Plan d’assurance sécurité

Plateforme Fulll

Date version actuelle	30/12/2022
Version	2.00
Etat	Publié
Classification	Restreint
Type de document	Plan d’assurance sécurité
Périmètre	Fulll
Description	Résumé des politiques de sécurité de l’information en vigueur chez Fulll et relatives à sa plateforme d’applications.

Ce document est la propriété de Fulll.

Toute copie, distribution ou communication de ce document, même partiellement, à des tiers non autorisés constitue une violation des droits de propriété et des règles de confidentialité établies.

Ce document ne peut en aucun cas être modifié sans l’approbation de Fulll.

Liste de diffusion
Collaborateurs Fulll
Clients/Prospects

Responsable du document et accès à la documentation

Propriétaire du document	L. FALORNI
Fonction du Propriétaire	Direction Fulll
Lieu de stockage	Espace SMSI

Suivi des approbations

Version	Approbateur	Principales remarques	Date
1.00	L. FALORNI (Direction Fulll)		17/12/2021
2.00	L. FALORNI		30/12/2022

Suivi des révisions

Version	Auteur	Principales modifications	Date
0.01	N. SOTO (RSSI)	Création du document, sur la base du document IED_SMSI_PRE_PAS version 1.00	05/11/2021
0.02	N. SOTO	Corrections mineures	01/12/2021
0.03	N. SOTO	Prise en compte de la relecture de la Direction	14/12/2021
1.01	N. SOTO	Révision annuelle	23/08/2022
1.02	N. SOTO	Corrections diverses	22/12/2022

Sommaire

Documents de référence

	Référence	Titre	Version
[DR1]	NF ISO/CEI 27001	Technologies de l'information – Techniques de sécurité – Systèmes de management de l'information – Exigences	Décembre 2013
[DR2]	-	Programmes de conformité - AWS	
[DR3]	-	Confidentialité des données chez AWS	

Glossaire

Terminologie	Définition
AWS	Amazon Web Services, fournisseur de services Cloud
Clients	Réfère aux clients de Fulll mais aussi aux éventuels prospects avec qui l'Entité pourrait être amenée à échanger des informations dans le cadre d'un projet de mission
PAS	Plan d'Assurance Sécurité
RSSI	Responsable de la Sécurité des Systèmes d'Information
SGBD	Système de Gestion de Base de Données
SMSI	Système de Management de la Sécurité de l'Information
TBD	Point restant à valider/définir

1 Généralités

1.1 Objet

Ce document décrit les engagements pris par Fulll en termes de sécurité des données et de ses applications hébergées sur sa plateforme cloud.

1.2 Domaine d'application

Ce document s'applique à toutes les applications conçues, développées et hébergées par Fulll, pour les besoins de ses clients.

Ce sont principalement :

- Le portail, ses widgets associés et ses applications inhérentes (Marketplace, Admin) ;
- L'application de production comptable, fiscale et sociale (Production) ;
- Les applications de dématérialisation (Scan, Documents, Image, Fact) ;
- Les applications de workflow et communication (Tâches, Messages) ;
- Les applications d'exploitation de données (Dashboard, Indicators, Bank) ;
- L'outil d'aide à la saisie de caisse.

Ce document s'applique également à l'ensemble des services web de Fulll nécessaires au bon fonctionnement des applications citées ci-dessus.

1.3 Conformité

Ce document est revu à minima annuellement et validé par la Direction de Fulll.

