Politique de protection des données personnelles

ClickImpôts Pro en SaaS

Version du 28 octobre 2020

De : HARVEST, société anonyme, au capital de 1 419 144 euros, immatriculée au RCS de PARIS sous le numéro 352 042 345 et ayant son siège au 5 rue de la BAUME 75008 PARIS.

A destination des Clients Professionnels d'HARVEST.

Sommaire

1. Préambule

La présente politique de protection des données à caractère personnel (ci-après la « Politique ») décrit les engagements mis en œuvre par HARVEST, en tant que sous-traitant de traitement de données à caractère personnel.

L'objet de cette Politique est de vous informer clairement de la manière dont les données personnelles sont gérées par HARVEST lorsque vous utilisez en tant que client le logiciel ClickImpôts (ci-après le « Logiciel ») dans le cadre de votre activité professionnelle.

La Politique est disponible sur le site de vente du Logiciel.

HARVEST est susceptible d'apporter des modifications à la présente Politique. La version en vigueur sera disponible sur le site de vente du Logiciel et HARVEST vous informera de tout changement par le biais du site de vente ou par tout autre moyen.

2. Quelles sont les données traitées par HARVEST ?

Seules les données strictement nécessaires au regard de la finalité pour laquelle elles sont traitées sont collectées par HARVEST. Le traitement des données demandées par HARVEST est indispensable pour l'utilisation du Logiciel.

Lors de l'utilisation du Logiciel les données personnelles collectées sont les suivantes :

- Données d'identification : telles que le numéro d'identification unique, l'identité, l'adresse, l'identité et l'adresse de tiers (personnes à charge, conjoint…etc)
- Caractéristiques personnelles et habitudes de vie : telles que la situation de famille, l'historique marital, frais professionnels
- Données de connexion : telles que le code client et le mot de passe
- Donnée de localisation : telle que l'adresse IP
- Données de santé : telles que la mise sous tutelle ou curatelle ou l'existence d'une carte d'invalidité
- Activités professionnelles et publiques : tels que l'emploi actuel, l'identification de l'entreprise
- Données économiques : telles que les données d'identification financières, les revenus, les dettes et dépenses
- Données judiciaires : mise sous tutelle/curatelle

3. Quelles sont les raisons pour lesquelles les données sont collectées ?

Les données personnelles ne sont collectées que pour les raisons suivantes :

- Etablir une déclaration fiscale
- Calculer et simuler des impôts
- Préparer la télédéclaration (EDI-IR et TDFC)
- Télédéclarer avec le portail fiscal HARVEST
- Contrôler la licence d'utilisation

Aucune donnée personnelle n'est utilisée pour une autre raison que celles énumérées ci-dessus.

4. Quels sont les destinataires des données personnelles ?

En cas de dépôt par voie dématérialisée des déclarations de revenus établies via le service de télédéclaration du Logiciel, les données personnelles seront alors transmises à la Direction Générale des Finances Publiques (DGFiP).

De plus, HARVEST est susceptible de communiquer les données personnelles à ses prestataires techniques, partenaires, dont l'intervention est strictement nécessaire pour exécuter les services nécessaires au bon fonctionnement du Logiciel. HARVEST s'assure que ces tiers traitent les données personnelles de manière à garantir leur intégrité, leur confidentialité et leur sécurité.

A ce jour les partenaires d'HARVEST sont :

- ASPOne qui est le prestataire assurant le service de Télédéclaration
- Waycom qui assure l'hébergement du Logiciel en SaaS

5. Comment sont sécurisées les données personnelles ?

HARVEST assure la sécurité des données personnelles en mettant en place une protection des données renforcée par l'utilisation de mesures techniques de sécurisation physiques et logiques afin de garantir l'intégrité des données personnelles, ainsi que leur traitement confidentiel et sécurisé.

Les mesures de sécurité mises en place par HARVEST sont décrites dans le document intitulé « Plan d'Assurance Sécurité (PAS) » se trouvant en annexe de la Politique.

