

PlayPlay s'engage dans la protection de vos données.





Présentation de PlayPlay	5
La sécurité chez PlayPlay	5
Structure du document	5
Cadre du document	6
Présentation fonctionnelle de PlayPlay	7
Architecture	8
Description technique des accès	8
Configuration des pare-feux	8
Architecture de l'application Cloud	9
Politique de Sécurité du Système d'Information	10
Organisation de la sécurité	10
Gouvernance de la sécurité de l'information et gestion du risque	11
Sécurité liée aux ressources humaines	12
Processus d'Onboarding & d'Offboarding	12
Entraînement et sensibilisation des équipes PlayPlay	12
Sécurité des données	13
Echanges des données	13
Stockage des données	13
Ségrégation des données	14
Classification de la donnée	14
Rétention de la donnée	14
Réversibilité et destruction	14
Gestion des données personnelles – Conformité au RGPD	15
Opérations de traitement des données personnelles	15
Objectif et finalité du traitement	15
Catégories des données personnelles	15
Personnes concernées	16
Les clients et les employés PlayPlay.	16
Localisation du traitement	16

Durée de traitement	16
Sous-traitants PlayPlay	16
Liste des sous-traitants	17
Gestion des biens	17
Contrôle d'accès	18
Comptes des employés PlayPlay	18
Compte des clients	19
Authentification avec un login et un mot de passe	19
Mots de passe	19
Single Sign-On Authentication – SSO	20
Gestion des Autorisations	20
Sécurité Physique et environnementale	21
Datacentres Google Cloud	21
Architecture physique & sécurité	21
Bureaux PlayPlay	22
Gestion de l'exploitation sécurité	23
Sauvegarde	23
Protection contre les codes malveillants	23
Scanner de Vulnérabilités	24
Gestion des Vulnérabilités	24
Supervision de la sécurité de la Plateforme Cloud	26
Environnements et données	27
Logging et surveillance	27
Sécurité sur les communications	27
Echange des informations	27
Protection contre les attaques DDOS	28
Acquisition, développement et maintenance des systèmes d'information	28
Secure Software Development Life Cycle	28
Gestion des incidents de sécurité	29
Notification dans le cas d'un incident	29
Gestion du plan de continuité de l'activité	31
Conformité	32

Infrastructure	32
Règlement Général sur la Protection des Données – RGPD	32
Campagnes de tests de pénétration	32

1. Présentation de PlayPlay

PlayPlay est une scale up B2B créée en 2017. PlayPlay est la solution de création de vidéos en ligne qui permet aux équipes de communication & marketing de transformer n'importe quel message en une vidéo engageante. Plus de 1500 entreprises sur plus de 15 pays font aujourd'hui confiance à PlayPlay pour créer des vidéos aux formats d'interview d'employés, de nouvelles, d'annonces d'événements ou encore d'offres de recrutements

2. La sécurité chez PlayPlay

La sécurité de nos systèmes et de nos données est un élément clé de notre produit et de notre entreprise. Nous accordons une extrême importance à l'implémentation de bonnes pratiques de sécurité et de mesures techniques et organisationnelles pour gérer la sécurité de manière appropriée et adéquate ainsi que pour garantir une résilience aux menaces et aux risques auxquels nous faisons face.

En tant qu'entreprise SaaS créée en 2017, PlayPlay a rapidement pris la place de leader sur le marché de la création vidéo. Cet accomplissement ne peut pas être durable dans le temps sans une posture de Cybersécurité forte.

Le programme de Cybersécurité de PlayPlay est en perpétuelle évolution pour refléter les ambitions de l'entreprise mais aussi pour adapter les protections face à l'augmentation constante des menaces ciblant les entreprises SaaS. .

La stratégie de sécurité est construite autour de ces 3 missions:

- La **Crédibilité et la Confiance** avec pour but premier de proposer des mesures de sécurité de niveau professionnel et d'assurer une conformité constante aux exigences des clients
- Le **Contrôle et la Résilience** qui reposent sur une stratégie d'approche par les risques nécessaire pour l'implémentation adéquate de mesures de Sécurité
- La **Détection et la Réponse** afin d'être en mesure de réagir de manière appropriée et dans un délai approprié en cas d'événements suspects

3. Structure du document

Ce document définit les différents processus, procédures et bonnes pratiques implémentés à PlayPlay dans un cadre conforme avec le standard **ISO/IEC 27001:2013**. Les chapitres et les informations de ce document peuvent donc être liés selon la structure générale du standard ISO/IEC 27001:2013.

4. Cadre du document

Ce document couvre le programme de sécurité PlayPlay au travers des différents domaines clés en CyberSécurité. Tous ces domaines sont représentés dans le contexte de l'entreprise PlayPlay en tant qu'entreprise SaaS - *Software as a Service*.

