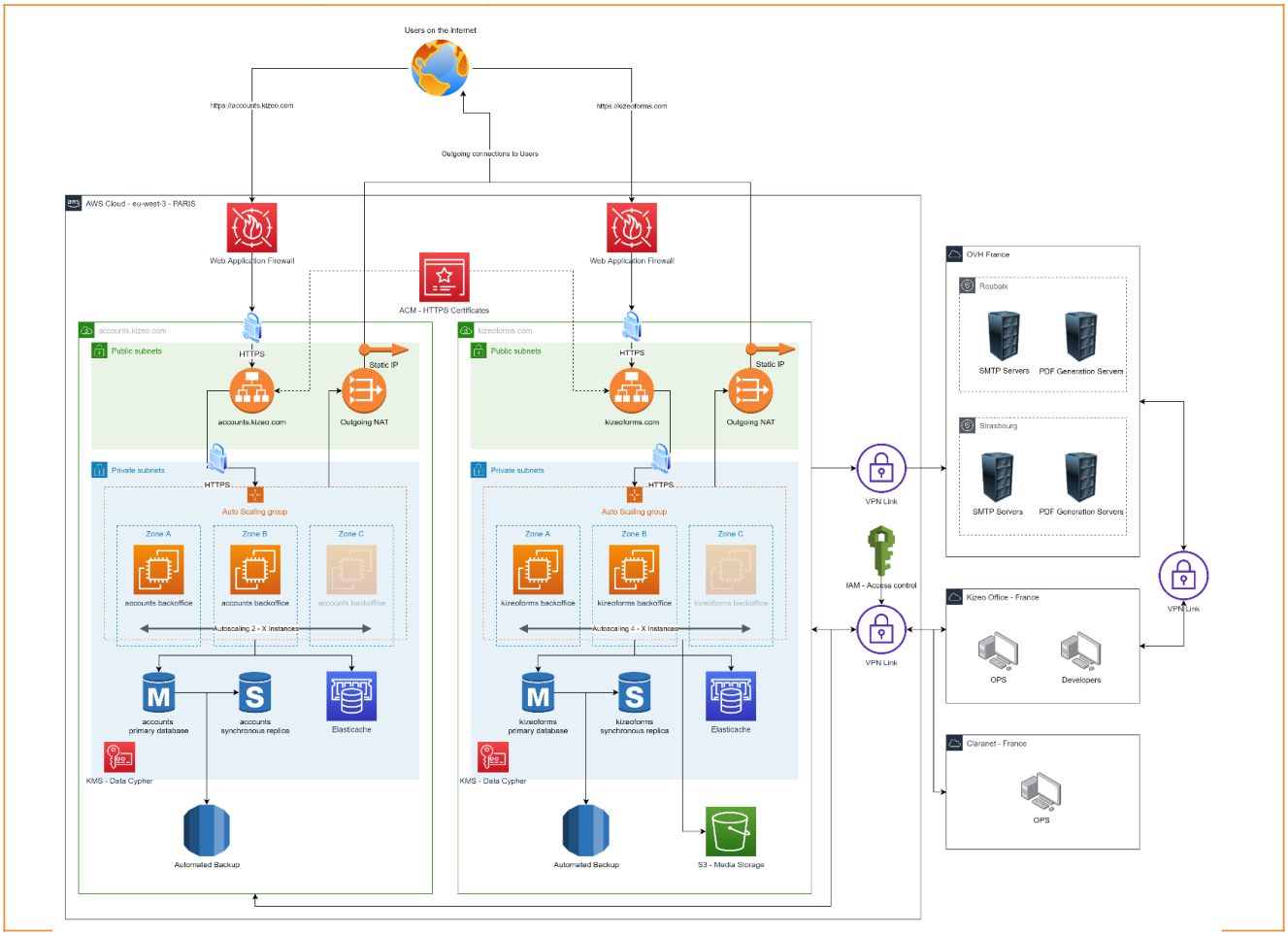
Document de sécurité Kizeo
Produit : Kizeo Forms