6. Quelle est la durée de conservation des données personnelles ?

Les données personnelles doivent être conservées uniquement pendant la durée nécessaire à l'accomplissement de la finalité pour laquelle elles ont été collectées. Elles seront ensuite supprimées. Elles peuvent également être conservées pour la durée nécessaire au respect par HARVEST de ses obligations légales.

HARVEST conserve les données pendant la durée de contrat lorsqu'elles sont nécessaires pour :

- Etablir une déclaration fiscale
- Calculer et simuler des impôts

HARVEST conserve les données pendant une durée de 10 ans (conformément à son obligation légale en tant que partenaire EDI) lorsqu'elles sont nécessaires pour :

- Préparer la télédéclaration (EDI-IR et TDFC)
- Télédéclarer avec le portail fiscal HARVEST

HARVEST conserve les données pendant durée du contrat lorsqu'elles sont nécessaires pour :

- Contrôler la licence d'utilisation

7. Les données personnelles sont-elles transférées hors de l'Union Européenne ?

Aucune donnée personnelle ne sera transférée en dehors de l'Union Européenne.

8. Quels sont les engagements d'HARVEST ?

HARVEST s'engage à :

- traiter les données à caractère personnel uniquement pour la ou les seule(s) finalité(s) qui fait/font l'objet de la sous-traitance
- traiter les données à caractère personnel conformément à vos instructions documentées. Si HARVEST considère qu'une instruction constitue une violation de la législation relative aux données personnelles (ci-après la « Législation »), HARVEST vous en informera immédiatement. En outre, si HARVEST est tenu de procéder à un transfert de données vers un pays tiers ou à une organisation internationale en vertu de la Législation, il vous informera de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public
- garantir la confidentialité des données à caractère personnel
- veiller à ce que les personnes autorisées à traiter les données à caractère personnel :
  - s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité
  - reçoivent la formation nécessaire en matière de protection des données à caractère personnel
- prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection des données à caractère personnel dès la conception et de protection des données par défaut
- vous aider à vous acquitter de votre obligation de donner suite aux demandes dont les personnes concernées vous saisissent en vue d'exercer leurs droits (information, effacement …etc.) et à vous communiquer toute demande de divulgation des données ou d'accès à celles-ci, qui lui aurait été faite directement. Dans ce cadre HARVEST s'engage à respecter des délais compatibles avec vos obligations au titre de la Législation
- vous notifier toute violation de données à caractère personnel dans un délai vous permettant de respecter vos obligations en la matière
- tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte des différents responsables de traitement
- mettre en œuvre les mesures de sécurité adaptées aux risques liés au(x) traitement(s) effectué(s)

ClickImpôts SaaS

Plan d'Assurance Sécurité (PAS)

Fichier : HVS - Plan d'Assurance Sécurité ClicImpôts SaaS V1.3.docx

Version	Diffusion le	Rédigée par	Objet de la version
1.0	20/10/2020	Projet/Exploitation	Version initiale
1.1	23/10/2020	Projet/Exploitation	Compléments
1.2	25/10/2020	RSSI	Contrôle et compléments
1.3	30/10/2020	Direction Juridique	Contrôle et compléments

Sommaire

1. Objectifs et contenu

Le Plan d'Assurance Sécurité (PAS) est un document applicable au titre du cadre contractuel qui lie HARVEST et LE CLIENT. On entend par « Assurance Sécurité » l'assurance que la prestation est réalisée dans les conditions de sécurité exigées.

En pratique, il définit le volet sécurité du Plan d'Assurance Qualité (PAQ) de la prestation et décrit les dispositions de sécurité mises en place par HARVEST pour l'offre de service contractualisée.

Ce document décrit les dispositions qu'HARVEST s'engage à mettre en œuvre pour répondre :

Aux risques qu'HARVEST a identifié sur ses services mutualisés/transverses utilisés dans le cadre de ses prestations :

- Mesures de sécurité
- Rôles et responsabilités

Il définit en particulier l'organisation qui sera mise en place, la méthodologie à suivre pour gérer la sécurité de la prestation et les mesures techniques, organisationnelles et procédurales mises en œuvre.