5. Présentation fonctionnelle de PlayPlay

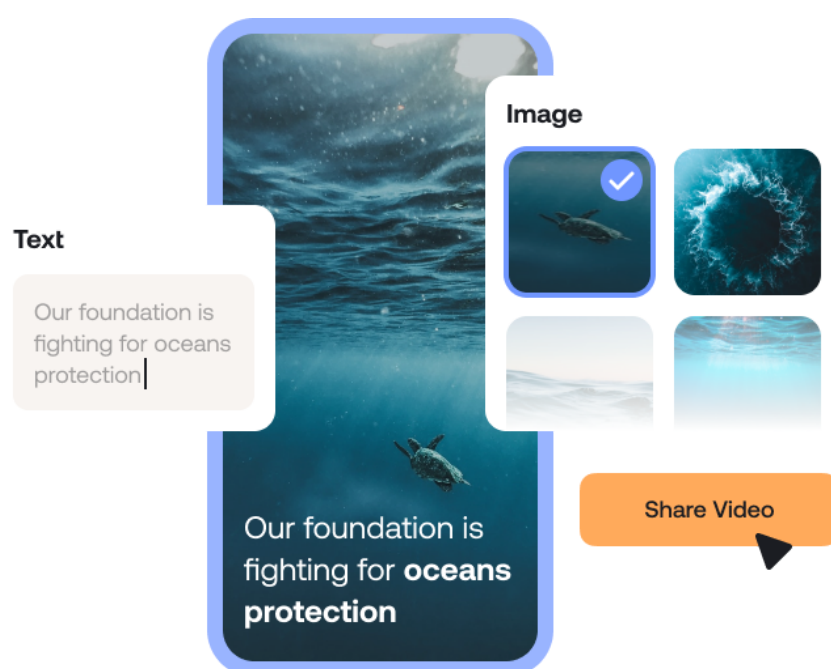
PlayPlay fournit aux clients un ensemble de services décrit en détails sur notre [Site Web](#), et en particulier:

- Des templates de vidéos
- La possibilité de customizer ces templates en intégrant des informations de branding
- La mise à disposition d'outils permettant d'assembler des écrans standards
- L'accès à du contenu de librairies de médias offert par PlayPlay

A partir de ces éléments, les clients peuvent produire des vidéos sur la plateforme. Pour la création de contenu, les clients peuvent:

- Choisir un template et des écrans à partir de ceux disponibles sur la plateforme;
- Compléter les champs spécifiques (auteur, quote, etc...);
- Choisir des médias depuis sa propre base de données (photo, vidéo , musique, etc...) ou sélectionner des contenus parmi la librairie de média proposée par PlayPlay

A la fin, les clients vont pouvoir visualiser la vidéo ou même la télécharger quand ils le souhaitent depuis notre plateforme.



6. Architecture

La plateforme PlayPlay est une application SaaS *multi-tenant* qui fournit une instance unique mais avec une isolation stricte sur les données des différents clients.

Les clients se connectent à la plateforme PlayPlay en HTTPs, avec l'utilisation de TLS de manière systématique pour l'ensemble des communications depuis et vers la plateforme PlayPlay. Les utilisateurs finaux accèdent à l'instance PlayPlay avec des navigateurs standards.

Description technique des accès

PlayPlay a été conçu pour être utilisé et accessible sans pré-requis techniques. Ainsi, il n'est pas requis d'installer un logiciel ou tout autre outil sur les machines de nos clients.

Cependant, dû à la complexité de certaines interfaces de notre plateforme mais également pour assurer une utilisation optimale des fonctionnalités, nous recommandons d'utiliser les dernières versions des navigateurs web les plus répandus - *Google Chrome*, *Mozilla Firefox*, *Apple Safari* ou encore *Microsoft Edge*.

Comme il s'agit d'un document de sécurité, nous recommandons également l'utilisation des dernières versions de navigateurs web pour des raisons de sécurité afin de recourir à des versions sans vulnérabilités.

Notre plateforme PlayPlay est accessible à l'adresse suivante : <https://playplay.com>

Configuration des pare-feux

Dans le cas où un pare-feu serait présent sur le réseau des clients, une configuration spécifique peut éventuellement être requise. Les accès à PlayPlay, à notre service de stockage de fichiers et aux services de stockage des médias doivent être autorisés.

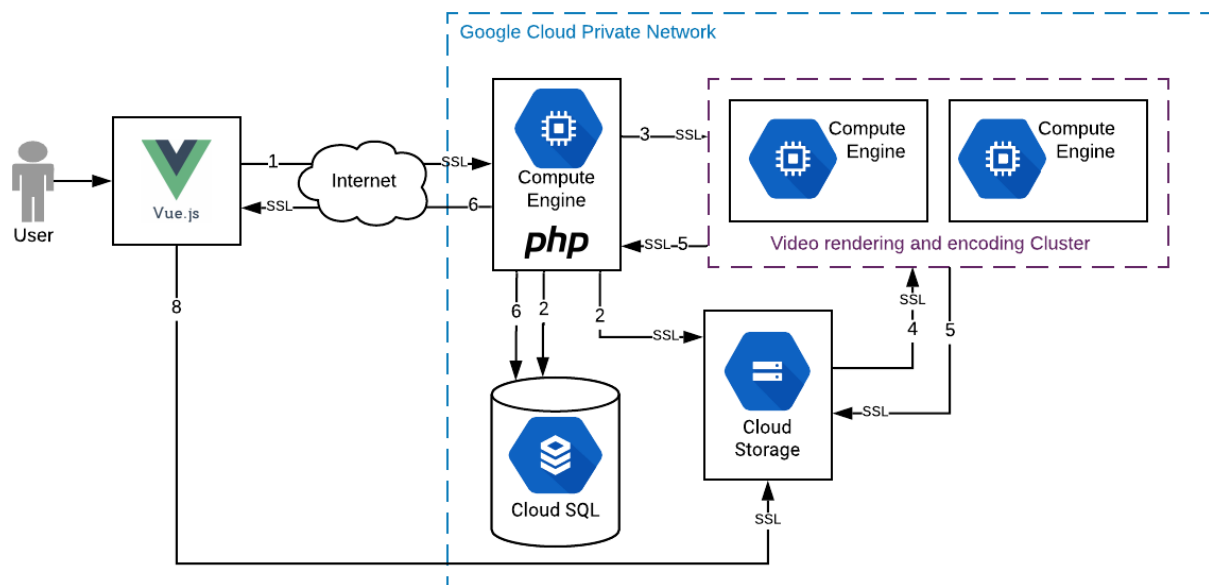
De manière à garantir un excellent niveau de service, l'architecture de PlayPlay est distribuée et s'appuie sur des services tiers hautement résilients. De ce fait, il est impossible de fournir une liste d'adresses IP spécifiques pour notre service, et la mise sur liste blanche devra passer par des noms de domaines.

