UNIVERSE

Hedge Finance UAB	Référence 11
Archivage, PCA, sécurité, conservations des données et RGPD	
Emetteur : Hedge Finance UAB	Destinataires : Tous collaborateurs concernés
Périmètre d'application : Toute l'organisation de Hedge Finance	
Version : Octobre 2024	

Historique du document

Version	Date	Rédacteur	Valideur	Objet de la mise à jour
V1	7/10/2024	Hedge Finance UAB	Hedge Finance UAB	Version initiale

Conservation du document

Dossier partagé Hedge Finance

Résumé de la procédure

Cette procédure a pour objet de :

- présenter les mesures mises en œuvre au sein de Hedge Finance ;
- détailler les obligations et diligences qui en résultent pour les collaborateurs ;
- rappeler les mesures des contrôles permanent et périodique en place ;
- préciser les références réglementaires applicables.

Important

Cette procédure est :

- mise en œuvre sous la responsabilité du PDG et du responsable de la conformité ;
- actualisée autant que nécessaire, notamment en cas d'évolution réglementaire et de changement d'organisation ou de gouvernance ;
- révisée a minima une fois par an.

SOMMAIRE

Dans le cadre de leurs fonctions, les collaborateurs de Hedge Finance UAB doivent accomplir les diligences définies par cette procédure ainsi que celles des documents connexes mentionnés.

1. CONTEXTE DE LA PROCÉDURE

1.1. INTRODUCTION

Hedge Finance UAB est une société privée à responsabilité limitée (UAB) créée le 09/09/2024, enregistrée au RCS de Lituanie sous le Numéro 306987021, dont le siège social est domicilié Didžioji g. 14-1, LT-01128 Vilnius.

La clientèle de Hedge Finance est composée en majorité de clients particuliers - personnes physiques - et marginalement de clients professionnels.

L'objet de cette procédure est de préciser la politique de Hedge Finance concernant l'archivage, conservation des données, le PCA/PUPA (Plan de continuité de l'activité / Plan d'urgence et de poursuite d'activité), la sécurité et le RGPD.

1.2. DÉFINITIONS UTILES

1.2.1. Le RGPD

En application depuis le 25 mai 2018, le Règlement Général sur la Protection des Données personnelles (RGPD), poursuit trois objectifs :

- renforcer les droits des personnes ;
- responsabiliser les acteurs ;
- les inciter à renforcer la coopération entre eux.

Ce règlement concerne toutes les sociétés établies sur le territoire de l'Union européenne, mais également les sociétés localisées hors de l'UE qui proposent des biens et des services, ou collectent des données relatives à des citoyens européens.

Il s'applique à toute entreprise qui collecte, traite et stocke des données personnelles dont l'utilisation permet d'identifier une personne physique.

Hedge Finance traite quotidiennement des données à caractère personnel relatives à ses clients ou collaborateurs. La mise en œuvre de traitements sur ces données doit se faire dans le respect des principes et obligations édictés par le règlement européen et sous le contrôle de la Commission Nationale Informatique et Libertés (CNIL) qui veille en Europe à l'application de la loi et du RGPD.

1.2.2. Les données personnelles

La CNIL définit les données personnelles comme toute information se rapportant à une personne physique identifiée ou identifiable.

Une personne physique peut être identifiée :

- directement (exemple : nom et prénom) ;
- indirectement (exemple : par un numéro de téléphone ou de plaque d'immatriculation, un identifiant tel que le numéro de sécurité sociale, une adresse postale ou courriel, mais aussi la voix ou l'image).

L'identification d'une personne physique peut être réalisée :

- à partir d'une seule donnée (exemple : nom) ;
- à partir du croisement d'un ensemble de données (exemple : une femme vivant à telle adresse, née tel jour et membre dans telle association).

Dans le cadre de son activité, Hedge Finance est amené à traiter des données personnelles relatives à l'identification des personnes, que ce soient ses salariés, ses clients ou des contreparties.

Toutes les données à caractère personnel stockées au sein de Hedge Finance, même ni utilisées ni traitées, même anciennes et archivées, sont concernées par la réglementation (par exemple : tout fichier, tableur Excel, bases de données de prospects, photocopies de pièces d'identités, adresses personnelles...).

1.2.3. La cybersécurité

« La cybersécurité » est définie comme l'ensemble des contrôles et des mesures d'organisation ainsi que des moyens (humains, techniques, etc.) utilisés pour protéger les éléments du système d'information et des réseaux de communication contre toutes attaques logiques, que celles-ci soient conduites par le biais de brèches de sécurité physique ou logique. Ces contrôles et mesures incluent la prévention, la détection et la réponse à toute activité informatique malicieuse visant des éléments du système d'information, et affectant potentiellement la confidentialité, l'intégrité ou la disponibilité des systèmes et des données, de même que la traçabilité des opérations effectuées sur ces systèmes et réseaux ».

De l'installation d'un antivirus jusqu'à la configuration de serveurs, ou encore le gardiennage des datas centers et des bureaux, la sécurité informatique impacte tous les métiers de la finance.

Outre les cyberattaques, la cybersécurité permet la mise en place de processus auprès des collaborateurs pour l'instauration de bonnes pratiques. En effet, les erreurs humaines sont des sources réelles de fuites de données. La sensibilisation des équipes aux problématiques de phishing ou d'usurpation d'identité est une composante importante d'une politique de sécurité informatique.

Hedge Finance a besoin de processus de cybersécurité fiable et performant afin de travailler dans de bonnes conditions. La protection des données sensibles est essentielle pour garantir l'intégrité de chaque collaborateur, mais aussi des clients et des partenaires.

1.3. CHAMP D'APPLICATION DE LA PROCÉDURE

Hedge Finance fournit pour les services d'investissement suivants (VASP) :

- échange entre actifs virtuels et monnaies fiduciaires ;
- échange entre une ou plusieurs formes d'actifs virtuels ;
- transfert d'actifs virtuels, c'est-à-dire effectuer une transaction pour le compte d'une autre personne qui déplace un actif virtuel d'une adresse ou d'un compte d'actif virtuel à un autre ;
- fournisseur de portefeuille dépositaire ; et
- participation et fourniture de services financiers liés à l'offre d'un émetteur ou à la vente d'un actif virtuel ou aux deux.

