RGPD

Politique de sécurité et de confidentialité des données personnelles

SOMMAIRE

DÉFINITIONS

DATA CONTROLLER / responsable du traitement
Organisation qui décide quelles données à collecter, et qui définit l'objectif de cette collecte de données.

VOUS

DATA PROCESSOR / sous-traitant
société ou personne qui traite les données personnelles pour le compte du responsable du traitement

iRaiser

DÉFINITIONS

UTILISATEUR A

ACTIONS

INSTANCE DÉDIÉE

SOUS-TRAITANT APPLICATIF

SOUS-TRAITANT HÉBERGEMENT

VOUS

amazon web services™

OVH.com Innovation is Freedom

SÉCURITÉ 

https://www.iraiser.eu/fr/notre-engagement-securite/

HÉBERGEMENT EXCLUSIVEMENT EN EUROPE
CRYPTÉE, SÉCURISÉ ET EN “HAUTE DISPONIBILITÉ” (99,9%)

amazon web services™

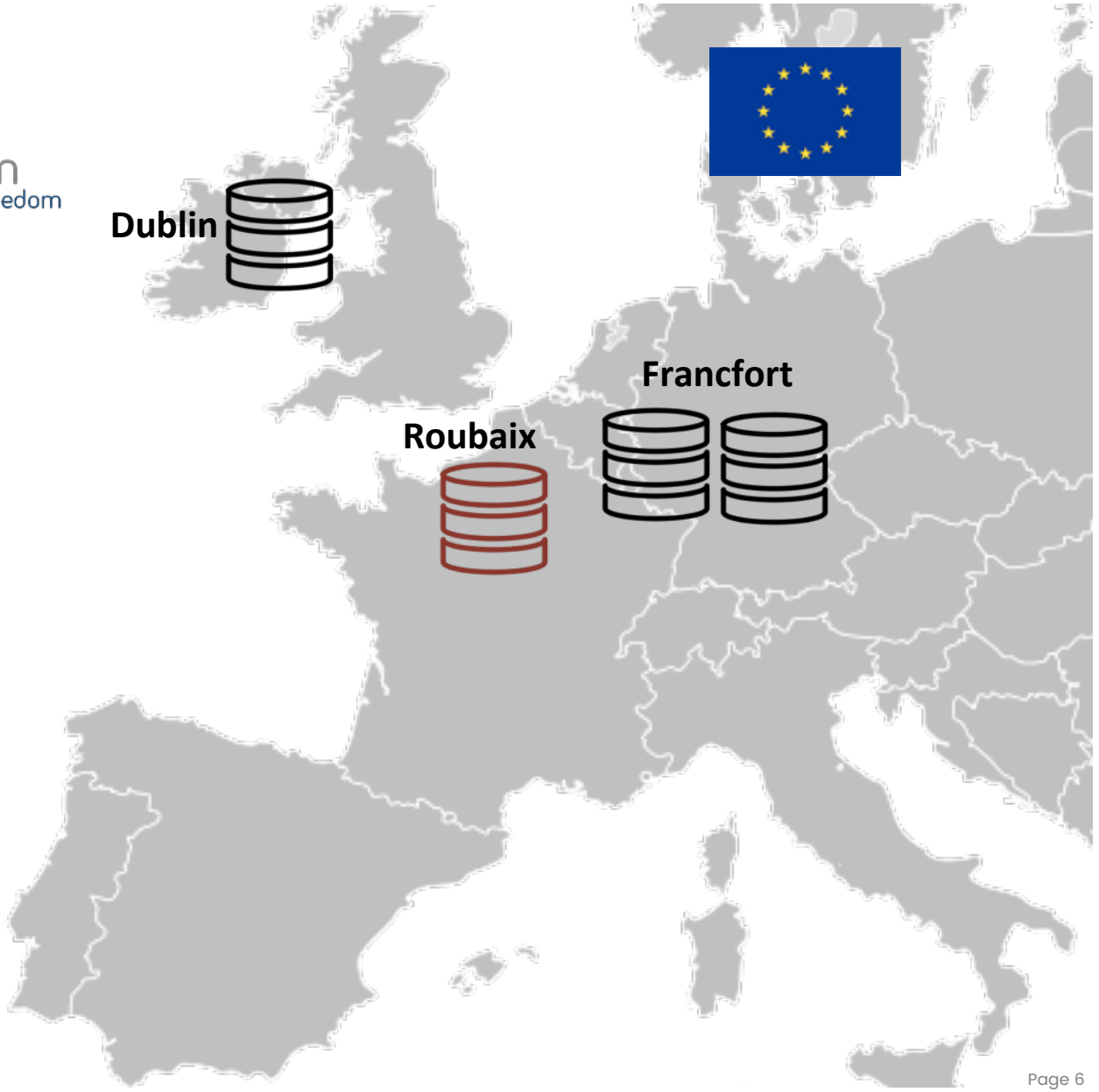
OVH.com Innovation is Freedom

Information Security Management System ISO 27001 Certified

PCI DSS PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS LEVEL 1 SERVICE PROVIDER

