Politique de sécurité des données personnelles

SCW-POL-009

1.0 - Mai 2024
Public

Scaleway

scaleway.com

Sommaire

Présentation

Vous trouverez sur cette annexe une description des mesures techniques et organisationnelles mises en place par Scaleway afin notamment de protéger les données de ses clients contre toute violation de sécurité pouvant entraîner de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à leurs données.

Ces mesures de sécurité techniques et organisationnelles sont complémentaires à notre Accord de Sous-traitance du traitement de données à caractère personnel (DPA) ainsi qu'à notre Politique de confidentialité.

Les mesures présentées ci-après portent uniquement sur les infrastructures et les services proposés par Scaleway. Conformément à nos conditions générales de Service, le Client demeure seul responsable de l'adéquation des Services souscrits avec les activités qu'il exerce grâce auxdits Services et avec la réglementation applicable à ces activités, notamment concernant le choix des options de sauvegarde, de chiffrement, de gestion des accès ou tout moyen qu'il estime nécessaires afin de se prémunir d'une éventuelle suppression, altération ou modification de ses données.

Gouvernance

Politique de sécurité de l'information

Scaleway dispose d'une politique de sécurité de l'information révisée chaque année en cas de modifications ou d'évolutions importantes (ex : changement majeur du cadre légal et réglementaire auquel Scaleway est soumise ou dans le cadre de l'amélioration continue suite à un audit).

Fonctions et responsabilités

Conformément à la norme ISO/IEC 27001:2022, Scaleway gère la sécurité de l'information par le biais de la gestion des risques, et dispose d'un Système de Management de la Sécurité de l'Information (SMSI). Les rôles affectés pour soutenir ce système sont définis et documentés (notamment : CIO, Head of Cyber Governance, Risk and Compliance et VP Trust & Security Operations).

Scaleway dispose également d'un DPO ainsi que d'une équipe dédiée à la protection des données.

Audits et certifications

Audits

Afin d'assurer un niveau de sécurité optimal, des audits externes et internes sont planifiés au moins une fois par an (cette fréquence peut varier en fonction des périmètres concernés).

Conformément à la réglementation, des audits peuvent être réalisés par les clients dans les conditions prévues dans notre Accord de Sous-traitance sur les données personnelles (DPA) et après validation de notre Accord relatif à la réalisation de tests d'intrusion.

Attestations et certifications

Scaleway dispose de certifications et s'engage sur le respect de différentes normes afin de garantir la sécurité de ses infrastructures et de son système d'information. Ces normes sont consultables sur l'espace Sécurité & Résilience et Scaleway peut également fournir des attestations sur demande.

Sécurité relative au personnel

Confidentialité

Scaleway s'assure que l'ensemble de son personnel traite les données de ses clients de manière sécurisée et confidentielle. A ce titre, notre personnel est contractuellement soumis à :

- un accord de confidentialité et de non-divulgation
- une charte informatique visant à encadrer de manière sécurisée l'utilisation des moyens mis à leur disposition

Sensibilisation et formation

L'ensemble du personnel de Scaleway est sensibilisé à la fois à la sécurité de l'information et à la protection des données via des parcours de formation obligatoires lors du processus de recrutement. Ces connaissances sont ensuite ré-actualisées tous les deux ans grâce à nos outils internes de formation continue.

Gestion des actifs

Inventaire et connaissance des actifs

Tous les actifs, qu'ils soient physiques ou virtuels, matériels ou logiciels, sont inventoriés et mis à jour dans notre système de gestion des actifs. De plus, chaque actif est affecté à un responsable, chargé de son maintien en conditions opérationnelles et en conditions de sécurité ainsi que de la gestion des accès et de leur désactivation.

Sécurité des postes de travail

Scaleway met en place sur chaque poste de travail les mesures afin de garantir un niveau de sécurité adéquat notamment :

- utilisation encadrée par une charte informatique (notamment conditions d'utilisation des usages personnels (BYOD), sécurité du stockage et du transport, interdiction des supports de stockage amovibles etc.)
- enrôlement dans un solution de gestion des terminaux mobiles
- verrouillage automatique de session et déconnexion automatique des applicatifs
- protection antivirus - antispam
- mises à jour de sécurité automatique
- limitation des droits utilisateurs
- espace de stockage sauvegardé et sécurisé
- maintenance encadrée et sécurisée
- chiffrement des disques

Fin de vie des actifs

Les actifs font l'objet d'une surveillance et les applications en fin de vie ne bénéficiant plus d'une maintenance sont supprimées ou remplacées.

Tout actif en fin de vie fait l'objet d'un effacement de données sécurisé conformément aux standards de l'état de l'art et, si nécessaire, d'une destruction physique.