Plus spécifiquement, il s'agit des produits suivants :

- tokens se référant à des obligations, actions, OPCVM, ETF, produits structurés, options.

2. DISPOSITIF D'ARCHIVAGE ET DE CONSERVATION DES DONNÉES

2.1. TYPE DE DONNÉES ET LIEUX DE STOCKAGE

Les données concernées par cette procédure peuvent être de format papier ou informatique. Pour les données au format papier, elles sont sauvegardées au sein du site d'AWS à Paris et dupliquées dans celui de Francfort s'agissant des documents contractuels et autres documents sensibles. Dans la mesure du possible, tous les documents doivent être conservés, en particulier, ceux contenant la signature de Hedge Finance sous forme de scan. Les données au format informatique sont conservées chez le prestataire suivant : AWS. Tous les documents, fichiers, enregistrements téléphoniques ainsi que les mails sont stockés sur les serveurs de Hedge Finance. Il est à noter que les factures émises par Hedge Finance sont conservées et archivées au siège de la société.

La société Hedge Finance possède des serveurs de production hébergés par AWS dans deux data centers situés dans 2 espaces géographiques différents, l'un à Paris, l'autre à Francfort. Le serveur principal est situé à Paris et le serveur de secours (serveur fail-over) est situé dans un data center à Francfort. La Société utilise l'offre "Business" de cloudflare pour permettre une atténuation des attaques DDOS, une Pare-Feu d'application web (WAF) grâce aux règles Cloudflare et OWASP ModSecurity.

Hedge Finance est en conformité avec les dernières normes PCI grâce aux pare- feu WAF de Cloudflare et au mode «Modern TLS Only » autorisant seulement l'utilisation des dernières normes TLS garantissant une sécurité optimale, notamment lors de la saisie de données bancaires et de cartes de paiement le cas échéant.

Hedge Finance est également titulaire d'un certificat SSL EV à Validation Étendue garantissant une sécurité optimale pour les banques en ligne et les organismes d'investissement. Hedge Finance a fait l'objet d'une vérification téléphonique via un test afin de vérifier l'existence de la société et confirmant notre volonté de garantir une sécurité optimale sur la plateforme.

Les outils de travail sont divisés sur plusieurs ordinateurs et machines virtuelles. Chaque employé de Hedge Finance dispose d'un ordinateur sur lequel il peut utiliser ses outils bureautiques.

Les développeurs possèdent un ordinateur depuis lequel ils peuvent utiliser leurs outils de développement afin de faire avancer le développement informatique de l'entreprise. Le responsable du développement a une machine virtuelle installée sur son ordinateur. Cette machine virtuelle sert uniquement à administrer nos deux serveurs de production et il est possible de les administrer uniquement via cette machine virtuelle, protégée elle-même par un mot de passe connu uniquement du responsable développeur.

2.2. DURÉE DE STOCKAGE

Le tableau ci-dessous présente les différentes durée, support, lieu de stockage selon la nature des données :

Thème	Type de document	Durée	Lieux
LCB-FT Abus de marché	Bénéficiaire effectif	5 ans à compter de la clôture des comptes ou de la cessation de la relation	- Armoire sécurisée située au 25 Rue Victor Hugo 69007 Lyon - Deux serveurs AWS
	Documents relatifs à l'identité des clients	5 ans à compter de la clôture des comptes ou de la cessation de la relation	- Armoire sécurisée située au 25 Rue Victor Hugo 69007 Lyon - Deux serveurs AWS
	Documents relatifs aux opérations effectuées par les clients	5 ans à compter de leur exécution	- Armoire sécurisée située au 25 Rue Victor Hugo 69007 Lyon - Deux serveurs AWS
	Caractéristiques des opérations donnant lieu à un examen renforcé	5 ans à compter de leur exécution	- Armoire sécurisée située au 25 Rue Victor Hugo 69007 Lyon - Deux serveurs AWS
	Déclaration abus de marché AMF, déclaration TRACFIN	5 ans	- Armoire sécurisée située au 25 Rue Victor Hugo 69007 Lyon - Deux serveurs AWS
Clients	Dossiers clients : Catégorisation, relation, ...	5 ans à compter de la fin de la relation	- Armoire sécurisée située au 25 Rue Victor Hugo 69007 Lyon - Deux serveurs AWS
Opérations	Tous les éléments relatifs aux ordres et aux opérations : Piste d'audit concernant les ordres passés : modèle quantitatif ; transactions ; ...	5 ans à partir de la réalisation de l'opération	- Armoire sécurisée située au 25 Rue Victor Hugo 69007 Lyon - Deux serveurs AWS
	Enregistrement téléphonique	5 ans	- Armoire sécurisée située au 25 Rue Victor Hugo 69007 Lyon - Deux serveurs AWS
Conformité Contrôle Interne	Procédures internes (toutes les versions successives)	Sans limitation	- Armoire sécurisée située au 25 Rue Victor Hugo 69007 Lyon - Deux serveurs AWS
	Documents relatifs aux contrôles réalisés (rapports trimestriels CiD, documents justificatifs des contrôles ...)	Sans limitation	- Armoire sécurisée située au 25 Rue Victor Hugo 69007 Lyon - Deux serveurs AWS
	Documents relatifs aux mesures prises en présence d'informations privilégiées (Mise en place de listes)	Sans limitation	- Armoire sécurisée située au 25 Rue Victor Hugo 69007 Lyon - Deux serveurs AWS