Les domaines suivants doivent être autorisés au niveau des pare-feux :

- Les services PlayPlay
 - playplay.com
 - storage.playplay.com
 - ws-eu.pusher.com

- Les services de stockage de médias
 - media0.giphy.com
 - media1.giphy.com
 - media2.giphy.com
 - media3.giphy.com
 - media4.giphy.com
 - media.gettyimages.com
 - delivery.gettyimages.com
 - download.gettyimages.com

Architecture de l'application Cloud



Les utilisateurs de PlayPlay accèdent au service au travers d'une interface Web. Cette application Web est conçue sur la base de JavaScript et communique avec nos serveurs en HTTPs JSON API.

Au niveau des bases de données, nous utilisons des bases de données **Google Cloud Storage** ainsi que des instances **Cloud SQL** qui sont provisionnées dans des segments réseaux isolés et non-routables. Les requêtes des utilisateurs finaux ne peuvent pas être émises directement sur les instances de stockage.

Les données clientes sont logiquement ségréguées dans ces instances de stockage.

Le diagramme suivant présente le workflow de génération vidéo :

1. Envoi des informations utilisateur à notre API (textes et médias)
2. Stockage des informations sur des services redondés
3. Envoi des listes de tâches nécessaires aux serveurs de rendu vidéo
4. Récupération des médias par les serveurs de rendu vidéo
5. Stockage de la vidéo finale et information de la fin du traitement à l'API

6. Enregistrement de la fin du traitement et information du front-end du nouveau statut
7. Récupération de la vidéo finale et affichage à l'utilisateur

7. Politique de Sécurité du Système d'Information

La structure de sécurité de PlayPlay est basée sur le standard **ISO/IEC 27001:2013**. La politique de Sécurité est le document de plus haut niveau sur lequel sont attachés des politiques, des standards, des procédures ou des méthodes pour composer tout le matériel documentaire qui est revu et mis à jour de manière régulière afin de refléter les évolutions du produit, de l'entreprise et des potentielles nouvelles menaces.

La politique de sécurité de PlayPlay est un document interne et confidentiel. Ce Whitepaper Security est basé sur cette politique de sécurité en reprenant les informations qui peuvent être partagées avec les clients. Le but est de fournir de manière transparente les informations aux clients désireux d'avoir du détail sur la gestion de la sécurité et les mesures mises en place chez PlayPlay.

8. Organisation de la sécurité

Le programme de Cybersécurité chez PlayPlay est dirigé par le *Head of Information Security* avec des interactions fortes et en coordination étroite avec le CEO, le CTO et des autres exécutifs chez PlayPlay.

Le *Head of Information Security* est supporté dans sa mission par une équipe sécurité dédiée et intégrée sur l'ensemble des fonctions de l'entreprise. L'équipe sécurité est en charge des différents domaines d'expertise qui incluent:

- Expertises Security sur le Cloud
- Expertises Security applicative
- Gouvernance, Risques et Conformité
- Expertise Security IT

L'équipe collabore étroitement avec l'ensemble des employés PlayPlay sur des sujets aussi bien stratégiques qu'opérationnels.

L'équipe représente également le point de contact privilégié pour les relations clients sur les sujets de sécurité.

La sécurité de l'Information chez PlayPlay est conduit à la fois:

- Au niveau stratégique avec des revues de direction régulières

- Au niveau opérationnel avec des suivis de plan d'actions, d'incidents et d'améliorations

Les représentants de chacune des fonctions sont responsables de l'application de la politique de sécurité et de son respect dans leurs divisions et équipes respectives.

Ci-dessous, les fonctions PlayPlay qui contribuent directement au programme de sécurité:

- **Thibaut Machet** - Co-fondateur et CEO (Chief Executive Officer)
- **Florent Poissonnet** - CTO (Chief Technology Officer)
- **Alexandre Butynski** - Head of Architecture & DPO (Data Protection Officer)
- **Jeremy Fridman** - Head of Information Security

9. Gouvernance de la sécurité de l'information et gestion du risque

Le système de management de la Sécurité est un élément essentiel chez PlayPlay pour maintenir l'efficacité du business ainsi que pour atteindre les objectifs. Il est également essentiel pour apporter une confiance supplémentaire aux clients de PlayPlay et pour leur garantir l'atteinte de leurs engagements.

De plus, une gouvernance Cybersécurité forte et efficace comportant des reportings transparents et de la visibilité sur les objectifs et résultats opérationnels est primordiale pour démontrer les capacités de PlayPlay à assurer la confidentialité et l'intégrité des données clients ainsi que la disponibilité des systèmes.

PlayPlay a défini un framework de gestion des risques sécurité pour efficacement et précisément gérer les activités sécurité sur la plateforme et globalement au travers de toute l'entreprise. L'approche par les risques de sécurité est gérée au travers d'évaluations régulières pour constamment contrôler les risques, leurs probabilités et leurs impacts. Les risques de sécurité sont manipulés à l'échelle de l'entreprise et sont des éléments nécessaires utilisés dans la prise de décision.