2. Responsabilités

2.1. Etablissement du PAS

Le PAS est défini conjointement entre LE CLIENT et HARVEST. Il est le référentiel commun en matière de sécurité des SI tout au long de la relation contractuelle.

2.2. Mise en application et suivi du PAS

HARVEST est responsable de la mise en application du PAS par chacun des intervenants. Afin d'assurer la protection des éléments sensibles liés à la prestation, HARVEST vérifie sa mise en œuvre et contrôle de manière directe l'application des exigences de sécurité.

2.3. Contrôle de respect du plan d'assurance sécurité

Dans le cadre de ces obligations HARVEST procède régulièrement à des contrôles de son S.I. et à la formation et sensibilisation de ses collaborateurs.

3. Sécurité des systèmes et des informations

3.1. Authentification

L'accès aux services et aux données de l'application se fait sur la base du profil de l'utilisateur, le compte et le mot de passe sont stockés chiffrés. L'accès à la solution ClickImpôts SaaS est protégé par système d'authentification OAuth2 avec un jeton JWT chiffré dans un cookie de session.

Harvest a fait le choix de la solution KeyCloak[1] en raison du support des protocoles standards OpenID Connect, OAuth 2.0 et SAML 2.0 et son interopérabilité avec les annuaires LDAP et Active Directory.

[1] https://www.keycloak.org/

3.2. Stockage des données ClickImpôts

Les données ClickImpôts sont stockées dans une base de données MySQL. Cette base intègre l'ensemble des données ClickImpôts propre au client.

Chaque client ClickImpôts dispose de sa propre base de données cloisonnées des autres bases clients. L'accès à cette base s'effectue avec un utilisateur spécifique à chaque client et qui dispose de droits d'accès restrictifs lui permettant uniquement l'accès à sa propre base. Le mot de passe d'accès est également spécifique à chaque client et stockés en cryptage AES 128-bits.

Il est également possible d'accentuer la sécurité des données en activant le cryptage de la base de données client complète ainsi que le chiffrement SSL de la connexion inter-composants (option payante).

3.3. Réseau

Le réseau d'Harvest est segmenté logiquement afin d'assurer le cloisonnement technique entre les différents environnements.

Tous les flux réseaux de la société sont contrôlés par un Firewall. Seuls les flux nécessaires à chaque service sont autorisés.

Les communications entre le navigateur internet de l'utilisateur et l'application sont chiffrées en HTTPS jusqu'au cluster Kubernetes Harvest (toutes les requêtes sont authentifiées et identifiées).

3.4. Sécurité du code

L'application est testée contre les attaques de type injection SQL, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF).

Les dépendances applicatives externes sont régulièrement mises à jour.

3.5. Traçabilité des connexions

Toutes les actions menées au niveau du système ou de l'application sont enregistrées dans les journaux d'évènements.

Par ailleurs, tous les flux réseaux sont tracés par le Firewall.

3.6. Sauvegarde et archivage

3.6.1. Plan de sauvegarde ClickImpôts SAAS :

- Données :
  - Sauvegardes incrémentales : entre 8h30 et 20h30, toutes les heures, tous les jours
  - Sauvegardes complètes : tous les jours de nuit
  - Rétention de 14 jours sur le serveur de sauvegarde local
  - Rétention de 18 mois sur les NAS distants
  - Réplication temps réel entre BDD Maitre et esclave sur 2 sites distincts)
- Applicatif :
  - Les sauvegardes applicatives sont réalisées par sauvegarde de l'environnement Kubernetes, deux fois par jour avec une rétention de 5 jours.

