

LA SÉCURITÉ AVEC APPCRAFT



AppCraft soutenue par



POUR RÉSUMER NOS MODULES

SÉCURITÉ

Nous sommes un prestataire reconnu sur ce marché comme étant celui le plus robuste.

Pour des raisons de souveraineté numérique, nous avons fait le choix d'héberger nos données chez OVH (leader français de l'hébergement)

Vos données sont donc stockées en France, protégées par les législations françaises et européennes.

LES + APPCRAFT

1. Deux audits par an effectués par Orange Cyberdefense ou Synacktiv

2. Notre écosystème (développeurs et serveurs) est localisé en France

3. AppCraft est ouvert aux tests d'intrusion des DSI de ses clients

4. AppCraft est certifié ISO 27 001: Pour la sécurité de vos données à 360°, à la fois technique que organisationnelle.



Nous avons par exemple **réalisé en 2023 une application et plateforme pour l'événement Very Tech Trip d'OVH cloud** en 100% physique à la Cité des Sciences et de l'Industrie. Il s'agissait de la première édition d'une convention pour les Techs.

Aussi, nous avons été **audité puis contre-audité par Orange Cyberdefense, Synactiv** et des **entreprises privées**.

Concernant la protection des données, **nous respectons la RGPD**.

LE CHOIX RESPONSABLE



Pour des raisons de **souveraineté numérique**, nous avons fait le choix d'héberger nos données chez OVH (leader français de l'hébergement).

POURQUOI EST-CE IMPORTANT POUR VOUS ?

Vos données sont stockées en France, protégées par les **légalisations françaises et européennes**.

Vos données ne dépendent pas d'un acteur américain du Cloud où un simple mandat ou une assignation l'oblige à **transmettre les données stockées sur les serveurs**. Que les serveurs soient aux USA ou sur d'autres continents, la justice américaine s'octroie ces droits. Les données à caractères personnels mais aussi brevets, savoir-faire, sont accessibles sur simple demande aux forces de l'ordre fédérales ou locales.

HÉBERGEMENT EN FRANCE



VS



The background of the image shows a person's hands typing on a laptop keyboard. Overlaid on this are various digital icons connected by glowing blue lines, suggesting a network or data flow. The icons include a magnifying glass, a group of people, a person silhouette, a balance scale, a classical building, a hand cursor, and a document with lines. The overall color scheme is blue and orange.

GESTION DES DROITS NUMÉRIQUES

Hébergement



Les solutions **AppCraft** sont composées d'un ensemble de micro-services dont la majorité est hébergée chez **OVH**, sur des serveurs dédiés en France. Ceci concerne entre autres le site de l'événement ainsi que les données liées à l'inscription. Les serveurs **AppCraft** sont exclusivement accessibles aux développeurs d'**AppCraft** travaillant tous en France et dont le contrat de travail intègre une clause de confidentialité.

Seuls les services suivants sont actuellement hébergé sur **Firebase** (Google) :

- chat
- quiz

CDN



Pour les fichiers web (JS, CSS), le CDN OVH est utilisé, avec un stockage sur OVH Object Storage. Pour les images utilisées dans l'application mobile ainsi que sur le site internet, AppCraft Events utilise comme CDN CloudImage, **un service français** spécialisé dans le redimensionnement des images à la volée et RGPD-compliant (<https://www.cloudimage.io>).

TECHNIQUE

PLATEFORME ET APPLICATION MOBILE



L'accès à la plateforme et à l'application mobile se fait par login (personnel) et mot de passe (personnel ou générique, selon les demandes Clients). Tous les échanges avec le serveur se font en **https**.

Le contenu de l'application est déterminé en fonction des besoins du client.

