaine public, y compris publiquement disponibles sur le site Web • Logiciel d'essai • Rapports financiers requis par les autorités de réglementation • Bulletins d'information pour le marketing externe
Propriétaire	Les informations exclusives sont réservées à un accès interne approuvé par la direction et protégées contre tout accès externe Un accès non autorisé pourrait influencer l'efficacité opérationnelle d'Indaïa, entraîner une perte financière importante, apporter un gain significatif à un concurrent ou provoquer une baisse importante de la confiance des clients. l'intégrité est vitale.	• Mots de passe et informations sur les procédures de sécurité de l'entreprise • Savoir-faire utilisé pour traiter les informations client • Procédures Opérationnelles Standard utilisées dans toutes les activités d'Indaïa • Tous les codes logiciels développés par l'entreprise, qu'ils soient utilisés en interne ou vendus à des clients

CATEGORIE	DESCRIPTION	EXAMPLES
Données confidentielles du client	Informations reçues des clients sous quelque forme que ce soit pour traitement en production par Indaïa. La copie originale de ces informations ne doit en aucun cas être modifiée. Les niveaux d'intégrité, de confidentialité et de disponibilité restreints les plus élevés sont essentiels.	• Données collectées par les clients • Transmissions électroniques des clients • Informations sur le produit générées pour le client par les activités de production Indaïa telles que spécifiées par le client
Données confidentielles de l'entreprise	Les informations collectées et utilisées par Indaïa dans la conduite de son activité pour embaucher, enregistrer et répondre aux demandes des clients, et gérer tous les aspects du financement de l'entreprise L'accès à ces informations est restreint au sein de l'entreprise. la confidentialité et la disponibilité restreinte sont vitales.	• Données comptables et rapports financiers internes • Données commerciales confidentielles des clients et contrats confidentiels • Accords de non-divulgation avec les clients et les fournisseurs • Salaires et autres données personnelles • Plan d'entreprise de l'entreprise

Email, médias amovibles et politique de transfert de données client

Notre politique est que les données confidentielles du client ne doivent pas être envoyées par courrier électronique ou par un service de communication électronique accessible au public sans être cryptées au préalable avec un mot de passe sécurisé conforme à nos règles de mot de passe internes. Les données ne doivent être transitées de cette manière que lorsque les autres méthodes d'orientation interne ne sont pas disponibles. Les mots de passe doivent être transmis par un support non associé autre que le support de transmission des fichiers, par exemple par appel téléphonique.

Nous n'autorisons généralement pas le stockage ou le transfert de données confidentielles du client sur des supports amovibles tels que des clés USB et des disques durs externes. Si cela est nécessaire ou inévitable, ces données transférées ou stockées sur un support amovible doivent être cryptées avec un mot de passe sécurisé conforme à nos règles de mot de passe internes.

Politique de signalement d'incidents de sécurité et de violation

Nous maintenons un système de reporting centralisé, rapide et sécurisé pour la communication de tous les problèmes de sécurité et de confidentialité. Si un problème de sécurité ou de confidentialité est soulevé, un directeur de l'entreprise est immédiatement notifié pour coordonner l'évaluation et la réponse nécessaire, et la nature de l'incident est enregistrée avec les détails, qui est impliqué, les actions prises et les propositions d'action future.

Si cela devait être considéré comme significatif au cours de cette évaluation, nous communiquons la nature de l'incident de sécurité ou de la violation aux parties concernées, y compris les clients dès que nous le pouvons dans le contexte de la situation et d'une manière qui n'excite pas l'aggravation de la question.

Nous informerons également les autorités compétentes dès que possible.

Mise à jour : 25 Mai 2018

Politique de bureau propre

Nous menons une politique de bureau propre chez Indaïa. Nous n'imprimons pas du tout les copies phy- siques des données client si nous pouvons l'éviter car nous sommes avant tout une opération numérique, mais dans de rares cas où nous devrons traiter de tels documents, ces éléments seront stockés dans des armoires verrouillées. le bureau pendant la nuit et détruit en toute sécurité sur place lorsqu'il n'est plus nécessaire.

Mise à jour de logiciels

Les mises à jour d'application sont gérées avec un flux de contrôle de version formalisé et passent par un processus de test de l'équipe de développement, des tests internes plus larges (automatisés et humains) et des tests de pré-lancement avec la base de données en ligne.

Le déploiement final d'une mise à jour d'application est automatisé et la migration vers une nouvelle version ne nécessite aucune indisponibilité perceptible par l'utilisateur.

Nous mettons à jour nos serveurs avec de nouveaux correctifs sur une base mensuelle. Nous surveillons également les vulnérabilités critiques du jour zéro et implémentons les correctifs dans les 24 heures ou plus tôt lorsqu'un correctif est disponible.

Plus d'informations sont disponibles dans notre document sur le cycle de vie du développement.

Calendrier d'examen des politiques

Nous passons en revue toutes nos politiques internes selon les besoins, et également sur une base annuelle.