Les éléments suivants font partie intégrante du framework:

- Une **analyse des risques** basée sur la méthodologie EBIOS-RM (délivrée et maintenue par l'ANSSI - Agence Nationale de la Sécurité des Systèmes d'Information - <https://www.ssi.gouv.fr/en/digital-risk-management/>) sur le périmètre de l'écosystème PlayPlay qui inclut la plateforme et ses

environnements de production et de développement, les bureaux de PlayPlay, les personnes et les outils & données d'entreprise

- La surveillance et le contrôle régulier de l'analyse de risques lors de **revues de direction**
- La **mise à jour régulière** de l'analyse de risques en cas de changements impactant la posture de sécurité chez PlayPlay
- L'**évaluation des risques** selon une probabilité et un impact
- Une approche par les risques maintenue au niveau produit pour adresser les sujets de sécurité dans les toutes premières phases des nouvelles initiatives, projets ou fonctionnalités.

10. Sécurité liée aux ressources humaines

Processus d'Onboarding & d'Offboarding

Dans les phases initiales du processus de recrutement, PlayPlay effectue des vérifications qui incluent des prises de références pour des emplois précédents. De plus, la signature d'une clause de confidentialité liée au contrat est un pré-requis pour débiter chez PlayPlay.

L'équipe People chez PlayPlay maintient les processus d'onboarding et d'offboarding pour gérer de manière adéquate tous les aspects liés à l'arrivée et au départs des employés de l'entreprise.

Le processus d'onboarding inclut la création des comptes et le provisionnement des accès basés sur les rôles et responsabilités de chacun.

Tous les employés PlayPlay sont amenés à prendre connaissance de notre charte informatique qui définit les bonnes pratiques de sécurité (Multi-factor authentication, gestion des mots de passe, ...), la bonne utilisations des outils et des données (gestion des médias amovibles, des logiciels...) et les obligations en tant qu'employé à se conformer à ces règles.

En cas de départ, notre processus assure que les accès sont supprimés dès la sortie de l'employé. PlayPlay maintient les traces et le suivi pour contrôler la bonne gestion des arrivées et des départs.

Dans le cadre des revues régulières de nos pratiques, ces processus sont régulièrement ajustés pour refléter l'évolution de l'entreprise et les potentiels changements dans l'organisation.

Entraînement et sensibilisation des équipes PlayPlay

PlayPlay s'engage à protéger les données clientes et c'est pour cela que nous prenons le sujet de la sensibilisation et de l'entraînement avec une attention importante.

Le développement de la sensibilisation de sécurité commence dès la phase d'onboarding pendant laquelle les bonnes pratiques de sécurité dans les bureaux sont partagées et expliquées. De plus, une autre session d'onboarding obligatoire se concentre sur les risques principaux et les menaces auxquelles une entreprise SaaS fait face. Durant cet onboarding, certaines techniques de cyberattaques (notamment le phishing) sont également revues en détail.

Par la suite, et durant toute la période d'emploi, les employés PlayPlay reçoivent des sensibilisations et des entraînements adaptés à l'exposition et aux risques associés à leurs fonctions.

Nous utilisons un outil de sensibilisation qui nous permet de développer une culture en Cybersécurité forte au niveau de toute l'entreprise. Cet outil permet aux employés de se familiariser avec les sujets clés tels que le phishing, le ransomware, la fuite de données... L'outil nous permet également de lancer des campagnes de simulation de cyber attaques comme des attaques de phishing.

Notre équipe de développeurs reçoit également des sensibilisations ciblées et des entraînements sur la connaissance des vulnérabilités de l'OWASP Top 10 et les bonnes pratiques de développement pour les éviter et les corriger.

11. Sécurité des données

La donnée est un asset critique qui doit bénéficier de mesures de traitement adéquates tout au long de son cycle de vie.

Echanges des données

Toutes les communications sont effectuées en HTTPS TLS 1.2+ avec un chiffrement fort. Le certificat SSL X.509 est contresigné par une autorité de certification reconnue.

Cela permet de protéger les communications contre des attaques communes comme l'espionnage, le man-in-the-middle, la falsification et la manipulation active des messages.

Stockage des données

Les données au repos sont systématiquement chiffrées par défaut. Le chiffrement se base sur les capacités natives des services de stockage pour chiffrer l'ensemble des données en utilisant l'algorithme standard *Advanced Encryption Standard (AES)* avec des clés de 256 bits.

Plus d'informations sont disponibles sur le lien suivant: <https://cloud.google.com/security/encryption/default-encryption>.

Ségrégation des données

PlayPlay est une application SaaS multi-tenant. Les données des clients sont gérées dans un même environnement technique, mais avec une stricte ségrégation logique appliquée sur les accès et le stockage des données. La mise en place de filtres bas niveaux sur l'application assure que les données clientes ne seront jamais rendues visibles à d'autres clients. Le contrôle d'accès au niveau de la donnée est systématiquement remis en question pendant les campagnes de test de pénétration que nous lançons régulièrement.

Classification de la donnée

PlayPlay applique une classification unique pour toutes les données clientes que nous stockons. Les précautions maximum sont appliquées pendant tout le cycle de vie de la donnée.

Les clients restent responsables des données qu'ils importent sur le produit PlayPlay. Les clients ont également la possibilité de gérer des permissions d'accès en utilisant la fonctionnalité de vidéo privée.

