Conformité RGPD et politique de Protection des Données chez Netkin

Dernière mise à jour : 21/07/2019

Le présent document explique comment Netkin assure la conformité avec la RGPD, et quelles sont les dispositions mises en place pour assurer la sécurité de vos données personnelles ainsi que de celles de vos participants.

Qu'est-ce que la RGPD ?

RGPD veut dire " Régulations Générales de Protection des Données" et il s'agit d'une nouvelle régulation de l'Union Européenne qui entre en vigueur le 25 mai 2018.

Ces régulations sont conçues pour **harmoniser les lois concernant la protection des données personnelles à travers l'Europe, augmenter la protection des données personnelles des citoyens de l'UE et améliorer la manière avec laquelle les organisations utilisent ces données**. Il est crucial de savoir quels seront les changements que cela implique, puisque la non-conformité pourrait mener à de lourdes amendes pour les entreprises et organisations.

En tant qu'organisateur d'événement, en quoi cela me concerne-t-il ?

Le plus grand changement est probablement la juridiction élargie de la RGPD. À compter du 25 mai 2018, les règles relatives à la protection des données s'appliqueront à toutes les entreprises qui traitent des données à caractère personnel des citoyens de l'UE, quel que soit l'emplacement de l'entreprise.

La RGPD s'appliquera également au traitement des données personnelles pour les citoyens de l'UE, lorsque les activités concernent : l'offre de biens ou de services (gratuits ou payants) aux citoyens de l'UE, ainsi que le suivi des comportements au sein de l'UE. Les

entreprises extracommunautaires par rapport à l'UE et qui traitent les données des citoyens de l'UE sont tenues de désigner un représentant dans l'UE.

De ce fait, tant que certains de vos participants sont citoyens de l'UE, vous êtes concerné, et vos processus et outils doivent être conformes à la RGPD.

Quels sont les risques en cas de non-conformité ?

Si votre entreprise ou organisation est reconnue coupable d'infraction à la RGPD, vous serez passible d'une amende substantielle. Le maximum peut atteindre 4% de votre chiffre d'affaires global annuel ou 20 millions d'euros, selon le montant le plus élevé. Les amendes sont imposées pour des infractions telles que :

- consentement insuffisant du client pour traiter les données ;
- les violations du concept de « (la prise en compte de) la vie privée dès la conception » ou « Privacy by Design » ;
- ne pas avoir implémenté suffisamment de mesures de protection des données ;
- ne pas informer l'autorité compétente et les personnes concernées d'une violation.

Quelles sont mes obligations et quelles sont les obligations de Netkin ?

La RGPD définit deux rôles dans le processus de gestion des données de vos participants : Le Responsable du traitement des données (Data Controller) et les Sous-traitants de données (Data Processor).

<u>Le Responsable du traitement</u> (Vous-même, et/ou votre client, en tant qu'organisateur d'événements)

Le Responsable du traitement des données désigne la personne ou l'entreprise qui décide quelles informations sont collectées, à quelles fins et de quelle manière elles sont traitées. Selon la législation de l'UE, les obligations du Responsable du traitement incluent, mais ne sont pas limitées à :

- fournir des informations claires à vos participants sur les données personnelles que vous collectez et dans quel but ;
- obtenir le consentement clair du participant : qu'il accepte de fournir ses données personnelles pour ce but précis
- fournir au participant un moyen simple de demander d'effacer et/ou d'arrêter la diffusion des données, et, potentiellement, que les sous-traitants tiers arrêtent le

traitement de ces données personnelles et que ces dernières soient restituées au participant dans un format lisible (Excel par exemple)

Depuis mai 2018, tous les sites d'inscription nouvellement réalisés avec la solution Netkin ont une case à cocher obligatoire sur la première étape d'inscription, avec un texte normalisé relatif à ces obligations.

- ***Nous vous conseillons fortement de lire attentivement ce texte avec votre service juridique interne ou avec celui de votre client, pour vous assurer qu'il est conforme avec la politique de l'entreprise ou du pays où vous et/ou votre client est implanté.***

Les obligations du Responsable du traitement comprennent également :

- conserver et traiter uniquement les données absolument nécessaires à l'accomplissement de ses missions (minimisation des données). En outre, limiter et contrôler l'accès des éventuels sous-traitants à ces données personnelles ;
- protéger les données personnelles contre la perte accidentelle, l'accès non autorisé, ou le traitement illégal ;
    - ***Netkin assure cette protection au niveau de la plateforme (voir ci-dessous), mais la sécurité de votre boîte aux lettres, de votre ordinateur, de votre logiciel, etc. est votre responsabilité***
- établir des accords écrits avec les sous-traitants des données - qui ont accès aux données du client sous votre autorité - qui les obligent à agir uniquement selon vos instructions et s'assurer qu'ils respectent toutes les exigences de protection des données ;
- informer les participants dans les 72 heures suivant une violation de données – ou de la prise de conscience d'un tel acte ;
- s'assurer que tous les sous-traitants de données répondent aux exigences (voir ci-dessous).