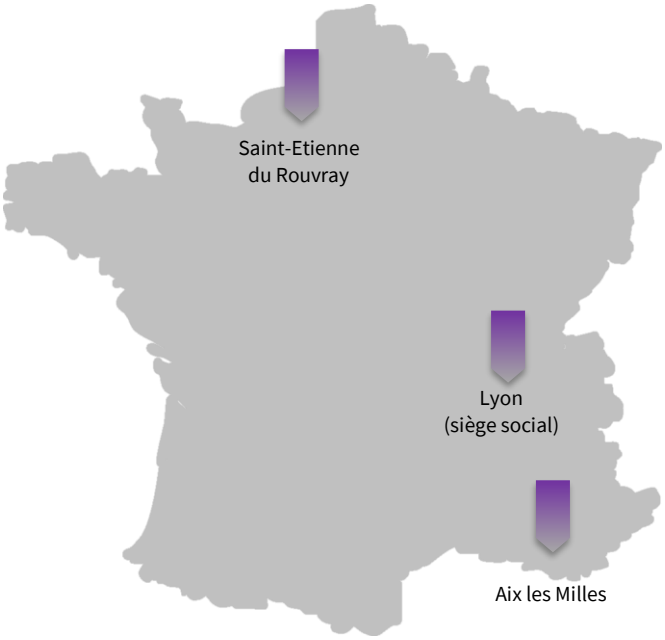
2 Présentation

2.1 Fulll

Fulll est spécialisée dans la conception, le développement et l'hébergement d'applications pour le monde de l'expertise comptable, à destination des TPE/PME.

Fulll est le fruit de la fusion de 3 entités spécialisées dans le développement d'applications.

Ces entités étaient initialement certifiées ISO 27001 depuis 2017.



Fulll dispose d'une équipe d'environ 200 personnes, composée de personnel permanent et assure principalement les activités suivantes :

- La gestion de produit / R&D
- L'hébergement et le maintien en condition opérationnelle de ses applications
- Le support applicatif
- La rédaction de la documentation d'exploitation

2.2 Enjeux

Les informations des clients et les systèmes d'information qui permettent de les traiter constituent une part essentielle du patrimoine de Fulll.

Ces systèmes d'information sont exposés à de multiples menaces pouvant porter atteinte à son activité ou à celle de ses clients. Ces menaces évoluent en permanence.

L'exposition et la complexité des systèmes d'information ainsi que leur interdépendance ne font que croître, dans un environnement ouvert, évolutif et flexible, un contexte de développement de services nouveaux, d'accès à des volumes de données croissants et des modes de restitution en évolution.

La sécurité de la plateforme et des données clients est donc d'une importance stratégique pour Fulll.

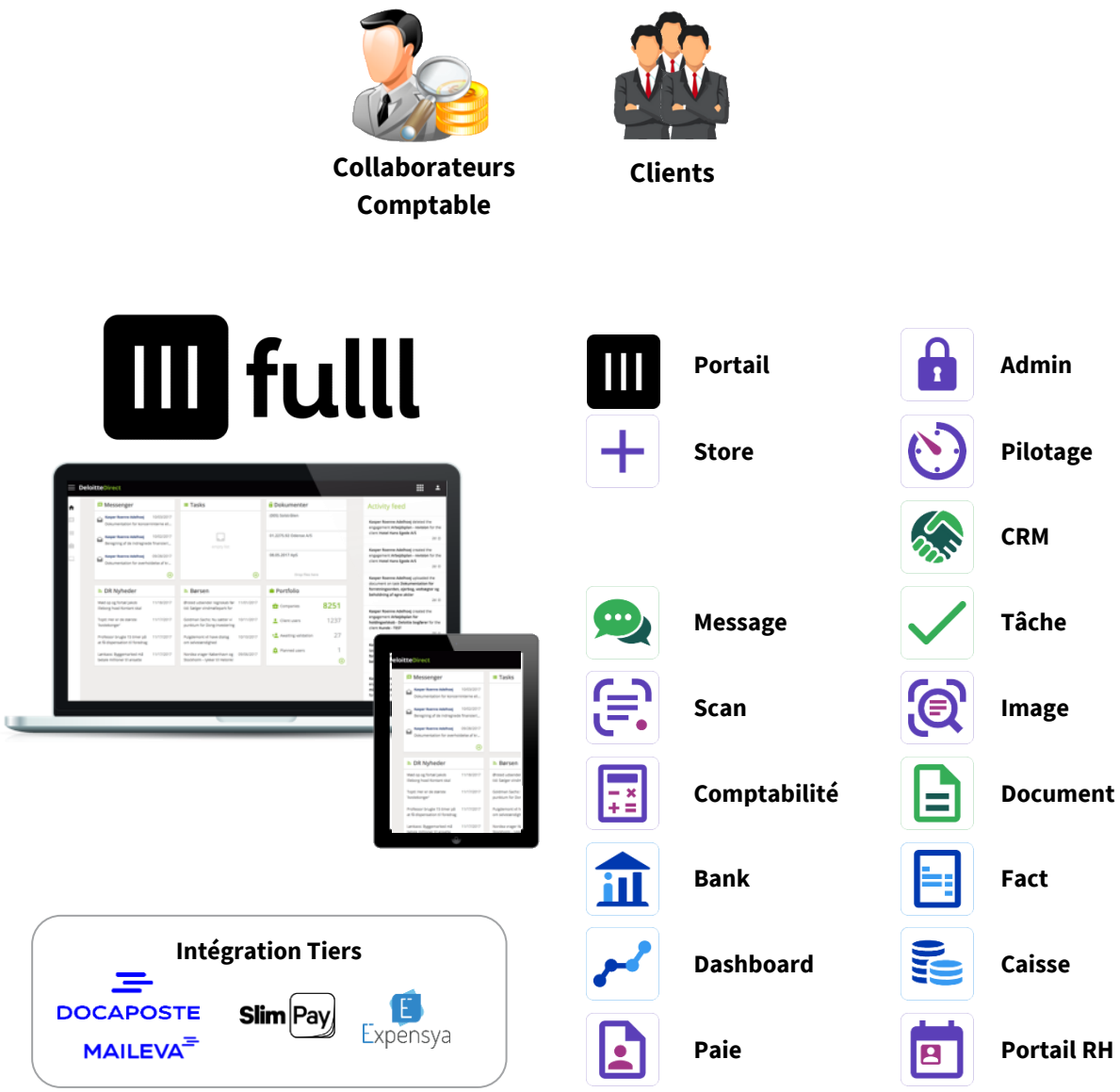
Fulll est certifiée ISO 27001, norme de référence internationale en matière de système de management de la sécurité de l'information.