Rétention de la donnée

Les données sont stockées tout au long du contrat et sont supprimées dans les 2 ans suivant la fin du contrat. Cependant, les données peuvent être supprimées avant cette période de 2 ans sur demande du client dans les 30 jours suivant la fin de contrat.

Pour les données personnelles associées aux comptes, ces données sont également supprimées 2 ans après la fin du contrat ou 2 ans après la désactivation du compte.

Réversibilité et destruction

Au terme du contrat, les clients ont la possibilité de récupérer l'ensemble des données.

PlayPlay s'engage à fournir ces données qui incluent:

- L'export de tous les contenus produits avec les informations suivantes: la date de création, le nom du projet, le nom de l'utilisateur, le format de la vidéo et le lien vers la vidéo
- L'export est réalisé selon une procédure convenue avec le client prenant en compte le volume des données

La procédure de réversibilité se lance comme suit:

- Le client fait une demande de réversibilité auprès de PlayPlay

- PlayPlay organise un atelier de travail pour définir le format d'échange et les termes de l'export
- Exécution de l'export des données
- Le client valide la bonne réception des données

Les clients ont 30 jours suivant la fin du contrat pour demander la mise en place du processus de réversibilité.

Cette procédure implique la destruction de tous les fichiers uploadés et produits sur la plateforme, la suppression de tous les textes et vidéos et l'anonymisation des données restantes. Cela nous permet de supprimer l'ensemble des données collectées tout en gardant de manière anonyme des données pour des besoins de statistiques.

12. Gestion des données personnelles - Conformité au RGPD

PlayPlay s'engage à suivre et implémenter toutes les mesures issues des lois de protection des données personnelles telle que le *RGPD - Règlement Général sur la Protection des Données* ou le *CCPA (California Consumer Privacy Act)*. Plus d'informations sur le traitement des données personnelles sont disponibles dans notre *Politique de Confidentialité* et dans notre *DPA (Data Processing Addendum)*.

Opérations de traitement des données personnelles

Collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, suppression ou destruction.

Objectif et finalité du traitement

La principale finalité du traitement est de permettre aux utilisateurs de PlayPlay de créer et de télécharger des vidéos. Nous identifions également deux finalités secondaires: La communication avec les utilisateurs PlayPlay (support et nouveautés du produit) et l'analyse de leurs usages de notre plateforme.

Catégories des données personnelles

- Données d'identification (prénom, nom, ID, adresse email, mot de passe)
- Données relatives aux vidéos (fichiers uploadés, contenu des vidéos)
- Logs d'accès (tentatives d'authentification, rapports d'erreurs, enregistrement des sessions)
- Informations techniques (Adresse IP, version de navigateur web, Système d'Information)

- Données d'usage/statistique (nombre de vidéos créées, paramètres des vidéos, type de média utilisé...)

Personnes concernées

Les clients et les employés PlayPlay.

Localisation du traitement

- Stockage des données: Le data center primaire est localisé en Belgique. Pour des besoins de haute disponibilité et de redondance, nous pouvons utiliser des datacenters distants mais exclusivement localisés en Europe.
- Union Européenne et USA pour une partie des données d'identification les logs d'accès, les informations techniques et les données d'usage.
- Accès: Seuls les employés de PlayPlay basés en France peuvent potentiellement accéder aux données clients.

Durée de traitement

Toute la durée du contrat sous lequel PlayPlay est engagé pour fournir les services. Les données seront supprimées deux ans après la fin du contrat ou avant en cas de demande explicite.

Sous-traitants PlayPlay

PlayPlay n'engage une relation de sous-traitance pour le traitement des données personnelles que si les conditions suivantes sont réunies.

- Signature d'un Accord sur le Traitement des Données Personnelles (« Data Processing Agreement » ou « DPA »).
- Assurance du respect du RGPD.
- Mise en place de pratiques de sécurité essentielles telles que le chiffrement des données en transit et au repos, le backup des données et leur suppression lorsque cela est nécessaire. Notre principal sous-traitant et hébergeur, Google Cloud, présente les meilleures garanties possibles en la matière avec, entre autres, une conformité aux normes ISO/IEC 27001/27017/27018/27701 et SOC 1/2/3.
- Pour ceux localisés en dehors de l'Union Européenne, dans des pays n'offrant pas un niveau de protection adéquat, mise en place des Clauses Contractuelles Types de la Commission Européenne ou de toutes garanties appropriées prévues par la réglementation applicable en matière de données personnelles - [European Commission-approved standard contractual data protection clauses](#).

Liste des sous-traitants

Informations légales	Objet du traitement	Données traitées	Localisation des données
Google France SARL Paris, France	Hébergement de PlayPlay	Toutes les données traitées par PlayPlay	Belgium
Amazon Web Services Ireland Limited Dublin, Ireland	Envoi d'emails	Email	Ireland
Restpack Inc. (AnnounceKit) Middletown, DE USA	Annonces de nouveautés produit	Email, ID	USA
Appcues, Inc. Boston, MA USA	Aide contextuelle	Email, ID	USA
Heap Inc. San Francisco, CA USA	Analyse des usages	Email, ID, informations techniques, données d'usage	USA
Hotjar Limited St Julian, Malta	Enregistrement de sessions utilisateurs	Email, ID, informations techniques, données d'usage	Ireland
Intercom Inc. San Francisco, CA USA	Discussion en ligne	Email, ID, informations techniques	USA
Planhat AB Stockholm, Sweden	Gestion du support client	Prénom, nom, email, ID et données d'usage	Belgium and Netherlands
Functional Software, Inc. (Sentry) San Francisco, CA USA	Rapports d'erreur	Email, ID, informations techniques	USA