Point Version actuelle	Conforme juin 2020	Remarques
Sécurité organisationnelle		
Nos employés		
Responsable sécurité	Oui	Philippe Gellet (Président) Vincent Demonchy (Directeur Technique)
Attestation de confidentialité	Oui	Tous nos collaborateurs ont signé un accord de confidentialité et de non-divulgation.
Confidentialité (extérieurs)	Oui	Toute personne amenée à avoir accès partiellement ou intégralement à vos données doit signer un accord de confidentialité et de non-divulgation.
Accès aux données des clients	Oui	Afin de vous accompagner lors d'une demande de support, nous pouvons avoir besoin d'accéder à vos données. Par défaut nous vous demanderons toujours un accord verbal ou écrit. Vous pouvez cependant nous demander de stipuler forcément un accord écrit.
Certifications *Pour l'instant, Kizeo ne prévoit pas d'effectuer de certifications. Néanmoins, nous prenons soin de travailler avec des prestataires eux-mêmes certifiés lorsque les données de nos clients sont impactées.*		
Sécurité	Non-certifié	Bien que notre infrastructure ait été réalisé en conformité avec le référentiel ISO/CEI 27001
Organisation	Non	
Hébergement des données		
Localisation des données *Toutes nos données sont stockées sur trois datacenters en France. La transmission des données entre les différents sites et avec les appareils de nos clients (mobile / ordinateur) est chiffrée.*		
Localisation en France	Oui	Datacenters AWS Paris (3 sites différents) Datacenters Roubaix/Strasbourg OVH
Localisation hors de France	-	Kizeo peut étudier cette demande.
Transfert des données chiffré entre les différents sites	Oui	
Transfert des données dans une	Oui	
Transfert des données chiffré avec les appareils clients	Oui	TLS 1.2 par défaut. TLS 1.0 pour les très vieux appareils (va probablement bientôt être abandonné complêtement).
Hébérgement	SAAS	Kizeo est une solution SaaS, cela signifie que nous gérons l'hébergement de la solution pour le client.
Serveurs dédiés (infra Kizeo)		Soumis à conditions commerciales
Prestataires *Afin d'assurer le meilleur service à nos clients, nous travaillons avec différents prestataires Voici ceux impliqués dans l'hébergement de leur données.*		
AWS		**Hébergeur principal**
ISO/CEI 27001 : 2013	Oui	
ISO 27017	Oui	
ISO 27018	Oui	
SOC 1	Oui	
SOC 2	Oui	
SOC 3	Oui	
PCI DSS 1	Oui	
HDS	Oui	

OVH		**Hébergeur**
ISO/CEI 27001 : 2013	Oui	Offre dedicated cloud
SOC 1 type II (SSAE 16 et ISAE	Oui	Private cloud
SOC 2 type II	Oui	Private cloud
Claranet		**Infogérance**
ISO/CEI 27001 : 2013	Oui	Applicable à l'ensemble des activités d'infogérance. Directement répercuté sur Kizeo pour assurer : - une garantie de sécurité vis-à-vis des dernières failles de sécurité - une maîtrise de la confidentialité, de l'intégrité et de la disponibilité de l'information - un suivi des incidents de sécurité.
HDS	Oui	https://www.claranet.fr/certification-hds
Réversibilité *Kizeo met en place un certain nombre d'outils afin de permettre la réversibilité des données stockés sur nos serveurs. L'ensemble de ces outils sont suffisants pour exporter les données dans des formats ré-exploitables.* *La conformité implique que nos clients soient capables d'extraire les informations dans suffisament de formats différents et de manière autonome.*		
Données	Oui	Le client est indépendant pour récupérer : - Exportations (.pdf, .docx, .xlsx, .csv) - Base de données (Access, MariaDB, PostgreSQL, SQL Server, Mysql) On peut également fournir sous ce format : - XML -JSON
Médias	Oui	Le client peut récupérer les médias depuis le back-office, le connecteur de base de données, le Web Service, par FTP, par DropBox.
Listes externes	Oui	Par Web Service (format textuel brut) Directement sur le back-office (format .xlsx)
Utilisateurs	Oui	Par Web Service (client autonome) Format .xlsx ou .csv fourni par Kizeo
Groupes	Oui	Par Web Service (client autonome) Format .xlsx ou .csv fourni par Kizeo
Formulaires	Oui	Format JSON par Web Service
Informations utiles au SI pour votre bon fonctionnement *Voici les informations utiles pour vos SI, comprenant notamment les adresses IP succeptibles d'être demandées.*		
Domaines à autoriser en HTTPS		Strict minimum : Tous les domaines ***.kizeoforms.com** Le domaine **accounts.kizeo.com**
IP entrantes ?		Kizeo communiquera toujours en HTTPS, même via Web Service, cela veut dire que nous maintenons un certificat à jour assurant notre identité lors des échanges. Afin de garantir la meilleure qualité de service, Kizeo ne recommande pas de faire du filtrage IP en entrée, mais par noms de domaine. En effet pour prévenir les pannes sur nos répartiteurs de charges, les adresses IP d'entrée peuvent changer.
Infrastructure		