Son certificat, n° IS 672984, a été délivré par BSI (British Standards Institution).

Fulll s'est engagée à garantir la confidentialité, l'intégrité et la disponibilité des informations de ses clients.

Cet engagement est reconduit chaque année.

2.3 La plateforme



La plateforme Fulll est hébergée dans l'Union Européenne, chez AWS, en France et en Allemagne.

AWS est fournisseur de référence dans le domaine des services managés dans le Cloud et dispose de nombreuses certifications en faveur de la sécurité de l'information : SOC x, ISO 27001, ISO 27017, ISO 27018, … (cf. [DR2] et [DR3]).

Les datacenters maintenus par AWS disposent d'une conception intégrant comme fonction des systèmes hautement résilients, et donc la disponibilité des services. Les datacenters AWS étant eux-mêmes répartis sur 3 zones physiquement isolées et séparées de plusieurs kilomètres. Grâce à l'utilisation des zones de disponibilité et de la réplication de données, les temps de récupération et de point de récupération sont extrêmement courts, ainsi que les niveaux les plus élevés de disponibilité des services.

La plateforme peut s'interconnecter avec des services tiers.

3 Principes d'ingénierie de la sécurité des systèmes

La sécurité est considérée par les équipes techniques de Fulll en charge de l'infrastructure selon des principes d'efficacité reconnue.

Ce chapitre décrit les principes de sécurités standards qui sont considérés dès la phase de conception.

3.1 Défense en profondeur

Le principe de défense en profondeur part du postulat qu'une seule défense ne peut pas faire face à toutes les menaces et qu'il est plus efficace d'accumuler des barrières de protection entre l'assaillant et l'objet à protéger. Le nombre de barrières devant être en rapport avec la valeur de la ressource à protéger.

Les barrières de sécurité mises en œuvre sont de plusieurs natures :

- **Humaines** Politiques de sécurité, formation, sécurité physique, …
- **Technologiques** Audit de code, tests de pénétration, chiffrement, firewall, MFA, …
- **Opérationnelles** Séparation des rôles, procédures opérationnelles, contrôles et audits, etc.

3.2 Angle Fonctionnel

L'accès utilisateur à la plateforme est basé sur une authentification préalable, aucune opération ne peut être effectuée sans cette authentification.

Chaque utilisateur ne peut accéder qu'aux fonctions et aux données auxquelles il a strictement besoin.