13. Gestion des biens

L'inventaire des biens est divisé en 3 parties:

- L'environnement Cloud sur lequel PlayPlay utilise les capacités natives et les services Cloud pour facilement identifier les éléments qui composent notre application

- L'inventaire des matériels (par exemple les ordinateurs utilisés par nos équipes) qui est géré par les équipes People et contrôlé via notre solution de MDM – *Mobile Device Management*
- Les logiciels et outils que les équipes utilisent pour les activités opérationnelles quotidiennes (par exemple les outils SaaS que nous utilisons)

Tous les biens sont identifiés avec un niveau de classification et un responsable.

L'usage acceptable de ces biens est géré en conformité avec le niveau de classification alloué. Les bonnes pratiques et les usages acceptables associés peuvent être trouvés dans la charte informatique PlayPlay, dans les procédures techniques ou dans des guides utilisateurs. Le responsable est chargé de la mise à jour des usages acceptables.

14. Contrôle d'accès

Contrôler les accès à la plateforme PlayPlay et aux outils d'administration associés est crucial pour assurer la sécurité des données de nos clients.

Comptes des employés PlayPlay

Tous les comptes ont un identifiant unique.

Une grande majorité des accès à nos outils et nos produits internes est gérée avec le mécanisme de SSO (Single Sign-On) qui rend plus facile et plus robuste l'authentification et la gestion des mots de passe en interne. La politique de mots de passe est conforme avec les recommandations de l'autorité française (CNIL).

De plus, tous les employés doivent utiliser un second facteur d'authentification (2FA) lorsque celui-ci est disponible. Cette mesure protège des menaces communes comme la compromission ou le vol de mots de passe.

L'accès des employés PlayPlay à la plateforme et aux outils d'administration est contrôlé au travers d'une gestion de droits basée sur les rôles qui permet d'allouer le minimum de droits pour chacun des utilisateurs – *accès basés sur le principe du moindre privilège*.

Ainsi, seuls les membres de PlayPlay effectuant le support et les équipes techniques sont capables de voir les vidéos produites par nos clients dans le strict cadre de démonstration ou de processus de support et en cas d'assistance technique. Pour des raisons de sécurité, l'équipe de sécurité de PlayPlay peut également avoir accès aux contenus.

Les comptes de PlayPlay sont créés pendant le processus d'onboarding et les permissions sont assignées au regard des rôles, fonctions et responsabilités.

Les permissions sont revues mensuellement pour les accès à hauts privilèges (par exemple les accès aux bases de données).

Pour les départs des employés, le processus d'offboarding assure la suppression de tous les accès dès la fin de contrat.

Compte des clients

Tous les accès à notre plateforme PlayPlay sont authentifiés.

Il existe deux mécanismes d'authentification sur la plateforme:

- Authentification avec un login et un mot de passe
- Authentification au travers d'une fédération d'identité avec du SSO (Single Sign-On)

Authentification avec un login et un mot de passe

L'authentification au travers d'un login et d'un mot de passe est gérée comme suit:

- Le compte est créé et configuré par l'équipe support de PlayPlay ou par un utilisateur avec un rôle Owner
- Un email contenant un lien invitant à créer un mot de passe est envoyé à l'utilisateur
- L'utilisateur est redirigé vers la plateforme PlayPlay pour créer son mot de passe en conformité avec la politique de mot de passe

A tout moment, l'utilisateur a la possibilité de soit:

- Modifier son mot de passe
- Réinitialiser son mot de passe

Aussi, le 2FA (2-factors authentication) est implémenté par défaut pour tous les utilisateurs. Le 2FA consiste en un code envoyé par email en supplément du mot de passe. Cela protège du risque de vol de mot de passe et d'autres menaces communes.

Mots de passe

Nous garantissons la confidentialité des mots de passe. Ils ne sont visibles à aucun moment que ce soit à la création ou à la modification. Les mots de passe ne sont jamais envoyés par email ou via d'autres canaux de communication.

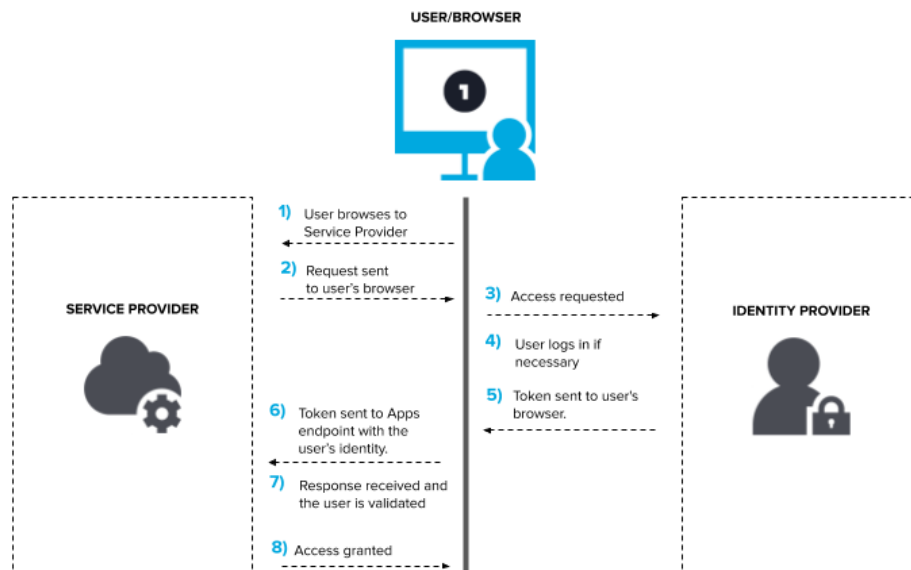
Le mot de passe doit être composé de 8 caractères incluant des minuscules, des majuscules et des caractères numériques.