<u>Le Sous-traitants de données</u> (Netkin, OVH notre société d'hébergement, et vos autres sous-traitants)

Le sous-traitant de données est toute personne ou entreprise qui traite des données personnelles pour le Responsable du traitement telles que la plateforme d'inscription, l'application événementielle, les services d'analytics, les services d'hébergement ou de stockage, etc.

IMPORTANT: Si vous exportez des données de la plateforme Netkin (par exemple sous forme de fichier Excel), vous êtes également sous-traitant des données, et les obligations des sous-traitants des données s'appliquent à vous, et à tous vos sous-traitants qui pourraient avoir accès à ces données exportées (pour l'inscription des participants gérée en freelance, ou pour la sous-traitance d'impression de badge par exemple).

Les exigences pour les sous-traitants des données incluent, mais ne sont pas limitées à :

- traiter les données de manière raisonnable, légale et à des fins légitimes ;
- mettre en oeuvre toutes les mesures de sécurité appropriées pour protéger les données personnelles ;
- informer immédiatement le Responsable du traitement de toute violation de données ;
- conserver les enregistrements internes de toutes activités de traitement de données ;
- renforcer la protection de la vie privée dès la conception : cela signifie l'inclusion de la protection des données dès le début de la conception des systèmes au lieu d'un ajout ultérieur. Plus spécifiquement, vous devez mettre en œuvre des mesures techniques et organisationnelles appropriées pour répondre aux exigences de la nouvelle réglementation et protéger les droits des personnes concernées. Netkin a mis en place des mesures appropriées pour se conformer entièrement à ces exigences. (Voir ci-dessous)

Politique de sécurité des données chez Netkin

Protection de la vie privée dès la conception (Privacy by design)

Depuis sa création, la solution Netkin respecte le principe de la confidentialité dès la conception.

- Chaque évènement possède sa propre plateforme (instance de notre solution), totalement isolée sur nos serveurs dédiés hébergés chez OVH (nous n'utilisons pas de cloud public), avec sa propre base de données privée.
- Chaque instance d'événement n'a aucun moyen de communiquer avec d'autres plateformes événementielles, malgré leur présence sur le même serveur physique : la technologie “Cage FileSystem” de CloudLinux isole chaque instance sur le serveur dans un système de fichier indépendant, l’empêchant de voir l'existence des autres instances sur le même serveur.
- Notre système de déploiement automatisé ne peut pas accéder aux instances d'événement après le déploiement, il ne peut que leur envoyer des instructions de configuration ou de backup, ne donnant en aucun cas l’accès au données. Même en cas de backup, c’est l’instance elle même qui crypte la sauvegarde en AES256-cbc, et envoie la clef de décryptage dans un “coffre sécurisé” situé sur un autre serveur dédié non accessible de l'extérieur. Cette clef est différente à chaque sauvegarde.
- Dans une instance d'événement, les utilisateurs privilégiés (administrateurs en charge de l'inscription des participants) ont un contrôle d'accès entièrement audité.

- Tous les utilisateurs privilégiés doivent s'authentifier par défaut en utilisant la 2FA (lien de connexion automatique avec code de confirmation à hash fort + SMS).
- Dans une instance d'événement, un participant ne peut pas accéder aux données d'autres participants, sauf dans le who's who, dans lequel vous pouvez choisir les champs à afficher. Par défaut, le courrier électronique, le numéro de téléphone ou d'autres données sensibles ne sont pas inclus, auquel cas ces données ne sont même pas téléchargées sur les machines des participants. Seuls les utilisateurs privilégiés que vous (l'administrateur principal du client) nommerez peuvent y accéder.
- Aucun membre du personnel de Netkin ne peut accéder à l'administration de votre plateforme d'événement sans votre autorisation explicite
- Parmi le personnel technique de Netkin, personne ne peut accéder au code source ou aux données de votre plateforme d'évènements sans l'approbation d'un associé Netkin.