ISO 27018 International Organization for Standardization

Norme ISO sur la protection des données à caractère personnel dans l'informatique en nuages



SAUVEGARDES QUOTIDIENNES COMPLÈTES
CONSERVÉES 90J ET STOCKÉES SUR 2 FOURNISSEURS DIFFÉRENTS

- Snapshot crypté quotidien sur AWS 

- Dump crypté quotidien sur OVH 

* L'accès aux sauvegardes est uniquement disponible à nos administrateurs.
Hormis ces administrateurs, aucun salarié, fournisseur, client peut avoir un accès direct à ces sauvegardes.

** Snapshot : capture par la baie de stockage d'une "photographie" à état à un instant donné des données d'un volume à des fins de sauvegarde et de protection de données.*

MONITORING COMPLET 24h/24 et 7j/7 DES ACCÈS ET DES EXPORTS RÉALISÉS

Date : 30/04/2018 16h58min2s
User : amartel
IP : 5.135.140.45
Actions : XXXXX

Détection des comportements suspicieux (IP, email, vitesse de saisie, …)
Utilisation de AWS Cloud Watch, Nagios et Fai2Ban
« Blacklistage » des adresses IPs suspectes
Blocage des accès en cas d'échecs multiples

Alerte email et SMS en cas d'indisponibilité, ralentissement ou attaque.

En cas de violation avéré, notification au(x) client(s) concerné(s)
ET aux autorités compétentes dans les 72h.

UN DIRECTEUR TECHNIQUE EXPÉRIMENTÉ

Tony BOURDIER

- Titulaire d'un **doctorat en informatique et analyse de données**, d'un diplôme d'**ingénieur en informatique** et d'un master en statistiques
- **Co-auteur de plusieurs conférences et ouvrages sur la sécurité** :
  - *Foundations and Practice of Security, 2012*
  - *Network and Information Systems Security, 2011*
  - *Journal of Information Assurance and Security, 2011*
  - *Security and Reliability Day, 2010*
  - *5th International Workshop on Security and Rewriting Techniques, 2010*
- **Enseignant à l'Ecole Nationale Supérieure des Mines de Nantes** (+ anciennement à l'Université de Lorraine et à Telecom Nancy)
- **Ancien chercheur au CNRS et à l'INRIA**
- Ancien membre du Conseil d'Administration de Telecom Nancy, du Conseil d'Administration de l'école doctorale IAEM, et du Conseil Scientifique de l'Université de Lorraine
- **Expert scientifique** pour des conférences internationales organisées par IEEE, ACM, ...

DES PROCÉDURES INTERNE RIGOUREUSES

- Tous les **ordinateurs des employés sont protégés** par un login et un mot de passe personnel, un parefeu et antivirus mis à jour automatiquement. Un scan hebdomadaire est réalisée pour se prémunir de tout virus, spamware, malware, trojan, worm ou bot.
- Tous les employés utilisent un **VPN** pour accéder à nos solutions.
- Les **accès et actions réalisés sont monitorés**.
- Les développeurs ont obligatoirement un **second niveau d'identification** pour se connecter aux serveurs de pré-production et de production.
- **Aucun employé de la société iRaiser ne peut avoir un accès aux cartes bancaires** de vos donateurs.
- Tous les **développements sont testés en pré-production** avant leur passage en production. Tous les développeurs sont particulièrement vigilants lors d'un passage en production que cela n'affecte en aucun cas la stabilité de la solution.
- Toutes les bases de données de nos clients sont compartimentées et aucun cas partagés.

UN BACK OFFICE SÉCURISÉ

- Le **back office est sécurisé par un login / mot de passe unique et propre à chacun**.
  Le mot de passe comprend un minimum de 8 caractères avec majuscules, minuscules, chiffres et caractères spéciaux.
  Le mot de passe doit être changé tous les 3 mois. Si jamais, l'utilisateur saisit un mot de passe erroné, il doit attendre 10s avant de faire une nouvelle tentative.