3.6.2. Plan de sauvegarde des satellites Click Impôts SAAS :

- Baie 1 Centre d'Hébergement principal
  - Voir document PAS concernant les éléments communs d'hébergement pour les environnements Keycloak, Frontal HA Proxy et Clusters Kubernetes.
- Baie 2 Centre d'hébergement secondaire

- Simulateurs Gamme Quantix (pas de données persistantes sur le serveur) :
    - Le processus de sauvegarde est géré quotidiennement entre 2h et 6 h du matin.
    - Les sauvegardes sont incrémentales du lundi au samedi et totales le dimanche
    - La rétention est de 14 jours
- Site marchand :
    - Sauvegardes incrémentales et complètes locales quotidiennes.
    - Backup full quotidien sur NAS distants.
- Portail Fiscal et Télédéclaration :
    - Le processus de sauvegarde est géré quotidiennement entre 2h et 6 h du matin.
    - Les sauvegardes sont incrémentales du lundi au samedi et totales le dimanche
    - La rétention est de 14 jours
    - Les sauvegardes sont effectuées sur le site physique du lieu d'hébergement de la plateforme puis répliqués sur un second centre d'hébergement. Il s'agit de sauvegarde sur NAS.
    - La durée maximum de perte de données entre 2 sauvegardes ne peut excéder 24 heures.

- Baie 3 Centre d'hébergement backup
    - Réplication des bases de données pour récupération des données en cas de PRA.

3.7. Sécurisation des accès à l'application

Les environnements font régulièrement l'objet de scans de vulnérabilités avec l'outil Nexpose de Rapid'7, le plan de remédiation est porté par la DSI.

Un scan de contrôle est effectué une fois que toutes les corrections ont été apportées.

4. Sécurisation des locaux

Harvest fait appel à un spécialiste de l'hébergement Waycom dont les infrastructures sont hébergées dans des centres (Datacenters). L'application ClickImpôts SaaS est exploitée depuis le Datacenter Datacenter Interxion France, situé à Saint Denis (93) et disposant des certifications suivantes :

- ISO (14001:2004, 27001 & 22301, 50001:2011),
- OHSAS 18001,
- ITILV3,
- PCI-DSS

Interxion dispose, en outre, de l'agrément d'hébergeur de données de santé à caractère personnel.

5. Organisation de la sécurité

5.1. Gestion des incidents

HARVEST dispose d'une organisation qui permet de gérer les incidents opérationnels ou de sécurité pouvant se produire sur ses activités.