Tests d'intrusion automatisés

- Chacune de nos nouvelles release est scannée en utilisant la dernière version d'Acunetix, directement sur le serveur de production, avant sa publication
- Sur demande, nous pouvons effectuer un tel scan de sécurité sur l'instance de votre évènement une fois qu'il est prêt, en tant qu'utilisateur anonyme et en tant que participant connecté uniquement (Le scan de sécurité en tant qu'utilisateur privilégié modifiera le contenu de votre plateforme). Compte tenu de nos prix compétitifs, ce scan supplémentaire fera l'objet un prix forfaitaire, et un rapport de scan vous sera remis.

Tests d'intrusion humains (pentests)

Chaque nouvelle version de notre solution est pentestée avant sa mise en production par Lexfo, et surveillée continuellement par leur solution Ambionics. Le résultat du dernier pentest est accessible sur demande.

En parallèle, plusieurs fois par an, nos clients demandent à effectuer des tests de pénétration ou des scans de sécurité en direct sur une instance. Cela ne peut être fait que dans le périmètre suivant : en effectuant des tests (de n'importe quel type) sur l'une de nos instances et / ou serveur, vous respectez pleinement les restrictions mentionnées ci-dessous - vous pourriez être responsable de tout dommage causé en ne respectant pas ces restrictions.

- Aucun accès technique au serveur ne sera fourni (ceci est strictement non négociable puisque notre code source n'est pas divulgué pour des raisons de sécurité).

- Le test ou le scan connecté avec un compte privilégié (administrateur) est strictement interdit car ceci pourrait altérer le site structure et / ou le contenu, et envoyer des e-mails indésirables. Les comptes privilégiés ont, de toute façon, la possibilité d'exporter toutes les données.
- Aucun test susceptible d'altérer les données et / ou la qualité de service n'est autorisé car votre instance cible est sur un serveur de production.
- Aucun test DDoS n'est autorisé (notre hébergeur OVH a une protection DDoS de niveau centre de données).
- Les tests ne peuvent être effectués qu'en tant qu'utilisateur anonyme (non connecté) et participant régulier (pas de privilège).
- Vous n'êtes pas autorisé à exporter ou à divulguer des données auxquelles vous pourriez avoir accès pendant le test.

Sécurité des serveurs de stockage et de production

Les données sont hébergées exclusivement sur des serveurs dédiés OVH en France, situés dans les centres de données principaux d'OVH à Roubaix (France), Gravelines (France) et Strasbourg (France).

- **Mesures de sécurité physiques des datacenters OVH :** https://www.ovh.com/fr/apropos/datacentres.xml et https://www.ovh.com/fr/apropos/securite.xml
- **Serveurs frontaux** (Apache 2.4, php 5.x) : CloudLinux 7.x (version durcie de CentOS 7.x), WHM / CPanel avec CPHulk (protection de force brute) et firewall intégré. Aucune base de données client sur ce serveur.
    - En utilisant la technologie CageFS (fournie par CloudLinux), chaque instance s'exécute dans son propre système de fichiers « en cage » et ne peut pas voir les fichiers, données, processus d'autres instances, ni les fichiers sensibles de la configuration du serveur. Plus d'information sur https://cloudlinux.com/index.php/cagefs
    - Aucun de nos clients n'a un accès administratif ou technique au serveur (pas d'accès FTP ou MariaDB, CPanel, ou shell, etc.)
    - Mises à jour et correctifs entièrement automatisés pour CPanel et CloudLinux/CentOS, avec un résumé envoyé par email à CSO, et une vérification humaine mensuelle
    - antivirus ClamAV avec analyse quotidienne automatisée
    - protection DDOS par OVH
    - Apache 2.4 / PHP 5.5
    - Filtre CSR OWASP Apache ModSecurity
    - Firewall applicatif CloudFlare disponible en option
    - Les accès administratifs au serveur sont tous filtrés via IP, seule la connection en passant par notre VPN sécurisé est possible. La connection à ce VPN est monitorée et limitée dans le temps.

    - Protection brute force sur tous les mécanismes d'authentification du serveur, et sur les mécanismes d'authentification de chaque instance.
    - Les logs Apache, Firewall, CPHulk sont analysés quotidiennement de manière automatisée, et chaque semaine de manière humaine, afin de détecter toute anomalie de sécurité ou de performance

- **Grappe de serveurs (cluster) de base de données (mariadb 10.1.x)** :
    - CentOS 7.x, seul le port 3306 est autorisé via le pare-feu, sur LAN privé (VRack by OVH), avec cryptage de données sur disque.
    - Ce cluster n'est pas accessible depuis Internet.