Les mots de passe sont stockés en base de données après avoir été hashés avec l'algorithme Bcrypt.

Single Sign-On Authentication - SSO

La plateforme PlayPlay supporte l'intégration avec SAML v2 ou OpenID avec une grande majorité de fournisseurs d'identité.

L'utilisation de SSO fournit un niveau supplémentaire de sécurité où le client est entièrement responsable de la gestion des données d'authentification de ces utilisateurs.



Gestion des Autorisations

Chaque utilisateur est assigné à une company et une équipe qui lui fournit des accès aux vidéos.

De plus, chaque utilisateur est assigné à un rôle spécifique qui associe des permissions sur la plateforme:

- Rôle **'member'**: L'utilisateur peut créer du contenu vidéo
- Rôle **'admin'**: L'utilisateur peut créer du contenu vidéo et peut gérer les utilisateurs (création, suppression, assignation) de son entreprise
- Rôle **'owner'**: L'utilisateur peut créer du contenu vidéo, peut gérer les utilisateurs et peut gérer les aspects et paramètres de Branding de son entreprise

15. Sécurité Physique et environnementale

Datacentres Google Cloud

La plateforme PlayPlay, les données et les services associés sont hébergés dans un datacenter de Google Cloud Platform dans la région de Belgique.

Comme défini dans le modèle de responsabilité partagée du Cloud, la sécurité physique des infrastructures d'hébergement des données est sous la responsabilité du fournisseur de Cloud.

Google documente et maintient à jour toutes les bonnes pratiques et mesures de sécurité mises en place sur les infrastructures d'hébergement.

Aussi, Google détient un grand nombre de certifications et d'accréditations qui apportent une confiance supplémentaire sur les mesures implémentées pour la sécurité physique.

Ci-après les document de Google Cloud Platform:

<https://cloud.google.com/docs/security/infrastructure/design>

PlayPlay bénéficie directement des bonnes pratiques de Google pour renforcer la sécurité, incluant:

- La haute disponibilité des réseaux et des serveurs au travers des zones de disponibilité
- La redondance des services sur différents data centers
- La redondance des serveurs sur différents data centers

Architecture physique & sécurité

La plateforme PlayPlay est hébergée sur un datacenter Google qui applique les meilleures pratiques de sécurité. Toutes les données sont hébergées en Europe (Belgique)

- <https://www.google.com/intl/en/about/datacenters/locations/st-ghislain/> pour le site primaire. Pour des besoins de haute disponibilité et de redondance, nous pouvons recourir à l'utilisation de datacenters distants mais qui restent exclusivement localisés en Europe.

Google Cloud Platform Regions



Le fournisseur de services Google Cloud Platform bénéficie d'une sécurité physique de haut niveau (contrôle d'accès, résilience au sinistres naturels, incendie...) et offre un niveau exemplaire de services comme une haute disponibilité basée sur de la redondance qui permet d'adapter la démarche de gestion de la sécurité.

Google Cloud Platform est certifié sur une large gamme de certifications sécurité et conformité comme l'**ISO/IEC 27001**, l'**ISO/IEC 27017** ou le **SOC2** qui sont régulièrement renouvelées par des acteurs externes indépendants.

Toutes les certifications de Google Cloud Platform sont accessibles ici - <https://cloud.google.com/security/>.

Bureaux PlayPlay

Les bureaux des équipes PlayPlay sont localisés sur 3 sites différents:

- Paris (France)
- New York (Etats-Unis)
- Berlin (Allemagne)

La sécurité des bureaux est gérée au travers de différentes mesures:

- L'accès aux bureaux est restreint par un badge personnel. L'inventaire des badges est géré par l'équipe People de PlayPlay qui suit une procédure pour l'assignation des nouveaux badges, la désactivation en cas de perte ou de vol ainsi que la remise du badge en fin de contrat.

- Des caméras sont installées dans les bureaux de PlayPlay et les images visionnées en cas d'activités suspectes
- Les bureaux sont également équipés d'un système d'alarme
- Les employés de PlayPlay ont à leur disposition des casiers protégés pour stocker leurs équipements professionnels pendant leur absence

PlayPlay n'héberge aucun serveur contenant de la donnée cliente dans ses bureaux.

16. Gestion de l'exploitation sécurité

PlayPlay met en place différentes procédures et processus pour maintenir la sécurité de l'ensemble des services proposés. Ce chapitre décrit une partie de ces opérations. Cette description n'est pas exhaustive mais représente les activités majeures permettant d'apprécier le niveau de maturité de sécurité.

Sauvegarde

La non-perte de données est garantie par l'utilisation d'architectures ou de services redondés. Ainsi, la base de données applicative et le système de stockage de fichiers sont répliqués sur deux datacenters différents dans la même zone géographique (Belgique) permettant de garantir qu'aucune donnée ne sera perdue en cas d'incident majeur. De plus, cela permet aussi d'assurer facilement la continuité du service dans ce type de situation.