3.3 Angle Données

Les données peuvent être confidentielles ou personnelles, elles sont séparées de la partie application, en s'appuyant autant que possible sur des SGBD standards.

L'accès aux données par un autre mécanisme que l'application est réservé aux tâches d'administration, par le personnel Fulll habilité.

Les mécanismes de mise en production permettent le changement du code de l'application indépendamment de la mise à jour des données.

Selon leur nature, les données sont sauvegardées selon une politique formelle.

3.4 Angle Applications

Les applications Fulll permettent la connexion des utilisateurs en protégeant leurs informations d'authentification, en se basant sur des protocoles chiffrement autorisés.

Le code des applications est non modifiable par l'utilisateur.

Les paramètres de configuration sont accessibles uniquement aux administrateurs concernés.

Les journaux de débogage sont accessibles qu'au personnel Fulll habilité.

3.5 Angle Technologies

Fulll veille à concevoir des applications qui s'appuient sur des technologies reconnues, maintenables et offrant la résilience requise.

Les services et solutions technologiques choisies sont validés par la direction technique.

4 Politiques de sécurité

Fulll a formalisé l'ensemble de ses politiques de sécurité, en lien avec la norme ISO 27001. Ces documents ne sont pas en accès public et leur diffusion nécessite l'accord préalable de la direction de Fulll.

Ce chapitre résume une partie de ces politiques.

4.1 Politique générale de sécurité de l'information

L'objectif de Fulll en matière de sécurité est d'assurer, la disponibilité, la confidentialité et l'intégrité des applications et des informations qu'elles contiennent sur les systèmes d'information qu'elle met en œuvre pour ses clients.

Pour atteindre cet objectif, plusieurs grands principes de sécurité sont définis pour lutter contre les menaces pesant sur les systèmes d'information, en tenant compte des activités et des enjeux.

Ces principes sont guidés par les exigences et les bonnes pratiques définies dans les normes ISO 27001 et ISO 27002 relatives à la Sécurité de l'Information.

Ces principes sont :

- Instaurer une culture de la sécurité
- Faire contribuer les prestataires et sous-traitants à la sécurité du système d'information
- Identifier et maîtriser les risques de sécurité du système d'information sur le long terme
- Maîtriser les actifs du système d'information
- Contrôler le niveau de sécurité du système d'information
- Assurer la conformité légale/réglementaire et contractuelle
- Rationaliser les solutions et les coûts

4.2 Organisation de la sécurité de l'information

La direction de Fulll est fortement engagée dans la sécurité de l'information.

Un RSSI et un service dédié ont la charge de maintenir et de faire évoluer le Système de Management de la Sécurité de l'Information (SMSI), avec l'appui de la direction et des managers.

Les politiques de sécurité sont revues une fois par an.

La stratégie de la sécurité de l'information est pilotée à minima annuellement, lors d'une revue de direction dédiée.

Au niveau opérationnel, des revues et contrôles sont effectués mensuellement, selon un programme défini et validé par la direction de Fulll.

Le SMSI est audité deux fois par an, par un prestataire externe et par l'organisme certificateur (BSI).

4.3 Gestion des risques

Une analyse de risques est réalisée selon une méthodologie formalisée.

Elle est revue à minima annuellement et donne lieu à de nouveaux plans d'actions, favorisant ainsi l'amélioration continue.

4.4 Sécurité dans les ressources humaines

Fulll dispose de personnel permanent qualifié.

Chaque salarié possède une fiche de poste qui décrit ses missions, son positionnement au sein de l'organisation, ses principales activités, et les savoir-faire et savoir-être qu'il doit maîtriser pour mener à bien ses missions. Cela inclut sa participation à la sécurité de l'information.

Tous les contrats de travail incluent des clauses de confidentialité et de secret professionnel.

Chaque nouveau collaborateur suit une formation interne de sensibilisation à la sécurité dispensée par le RSSI ou par un membre du comité sécurité.

Des processus formels encadrent l'arrivée et le départ de collaborateurs, incluant l'affectation et la restitution d'actifs et d'accès logiques.

Fulll peut faire appel à des prestataires, notamment pour renforcer ses équipes de développement. Ces prestataires ont des accès très limités et contrôlés, ils ne peuvent accéder aux données clients sans l'accord formel de la direction.

