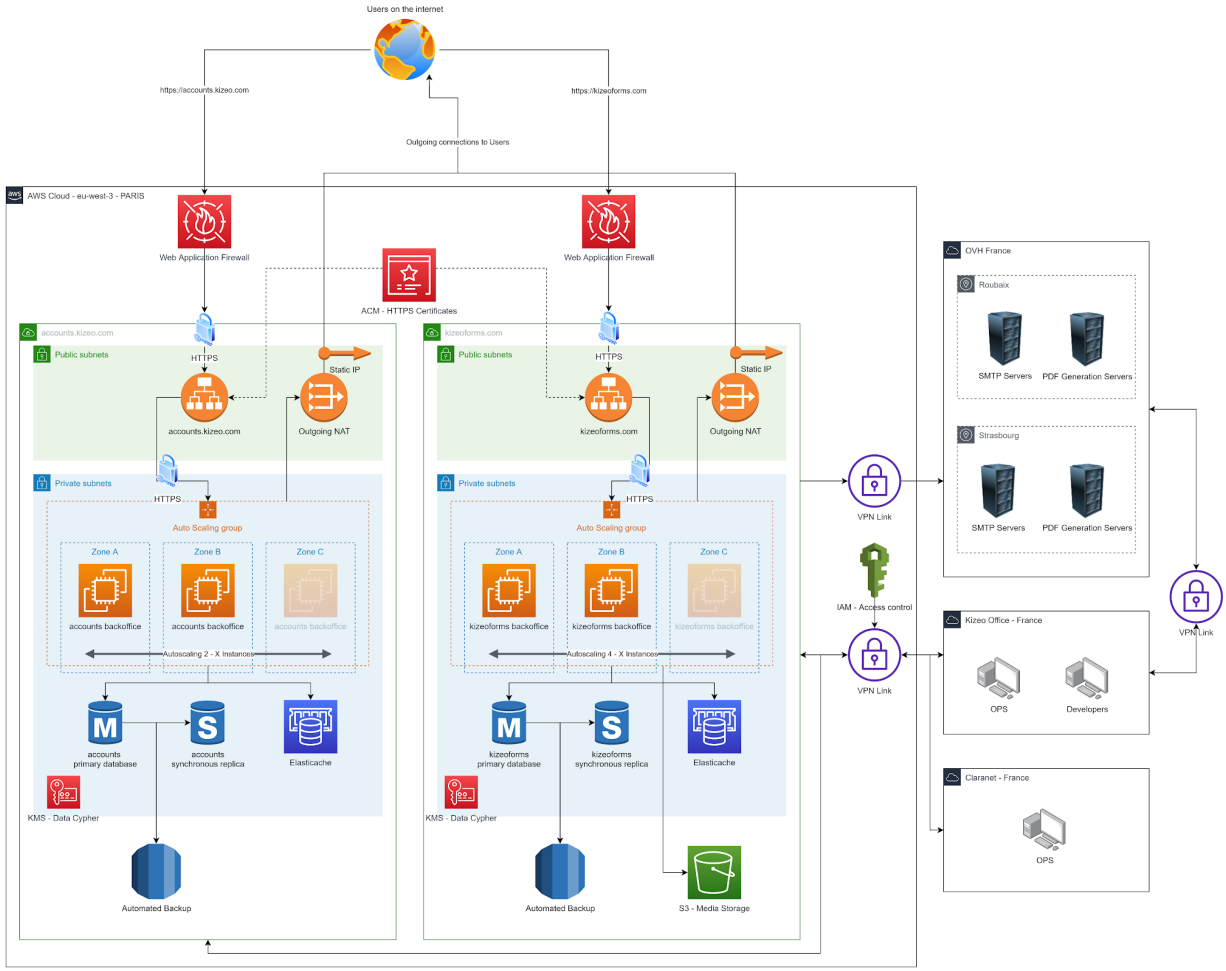
Kizeo security document

Current version	April 2022	EN
Point	**Conformity**	**Complementary note / comments**
Organisational Security		
Our employees		
Security managers	Yes	Philippe Gellet (CEO) Vincent Demonchy (CTO)
Non-divulgation	Yes	All of our employees has signed a confidentiality and non-divulgation agreement.