Les données et modules suivants, qui peuvent être intégrés selon les cas, sont susceptibles de contenir ou générer des informations personnelles :

- liste des participants (champs exposés au choix)
- chat entre participants
- partage de photos
- networking avec recherche de profils similaires et mises en relation

LOAD BALANCER



La solution utilise le load balancer d'OVH en mode multi-zone (Roubaix + Gravelines) pour garantir une meilleure disponibilité.

ENVOI DE MAILS

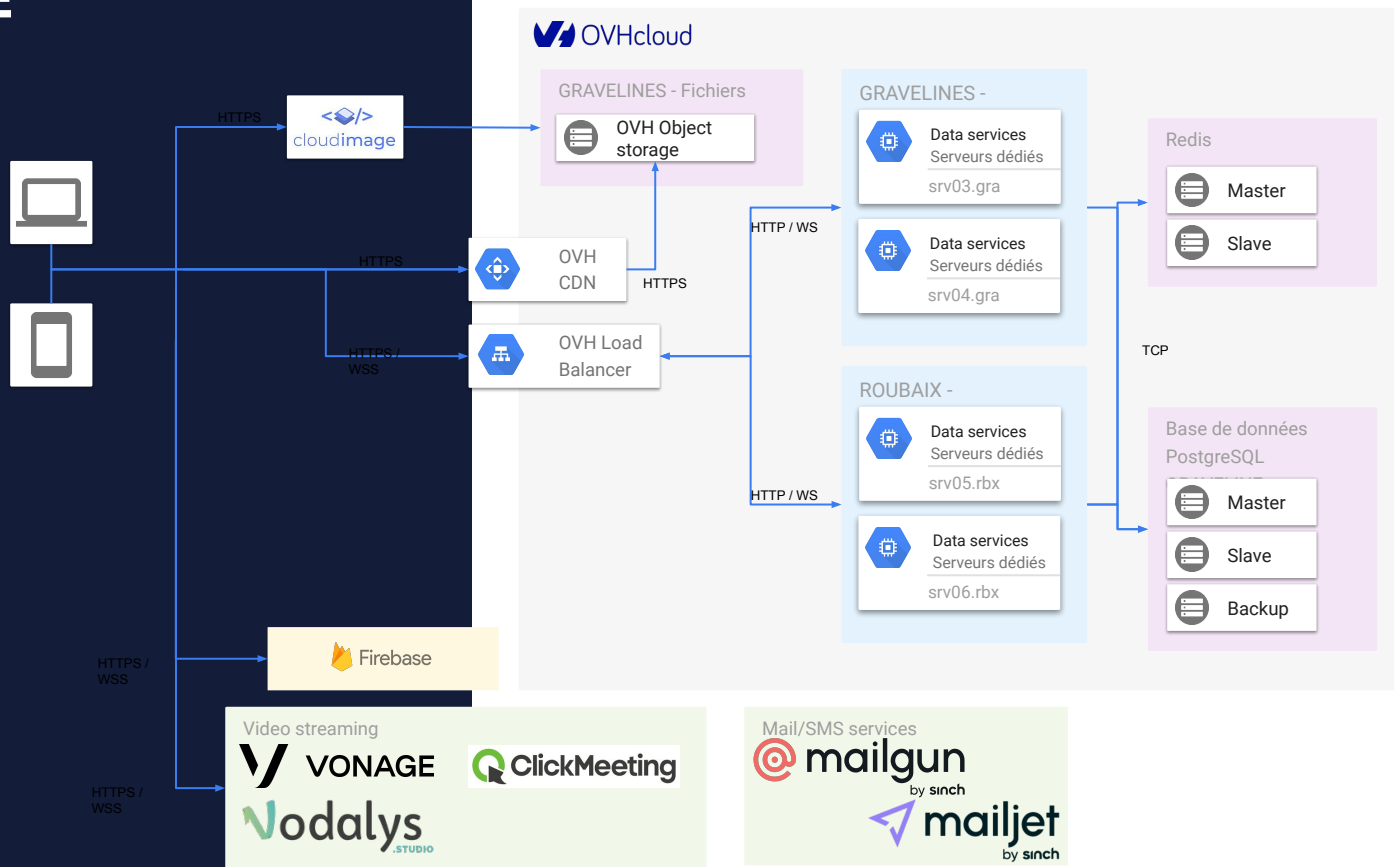


La solution utilise actuellement 2 prestataires RGPD-compliant pour les envois de mail :

- Mailjet, un service français
- Mailgun, en utilisant leurs serveurs européens

ARCHITECTURE

Une architecture
modulaire de
micro-services,
très évolutive.