Gestion des données sensibles (inc. RGPD)		
Données sensibles récoltées par Kizeo.		
Mots de passe utilisateurs	Oui	Empreinte du mot de passe seulement (hashés + salt)
Géolocalisation	Oui	Uniquement si le client en fait l'usage dans ses formulaires.
Email	Oui	3 jours de rétention dans nos logs (uniquement si envoyés par Kizeo Forms)
Note : De par le fonctionnement de Kizeo Forms, par défaut, nous ne récoltons pas d'informations sensibles. Cependant, la liberté de configuration de notre produit implique que vous êtes dans la capacité de stocker des informations sensibles à notre insu. Il est de votre devoir de faire toutes les déclarations nécessaires et d'utiliser la palette d'outils que nous mettons à votre disposition afin de respecter les normes en vigueur dans votre région.		
Note (Listes externes) : Le principe même des listes externes est de diffuser un grand nombre d'information sur un sujet à vos utilisateurs pour simplifier les saisies de ceux-ci. Attention cependant à ne pas les utiliser afin de stocker et diffuser des données personnelles qui ne seraient pas justifiées par votre activité professionnelle (email, géolocalisation).		
Conformité relatives aux données médicales *AWS est entièrement compatibles HDS (France/Europe) et HIPAA (US).* *Kizeo n'est pas certifié, mais notre infrastructure a été conçu pour l'être.*		
Récolte par Kizeo	Aucune	Aucune donnée médicale n'est récoltée par Kizeo.
HDS (France/Europe)	Non-certifié	Kizeo ne possède pas l'agrément HDS, **mais notre infrastructure a été conçu pour l'être.**
HIPAA (USA)	Non-certifié	Kizeo ne possède pas l'agrément HIPAA, **mais notre infrastructure a été conçu pour l'être.**
Politique de mot de passe et sécurité des comptes clients		
Validité token mobile	1 jour	

Complexité configurable	Oui	Sous forme d'expression régulière
Péremption	Non	
Double authentification	Oui	
Azure Active Directory (OAuth)	Oui	
SAMLv2	Non	
OpenId Connect	Oui	
OAuth2	Oui	
LDAP (conn. directe)	Non	Nous avons dépreciée cette fonctionnalité au profit d'Azure AD, plus
Restriction d'IP	Non	Prévu
Anonymisation des donnnées *Kizeo ne vous empêche pas d'anonymiser vos utilisateurs s'ils sont amenés à renseigner des informations personnelles à leur sujet.* *Si vous récoltez des données sensibles sur des citoyens de l'union européenne, vous devez vous assurer que ceux-ci ne soient pas identifiables.*		
Possible	Oui	
Chiffrage des champs sensibles	Oui	**Toutes les données Kizeo sont chiffrées (repos + transit)**
Droits		
Accès	Oui	La donnée peut être accédée par la personne l'ayant saisie
Edition/Rectification	Oui	On peut autoriser la modification des données
Droit à l'oubli	Oui	L'effacement des données est possible
Effacement définitif	Oui	Automatisable par Web Service
Restriction	Oui	La visibilité de la donnée est paramétrable en fonction de nos tables de droit
Portabilité	Oui	Formats : XLSX / CSV / XML / JSON / DOCX / PDF / XLSX / Bases de données Via : FTP / Dropbox / Web Service / IHM / Connecteur
Traçabilité *Continuellement, nous améliorons grandement les outils de traçabilité disponibles pour les administrateurs.*		
Utilisateur : Connexion	Oui	Accessible à Kizeo seulement (rétention 1 mois)
Utilisateur : Droits d'accès	Oui	
Utilisateur : Edition	Oui	
Utilisateur : Suppression	Oui	
Données : Accès	Oui	
Données : Export	Oui	
Données : Edition	Oui	
Données : Suppression (soft)	Oui	Depuis les IHM ou Web Service
Données : Suppression (hard)	Oui	Par Web Service
Formulaires : Edition	Oui	
Formulaires : Suppression	Oui	
Formulaires : Droits d'accès	Limité	On trace le changement mais pas l'information de ce qui est changé
Listes externes : Edition	Oui	
Listes externes : Suppression	Oui	
Durée de rétention		
Sauvegardes	30 jours	
Logs	30 j. à 3 mois	
Informations pour traçabilité	1 mois à 5 ans	
Données (fin de contrat)	2 ans	Réductible à 3 mois. Cette durée de rétention est pour protéger les données des clients avec un usage saisonnier de Kizeo.
Données (soft deleted)	6 mois	Afin de prévenir une erreur de manipulation