	Registre des conflits d'intérêts	Sans limitation	- Armoire sécurisée située au 25 Rue Victor Hugo 69007 Lyon - Deux serveurs AWS
	Pièces déclaratives des transactions personnelles et preuve des contrôles	Sans limitation	- Armoire sécurisée située au 25 Rue Victor Hugo 69007 Lyon - Deux serveurs AWS
	Cartes professionnelles et leur dossier (sauf celle du RCSI conservée par l'AMF)	10 ans après la cessation des fonctions ayant donné lieu à la délivrance de la carte professionnelle	- Armoire sécurisée située au 25 Rue Victor Hugo 69007 Lyon - Deux serveurs AWS
Entreprise d'investissement	Agrément ACPR	Sans limitation	- Armoire sécurisée située au 25 Rue Victor Hugo 69007 Lyon - Deux serveurs AWS
	Appartenance à une association professionnelle	Sans limitation	- Armoire sécurisée située au 25 Rue Victor Hugo 69007 Lyon - Deux serveurs AWS
	Conventions prestataires successives : RCSI, Informatique, Emetteurs...	Sans limitation	- Armoire sécurisée située au 25 Rue Victor Hugo 69007 Lyon - Deux serveurs AWS
	Rapports de contrôle AMF, comptes annuels, franchissement de seuils, reporting officiel, tout échange avec les autorités	Sans limitation	- Armoire sécurisée située au 25 Rue Victor Hugo 69007 Lyon - Deux serveurs AWS
Risques	Tout document relatif à la gestion des risques	Sans limitation	- Armoire sécurisée située au 25 Rue Victor Hugo 69007 Lyon - Deux serveurs AWS

Les autres types de documents (états comptables, documents RH, les factures, les quittances de loyer...) ne sont pas mentionnés ici. Les délais de conservation de ces documents pour les entreprises peuvent être consultés à l'adresse suivante :

http://vosdroits.service-public.fr/professionnels-entreprises/F10029.xhtml

De façon générale, les mails et tous les fichiers informatiques présents sont archivés sur le serveur. Pour les documents au format papier, ils sont conservés dans les locaux de Hedge Finance. La politique est néanmoins de scanner tous les documents importants afin d'en assurer leur conservation.

3. DISPOSITIF RELATIF A LA CONTINUITÉ DE L'ACTIVITÉ (PCA-PUPA) ET LA SÉCURITÉ

Les personnes en charge de la gestion et du pilotage du PCA / PUPA sont les suivantes : Boris FRERE et Mathis GAUTHIER.

3.1. LE PCA / PUPA

3.1.1. Principes du PCA / PUPA

Le plan de continuité d'activités comprend 4 grandes étapes qui sont :

- La notification de la rupture : Détection de la rupture et notification au personnel de celle-ci ;
- L'analyse et le rétablissement : Identification des systèmes et des ressources impactés, identification des dommages causés, prise de décision afin de fournir un service palliatif ;
- La restauration : Remise à niveau des systèmes impactés, analyse des origines de la rupture, mise en place et amélioration des systèmes afin d'éviter une future rupture identique ;
- La communication : Envois réguliers d'information vers le personnel impacté et les différentes personnes impliquées dans la résolution.

La responsabilité de l'application des consignes de sécurité de Hedge Finance relève du Président Directeur général, en son absence le Directeur général délégué.

3.1.2. Elaboration du plan, ressources et champs d'application

Le PCA a été élaboré en fonction de 2 cas clés :

- Hedge Finance ne peut pas exercer son activité.
- Hedge Finance n'est pas en mesure d'exercer pleinement son activité.

Plusieurs hypothèses ont été retenues afin de développer ce plan :

- Indisponibilité des systèmes due à un fait interne entraînant une identification des systèmes impactés, des conséquences entraînées et de la prise de mesure afin de rétablir l'activité.
- Indisponibilité des systèmes due à un fait externe entraînant une identification des systèmes impactés, des fournisseurs externes à contacter et à coordonner et de la prise de mesure afin de rétablir l'activité.
- Indisponibilité des systèmes due à un fait interne et externe entraînant une mise en relation des fournisseurs externes avec le personnel interne afin d'identifier les systèmes impactés, les conséquences entraînées et la prise de mesure nécessaire pour le rétablissement d'une situation normale.

Le plan de continuité d'activité s'applique aux ressources et aux fonctions nécessaires pour reconstituer et reprendre l'exploitation des systèmes comme à l'origine. Hedge Finance dispose d'un espace alloué dans une structure située à Paris pour la production et à Francfort pour le backup laquelle sert de centre technique pour assurer la continuité de l'activité avec :

- Une gestion de la messagerie (logiciel anti-spam, consultations à distance...) ;
- Un serveur de sauvegarde des fichiers en « miroir » du serveur local (lui-même installé en salle protégée dans les locaux de Hedge Finance) ;
- Des serveurs d'administration Jump Cloudfare.

3.1.3. Scénario 1 : Indisponibilité du serveur principal

Dans le cas d'une indisponibilité totale (destruction, incendie, dégâts des eaux...) sur le serveur principal, le jump serveur cloudflare de Hedge Finance s'occupe de redistribuer les requêtes vers le serveur de backup (secours).

En cas d'indisponibilité partielle, si celle-ci indique un manquement quelconque des services fournis par Hedge Finance aux clients, alors, les requêtes sont automatiquement redirigées vers le serveur de secours grâce aux jump serveurs de cloudflare.

En cas d'indisponibilité totale ou partielle du serveur principal, le responsable du service support est chargé d'identifier la source de l'erreur et de la corriger au plus vite. Le cas échéant, le PDG est informé de la résolution des indisponibilités.

3.1.4. Scénario 2 : Inaccessibilité des bureaux de la société

La machine virtuelle d'administration du serveur est stockée sur une clé USB située en dehors des locaux de Hedge Finance dans un coffre en banque. Le responsable du service support a accès à la clé USB et peut administrer les serveurs de Hedge Finance depuis un nouvel ordinateur.

Le PDG est informé de la résolution de l'inaccessibilité des bureaux de Hedge Finance.

3.1.5. Scénario 3 : Inaccessibilité des systèmes de production et cellule de crise

En cas extrême d'inaccessibilité totale des deux systèmes, Hedge Finance met en place une cellule de crise, sous la direction du PDG.

Celle-ci est composée de l'équipe de direction, du CTO et de l'équipe de développement. Cette cellule a pour objet d'envoyer un mail d'information à chaque client, lui notifiant l'indisponibilité des services via un outil externe.