ARCHITECTURE

Une architecture
modulaire de
micro-services très
évolutive.

- AppCraft dispose chez OVH de serveurs de données dédiés et isolés
- Une intégrité totale est assurée entre les serveurs et les quelques postes de travail pouvant y accéder
- Chaque poste de travail dispose d'une protection contre les programmes malveillants et les salariés d'AppCraft sont sensibilisés aux risques de sécurité ou d'intrusion.
- L'importation de bases de données historiques du Client est possible et facile à mettre en œuvre



FLUX ENTRÉE / SORTIE

Une architecture
modulaire de
micro-services très
évolutive.

- Les communications entre les différents micro-services et ressources d'AppCraft ont lieu à l'aide de connexions sécurisées SSL et HTTPS
- Les requêtes d'accès à ces services se font également par des connexions client sécurisées
- Les informations sensibles (mot de passe) sont hachées pour une sécurité maximale
- Chaque client une fois authentifié sur la plateforme obtient les informations spécifiques à son événement

SÉCURITÉ



- Nous procédons à des évaluations périodiques, externes et indépendantes sur la sécurité de l'infrastructure AppCraft et sur les informations qui y sont déposées ainsi que des risques liés (tests d'intrusion, etc ...)
- Le backoffice est accessible via un système d'authentification forte pour les mots de passe
- Les transferts de données sont chiffrés. Les données au repos sont également stockées chiffrées
- Toute atteinte à la sécurité est signalée le plus tôt possible au Client (dans les 48 heures max)

SLA OVH

<https://www.ovhcloud.com/fr/enterprise/products/hosted-private-cloud/sla/>

SLA AppCraft

Niveaux de services (jours & heures ouvrés)		
Au cours d'un Événement (accueil des Participants)	Garantie de Temps d'Intervention :	<30 minutes pour les Anomalies bloquantes
	Garantie de Temps de Rétablissement :	< 4 heures pour les Anomalies bloquantes à compter de l'intervention
Hors période d'Événement	Garantie de Temps d'Intervention :	8 heures ouvrés
	Garantie de Temps de Rétablissement :	24 heures

FAQ

HÉBERGEMENT

Où sont hébergées les infrastructures techniques de l'application mobile et du site web ?



Toutes les données sont hébergées chez OVH, en France. L'interactivité (quiz) est hébergée sur le service Firebase Europe.

ACCÈS SÉCURISÉ

Comment les accès administrateurs techniques aux infrastructures du site web et de l'application mobile sont-ils protégés (filtrage par IP, chiffrement des flux, ...)



Les accès aux machines sont uniquement en SSH, sur un port différent du port 22. Seuls les ports 80 et 443 sont ouverts (en plus du port SSH modifié).

Comment sont gérées les authentifications des administrateurs techniques et fonctionnels aux infrastructures techniques ?



Pour le backoffice, authentification avec génération d'un JWT utilisé pour les requêtes vers le backend. Pour l'accès aux infrastructures, accès SSH.

Des traces des accès et des opérations effectuées par les administrateurs et les utilisateurs sont-elles générées ? combien de temps sont-elles stockées ? ou sont-elles stockées ?



Pour les utilisateurs une table en base est dédiée à l'historique des modifications. Ces données sont purgées après l'événement suite à validation du client.