Sécurité physique des locaux

Impact
Nos locaux n'ont pas d'impact sur la sécurité des données de nos clients. En effet, rien n'est stocké au sein de ceux-ci. Tous nos ordinateurs sont protégés par mot de passe et tout élément clé permettant l'accès aux données de nos clients est chiffré.
En cas de vol d'un équipement important, il serait très simple de révoquer les clés stockées sur celui-ci. De plus, le nombre d'équipements concernés est limité au strict minimum.

Données physiques	Oui	Kizeo ne garde pas de données clients physiquement dans ses locaux.
Clés SSH chiffrées	Oui	
Contrôle des accès		
Accès global au site	Oui	Système de clés de sécurité et d'alarmes
Accès spécifiques	Oui	
Télésurveillance	Oui	Caméras à l'entrée
Vitesse d'intervention	Oui	Intervention en moins de 30 minutes en cas d'alarme
Identification	Oui	Clé électronique personnellement identifiable

Sécurité du SI

Gestion des sauvegardes
Nos sauvegardes "froides" sont stockées sur le site de Strasbourg (OVH). Elles ne sont accessibles qu'aux responsables techniques de Kizeo.
Les sauvegardes "courte-durée" sont stockées dans la même infrastructure que la solution Cloud qui est accessible aux responsables techniques de Kizeo et aux équipes d'infogérance d'Claranet certifiées ISO 27001.

Site séparés géographiquement	Oui	Trois sites différents géographiquement distincts en France
Accès	Oui	Philippe Gellet (Président) Vincent Demonchy (Directeur Technique)
Chiffrées	Oui	

S.I. solution Cloud
Nous bénéficions de l'ensemble des solutions disponibles pour garantir la stabilité de notre réseau chez AWS (incluant Firewall, réseaux Vrack privés, protections anti-DDOS). Claranet, en sa qualité de prestataire d'infogérange nous assure une veille permanente et une action rapide sur les actions à mener pour maintenir un niveau de sécurité optimal face aux failles de sécurité.

Anti-DDOS	Oui	Fourni par AWS
Firewall	Oui	
Anti-virus	Oui	Serveurs Windows : Oui Linux : Non, mais infogérance chargée du suivi des failles et de leurs corrections rapides.
Intrusions	Oui	IPs whitelisting, Firewall, VPN

S.I. Interne à Kizeo
Cette section concerne les ordinateurs de nos employés

Anti-DDOS	Non	
Firewall	Oui	
VPN	Oui	
Antivirus	Oui	Sur tous les postes
Portable	Oui	
Mots de passe	Oui	Rotation trimestrielle
Protections des accès		
Clés SSH d'au moins 2048 bit	Oui	
Clés SSH chiffrées	Oui	
Restrictions des droits d'accès	Oui	Equipes techniques : Pas accès Responsables techniques : Accès en modifications Claranet : Accès en modifications
Audits de sécurité		
Tests de pénétration réguliers	Oui	Tous les 6 mois

Publication des résultats	Oui	Une fois par an

SLA		
SLA Back-Office Kizeo Forms	99.8%	Annuel

Plan de continuité		
PCA sur trois sites *Depuis Mars 2018, Kizeo Forms repose sur un PCA (contre un PRA précédemment) basé sur les sites géographiques d'AWS. Cela a pour but de faciliter la reprise si l'un des trois datacenters tombe.*		
Redondance géographique	Oui	Fonctionnement permanent sur 3 sites géographiques