Le poste de travail du CTO (« Chief Technologique Officer) met à jour automatiquement (deux fois par jour) les adresses emails de nos clients via un script et les stocke sur son poste de travail. La mise à jour des données du CRM est réalisée par l'équipe technique.

L'équipe de direction organise le fonctionnement de la cellule de crise afin de permettre à chaque membre de pouvoir répondre au standard téléphonique, avec une ligne spécifique dédiée à cet usage, et de passer provisoirement les ordres manuellement. En outre, l'équipe support se charge d'identifier la source de l'inaccessibilité des serveurs et des services de nouveaux accessibles si nécessaire.

La cellule de crise a pour fonction d'assurer la continuité de l'activité de Hedge Finance pendant toute la durée d'inaccessibilité des systèmes. Une fois le problème résolu, le poste de travail du CTO (Chief Technical Officer) envoie un mail de rétablissement des systèmes aux collaborateurs de Hedge Finance.

3.1.6. Résolutions des cas d'indisponibilité et d'inaccessibilité des systèmes

Une fois les problématiques d'inaccessibilité des serveurs résolues, un mail est envoyé à tous les clients les informant du rétablissement des systèmes de Hedge Finance.

L'équipe de direction met fin au protocole mis en place et rédige un rapport d'incident dans lequel sont décrites les causes des incidents et la manière dont ils ont été résolus. Ce rapport est à destination du RCSI et du comité des risques présidé par le PDG.

3.2. LA SÉCURITÉ

3.2.1. Actions de prévention de la sécurité

Système d'Information :
L'architecture du système informatique de Hedge Finance est détaillée en annexe 1. Hedge Finance doit veiller à ce que les informations soient protégées – avant que la société ne soit victime d'une atteinte à la sécurité de l'information et que des données soient volées, altérées, effacées ou perdues.

Une bonne gestion des processus de sauvegarde inclut la validation du contenu de l'information et des données des fichiers sauvegardés ainsi que des tests de récupération. Les supports matériels tels que les bandes magnétiques ou disques durs utilisés pour stocker les données sauvegardées sont aussi vulnérables aux risques.

Les sauvegardes doivent bénéficier du même niveau de protection que les données sources, en particulier en ce qui concerne leur sécurité matérielle, car ces éléments sont faciles à transporter.

Systèmes de sauvegardes :

L'archivage et les sauvegardes informatiques s'effectuent selon le type d'équipements et au travers d'une méthode et une vérification du fonctionnement des processus de sauvegarde.
Les éléments de Hedge Finance concernés par le système de sauvegardes sont les suivants :

- Bases de données relatives à l'activité de Hedge Finance et aux clients et prestataires de Hedge Finance ;
- Les équipements informatiques et réseaux (ordinateurs, téléphonie, serveurs...).

Formation des collaborateurs :

Le personnel de Hedge Finance doit posséder les connaissances de base sur les cybermenaces et les questions de sécurité ; Ces connaissances doivent être en permanence entretenues. La formation des collaborateurs garantit que tous ceux qui ont accès aux données et aux systèmes d'information soient conscients de leurs responsabilités quotidiennes dans leur traitement et dans leur protection, ainsi que dans le soutien aux activités de sécurité de l'information de la société.

Sans une formation appropriée, les collaborateurs peuvent rapidement devenir une source de risques au sein de la société et être à l'origine d'incidents de sécurité ou de vulnérabilités dont des adversaires peuvent profiter pour contourner vos mesures de sécurité.

La société doit établir une culture de gestion du cyber-risque. L'investissement dans la formation renforcera les messages sur la sécurité de l'information destinés au personnel et développera ses qualités et ses compétences en matière de sécurité.

Mises à jour des systèmes :

Les systèmes et logiciels de toutes sortes, y compris les appareils et les équipements de réseau, doivent être mis à jour chaque fois que des correctifs ou des mises à niveau de micrologiciel sont disponibles. Ces mises à niveau et correctifs de sécurité remédient à des vulnérabilités des systèmes dont des attaquants peuvent profiter.

Bon nombre d'entre eux parviennent à exploiter des failles de sécurité pour lesquelles des mises à jour étaient disponibles, souvent même depuis plus d'un an. La société doit autant que possible utiliser des services de mise à jour automatique, en particulier pour les systèmes de sécurité tels que les programmes anti-malicieux, les outils de filtrage web et les systèmes de détection d'intrusion. Les processus de mise à jour automatique peuvent contribuer à faire en sorte que les utilisateurs appliquent des mises à jour de logiciels de sécurité valides provenant directement du fournisseur d'origine.

Lignes de défense et réduction du risque :
La sécurisation du périmètre de réseau et le contrôle d'accès traditionnel ne sont pas suffisants, surtout quand le système d'information est connecté à l'internet et à des prestataires de services internet, des services externes, des services cloud, des fournisseurs et des partenaires, ainsi qu'à des appareils mobiles qui se trouvent hors de portée et de contrôle de la société.

Une protection efficace contre les virus, les équipements malveillants et les pirates informatiques exige plusieurs niveaux de mesures défensives afin de réduire le risque d'un incident de sécurité de l'information.

La combinaison de plusieurs techniques (le filtrage web, les antivirus, la protection proactive contre les logiciels malveillants, les pares-feux, de solides politiques de sécurité et une formation des utilisateurs) pour contrer le cyber-risque peut significativement réduire la probabilité de voir une atteinte minime se transformer en un grave incident.

De multiples lignes de défense permettent de restreindre la liberté d'action des adversaires et améliorent les chances de détection par les systèmes de surveillance de l'entreprise.

La société qui s'assure contre les cyber-risques permet de limiter les conséquences financières d'un incident, mais aussi de gérer pro activement les menaces et de renforcer sa gestion interne du risque.

3.2.2. Mesures internes

Les Locaux :
Les bureaux de Hedge Finance sont situés au 25 rue de l'Université, 69007 Lyon.
L'accès aux locaux est réservé aux collaborateurs de Hedge Finance est sécurisé (badge individuel), ce qui permet de garantir la confidentialité de ses activités, d'assurer son indépendance et de prévenir tout risque de conflits d'intérêts.