4.5 Gestion des actifs

Tous les actifs constituant la plateforme et ceux des collaborateurs Fulll sont identifiés et répertoriés. Des inventaires sont effectués régulièrement par la direction technique et les comités sécurité de chaque site.

Les supports amovibles tels que les clés USB sont limités et encadrés.

La mise au rebut / destruction est contrôlée par un processus formel, sous la responsabilité de la direction technique.

Les dispositifs de stockage des informations client sont classés comme critiques et sont traités comme des éléments à fort impact tout au long de leur cycle de vie. Pour exemple, les dispositifs de stockage sont mis hors service par AWS selon les techniques définies dans la spécification NIST 800-88.

4.6 Gestions des accès logiques

Fulll applique le principe du juste besoin et au seul besoin d'en connaître.

Les accès aux systèmes d'information et aux données clients sont limités et contrôlés.

Les demandes d'accès suivent un processus formel et doivent être validées par la direction de Fulll lorsqu'elles concernent des éléments du système d'information contenant des informations client.

Les droits d'accès aux données clients et aux éléments de l'infrastructure sont contrôlés régulièrement, sous la responsabilité du RSSI et validés par la Direction de Fulll.

Fulll dispose d'une politique de gestion des mots de passe, précisant les règles de stockage, d'utilisation de comptes nominatifs et favorisant autant que possible les mécanismes de double d'authentification.

Les applications Fulll utilisent un mécanisme d'authentification pour effectuer toutes les actions sur le système. L'authentification renvoie un ensemble de droits pour un utilisateur donné limitant ses actions possibles par l'application.

4.7 Cryptographie et sécurité des télécommunications

Les échanges entre les applications web et les postes clients s'effectuent via le protocole HTTPS/TLS 1.2 (à minima) et utilisent des mécanismes d'authentification, sous forme de *token* à durée de vie limitée dans le temps.

Les échanges avec les API tierces sont également sécurisés (token, HTTPS/TLS 1.2).

Les bases de données de la plateforme sont chiffrées, utilisant notamment l'algorithme de chiffrement AES-256 standard.

Les documents client sont stockés sur des dispositifs chiffrés (chiffrement AWS SSE-KMS).

La gestion des clés de chiffrement de la plateforme est encadrée par la direction technique de Fulll.

Fulll met en œuvre des réseaux VPN cloisonnés pour accéder aux éléments de la plateforme, à des fins de maintenance.

Les stations de travail des collaborateurs et les réseaux internes WIFI sont également chiffrés.

4.8 Sécurité physique et environnementale

Fulll dispose de systèmes de sécurité anti-intrusion, anti-incendie et d'un accès internet redondé pour ses propres locaux.

Les données clients d'exploitation sont hébergées dans les datacenters sécurisés en France et en Allemagne.

Les équipes sous la responsabilité des hébergeurs surveillent et effectuent une maintenance préventive des équipements électriques et mécaniques pour assurer le fonctionnement continu de ses systèmes.

Les défaillances matérielles sont détectées par les hébergeurs, qui réagissent selon leurs procédures internes de maintenance du matériel.

Si des services critiques sont impactés, la direction technique de Fulll est alertée par emails/système de notifications rapides.

Les datacenters utilisent des mécanismes pour contrôler les conditions climatiques et maintenir une température de fonctionnement appropriée pour les serveurs et autres matériels, afin de prévenir la surchauffe et de réduire les risques de pannes d'alimentation. La température et l'humidité sont surveillées et régulées à des niveaux appropriés par le personnel et divers systèmes.

Les datacenters sont dotés d'équipements de détection et d'extinction automatiques des incendies.

Les systèmes d'alimentation électrique des datacenters sont conçus pour être totalement redondants et gérables sans que cela ait une quelconque incidence sur les opérations, 24h/24.

Les infrastructures d'AWS reposent sur des régions et des zones de disponibilité. Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, reliées par un réseau à latence faible, à débit élevé et à forte redondance.

Les datacenters AWS sont conçus de façon à anticiper les pannes et à y résister, tout en maintenant des niveaux de service optimaux. En cas de défaillance, le trafic des données est réacheminé automatiquement.