FAQ

PROTECTIONS CYBERATTQUES

L'accès aux infrastructures est-il sécurisé par un pare-feu ? quels sont les protocoles réseau autorisés ?



Un pare-feu bloque tous les ports autres que les ports 80, 443, et le port SSH que nous avons changé.

Des mécanismes anti-DDOS sont-ils en place en amont des serveurs web ?



Notre hébergeur OVH offre des mécanismes anti-DDOS.
<https://www.ovh.com/fr/anti-ddos/>

FLUX

Comment les flux de connexion des utilisateurs standards au site web et à l'application sont-ils protégés ? via chiffrement ? Quel est le protocole appliqué ?



Tous les échanges se font en HTTPS en TLS 1.2

MOTS DE PASSE

Quelle est la politique de mot de passe des administrateurs fonctionnels du site web et de l'app mobile ?



Mots de passe d'au moins 10 caractères, générés aléatoirement.

FAQ

MAILING

Comment est sécurisé l'accès à la boîte aux lettres ?



Boîte mail hébergée par OVH, reposant sur le système Outlook de Microsoft.

Quelle est la politique de mot de passe liée à la boîte aux lettres (nombre de caractères, complexité,...) ?



Mot de passe d'au moins 12 caractères avec minuscules, majuscules, chiffres, et au moins 1 caractère spécial.

JURIDIQUE

RGPD

*Vos données sont un actif précieux.
Nous les sécurisons et nous en prenons soin.*

Les données personnelles fournies par les clients sur la plateforme AppCraft ne sont utilisées que pour les besoins des participants (de façon optionnelle, mise à disposition d'une liste de participants avec nom/prénom, numéro de téléphone, etc.) et des organisateurs (type de repas par exemple).

AppCraft SAS ne fait aucun usage de ces données, que ce soit pour des usages de statistiques ou autre.

Nous proposons à nos clients de supprimer les données relatives aux participants et aux contenus partagés (chat/photos) 1 mois après la fin de l'événement. Les autres données (contenu de l'application, styles, fichiers, programme, ou autre) peuvent être conservés plus longtemps par le client s'ils ne contiennent pas d'informations personnelles.



CGU

***Vos données sont un actif précieux.
Nous les sécurisons et nous en prenons soin.***

Rappel de nos CGU sur le traitements des données personnelles

Le Client garantit que les données collectées et communiquées à AppCraft l'ont été dans le respect de la RGPD et de la loi CNIL de 1978 (Art 6 - traitement licite / Art7 - Consentement / Art 9 - Données sensibles / Art 21 droit d'opposition).

Le Client s'engage à respecter ses obligations de notifications auprès des personnes physiques dont les données ont été collectées.

Le Client s'engage à ne pas utiliser la plateforme AppCraft pour des opérations de profilage, opérations que s'interdit également AppCraft (Art 22).

AppCraft fournit au Client un accès pour mettre à jour les données en temps réel afin d'être conforme aux droits d'accès et de rectification (Art 15 & 16 de la RGPD).

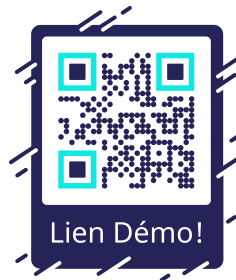
Sur demande du Client, AppCraft s'engage à effacer l'ensemble des données collectées (Art 17 de la RGPD). Des fonctions de suppression sont aussi mises à la disposition du Client.

AppCraft garanti par défaut une limitation du traitement des données au temps du contrat avec sanctuarisation possible non accessible aux tiers (sauvegardes)

AppCraft garantit une portabilité complète des données grâce aux fonctions d'export.

AppCraft s'interdit tout usage sur les données collectées autre que celles prévues au contrat en particulier de communiquer les données collectées à des tiers ou hors de France.

GARDONS CONTACT



hello@appcraft.fr



09 72 51 22 90



AppCraft

French Event Booster
1 Place de la Porte de Versailles
75015 PARIS

