AXIALYS
CLOUD TELECOM SERVICES

Service PushSMS

1. Principe général et finalités du traitement

Ce service correspond au produit PushSMS vendu par Axialys.
Il consiste dans l'envoi de SMS, de façon unitaire ou sous forme de batches, de SMS depuis nos clients vers des téléphones mobiles en France et dans le monde.
Nos clients nous soumettent les SMS à envoyer par divers moyens (FTP, interface web…), nous les stockons et les soumettons ensuite à divers partenaires. Nous traitons également les réponses suivant le même principe (mais à l'envers).

Dans le cadre de ce traitement Axialys agit en tant que processeur de données pour le compte de ses clients, qui sont, dans ce cas contrôleurs des données.

Ce traitement est réalisé dans notre datacenter de Courbevoie, où les données sont stockées.

2. Catégories de personnes concernées

Toutes personnes, notamment :
- clients de nos clients
- prospects/contacts de nos clients

3. Catégories de données personnelles

Les données personnelles traitées sont :
- numéros de téléphone des destinataires
- contenus des messages transmis; bien que ces derniers ne soient que rarement, en pratique, des données personnelles dans le cadre de mailings ou de notifications, ils sont néanmoins considérés comme telles

Ce traitement ne traite pas de données personnelles sensibles au sens du RGPD.

4. Destinataires des données

4.1 Destinataires internes

D'une façon générale, aucune personne chez Axialys n'est destinataire de données dans le cadre de ce traitement, qui est pour l'essentiel automatisé.

Néanmoins :
- L'accès aux données personnelles est possible, pour des raisons de contrôle et de vérification, à l'équipe de support fonctionnel du service PushSMS
- L'équipe d'exploitation IT peut être amenée à accéder aux données personnelles, dans le cadre normal des opérations de maintenance et d'exploitation de nos systèmes

4.2 Destinataires externes et sous-traitants

Axialys, pour la fourniture de ce service, fait appel :
- à des opérateurs télécom
- à des "facilitateurs", dont le métier est de de servir d'intermédiaires entre Axialys et un grand nombre d'opérateurs télécom

La liste de ces partenaires est confidentielle [PPPUSHSMS].

Axialys garantit néanmoins avoir obtenu des partenaires en question des assurances quant à leur propre conformité au RGPD.

4.3 Export hors UE

Ces données personnelles ne font pas l'objet d'un transfert hors UE.

Les seules données personnelles transmises hors UE concernent les messages et numéros de téléphone des destinataires résidant hors UE, par essence exclues du scope du RGPD.

5. Délais effacement

Les données sont conservées à titre historique pendant une durée de 12 mois, suivant nos obligations vis-à-vis du CPCE.

6. Impact en cas de compromission

6.1 Compromission de la confidentialité

En cas de vol de données, le risque est que des numéros de téléphone mobile et/ou des messages personnels soient connus à l'extérieur; en outre, le nom de la personne n'est pas forcément associé. Le principal risque est l'exploitation du numéro de téléphone pour de l'envoi publicitaire.

impact ***modéré***.

6.2 Compromission de l'intégrité

En cas de compromission de l'intégrité des données ou de destruction, le principal impact est sur le service rendu par Axialys. Les données elles-même provenant du client, ce dernier est supposé en disposer.

Impact ***faible***

6.3 Compromission de la disponibilité

Le service n'est à priori pas utilisé par les personnes dont il est question des données, mais par des fournisseurs ou autres partenaires pour leur communiquer des informations. Une indisponibilité temporaire du service ne représente donc pas de risque important du point de vue de l'usage personnel.

Impact ***faible***

7. Risques et mesures de sécurité opérationnelles

Ce traitement ne représente pas à priori de risque spécifique :

- ✓ sensibilité des données personnelles : non
- ✓ attractivité qu'il pourrait susciter auprès de tiers malveillants : généralement faible, le seul risque identifié étant celui d'éventuelles tentatives d'abus (envoyer des SMS sans les payer par exemple), ce risque étant sans rapport avec les données personnelles.

D'une façon générale, les mesures de prévention et de sécurité globales aux services exploités par Axialys s'appliquent. Cf Mesures de sécurité applicables à tous les traitements internes.

De façon plus spécifique :
- transferts HTTP : les transferts de données, via l'interface web et l'API client, sont encryptés en SSL, grâce à un certificat émis par COMODO signé par une clef 2048 bits utilisant les standards PKCS#1. Il est de la responsabilité du client de s'assurer que les requêtes effectuées vers lui sont cryptées suivant un standard adapté.
- transferts FTP : les transferts de fichier batch sont effectués via SFTP. Axialys recommande l'usage d'une clef Ed25519
- emails : le transfert des fichiers par email non crypté n'est plus recommandé par Axialys
- stockage des données : les données afférentes à ces traitements sont stockées sur un cluster de deux serveurs de base de données interne, non crypté, inaccessible depuis l'extérieur (firewall). Ces serveurs fonctionnent en réplication en temps réel, de sorte que le serveur esclave puisse immédiatement poursuivre le service en cas d'indisponibilité avec le maître.