AWS a identifié des composants système critiques nécessaires au maintien de la disponibilité de ses systèmes et son service de récupération en cas de panne. Les composants système critiques sont sauvegardés sur plusieurs emplacements isolés, appelés zones de disponibilité. Chaque zone de disponibilité est conçue pour fonctionner de façon indépendante avec une fiabilité élevée. Les zones de disponibilité sont connectées, ce qui permet un basculement automatique entre ces zones de disponibilité sans interruption.

4.9 Sécurité liée à l'exploitation

4.9.1 Supervision et journalisation

Les serveurs, les services managés et les réseaux de la plateforme sont supervisés en permanence par les équipes AWS et par la direction technique de Fulll.

Les membres du service support de Fulll peuvent également alerter la direction technique en cas d'anomalie constatée par les utilisateurs.

Les équipes techniques de Fulll disposent de moyens de journalisation permettant des analyses en profondeur. Cette journalisation suit une politique formelle et tient compte des exigences légales en la matière.

L'accès aux journaux est limité et encadré.

4.9.2 Dimensionnement

La plateforme profite des fonctions de scalabilité offertes par AWS.

Ceci permet de dimensionner automatiquement, en fonction de la charge ou sur période, les éléments d'infrastructure sollicités. Cela concerne également les capacités des dispositifs de stockage.

Le redimensionnement est effectué à la volée, sans interruption sur la plupart des services.

Le bon dimensionnement des éléments est surveillé par le pôle infrastructure, grâce aux fonctions de monitoring et d'alarme sur seuil proposées par les services et les outils mis à disposition par les hébergeurs.

4.9.3 Gestion des mises à jour

La gestion des mises à jour suit une politique formelle de gestion des changements. Celle-ci couvre les mises à jour des systèmes, les mises à jour de sécurité et les mises à jour des applications.

Des plateformes dédiées au développement et aux tests permettent la validation des mises à jour avant leur mise en production. Les tests sont réalisés par les équipes qualité sous la responsabilité des chefs de produit.

Les mises à jour sont automatisées (*continuous delivery*), autant que possible, afin de limiter le risque d'erreurs humaines et soumises à des restrictions d'accès.

Les mises à jour majeures, entraînant une potentielle interruption de service, sont effectuées en dehors des horaires d'exploitation et après une communication préalable auprès des utilisateurs.

Fulll veille toujours à garder la possibilité de retour en arrière (*rollback*) suite à la défaillance d'une de ses applications.

4.9.4 Gestion des vulnérabilités

La plateforme dispose de protections telles que le cloisonnement, les pare-feux, filtrage IP et systèmes de détection d'intrusion.

Les stations de travail des collaborateurs disposent d'un antivirus à jour et d'un système de détection de code malveillant.

Afin de prévenir les vulnérabilités :

- Une veille est réalisée afin de maintenir les systèmes d'exploitation et les applications des stations de travail.
- Le processus de développement des applications de Fulll tient également compte de la mise à jour des codes/librairies tierces.

4.9.5 Audits techniques de sécurité

Fulll effectue annuellement un audit technique de sécurité (*pentest*).

Les résultats de cet audit sont portés à la connaissance de la direction, qui valide, s'il y a lieu, des plans d'actions menés par la direction technique.

Le RSSI est systématiquement informé des constats et suit, via le comité sécurité de chaque site, l'avancement des plans d'actions.

4.9.6 Sauvegarde

Les données clients sont sauvegardées à minima une fois par jour, en dehors des horaires d'exploitation et de façon automatique.

La direction technique est immédiatement alertée en cas d'erreur lors de la sauvegarde.

Les archives de sauvegarde sont stockées en Union Européenne, dans une localité distante de l'infrastructure d'exploitation.

Les sauvegardes sont conservées pendant deux semaines à minima. Leur accès est protégé et limité à la direction et à la direction technique.

Aussi, le code sources des applications et les éléments d'infrastructure de la plateforme sont versionnés et disposent de leur propre plan de sauvegarde.

Les sauvegardes sont contrôlées périodiquement par les comités sécurité, selon un programme validé par la direction de Fulll.

4.9.7 Rétention

Les données clients sont conservées pendant 10 ans, à minima.