- iRaiser peut **restreindre l'accès du backoffice** via un filtre sur un ou plusieurs adresses IP.

- Chaque **accès et actions réalisées sont monitorés et conservées** pendant une durée de 2 ans.

- Si aucune activité est enregistré pendant une durée de 5 minutes, la **session est automatiquement fermée** et l'utilisateur devra s'identifier à nouveau.

AUDITS DE SÉCURITÉ

EXTERNE

Secours Populaire	**Orange CyberDefense**	**mai-17**
Restos du Cœur	**Enki-security.com**	**mai-17**
Fondation Apprentis d'Auteuil	**HSC by Deloitte**	**mai-16**
Amnesty International	**Advens**	**août-15**
Action Contre la Faim	**securitymetrics.com**	**avr-14**
Perce Neige	**Xmco**	**déc-13**
...		

INTERNE

Test de pénétration tous les 3 mois
Test de charge tous les 3 mois
Audit de sécurité tous les 3 mois
Changement des mots de passe tous les mois

CRYPTAGE SYSTÉMATIQUE DES DONNÉES

AWS Key Management Service

https://aws.amazon.com/fr/kms/

AWS Key Management Service (KMS) est un service géré qui vous permet de créer et de contrôler facilement les clés de chiffrement utilisées pour chiffrer vos données. Il utilise des modules de sécurité matériels conformes à la norme FIPS 140-2 pour assurer la sécurité de vos clés. AWS Key Management Service est intégré à la plupart des autres services AWS afin de vous aider à protéger les données stockées avec ces services.

AWS Key Management Service est également intégré à AWS CloudTrail pour vous fournir des journaux contenant des informations sur toutes les utilisations de vos clés, dans le but de vous aider à répondre à vos besoins en matière de réglementation et de conformité.

EXPORT AUTOMATIQUE DES DONNÉES

~~EMAIL~~ ~~FTP~~ › SFTP

Mise à disposition d'un SFTP dédié en lecture / écriture pour l'ensemble de nos clients.

L'export de données depuis le backoffice sera bien évidemment toujours possible
mais on vous invite à pas stocker des fichiers de données personnelles sur votre ordinateur.

COOKIES

DÉPOSÉS OU LUS SANS RECUEILLIR LE CONSENTEMENT DES PERSONNES

✔ 

Cookies strictement nécessaires à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur.

✔ 

Cookies dont la finalité exclusive est de permettre ou faciliter la communication par voie électronique

✗ 

Cookies liés aux opérations relatives à la publicité ciblée

✗ 

Cookies de mesure d'audience

✗ 

Cookies traceurs de réseaux sociaux générés par les boutons de partage de réseaux sociaux

COOKIES

DÉPOSÉS OU LUS SANS RECUEILLIR LE CONSENTEMENT DES PERSONNES

Pour tous les autres cookies, le consentement doit être recueilli via un bandeau de type « En continuant votre navigation sur ce site, vous acceptez que s'installent des cookies poursuivant les finalités suivantes : […]. Pour en savoir plus sur les cookies et sur vos possibilités de vous y opposer, cliquer ici [renvoi vers une cookie policy] ».

La durée de validité du consentement (et donc de manière corollaire la durée de vie des cookies) est de 13 mois max, durée à l'issue de laquelle le consentement doit de nouveau être recueilli.

DIFFÉRENTES SOLUTIONS
DIFFÉRENCES CATÉGORIES DE DONNÉES

DONNÉES MARKETING : 3 ANS	DONNÉES FISCALES & COMPTABLES : 10 ANS
BANNIERE PREHOME PAGES INSCRIPTION ÉVÉNEMENT PETITION MANIFESTE PLAIDOYER MARKETING AUTOMATION EVENT FUNDRAISING PEER TO PEER FUNDRAISING CROWDFUNDING	EVENT FUNDRAISING PEER TO PEER FUNDRAISING CROWDFUNDING CRM PAIEMENT

Exemple :
- Signature d'une pétition
- Création d'une page de collecte

Exemple :
- Engagement régulier SDD SEPA,
- Dons ponctuels par Carte Bancaire

Il est possible de modifier la durée de conversation avant anonymisation.

FINALITÉ DES TRAITEMENTS DE DONNÉES SUR UN PAIEMENT

- Émettre en conformité avec la loi le reçu fiscal et pouvoir fournir toutes les preuves à l'administration fiscale : Montant du don, Date du don, Coordonnées du donateur, Mode de paiement

- S'assurer de la véracité du don et de son donateur et prévenir les fraudes : Origine, Vitesse de saisie, Comportements, Adresse IP, Eempreinte de la machine.