Non-divulgation (externals)	Yes	Every third-party person who will work with or for Kizeo requiering a partial access to our data has to sign a confidentiality and non-divulgation agreement.
Access to customers' data	Yes	For support purpose, we may need to have access to your data. By default, we will always ask you for verbal or written agreement. You can request us to have a mandatory written agreement.
Certifications *For the moment, Kizeo does not plan to get certified. Nevertheless, we only work with ISO/CEI 27001 certified third-party partners when our customers' data is involved.*		
Security	Not certified	But our infrastructure was designed according to ISO/CEI 27001.
Organisation	No	
Data hosting		
Localisation *All data are stored in multiple datacenters in France. Every transmission between datacenters and external devices (browsers, mobile apps) are secured.*		
Hosting in France	Yes	In datacenters localised in Paris / Roubaix / Strasbourg / Gravelines
Hosting outside of France	-	Kizeo can consider this request depending on the situation.
Encrypted transfers inside Kizeo system	Yes	
Transfers inside Kizeo system go throught in private network	Yes	
Encrypted transfer between Kizeo and customer's devices.	Yes	**Global: TLS 1.2 by default** **Kizeo Forms: TLS1.0 is only used with oldest devices/browsers (it may change soon).**
Hosting	SAAS	Kizeo is a SaaS solution, this means we manage the infrastructure for our customers.
Dedicated servers (managed by Kizeo)		Under some commercial restrictions.
Providers *With the purpose of garanteing the best services, we work with some third-party providers. Here are the ones implied in the hosting and the security of your data.*		
AWS		**Main hosting service**
ISO/CEI 27001 : 2013	Yes	https://aws.amazon.com/fr/compliance/programs/
ISO 27017	Yes	
ISO 27018	Yes	
SOC 1	Yes	
SOC 2	Yes	
SOC 3	Yes	
PCI DSS 1	Yes	
HDS	Yes	
BSI-C5	Yes	Equivalent to other EU certifications on behalf of SOG-IS and CCRA (https://www.ssi.gouv.fr/entreprise/produits-certifies/cc/les-accords-de-reconnaissance-mutuelle/)
OVH		**Hosting service**
ISO/CEI 27001 : 2013	Yes	Dedicated cloud
SOC 1 type II (SSAE 16 and ISAE 3402)	Yes	Private cloud
SOC 2 type II	Yes	Private cloud
Claranet		**Outsourcing and security**
ISO/CEI 27001 : 2013	Yes	Applied to all outsourcing activities. It directly echoes to Kizeo services for: - garanteing the security of services, preventing security breaches. - keeping your data confidential and ensuring their integrity - tracking security incidents.

HDS	Yes	https://www.claranet.fr/certification-hds
Reversability *Over the years, Kizeo developped various tools granting the reversability of data stored on our server. Thanks to those, you can extract your data in multiple formats.* *Our conformity implies that our customers can extracts their data in a lot of format without requiering Kizeo contribution.*		
Global		
Users	Yes	Via Web service or XLSX or CSV file given by Kizeo
Groups	Yes	Via Web service or XSLX or CSV file given by Kizeo
Kizeo Forms		
Data	Yes	Customers can extract alone to : - files (.pdf, .docx, .xlsx, .csv) - database (Microsoft Access, MariaDB, PostgreSQL, Sql Server, Mysql) - Sharepoint They can also extract data to XML and JSON formats.
Media	Yes	Media can be retrieved from our web application, the database connector, the Sharepoint connector, the web service, FTP or Dropbox.