4.9.8 Utilisation des données clients

Le client reste le seul propriétaire de ses données.

Les données ne sont pas cédées par Fulll sans le consentement du client.

Fulll peut toutefois être amenée à utiliser ces données pour :

- La résolution d'anomalies remontées par le client ;
- L'amélioration de ses applications, dans le cadre de demandes d'évolution émises par le client ;
- La réalisation de statistiques, de benchmarks et de règles d'apprentissage

4.10 Politique de développement sécurisé

Fulll utilise des méthodes et outils dits *Agiles* et s'efforce d'inclure dans ses applications les concepts de *security by design* et *privacy by design*.

Fulll a formalisé une politique de développement sécurisé et des standards de bonnes pratiques qu'elle met à disposition de l'ensemble de ses développeurs, chefs de produits et de ses prestataires.

Le standard de bonnes pratiques tient compte notamment du top 10 OWASP, de l'état de l'art, des codes et outils déjà mis en œuvre par Fulll.

Le code source des applications est protégé contre les changements et toute évolution doit faire l'objet d'une expression formelle du besoin, sous la responsabilité des chefs de produit.

Des outils permettent de vérifier automatiquement le code source et de garantir la qualité des changements réalisés.

Le code source est versionné et géré par un des outils de référence du marché. Son accès est limité et contrôlé.

Des environnements dédiés aux développements et aux tests sont mis en œuvre et sont séparés de l'environnement de production.

4.11 Relation avec les fournisseurs

La relation avec les fournisseurs est gérée par la direction de Fulll, selon une politique formelle.

Les contrats avec les fournisseurs contiennent des clauses liées à la sécurité, en fonction du niveau de risque.

Une revue des fournisseurs et de leur niveau de risque est effectuée chaque année par le RSSI et les comités de sécurité.

4.12 Gestion des incidents de sécurité

Fulll a formalisé sa politique de gestion des incidents de sécurité, définissant l'organisation et la gestion de la crise. La direction et l'ensemble des acteurs de Fulll sont impliqués dans cette gestion.

Dans les cas les plus graves, des analyses d'incident sont réalisées et validées par la direction. Elles conduisent à des plans d'actions visant à éliminer, dans la mesure du possible, les causes racines de l'incident.

Une politique de relation avec les autorités et groupes de travail spécialisés est formalisée. Elle tient compte notamment des exigences légales de déclaration des incidents de sécurité.

4.13 Gestion de la continuité d'activité

Fulll dispose d'un Plan de Reprise et de Continuité d'Activité (PRA/PCA).

Ce document décrit l'organisation de la cellule de crise, autour de la direction de Fulll avec tous les acteurs nécessaires à la remédiation.

Ce document fait également état des mesures préventives, des éléments de redondances en couvrant les éléments de l'infrastructure et les processus de Fulll.

Les scenarii envisagés de crise concernent les moyens matériels et humains : destruction de datacenters, indisponibilité totale des locaux Fulll, pandémie, etc.

Le PRA/PCA est mis à jour annuellement ou sur événement.

Des tests de scénario sont réalisés chaque année, selon le plan de revues validé par la direction de Fulll.

A noter qu'AWS dispose de son propre PRA/PCA.

4.14 Gestion de la conformité

Toutes les politiques de sécurité sont revues annuellement, sous la responsabilité du RSSI, et validées par la direction de Fulll.

La conformité du système de management de la sécurité de l'information est contrôlée annuellement par BSI, organisme certificateur ISO 27001.

Fulll dispose de moyens internes pour garantir la conformité aux exigences légales/règlementaires de ses applications. Ces derniers veillent à lui transmettre toutes les exigences qui doivent être respectées par la plateforme.

Fulll est un sous-traitant et ne traite les données que pour le compte du responsable de traitement. Les demandes liées aux droits des personnes sont supervisées et sous la responsabilité du responsable de traitement.

Fulll a nommé un DPO (Délégué à la Protection des Données) et formalisé une procédure de gestion des demandes d'exercice de droits RGPD.
Ces droits peuvent être exercés par mail à dpo@fulll.fr ou par courrier postal envoyé à l'adresse : 14 rue Rhin et Danube 69009 LYON, en justifiant son identité par tous moyens.