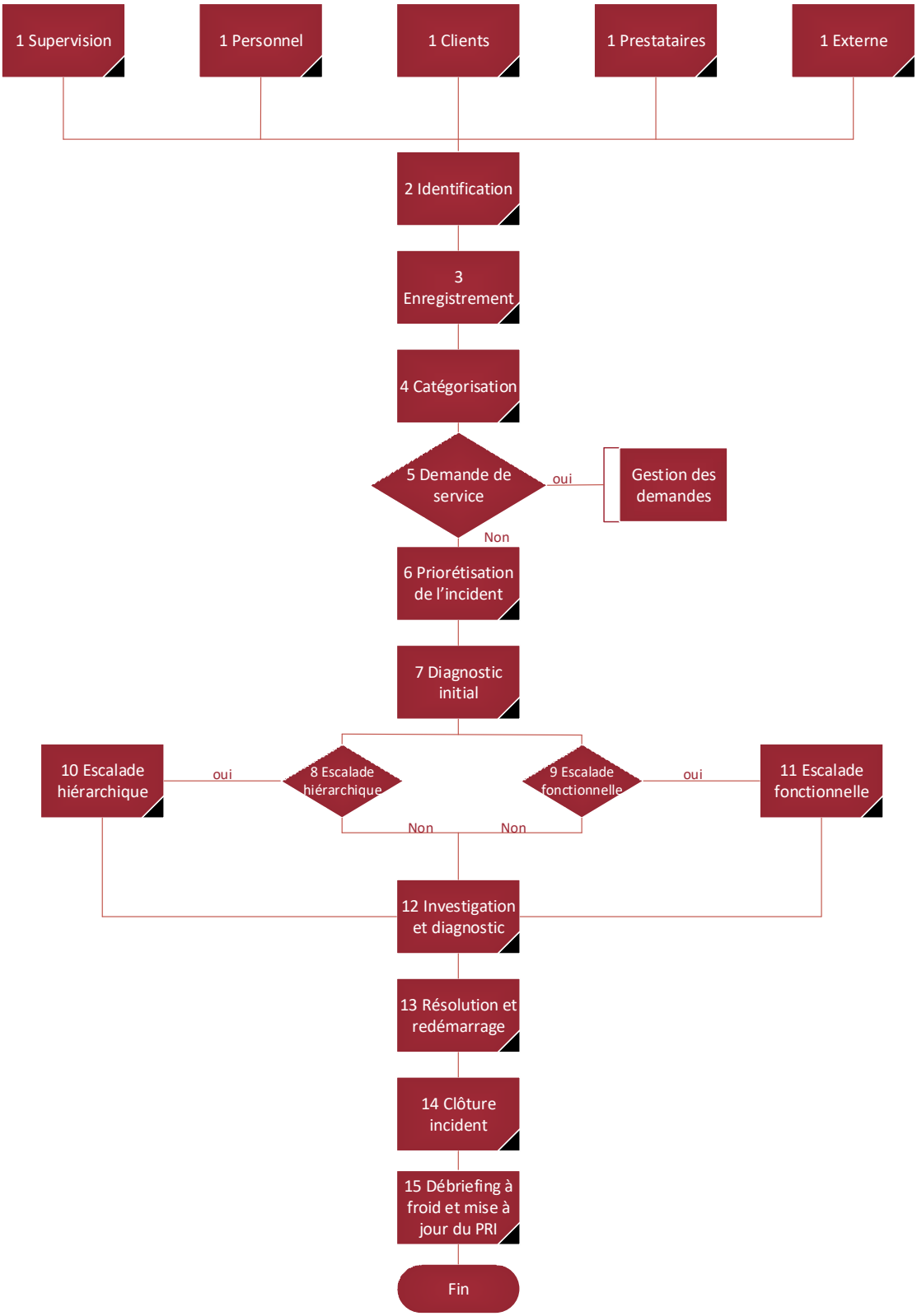
L'ensemble des incidents et les corrections apportées sur le S.I. ou les procédures, sont présentés au comité des risques qui se tient deux fois par an.

Les infrastructures sont monitorées 24h/24 et 7j/7 par la DSI d'Harvest.

Les membres d'une cellule de crise sont désignés. Le fonctionnement de la cellule de crise est formalisé. Les processus de gestion des incidents sont formalisés.

5.2. Processus d'escalade des incidents

Le diagramme ci-dessous décrit le processus de qualification et d'escalade des incidents mis en place chez HARVEST.



5.3. Matrice de priorité des incidents

La matrice ci-dessous permet de qualifier la criticité d'un incident chez Harvest et le cas échéant de déclencher la cellule de crise.

Matrice de prorité des incidents Un incident classifié "P1" est un incident de crise sur les infrastructures mutualisées, salle informatique, système informatique partagé, infrastructure logistique,						
Classification des tickets d'incident et priorité						
		Impact				
		Interruption de service de plusieurs clients		Interruption de service d'un client	Incident partielle d'un service	Pas d'interruption de service
		Incident provoquant une interruption de service pour plusieurs clients		Incident provoquant une interruption totale d'un service ou d'une application pour un client	Incident provoquant une interruption partielle d'un service d'un client	Inciendent ne provoquant aucune interruption de service
		Harvest		Options client		
Urgence	**Elevée** Evaluée selon le niveau de service souscrit par le client	**P1** **(Crise)**		**P2** **(Critique)**	**P3** **(Majeur)**	**P4** **(Majeur)**
	Normale Evaluée selon le niveau de service souscrit par le client	**P1** **(Crise)**		**P2** **(Critique)**	**P4** **(Majeur)**	**P5** **(Mineur)**
	Basse Evaluée selon le niveau de service souscrit par le cleient	**P1** **(Crise)**		**P3** **(Majeur)**	**P4** **(Majeur)**	**P5** **(Mineur)**