External lists	Yes	Via Web service (raw text format) Via the web application (.xlsx)
Forms	Yes	JSON format (via Web Service)
Kizeo Tempo		
Data	Yes	files (.xlsx, .ics) via the web application
Documents & Media	Yes	Via the web application
Usefull stuff for your SI *If your SI ask you technical stuff, it may be right there.*		
Allow HTTPS on those domains		You should at least allow : Every domains of ***.kizeoforms.com** and ***.kizeo.com**
Input IP ?		Kizeo only works with HTTPS, even through the Web Service, this means we have trustable and verifiable certificates that insure our identity. For the best quality of service, input IPs must be changeable very quickly, so we do not recommend to filter using IPs but using DN.
Connectivity to Client's Infrastructure	No	Kizeo offers SaaS products, and does not connect to the Client's internal network and infrastructure
Infrastructure		



Sensitive data (inc. RGPD)		
Sensitive data collected by Kizeo		
Global		
Users' password	Yes	Footprint only (hashed + salt)
Kizeo Forms		
Geolocation	Yes	Only if used by the customer in their forms
Email	Yes	We keep logs of sent email by Kizeo Forms for 3 days.
Note : By default, Kizeo Forms does not store sensitive personnal data. But our customers are free to customised their app the way they want, implying that they can store personnal information we are not able to identify if they do not notify us. It is our customer duty to declare what is necessary and to use the tools we provide them to respect and keep in conformity according to laws in their region.		
Note (External lists) : External lists are intrinsically made for sharing information about some subject to your users, making simpler for them to complete forms. It can be the list of products sold by your company, the retaillers in the different regions and other stuffs. Keep in mind that you do not use them to store and share personnal data unjustified by your professionnal are legal needs.		
Kizeo Tempo		
Geolocation	Yes	Used for each clockin/clockout only if configured with geolocation
Compliance with medical data *AWS is certified for HDS (France and Europe) and HIPAA (US).* *Kizeo is not yet certified, but we created our infrastructure according to those certifications.* **https://aws.amazon.com/compliance/agence-francaise-de-la-sante-numerique-hds/?nc1=h_ls** **https://aws.amazon.com/health/healthcare-compliance/?nc1=h_ls**		
Collected by Kizeo	None	We do not collect medical data
HDS (France/Europe)	Not certified	We did not apply for a HDS compliance for the moment. If you require it, please contact our commercial service.
HIPAA (USA)	Not certified	We did not apply for a HIPAA compliance for the moment. If you require it, please contact our commercial service.
Password policy and account security		
Token validity (mobile devices)	1 day	
Customisable complexity	Yes	With regular expression
Expiracy	No	
2 Factors authentication	Yes	

Azure Active Directory (OAuth2)	Yes	
SAMLv2	No	
OpenId Connect	Yes	
Google (OAuth2)	Yes	
LDAP (throught SSH)	No	Deprecated for security issues. We strongly recommend Azure AD.
Okta (OAuth2)	Yes	
IP restrictions	No	Planned
Extension to another provider	-	The Client can contact us with their requirements and we will evaluate the possibility to integrate with the proposed provider. We strongly suggest that you use an existing integration.
Anonymisation of data *Kizeo does not prevent you from anonymising your users if they will write personnal information in our app.* *If you collect personnal data about EU citizens, you must ensure that they can not be identified.*		
Possible	Yes	
Encryption of sentitive data	Yes	**All data are encrypted (at rest & in transit)**
Rights		
Kizeo Forms		
Access	Yes	The user who wrote down the information can access it at anytime during the information's lifespan.
Edit/Correct	Yes	You can allow data edition
Right to be forgotten	Yes	Data can be erased
Irreversible erase	Yes	Via Web Service
Restriction	Yes	We provide a complex rights configuration to answer your needs.
Portability	Yes	Formats : XLSX / CSV / XML / JSON / DOCX / PDF / XLSX / Database Via : FTP / Dropbox / Web Service / HMI / Connector
Kizeo Tempo		
Access	Yes	The user who wrote down the information can access it at anytime during the information's lifespan
Anonymization	Yes	Admin can rename user identity
Edit/Correct	Yes	Only an administrator can edit the data. If a user wants to edit his data, he must contact his administrator.