Principes de sécurité lors du développement logiciel

Chaque contribution de code de nos développeurs est examinée par le CTO et CSO Netkin pour détecter tout problème de performance ou de sécurité, notamment selon les recommandations OWASP (https://www.owasp.org/index.php/OWASP_Code_Review_Guide_Table_of_Contents), parmi lesquelles:

- Les environnements de developpement, test et production sont séparés physiquement au niveau réseau (OVH v-rack), et sur des machines physiques différentes.
- La sécurité du transport :
    - https obligatoire avec certificat indépendant pour chaque instance en auto-renouvellement tous les 3 mois, et HSTS activé
    - les chiffrements ou protocoles faibles ont été désactivés
    - note Qualys SSL Labs: A+
    - Rapport d'analyse : https://www.ssllabs.com/ssltest/analyze.html?d=pentest.event.netkin.io&hideResults=on
- Sécurité d'authentification
    - Afin de ne pas risquer de collecter les mots de passe de vos utilisateurs, nous utilisons exclusivement des lien d'auto-connexion pour accéder à la plateforme.
    - Les liens d'auto-connexion utilisent un jeton aléatoire avec un hash de vérification très long, de la forme : https://nameoftheventwebsite.com/trk/437-FDimZkGaIfmYdMDkimWT--nkwsid169-7a3505564affeec839987386ee0a41f0c08aeb2bb122b85d26e4d0a7fa4dde6e-c5d4156451-bfe7a71f3abc87ac28ecb051e2484b7c9dfa1ea917eb2921f69bda96f11b8c25
    - L'unicité de chaque chaîne aléatoire est appliquée en stockant leur hash sha256.
    - Protection par force brute IP de 8 tentatives, désactivant la capacité d'authentification pour l'adresse IP pendant 30 minutes

    - L'accès administratif de l'instance peut être sécurisé en utilisant une 2FA à usage unique (lien jeton à usage unique envoyé par courriel en fonction de la session du navigateur, qui doit être validé en utilisant le code temporaire à usage unique envoyé par SMS)
    - Lorsqu'un utilisateur privilégié se connecte à partir d'une adresse IP inconnue ou d'un nouveau navigateur, tous les utilisateurs disposant du privilège de gestion des droits utilisateur peuvent être notifiés par courrier électronique, avec un lien à usage unique permettant le verrouillage immédiat du compte.
    - Les cookies d'authentification et les cookies de session sont HttpOnly et Secure. Notre application stocke une représentation hachée de la valeur du cookie quand il est envoyé, puis compare la valeur du cookie reçu pour s'assurer qu'ils sont les même.
- Contenu mixte :
    - Toutes les ressources sont chargées à partir du nom de domaine de l'instance, pas d'utilisation de CDN
    - Protection Cross Site Request Forgery (XSRF ou CSRF) : Les demandes de modification de données ne sont effectuées que via POST. Chaque requête de POST est validée avec un jeton CSRF. Si ce dernier est manquant ou faux, la demande est bloquée.
    - Cross Site Script Inclusion (XSSI) : Toutes les requêtes JSON sont effectuées via POST uniquement
    - Détournement de clicks « Clickjacking » : en-tête X-Frame-Options: SAMEORIGIN envoyé sur chaque page, et détection javascript d'inclusion iframe.
- Validation des entrées
    - Injection SQL : toutes les requêtes contenant des entrées d'utilisateurs utilisent des requêtes paramétrées
    - XPath Injection : pas d'utilisation de X-Path
    - Injection LDAP : aucune utilisation des requêtes LDAP
    - Injection de commande : pas d'utilisation de ligne de commande dans le code php
- Path Traversal : l'optimisation et le recadrage d'image valident le type MIME du fichier demandé et se limitent au répertoire d'images de contenu utilisateur
- « Cross Site Scripting » (XSS) ou Injection SQL: les données collectées par l'utilisateur sont nettoyées de tout contenu HTML ou caractères spéciaux avant stockage en base de données, affichées à l'aide de la fonction d'échappement appropriée
- « Débordements d'entier » : pour chaque entrée numérique, la longueur et le type sont validés

Sécurité des bureaux et de l'équipement Netkin

- Réseau local protégé par appliance WatchGuard Firebox M200

- Avast Business Antivirus (version payante entièrement fonctionnelle, avec système de gestion centralisé et mise à jour automatique, les utilisateurs ne peuvent pas désactiver, désinstaller ou paramétrer l'antivirus. Sensibilité heuristique élevée par défaut avec émulation de code, analyse de tous les fichiers à leur ouverture, et firewall intégré bloquant toute connection non connue par défaut.)
- Détection d'intrusion et détection d'incendie par Securitas Direct / Verisure (certification APSAD R31 P3)
- Vidéo-surveillance de tous les lieux de passage dans nos locaux, avec rétention des vidéos pendant 30 jours.
- Les comptes de messagerie de nos employés sont des comptes Gmail Enterprise avec 2FA activés
- Pas d'accès wifi autorisé au réseau local