La sécurité d'accès aux locaux est très importante. Les locaux sont équipés d'extincteurs, pour lesquels un contrat de maintenance a été établi. Ainsi, les extincteurs sont vérifiés lors d'une visite de contrôle annuels.

Le « back end » de Hedge Finance :
Hedge Finance dispose d'un « jump server » permettant de contrôler l'accès à nos serveurs de toutes les IP dans le monde et de basculer vers notre serveur « failover » dans le cas où le serveur principal ne répond plus.
Afin de garder les données intactes et de permettre l'accès à celles-ci sur nos deux serveurs, Hedge Finance a développé un « middleware » sur le serveur principal chargé de répliquer la base de données en temps réel sur les deux serveurs.

Hedge Finance a pris des mesures internes afin de garantir une sécurité face aux vulnérabilités les plus répandues. Cette liste est fournie par l'OWASP ("Open Web Application Security Project") :

Concernant le cas d'« Injection »(A1:2017) : Hedge Finance utilise la bibliothèque « Sequelize » afin d'effectuer des requêtes SQL depuis javascript. Cette librairie remplace automatiquement les caractères d'échappement. Les caractères d'échappement sont la première source des injections SQL dans le monde. « Sequelize » sépare également l'envoi des paramètres de la requête SQL en elle-même et envoie les paramètres après la requête.

Concernant le cas de « Broken Authentication »(A2:2017) : Hedge Finance empêche la création de compte avec un mot de passe trop faible. Les mots de passe doivent avoir une longueur comprise entre 8 et 64 caractères. Ils doivent contenir au moins 1 caractère spécial, un chiffre, une majuscule et une minuscule. Tous les caractères unicode sont autorisés. Les répétitions de plus de 3 caractères à la suite sont interdites. Les mots de passe sont comparés à une liste des 10 000 mots de passe les plus fréquents et seront automatiquement rejetés s'ils font partie de cette liste. Hedge Finance respecte les règles du guide du NIST (National Institute of Standards and Technology), lui-même recommandé par l'OWASP
(https://pages.nist.gov/800-63-3/sp800-63b.html#memsecret).
Hedge Finance récupère l'IP des clients souhaitant se connecter afin de détecter une attaque potentielle brute force. Si une attaque brute force est détectée, les administrateurs de la plateforme web de Hedge Finance seront notifiés par mail. Hedge Finance stocke les IP suspectes et empêche l'accès clients à ces IP. Le seul moyen de retrouver l'accès aux services clients quand une IP est bloquée est de contacter la société et le responsable développeur qui devra débloquer la situation le cas échéant.

Concernant le cas de Sensitive Data Exposure » (A3:2017) : Les données considérées sensibles stockées par Hedge Finance sont les mots de passe des clients et les RIB. Ces informations ne sont pas stockées sous leur forme originelle en base de données. Elles sont hachées et un salt leur est ajouté grâce à la fonction de hachage Bcrypt. Bcrypt utilise l'algorithme Blowfish, qui n'a à l'heure actuelle jamais été cracké. Bien que l'algorithme Blowfish soit vulnérable aux « Attaques des anniversaires », Hedge Finance détecte et empêche les attaques brute force ce qui met un terme à toutes les attaques de type brute force, dont les « Attaques des anniversaires » font partie.
Concernant les paiements en ligne, Hedge Finance utilise Stripe, une plateforme de paiement en ligne américaine sécurisée et constamment maintenue à jour. Les données transitant entre le site web et les serveurs back-end de Hedge Finance sont cryptés via TLS et HTTPS. Le certificat SSL avec validation étendue détenue par la société Hedge Finance a été obtenu après une vérification des données administratives de la société et du dirigeant de la société par GEOTrust. Ce certificat SSL offre un chiffrement de 256 bits, adapté pour les banques et les plateformes de services d'investissement financier ou encore de gestion de patrimoine.

Concernant le cas de XML External Entities XXE (A4:2017) : L'API back-end de Hedge Finance n'offre pas la possibilité d'envoyer, de recevoir, de supprimer ou encore de mettre à jour des données au format XML. Aucune donnée au format XML n'est stockée en base de données. Hedge Finance ne stocke les données qu'au format JSON est n'est donc pas vulnérable aux failles de sécurités liées au format XML.

Concernant le cas de Broken Access Control (A5:2017) : Hedge Finance limite au maximum les « routes » permettant la modification de données. Les « routes » de l'API permettant la lecture ou l'écriture de données sensibles sont réservées aux administrateurs. Elles sont protégées en HTTPS via la méthode « basic auth » et un mot de passe de 30 caractères composé de caractères spéciaux. Elles sont aussi codées pour détecter les tentatives de brute force, bloquer l'accès aux adresses IP suspectes et avertir par mail les administrateurs en cas de suspicion d'attaque brute force. Les clients peuvent modifier uniquement leurs données, via leur UUID qui leur est propre. Il est ainsi impossible pour un client de modifier les données personnelles d'un autre client. Un client non connecté ne pourra modifier aucune donnée.

Concernant le cas de Security Misconfiguration (A6:2017) : Toutes les variables d'environnement de Hedge Finance sont configurées via un fichier « .env » à la racine des projets. Ce fichier contient les mêmes variables que ce soit pour l'environnement de développement ou de production. Il est ainsi facile et rapide de configurer un nouvel environnement en cas de besoin. Les développeurs de Hedge Finance n'utilisent que les librairies qu'ils connaissent et suppriment toute librairie n'étant plus utile ou utilisée au sein de l'application afin de limiter les risques de faille de sécurité et les bugs au sein des applications de Hedge Finance. Les développeurs sont chargés de vérifier le plus souvent possible si des failles de sécurité ont pu se glisser. Les développeurs ont également développé un programme chargé de vérifier l'intégrité et l'exactitude des variables d'environnements.

Concernant le cas de Cross-Site Scripting XSS (A7 :2017): Le site web de Hedge Finance est conçu en « React. js » garantissant une sécurité contre le cross scripting en échappant les scripts XSS automatiquement.

Concernant le cas de Insecure Deserialization (A8 :2017) : Toutes les données envoyées au service back-end de Hedge Finance ont une signature digitale ce qui permet une protection accrue contre les sérialisations non sécurisées.