Right to be forgotten	Yes	c.f Anonymization
Irreversible erase	No	
Restriction	Yes	User vs Administrator
Portability	Yes	ICS & XLSX
Traceability *We continuously improve trace tools for our customers' administrators.*		
Global		
User: Connection	Yes	Only for Kizeo (ret: 1 month)
User: Access rights change	Yes	
User: Edition	Yes	
User: Deletion	Yes	
Kizeo Forms		
Data: Access	Yes	Ret: 3 months
Data: Export	Yes	Ret: 3 months
Data: Edition	Yes	
Data: Deletion (soft)	Yes	
Data: Deletion (hard)	Yes	
Forms: Edition	Yes	
Forms: Deletion	Yes	
Forms: Access rights	Limited	We notice a change, but not what has changed
External lists: Edition	Yes	
External lists: Deletion	Yes	
Kizeo Tempo		
Events	Yes	clockin/clockout, photos, comments: mail notification + display in Mobile history + display in Web history
Reports	Yes	Last 10 exports
Duration of retention		
Backups	30 days	
Logs	30 d to 3 months	

Trace logs	1 m. to 5 y.	
Data (after end of contract)	2 years	Can be reduced to 3 months if asked. This retention time is to protect integrity for saisonnal customers.
Data (soft deleted)	6 months	To prevent unintended deletions.
Physical security of the premises		
Impact *First of all, we do not store customers' data in our offices. Every computers are protected with a password and every tunnel/VPN allowing access to data is encrypted.* *In case of roberry, we can easily revoke the access of keys used as they are personnal and not shared. Furthermore, computers with data access are limited to the minimum requirement.*		
Physical access	Yes	We do not store customers' data on our physical devices.
Encrypted SSH keys	Yes	min 2048 bytes
Access control		
Global access control	Yes	Digital access keys and alarms.
Personnal access key	Yes	
Video surveillance	Yes	
Intervention speed	Yes	less than 30 minutes
Identification	Yes	Digital personnal keys
SI Safety		
Back-ups *Back-ups are stored on multiple geographically separated sites in France. Access is restricted to qualified technical employees of Kizeo and outsourcing teams of Claranet (certified ISO/CEI 27001).*		
Geo-separation	Yes	3 geographically separated sites in France
Access	Yes	Vincent Demonchy (CTO) DevSecOps Team
Encrypted	Yes	
Cloud solution *We benefit from the whole AWS and OVH infrastructure (incl. firewalls, VPN, anti-DDOS systems).* *Claranet, as our outsourcing partner, ensures we are safe from security breaches.*		
Anti-DDOS	Yes	By AWS
Firewall	Yes	
Anti-virus	Yes	Windows Servers : Oui Linux : No but a very strict security policy is applied, and security fixes are managed by Claranet.
Intrusions	Yes	IPs restriction, Firewall, VPN
Internal Kizeo SI *This section deals with our employees' computers.*		
Anti-DDOS	No	
Firewall	Yes	
VPN	Yes	
Antivirus	Yes	On all devices (Avast Business Edition)
Portable	Yes	
Password	Yes	3-months rotation
Access protection		
SSH Key length	Yes	2048 characters
Encrypted keys	Yes	
Access restriction	Yes	IT Team : No access IT managers or senior support technicians : Access (edition) Claranet : Access (edition)
Security audits		
Global		
Regular penetration testing	Yes	Once every 6 months
Publishing of the results	Yes	Once a year
Kizeo Tempo		
Regular penetration testing	-	Planned starting in 2022

SLA		
Global		
SLA Web App : Kizeo Forms	99.8%	Annual (equivalent to 17h of downtime by year)
RTO	4h	
RPO	8h	
Kizeo Tempo		
SLA	99.8%	Annual (equivalent to 17h of downtime by year)
RTO	24h	
RPO	36h	
Service continuity plan		
Service Continuity on 3 sites minimum *In March 2018, we deploy a new infrastructure based on at least three datacenters. Thanks to this, we would be able to deal with a datacenter complete failure.*		
Geographic redundancy	Yes	At least 3 datacenters