5.4. Délai / fréquence d'information pour les clients

Classification	Escalade hiérarchique	Délai d'information	Actions vers les clients
P1	Obligatoire	Toutes les heures	Attente du redémarrage des services et déclenchement du DRP si approprié
P2	Obligatoire	Toutes les 2 heures	Attente du redémarrage des services
P3	Obligatoire	Toutes les 1/2 journées	Attente du redémarrage des services
P4	Option	Option	Attente du redémarrage des services
P5	Non	Option	Attente du redémarrage des services

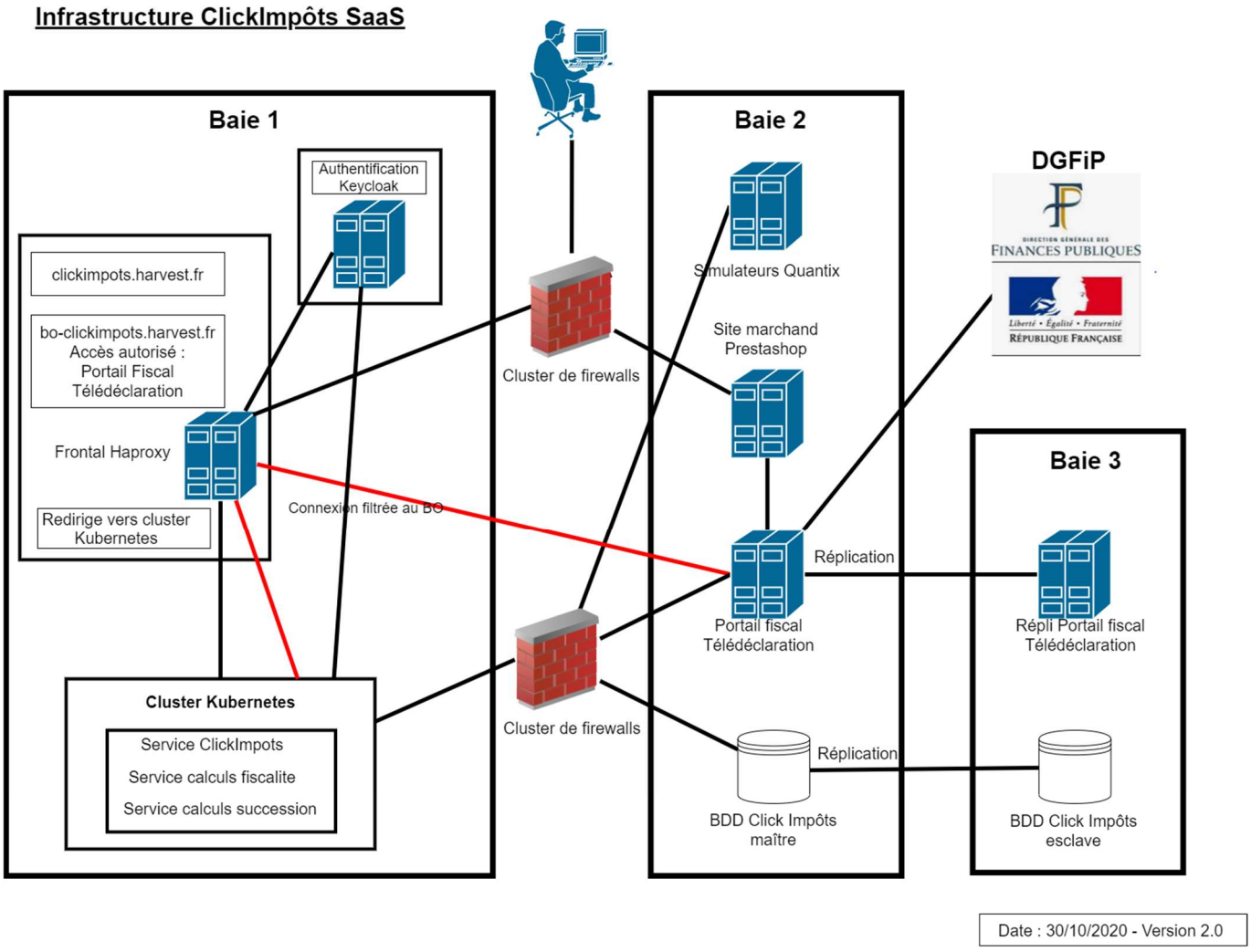
6. Continuité de service

La compétence nécessaire à la réalisation des visites de conformité et des audits est partagée par plusieurs acteurs afin de garantir la continuité d'activité en cas de défaillance humaine.