Concernant le cas de Using Components with Known Vulnerabilities (A9 :2017) : L'équipe support de Hedge Finance prête le plus souvent possible attention aux librairies et aux frameworks qu'elle utilise. Les développeurs sont chargés de régler toutes les erreurs de dépendances et si cela n'est pas possible, de ne pas utiliser la bibliothèque ou le framework correspondant.

Concernant le cas de Insufficient Logging & Monitoring (A10:2017) : Toutes les actions côté serveur sont affichées en temps réel et consultables à n'importe quel moment par

toute l'équipe de Hedge Finance. L'IP des clients est affichée pour chaque requête ce qui permet à l'équipe de Hedge Finance d'isoler les adresses IP responsables d'actions suspectes.

La partie docker de Hedge Finance constituée d'un conteneur docker contenant une base de données postgreSQL ainsi que d'un serveur javascript fait avec Express.js. Ce serveur respecte une architecture MVC (Modèle, Vue, Contrôleur).
Les modèles de données sont les suivants : Les contrôleurs (ou fonctions contrôleurs) permettent la gestion de l'ensemble de ces données ainsi que la gestion de la persistance des données à l'aide des opérations CRUD (create, read, update, delete), à savoir :

- Création,
- Consultation,
- Mise à jour,
- Suppression,
- Exportation au format CSV concernant les modèles « savingsCustomer » et « tradingCustomer ».

Ces données peuvent être exportées au format CSV afin d'être insérées dans l'outil d'emailing, SendinBlue afin d'envoyer les emails de la newsletter. Dans le modèle MVC, les vues représentent les pages du site web permettant l'accès à l'API. Tous les fichiers transmis par les clients sont stockés sur un serveur SFTP (SSH File Transfert Protocol).

Le diagramme d'entité en annexe 2 présente les différents composants de la base de données utilisés par Hedge Finance.

Le « Front end » de Hedge Finance :
Cette partie contient l'ensemble des contenus qui seront affichés sur le site web de Hedge Finance. La communication avec le site et l'utilisateur est sécurisée en HTTPS grâce à un certificat SSL avec validation étendue, obtenue après vérification de l'existence de Hedge Finance et de l'identité du dirigeant de la société. Cette partie tourne sur le serveur principal et le serveur secondaire. Le site est codé à l'aide de « React.JS ». Elle communique avec le back-end via une API, pour envoyer les informations entrées par l'utilisateur sur le site.

Pour l'envoi des requêtes au back-end, on utilise des requêtes HTTPS grâce à la librairie "axios".

Ci-dessous, la liste des logiciels et applicatifs utilisés par Hedge Finance :

- Suite Adobe complète : Ces logiciels servent à la réalisation de graphismes, maquettes, visuels pour le compte de la société.
- Canva Premium : Ce logiciel a pour but de réaliser des visuels pour les réseaux sociaux.
- Trading Work Station : Ce logiciel sert à analyser les marchés financiers.
- Pro Real Time : Ce logiciel est utilisé afin de réaliser des analyses techniques long terme pour nos analyses postées gratuitement sur les réseaux sociaux.

- Pack office pour chaque poste de travail : Ces logiciels servent à la création de contenus textes, visuels et comptables.
- Github : C'est une plateforme en ligne permettant d'accéder à l'outil gestion de version Git. La société héberge le code source des projets de développement sur ce logiciel de manière privée et sécurisée.
- Shopify : Cette plateforme permet d'héberger sur le site de vente de formations, de gérer les ventes et les comptes clients.
- Salesforce : Cet outil permet de gérer la facturation de nos abonnements et des ventes de formations.
- Zoom : Cet outil, nous permet d'organiser des réunions en visio -conférence.
- Mail : Cet outil permet à chacun de gérer ses mails.

Dispositif de réaction en cas d'incident :

En cas de cyber-attaque (infection par un virus à la suite de l'ouverture d'un e-mail, etc.) à l'encontre de Hedge Finance, l'équipe informatique procède aux opérations ci-dessous :

- Déconnexion d'internet ;
- Procéder aux constatations ou contacter un service de police ou de gendarmerie pour faire intervenir un spécialiste en cybercriminalité aux fins de constatations immédiates ou faire appel à un expert ou une société spécialisée dans la réponse à incident ou faire appel à un huissier ;
- Mettre en quarantaine les postes informatiques concernés par l'incident ;
- Écarter et protéger les supports informatiques concernés par l'incident : clé USB, CD, DVD, disques durs (internes/externes) ;
- Couper tous les accès réseaux pour stopper l'incident ;
- Sauvegarder les journaux d'événements (connexions Web, événements systèmes, ...), les documents, emails, fichiers, le trafic réseau supervisé (firewalls, etc. ...), copie de supports informatiques ;
- Collecter les renseignements internes : auprès des premières personnes à avoir détecté l'incident et à avoir donné l'alerte et auprès des employés témoins de l'incident ;
- Collecter les renseignements externes : auprès des prestataires de services (télécommunications, développement d'application, maintenance matériels, ...) ;
- Communiquer aux personnels ciblés de l'entreprise les recommandations adaptées à la gestion de l'incident ;
- Figer le système en l'état et faire une copie des données utiles avant de résoudre l'incident ;
- Balayage des ordinateurs au moyen de logiciel antivirus et Antimalware pour vérifier s'il est infecté et, le cas échéant, éliminer le virus ;
- Procéder à une restauration complète des ordinateurs si besoin ;
- Faire appel à un expert si le fonctionnement des ordinateurs est toujours compromis ;
- Modifier tous les mots de passe ;
- Conserver des images de ce qu'on voit en utilisant la fonction « Imprimer écran » ;

- Lister tous les préjudices subis ;
- Regrouper tous les éléments qui semblent pertinents : traces informatiques qui font penser à une attaque, fichier encrypté suite au virus, etc.
- Procéder au dépôt de plainte au commissariat ou à la gendarmerie ;
- Reporter l'incident dans un registre (informatique ou opérationnel).

L'équipe informatique ou la direction de Hedge Finance sont chargés de la communication aux collaborateurs et aux partenaires externes le cas échéant.