Protection des informations

Classification et marquage des informations

Tout document de Scaleway bénéficie d'une classification et d'un marquage indiquant son niveau de confidentialité.

Transfert des informations

Scaleway n'utilise que des outils sécurisés ayant été préalablement validé par le service IT afin d'échanger des informations confidentielles ou internes (messagerie instantanée, courrier électronique, partage de fichiers). Les informations confidentielles transmises à des tierces parties externes nécessaires au fonctionnement des services ou à la vie de l'entreprise sont transmises de manière chiffrée et via un accord de non-divulgation (NDA).

Durée de conservation et suppression des informations

Scaleway s'engage à supprimer ou anonymiser les données personnelles qui ne sont plus nécessaires au traitement ou dont le traitement est arrivé à terme et qui ne nécessitent pas un archivage complémentaire pour garantir le respect d'une obligation légale ou d'un intérêt légitime de l'entreprise.

Masquage des données

Dès que cela est possible, afin d'améliorer la confidentialité des données traitées, Scaleway a également recours à la pseudonymisation afin de dissocier le lien entre l'identité de la personne concernée et d'autres informations sensibles la concernant.

Données de tests

Scaleway interdit de copier les données personnelles des environnements de production vers les environnements de tests présentant un niveau de sécurité inférieur.

Sécurité physique

L'ensemble des bureaux, entrepôts ou data centers utilisés par Scaleway bénéficient d'une protection renforcée notamment via les dispositifs suivants :

- contrôle d'accès par badge avec numéro d'identification ;
- restriction des droits d'accès aux zones sécurisées en fonction d'un profil d'autorisation ;
- système de journalisation des accès ;
- encadrement des visiteurs et personnes externes par un accompagnement et supervision adaptée au périmètre accessible ;
- dispositif de vidéosurveillance aux entrées et sorties des bâtiments ;
- dispositif de lutte contre les incendies ;
- protection contre les menaces physiques et environnementales grâce à des établissements conformes à la réglementation applicable ;
- contrôles, inspections et tests réguliers des services supports (électricité, télécommunications, distribution d'eau, ventilation et air conditionné) nécessaires au matériel et au fonctionnement des centres de données ;
- encadrement de la maintenance par des contrats de maintenance

Sécurité des systèmes et réseaux

Authentification sécurisée

Scaleway dispose d'une politique d'authentification sécurisée qui s'applique à l'ensemble de son personnel :

- Implémentation d'une architecture basée sur le modèle dit de "Zero Trust" et non sur une confiance implicite
- Mots de passe complexes et réinitialisés à échéances régulières
- Authentification forte avec un second facteur (2FA) pour les comptes à privilèges

Sécurité des systèmes

Les droits à privilège sont restreints et leurs utilisations tracées

Sécurité des réseaux

Scaleway implémente une segmentation réseau stricte afin de séparer les accès.

Le principe de séparation des pouvoirs est strictement respecté et seuls les collaborateurs habilités peuvent administrer les équipements réseaux.

Sécurité des échanges

La sécurité des échanges est assurée par les dispositifs suivants :

- Authentifications sécurisées des messageries avec protection anti-hameçonnage et d'usurpation d'identité
- Chiffrement de bout en bout des partages de fichiers sensibles (avec accord de non-divulgation si nécessaire).

Gestion du changement

La gestion du changement est encadrée par une procédure de gestion du changement. Les changements sont documentés et analysés. Lorsque des impacts clients sont identifiés, ils sont publiés sur une page dédiée.

Encadrement des tests d'audit

Des tests d'intrusion internes sur le système en production sont planifiés conformément aux contraintes et besoins du personnel en charge de l'infrastructure technique. Pour chaque test, la portée technique est clairement définie et partagée avec les parties concernées et les informations fournies aux testeurs sont limitées au strict nécessaire pour réaliser l'audit. Ces tests n'ont aucun impact opérationnel sur les données ou les services utilisés par nos clients.

Protection des données dès la conception et par défaut

Cycle de vie du développement sécurisé

Scaleway attache une grande importance à l'intégration de la sécurité dans les différentes étapes des opérations de développement :

- Phase de planification : Réalisation d'une analyse des risques et de mise en conformité dès la conception et par défaut
- Phase de conception : respect des règles de codage sécurisé
- Phase de déploiement : déploiement au sein d'un environnement de préproduction et vérification au moyen de tests d'acceptation de sécurité
- Phase d'exploitation : surveillance des journaux d'applications afin de détecter toute activité suspecte

Codage sécurisé

- Des protections adaptées contre les vulnérabilités les plus critiques des applications web sont mises en place conformément au ASVS (Application Security Verification Standard) développé dans le cadre du projet OWASP (Open Web Application Security Project).
- Une analyse type SAST (Static Application Security Testing) est effectuée systématiquement sur tous les codes sources qui s'y prêtent

Analyses d'impact

Scaleway réalise des analyses d'impact sur la protection des données (AIPD) si le traitement est susceptible d'engendrer un risque élevé sur les droits et libertés des personnes concernées.