Tous les serveurs hébergeant les applications Harvest sont dans une architecture redondée ce qui permet une très forte disponibilité du réseau, des ressources matérielles et logicielles.

En cas de sinistre, Harvest et son hébergeur seraient à même de redéployer la solution sur une ou plusieurs infrastructures accessibles par l'hébergeur, toutes situées en France métropolitaine.

7. Schéma de l'infrastructure



8. Classification des données, extrait du chapitre 2.1 de la PSSI d'HARVEST

8.1. C1 Publique

Classifier l'information comme « Publique » si sa divulgation ne peut pas avoir comme résultat la nuisance grave de la réputation ou du statut financier d'HARVEST ou d'un client ou d'un partenaire d'HARVEST et si l'information est destinée à toutes les personnes externes et internes concernées. Cette classification est appropriée si l'information ne doit être restreinte d'aucune manière et si le Département Marketing a approuvé l'accès public.

8.2. C2 Externe restreint

Classifier l'information comme « Externe » si sa divulgation en dehors des personnes externes (clients, fournisseurs, prospects, etc.) pourrait être inappropriée ou problématique. Cette classification est appropriée pour la plupart des échanges en dehors du réseau d'HARVEST avec

des personnes ou des sociétés avec lesquelles HARVEST a des échanges dans le cadre de son activité.

8.3. C3 Interne

Classifier l'information comme « Interne » si sa divulgation en dehors d'HARVEST pourrait être inappropriée ou problématique. Cette classification est appropriée pour la plupart des informations commerciales HARVEST et c'est la catégorie de classification utilisée le plus fréquemment. Une note interne sur les changements de personnel est un exemple d'information « Interne ».

8.4. C4 Confidentiel HARVEST

Classifier l'information comme « Confidentiel HARVEST » si sa divulgation en dehors de la Société pourrait affecter la réputation ou le statut financier d'HARVEST, d'un client ou d'un partenaire d'HARVEST. Cette classification est appropriée pour les informations qui ne sont pas nécessaires à chaque employé d'HARVEST, mais il y a des situations où ces informations doivent être partagées avec un client ou fournisseur externe. Cette classification s'applique aux informations divulguées selon le principe « besoin de connaître ». Par exemple, les informations requises pour soutenir un projet spécial peuvent être des informations « Confidentiel HARVEST ».

8.5. C5 Distribution Restreinte HARVEST

Classifier l'information comme « Distribution Restreinte HARVEST » si sa divulgation peut avoir comme résultat la nuisance grave de la réputation ou du statut financier d'HARVEST ou d'un client ou d'un partenaire d'HARVEST. Les informations relatives à une acquisition, aux résultats financiers trimestriels ou annuels, à une réduction imminente des effectifs et du salaire d'un employé sont des exemples d'informations qui doivent être classifiées comme « Distribution Restreinte HARVEST ». Généralement, cette classification ne sera pas utilisée si les données doivent être partagées avec un client ou une partie externe.

8.6. Synthèse

Niveau	Désignation	Exemple
C1	Public	Informations du site Internet http://www.harvest.fr
C2	Externe restreint	Clients et prospects, diffusion restreinte
C3	Interne	Informations à la destination exclusive du personnel Harvest
C4	Confidentiel Harvest	Informations concernant des projets internes, diffusion limitée
C5	Restreinte Harvest	Informations stratégiques

9. Domaines couverts par la PSSI d'HARVEST

Sommaire