4. DISPOSITIF RELATIF AU RGPD

Hedge Finance s'engage à respecter le RGPD en qualité de responsable de traitement des données à caractère personnel pour ses activités dans l'espace européen, pour tout transfert de données hors de l'Union européenne via le respect des clauses contractuelles types émises par la commission européenne.

4.1. DISPOSITIONS INTERNES

Hedge Finance mettra en place un dispositif de Conformité spécifique au RGPD avec les mesures ci-dessous (cartographie des traitements de données, gestion des risques).

Les Liste des données à caractère personnel détenues par Hedge Finance et des traitements effectués :

- personnes concernées ;
- finalité du traitement ;
- destinataires ;
- durée de traitement et de conservation des données ;
- organiser la cartographie pour permettre sa mise à jour rapide et effective.

Hedge Finance veillera ainsi à :

- ne conserver que les données et les traitements strictement nécessaires ;
- mettre à jour la cartographie à chaque nouveau traitement de données ;
- permettre l'accessibilité et la lisibilité de la cartographie en cas de contrôle des autorités.

Le respect des dispositions du RPGD par Hedge Finance se fera notamment à travers les dispositifs suivants :

- la mise en place des différentes mentions, demandes d'autorisation sur tous les supports appropriés : par exemple les mentions légales et conditions d'utilisation sur les sites internes, les formules de consentement sur les sites internet et les supports marketing, mettre en place les contrats appropriés avec les prestataires de services, partenaires, clients selon que l'entreprise est responsable de traitement ou sous- traitant, définir les mesures de sécurisation des données que l'entreprise entend répercuter aux sous-traitants en fonction des catégories de traitement ;
- la cartographie des risques en fonction de la nature et de la sensibilité du traitement et des données concernées le cas échéant ;
- la réalisation d'études d'impact lorsqu'elles sont requises ;
- la mise en place d'indicateurs de suivi des risques ;
- la notification des violations de données ;
- la mise en place de correctifs en cas de violation de données ;
- le respect du principe de privacy by design et by default ;
- la ventilation des accès aux données ;

- la mise en place de mesures de confidentialité ;
- la mise en place de sécurisation logique et physique des accès aux données ;
- l'information et la formation des équipes internes ;
- la conservation et la mise à jour de la documentation interne relative au RGPD.

4.2. SPÉCIFICITÉS RELATIVES AUX DONNÉES PERSONNELLES

4.2.1. Finalités des traitements

Les données que nous collectons dans le cadre de nos services d'investissement et de gestion d'OPC sont utilisées par Hedge Finance pour tout ou partie des finalités suivantes :

- Le suivi du passif de nos OPC ;
- La gestion administrative et/ou comptable des avoirs placés dans les OPC gérés par notre société ;
- L'exercice des recours et la gestion des réclamations ;
- Les prestations de services d'investissement rendues à votre profit ;
- L'exécution des dispositions légales, réglementaires et administratives en vigueur.

Nous sommes également amenés à collecter vos données dans le cadre des opérations relatives à la gestion de nos clients et à la prospection commerciale, en particulier :

- Les opérations relatives à la gestion des clients (suivi de la relation client) ;
- L'élaboration de statistiques commerciales ;
- L'information de nos clients et prospects sur nos produits et services ;
- La gestion des demandes de droit d'accès, de rectification et d'opposition.

Afin de respecter nos obligations légales et règlementaires, nous collectons également vos données afin de lutter contre le blanchiment d'argent et le financement du terrorisme, ainsi que contre la fraude à l'assurance.

4.2.2. Fondements juridiques

Exécution de contrats ou d'engagement juridiques

Il peut nous être nécessaire de traiter vos données personnelles afin d'exécuter un contrat avec vous concernant notre activité de société de gestion de portefeuille ou des services annexes accessoires ou qui sont nécessaire ou le prolongement de notre activité réglementée, ou de prendre des mesures à votre demande avant de conclure un contrat et plus généralement lorsque l'utilisation de vos données est nécessaire pour respecter nos obligations dans le cadre d'un contrat conclu avec votre entreprise ou d'un service d'investissement rendu à votre profit, dans le cadre de la souscription à l'un des OPC géré par notre société de gestion.

Respect de nos obligations légales et réglementaires

En tant que société de gestion de portefeuilles, nous sommes soumis à un certain nombre d'obligations légales et réglementaires qui peuvent nous obliger à collecter, stocker ou divulguer des données personnelles, non limitativement aux fins suivantes :

- La lutte contre le blanchiment de capitaux et le financement du terrorisme (AML) ;
- La connaissance du client (KYC) ;
- Les obligations réglementaires ou fiscales : autorités fiscales ou régulateurs et autres autorités publiques européennes ;
- Plus généralement, le respect de nos obligations en qualité de société de gestion de portefeuille.

L'utilisation de vos données peut être nécessaire pour servir nos intérêts légitimes à travers notamment :

- La gestion des relations avec les clients et les fournisseurs ;
- L'analyse commerciale et développement de produits et services ;
- Les activités liées à la sécurité de l'information et à la sécurité des bâtiments, y compris l'utilisation de l'enregistrement en circuit fermé ;
- L'enregistrement de lignes téléphoniques et surveillance de communications électroniques à des fins commerciales et de conformité ;
- Le fait d'évaluer, apporter ou défendre des réclamations légales ;
- La commercialisation et gestion des produits financiers ;
- Les audits.

4.2.3. Catégories de données que nous collectons

En fonction des finalités décrites ci-dessus, Hedge Finance réalise la collecte des données suivantes, relatives à l'identification des clients, à savoir :

- L'état civil : il s'agit notamment des noms, prénoms et civilité ;
- Les coordonnées : il s'agit notamment des adresses postales, numéros de téléphone (fixe et mobile), et des adresses électroniques ;
- La résidence fiscale : connaître la résidence fiscale est l'une des informations qui permet de déterminer quelles sont les éventuelles obligations de Hedge Finance notamment fiscales à l'égard de l'Etat dont le bénéficiaire est un ressortissant mais également en termes de prélèvement sociaux ;
- Les données relatives à la situation économique et financière.