Politique de sécurité du personnel Netkin et sous-traitants évènementiels

- Tous les employés sont en CDI à temps complet et ont signé un accord de non-divulgation (NDA) spécifique couvrant toutes les données internes et clients.
- Seuls les employés requis sont autorisés à accéder aux données et ces derniers ne sont pas autorisés à conserver une copie des données. Tous les employés ont signé ceci dans le cadre de leur NDA.
- Les employés ne sont pas autorisés à conserver la copie des données client en dehors de l'instance du client. Toute copie provisoire (reçue par un biais quelconque, y compris un courrier électronique) ou extrait de l'instance client doit être supprimée immédiatement après utilisation. Toute extraction de données doit être effectuée par le client en utilisant son accès administratif à la plateforme. Nous n'effectuons pas l'extraction de données pour le compte de nos clients.
- Dans le cas où un évènement nécessite l'intervention d'un sous-traitant (freelance notamment), cela ne se fait pas sans accord de notre client, et nous signons un contrat de sous-traitance des données avec le sous-traitant

Politique de sécurité du personnel technique

- Développement sur serveur local dans nos bureaux, serveurs de test et de staging chez OVH avec analyse antivirus automatique, tests fonctionnels automatisés et humains, et scan Acunetix effectué par le CSO sur chaque release candidate avant sa publication.
- Les instances de production sont ensuite déployées automatiquement par une application de déploiement locale située sur un serveur dédié dont l'accès est filtré par IP.

- Cette solution installe le code source, la base de données, les boîtes aux lettres, les certificats SSL et envoie un accès administratif au client, qui peut alors accorder l'accès à notre équipe de projet si nécessaire.
- Les développeurs n'ont pas accès au code source de l'application, ni à la base de données ou au serveur.
- Cela garantit le fait que nos employés n'ont pas accès aux instances de production des clients, sauf autorisation expresse de la direction et/ou du client (uniquement sur demande écrite, les demandes téléphoniques n'étant pas autorisées).

Politique de continuité d'activité (sauvegarde et rétablissement des données, temps de remise à niveau)

- Chaque instance est sauvegardée de manière cryptée une fois par jour sur un serveur de stockage OVH situé dans un autre datacenter. Les sauvegardes sont conservées quotidiennement pendant une semaine, puis hebdomadairement ou mensuellement, jusqu'à la destruction des données (voir ci-dessous).
    - Sauvegarde quotidienne automatisée des bases de données et des fichiers utilisateurs, cryptée avec AES-256-CBC, vers un serveur de stockage sécurisé dans un datacenter différent des serveurs de production. Le RPO est donc de 24h.
    - Surveillance de la sauvegarde automatisée
    - Temps de rétablissement des données en cas de panne (aussi appelé RTO) :
        - Site d'inscription (utilisé **avant** l'évènement) : sous 4h
        - App Netkin Live (utilisé **pendant** l'évènement : interactivité, réseau social, who's who, etc.) : L'application d'interactivité effectue une répartition de charge (load balancing) au niveau client, vers 4 serveurs différents contenant exactement les mêmes données, en réplication constante et tolérant les interruptions de réseau, situés dans 2 datacenters différents (Roubaix et Strasbourg). Le temps de rétablissement d'un serveur défaillant n'a donc aucun impact sur le bon fonctionnement de l'application.
- Nous nous engageons à un niveau de service (SLA) de 99,95% sur la disponibilité générale de la plateforme.
- Cela exclut toute mauvaise configuration effectuée par le client lors de 'auto-administration de la plateforme, ainsi que les navigateurs ou matériels mal configurés ou obsolètes qui pourraient ne pas être en mesure d'accéder à ou d'afficher le site web ou l'application de l'événement.

Politique de Conservation de Données

- Par défaut, 1 an après le déploiement de l'instance d'un évènement (site + app) , les données participant sont automatiquement effacées, après 3 alertes email à l'administrateur principal du site.
- Au bout de 3 ans, toutes les données sont automatiquement détruites, ceci incluant les sauvegardes (backups). Si vous le souhaitez, vous pouvez, nous demander de réduire ou d'augmenter cette période, dans le respect de la législation en vigueur

Des questions ?

Pour toute information complémentaire, n'hésitez pas à nous à l'adresse email suivante : support@netkin.fr