Gestion des identités et des accès du personnel de Scaleway

Scaleway met en oeuvre une politique de gestion des identités et des accès stricte concernant les accès et droits assignés à son personnel, notamment via les dispositifs suivants :

- Respect des principes du moindre privilège et du besoin d'en connaître
- Revue des droits et des accès régulière, et ce tout au long du cycle de vie des comptes utilisateur confié (arrivée, mobilité, départ)
- Interdiction des comptes utilisateurs partagés sauf en cas de nécessité
- Centralisation des identités
- Journalisation des accès

Lors du départ d'un collaborateur, l'intégralité de ses accès et droits sont révoqués.

Gestion des identités et des accès clients

Scaleway met à disposition de ses clients, notamment via le produit IAM (Identity and Access Management), les dispositifs de sécurité suivants afin de sécuriser l'accès à leurs ressources :

- Mot de passe avec niveau de complexité minimum requis
- Stockage sécurisé des mots de passe conformément aux standards à l'état de l'art
- Possibilité d'activer l'authentification multi-facteurs (MFA)
- Possibilité de paramétrage fin des permissions accordées sur les ressources de l'organisation à des utilisateurs humains ou des applications
- Journalisation des accès et de l'usage des droits à privilège

Monitoring des services et infrastructures

Scaleway dispose notamment des outils suivants afin de monitorer ses services et infrastructures :

- Un système de gestion des informations et des événements de sécurité (SIEM) permettant notamment de détecter les incidents de sécurité
- Un système de surveillance des actifs critiques et un dispositif de signalement en cas d'incident
- Un dispositif de détection anti-fraude

Conformément à nos conditions générales de service, nous rappelons que Scaleway n'a pas accès aux données hébergées par ses clients auxquels revient la responsabilité de monitorer et mettre en place les systèmes de détection adéquates dans le cadre du périmètre ne dépendant pas des services et infrastructures de Scaleway.

Gestion des menaces et vulnérabilités

Scaleway collecte et traite des renseignements sur les menaces et vulnérabilités à l'aide :

- d'une équipe interne CSIRT dédiée à la réponse aux incidents ;
- de ses relations avec des groupes ou dispositifs externes (dont les autres CSIRT/CERT).

Les vulnérabilités affectant les actifs de l'entreprise sont constamment identifiées à l'aide de différents outils de détection complémentaires, dont des scanners de vulnérabilités techniques réguliers ou encore des processus de veille.

Continuité d'activité

La continuité d'activité des infrastructures et services de Scaleway est assurée par les dispositifs suivants :

- Plan de Continuité d'Activité (PCA)
- Opérations critiques identifiées et associées à une procédure de restauration
- Informations répondant à des critères de disponibilité régulièrement sauvegardées
- Redondances des moyens de traitement de l'information
- Suivi du dimensionnement des actifs

Scaleway rappelle que le Client est responsable de la continuité de son système d'information (exemple : le choix des mesures de sauvegarde et de restauration ou encore le dimensionnement adéquat pour assurer le bon fonctionnement de son système d'information).

Sécurité des relations avec les sous-traitants

Scaleway s'assure que l'ensemble de ses sous-traitants bénéficient d'un niveau de sécurité équivalent par les mesures suivantes :

- Contrôle du niveau de sécurité et de mise en conformité relatif à la protection des données avant la conclusion du contrat
- Contrôle au minimum à chaque renouvellement de contrat et tous les deux ans pour les sous-traitants critiques
- Utilisation des Clauses Contractuelles Types ou de dispositif d'adéquation en cas de recours à un sous-traitant situé dans un pays non adéquat
- Inventaire des sous-traitants et documentation des contrats
- Surveillance, révision et gestion régulière des contrats avec les sous-traitants

Gestion des évènements liés à la sécurité de l'information

Scaleway met en place les dispositifs suivants afin d'assurer la gestion des évènements liés à la sécurité :

- Des processus et des outils de signalement internes et externes des évènements et des incidents, notamment un dispositif externe de remontée des incidents de sécurité via l'adresse csirt@scaleway.com.
- Des moyens humains et automatisés d'analyse des journaux et de détection des incidents (SOC)
- Une équipe entièrement dédiée à la réponse aux incidents de sécurité (CSIRT)
- Un processus d'amélioration continue relatif à la réponse aux incidents de sécurité dans un objectif d'apprentissage constant.