4.2.4. Destinataires

Nous pouvons être amenés à communiquer vos données aux différentes catégories de destinataires suivantes (non limitativement) :

- Les membres habilités de notre personnel et toute personne physique ou morale autorisée par le DPO à traiter les données à caractère personnel ;

- S'il y a lieu les juridictions concernées, les arbitres, les médiateurs ;
- Les ministères concernés, autorités de tutelle et de contrôle et tous organismes publics habilités à les recevoir ;
- Les centralisateurs, les commissaires aux comptes de nos OPC ;
- Les services chargés du contrôle tels que les commissaires aux comptes et les auditeurs ainsi que les services chargés du contrôle interne ;
- Les systèmes de règlement livraison.

Ces destinataires peuvent être situés en dehors de la Lituanie.

4.2.5. Transferts de données en dehors de l'Union Européenne

Hedge Finance et ses clients peuvent être actifs dans le monde entier, et conformément aux objectifs décrits ci-dessus, ils peuvent être transférés vers des pays de l'UE ou vers des pays tiers, c'est-à-dire hors de l'UE ou de l'EEE. Les lois des pays tiers concernant les données personnelles peuvent ne pas être aussi complètes que les lois applicables sur le territoire de l'UE. Toutefois, si Hedge Finance utilise des prestataires de services dans un pays tiers, elle exige d'eux qu'ils appliquent le même niveau de protection à vos données que celui applicable au sein de l'UE. Typiquement, nous y parvenons en utilisant des clauses standard de protection des données approuvées et publiées par la Commission européenne à cet effet. Plus généralement, nous ne transférerons vos données personnelles vers un pays tiers que d'une manière autorisée par la loi européenne sur la protection des données.

4.2.6. Durées de conservation des données

Hedge Finance conserve les données personnelles pendant une durée n'excédant pas celle nécessaire aux fins pour lesquelles elles sont traitées. Les durées de conservation sont synthétisées ci-dessous :

- Prospection commerciale : 3 ans à compter de la collecte des données par le responsable de traitement ou du dernier contact émanant du prospect ;
- Contrats : 10 ans après la date d'échéance ou de résiliation ;
- Données réglementaires : 5 à 10 ans ;
- KYC / AML : Lutte contre le blanchiment de capitaux et le financement du terrorisme : 5 ans à compter de la cessation des relations avec la personne concernée.

4.2.7. L'exercice des droits relatifs au RGPD

Conformément à la réglementation en vigueur, les clients de Hedge Finance bénéficient des droits suivants :

- L'accès à et/ou l'envoi d'une copie de certaines données détenues par Hedge Finance ;
- La mise à jour des données obsolètes ou incorrectes ;
- La suppression de certaines données détenues ;
- Limiter la façon dont nous traitons et divulguons certaines de vos données pour motif légitime ;
- Transférer vos données vers un prestataire de services tiers ;
- Retirer à tout moment votre consentement accordé pour un traitement fondé sur cette base juridique, étant précisé que l'exercice de ce droit ne porte pas atteinte à la licéité du traitement fondé sur le consentement accordé avant le retrait de celui-ci.

Nous étudierons toutes les demandes et vous communiquerons notre réponse dans les délais légaux.
Veuillez noter, toutefois, que certaines données peuvent être exclues de ces demandes dans certaines circonstances, notamment si nous devons continuer à traiter vos données pour servir nos intérêts légitimes ou respecter une obligation légale. Nous pouvons vous demander de nous fournir un justificatif d'identité pour confirmer votre identité avant de répondre à votre demande.

Conformément aux dispositions de l'article L. 561-45 du code monétaire et financier, le droit d'accès aux traitements mis en œuvre aux seules fins de l'application des dispositions relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme s'exerce auprès de la CNIL via une procédure de droit d'accès indirect en écrivant à l'adresse rappelée ci-dessous. Les traitements mis en œuvre afin d'identifier les personnes faisant l'objet d'une mesure de gel des avoirs ou d'une sanction financière restent soumis à la procédure de droit d'accès direct auprès du responsable de traitement : dpo@universe-bank.com

En tout état de cause, il vous est possible de saisir directement la CNIL à l'adresse suivante :
3 Place de Fontenoy
– TSA 80715 –
75334 PARIS CEDEX 07

4.3. NOMINATION D'UN DPO

Hedge Finance nomme un délégué à la protection des données pour piloter la gouvernance des données personnelles.

Il conseille et accompagne Hedge Finance dans sa conformité.

Son rôle est de recueillir des informations relatives aux données détenues par l'entreprise, d'analyser et de vérifier la conformité des traitements de données effectués par

l'entreprise, d'informer, conseiller ou adresser des recommandations au responsable du traitement ou au sous-traitant.

5. CONTRÔLES PERMANENT

5.1. CONTRÔLES INTERNES

Les contrôles de premier niveau sont effectués par chaque collaborateur lors de l'exécution quotidienne de ses missions. Il correspond au respect, par chacun des collaborateurs, de la réglementation applicable à l'activité de la société et des procédures internes.

Les collaborateurs sont tenus d'informer le MLRO et la Direction de toute anomalie ou dysfonctionnement détecté. Les missions de contrôles permanent (2nd niveau) et périodique (3ème niveau) peuvent s'appuyer sur ces contrôles.

6. RÉGLEMENTATION & DOCTRINE APPLICABLES

Règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'Autorité de contrôle prudentiel et de résolution.

Loi n°2018-133 du 26 février 2018 sur la sécurité des réseaux et des systèmes d'information (Transposition de la directive NIS).

Décrets n°2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique.

Arrêté du 13 juin 2018 fixant les modalités des déclarations prévues aux articles 8, 11 et 20 du décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique.

Arrêté du 01 août 2018 relatif au coût d'un contrôle effectué par l'Agence nationale de la sécurité des systèmes d'information en application des articles 8 et 14 de la loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité.

Arrêté du 14 septembre 2018 fixant les règles de sécurité et les délais mentionnés à l'article 10 du décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique.

Historique des modifications :

Création le 07/10/24
Dernière modification le 07/10/24