- Affecter comptablement le don au(x) projet(s) souhaité(s) par le donateur : code(s) affectation(s)

- ...

ANONYMISATION DE CERTAINES DONNÉES

MONSIEUR ANTOINE MARTEL
AMARTEL@iRAISER.EU
15/12/1978
06 04 59 22 34

199 ROUTE DE CLISSON
44230 SAINT SEBASTIEN SUR LOIRE
FRANCE

100€
MASTER CARD **** **** **** 6250 / 03-2020

Campagne CID : 28

Date : 30/04/2018
IP : 5.135.140.45

MONSIEUR ANTOINE MARTEL
********@*********
//****
** ** ** ** **

199 ROUTE DE CLISSON
44230 SAINT SEBASTIEN SUR LOIRE
FRANCE

100€
MASTER CARD **** **** **** 6250 / 03-2020

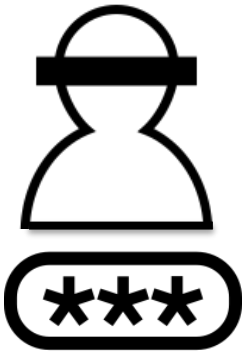
Campagne CID : 28

Date : 30/04/2018
IP : *.***.***.**

ANONYMISATION DES DONNÉES

Les données ne sont pas supprimées.
Elles sont automatiquement anonymisées
de manière définitive et irréversible après une certaine durée.

Monsieur Antoine Martel
amartel@iraiser.eu



AUTONOMIE
POUR L'ÉDITION DES DONNÉES ET DES CONTENUS

- Vous avez la main pour ajouter de manière autonome vos mentions légales et détailler ainsi les flux de collecte et de traitement de données.

- Vos visiteurs peuvent, une fois identifiés, consulter et modifier leurs informations personnelles

- Vous pouvez restituer à la demande l'intégralité des données collectées : https://data.iraiser.eu/demo/index.html
- Vous pouvez également anonymiser définitivement certaines données.

RAPPEL

[…]Vos identifiants sont **confidentiels, uniques et personnels**.
Le client est **seul responsable de leur utilisation**.
Les identifiants de connexion peuvent être **changés à tout moment** à l'initiative du client, ou à l'initiative de la société sous réserve d'en informer préalablement le client.
Le client s'engage à **apporter tous les efforts et les soins nécessaires en vue de garder secret les identifiants de connexio**n qui lui ont été remis.
En cas de perte ou de vol de son mot de passe, ou dans le cas où il aurait connaissance d'un accès non autorisé aux services, le client en informera la société sans délai par courrier électronique à l'adresse help@iraiser.eu et suivra les instructions qui lui seront communiquées. […]

SUPPRESSION

Sur une simple demande par ticket ou par email et après confirmation par appel téléphonique avec notre référent chez le client, nous pouvons procéder à une destruction de l'intégralité des données d'un client (données + backup)

LISTE DE NOS SOUS-TRAITANTS

Cette liste est mise à jour régulièrement sur la page suivante :
https://www.iraiser.eu/fr/nos-sous-traitants/

HÉBERGEMENT ET SAUVEGARDE :

- **Amazon** – PCI-DSS de niveau 1, ISO 27001 et ISO 27018
  https://aws.amazon.com/fr/compliance/gdpr-center/

- **OVH** – PCI-DSS de niveau 1, ISO 27001 et ISO 27018
  https://www.ovh.com/fr/protection-donnees-personnelles/gdpr.xml
  https://www.ovh.com/fr/apropos/certifications.xml

PAIEMENT EN LIGNE :

- Ingenico ePayments – PCI-DSS de niveau 1
  https://payment-services.ingenico.com/int/en/ogone/support/products/pci
  https://www.ingenico.com/epayments/legal/certifications
- Slimpay : https://www.slimpay.com/fr/blog/donnees-de-paiement-rgpd/
- Gocardless : https://gocardless.com/fr/blog/rgdp +
  https://support.gocardless.com/hc/fr/articles/360000281005-GoCardless-et-le-RGPD
- GestPay : https://www.gestpay.it/features/security/
- PayPal : https://www.paypal.com/fr/webapps/mpp/paypal-safety-and-security

MERCI DE VOTRE ATTENTION.

Contact :

Téléphone : +33(0)184178492

Email : rgpd@iraiser.eu