Pour prévenir les cas les plus extrêmes (suppression de données par erreur, service Google Cloud globalement indisponible...) un backup des données supplémentaire est réalisé chaque jour et stocké dans un troisième datacenter. L'accès à ces sauvegardes bénéficie des mêmes critères de sécurité que la base de données principale (accès nominatifs basés sur des droits individuels).

Protection contre les codes malveillants

Dans l'objectif de limiter la propagation de fichiers malveillants sur la plateforme PlayPlay, les fichiers uploadés sont systématiquement scannés et ré-encodés avant d'être utilisés.

Ainsi, tous les fichiers qui sont affichés ou téléchargés (la vidéo finale, les fichiers uploadés par un utilisateur tiers) sont scannés par des solutions antivirales.

Le système d'antivirus ClamAV est installé sur les instances de serveurs où les médias sont uploadés et également où les vidéos prêtes à être téléchargées sont stockées.

Scanner de Vulnérabilités

PlayPlay lance régulièrement des scans de vulnérabilités qui permettent d'identifier des vulnérabilités communes à la fois sur la partie applicative mais aussi sur la configuration de nos environnements. Nous utilisons des solutions open source pour faire ces scans. Le scan de vulnérabilités fait également partie des campagnes de tests de pénétration que nous lançons régulièrement sur la plateforme PlayPlay.

Gestion des Vulnérabilités

La gestion des vulnérabilités est une pratique de sécurité pour prévenir de manière proactive l'exploitation de vulnérabilités de toutes sortes dans une organisation.

Les vulnérabilités sont des défauts qui peuvent être exploités par une entité ou un acteur malicieux pour obtenir des accès ou des permissions supplémentaires sur un système.

PlayPlay impose un processus de gestion de vulnérabilités qui a pour but de gérer l'ensemble des vulnérabilités dans une approche commune quelque soit la source de vulnérabilité.

Nous distinguons les domaines suivants où des vulnérabilités peuvent être identifiées et exploitées:

- Les composants natifs Cloud / Services managés: En lien avec le modèle de responsabilités partagées du Cloud, les vulnérabilités et les patchs sur les services managés par Google sont sous la responsabilité du fournisseur de service Cloud. Par conséquent, ces vulnérabilités ne sont pas traitées au travers du processus de gestion des vulnérabilités PlayPlay
- Services Cloud gérés par PlayPlay (par exemple les bases de données, les Systèmes d'exploitation dans les VM sur le Compute Services Google): Nous maintenons à jour la liste des composants et leurs versions et nous utilisons des bases de données de vulnérabilités pour être notifié en cas de nouvelles vulnérabilités (CVE). Les nouvelles CVEs sont gérées au travers de notre processus de gestion de vulnérabilités.
- Les vulnérabilités de niveau applicatif (par exemple les librairies): Nous utilisons un outil de SCA (*Software Component Analysis*) - **Dependabot** - qui identifie de manière automatique les composants contenant des vulnérabilités connues (CVE). Comme nous implémentons une approche d'intégration continue/déploiement continu, nous avons la facilité de déployer des patchs de manière très rapide. Bien entendu, le patch peut avoir des impacts mais nous mettons en œuvre toutes les mesures

appropriées pour éviter des impacts fonctionnels tout en contrebalançant avec les aspects de sécurité.

- Vulnérabilités issues des campagnes de pentests - Les vulnérabilités découvertes lors des campagnes de pentest sont requalifiées dans le cadre de notre processus de gestion des vulnérabilités.
- Vulnérabilités "sauvages" - Ce type de vulnérabilité peut être identifié soit par des équipes de PlayPlay ou potentiellement par des clients. Ces vulnérabilités sont analysées par l'équipe sécurité de PlayPlay via le processus de gestion de vulnérabilités.

Les clients peuvent à tout moment contacter l'équipe sécurité pour partager des potentiels problèmes, événements ou vulnérabilités de sécurité qui nécessitent un support spécifique en écrivant à l'adresse suivant: security@playplay.com

Le processus de gestion de vulnérabilités est divisé selon les étapes suivantes:

- **Reporting** de la vulnérabilité (voir chapitre précédent)
- **Analyse et investigation:** Cela inclut la vérification d'applicabilité, les impacts potentiels et l'exposition. Les métriques vont déterminer du niveau de criticité de la vulnérabilité et vont conditionner le plan de remédiation
- La **remédiation** peut se faire soit sur l'application avec la mise en place d'un patch, soit via la mise en place d'une solution de contournement, ou encore via l'ajout d'une barrière de sécurité supplémentaire pour réduire l'exposition ou pour supprimer complètement la vulnérabilité.

Les vulnérabilités sont gérées et suivies par l'équipe sécurité.

Les vulnérabilités identifiées sont classifiées selon un niveau de criticité et nous implémentons les remédiations selon ce niveau:

Criticité	Time to remediate
Critique	48h
Haut	7 jours
Moyen	30 jours
Faible	Plusieurs Mois

Supervision de la sécurité de la Plateforme Cloud

Le fournisseur de services cloud offre en ensemble d'outils de sécurité pour superviser et évaluer la posture de sécurité d'un environnement. PlayPlay utilise certains de ces outils pour avoir le détail de la conformité de sécurité de l'environnement et des services utilisés mais aussi pour détecter des potentielles mauvaises configurations. Les outils sont sous la responsabilité des équipes Sécurité et Plateforme à PlayPlay.

Gestion du changement

Les nouvelles fonctionnalités, les corrections, les améliorations ou les nouvelles versions sont déployées de manière continue avec plusieurs déploiements par semaine. La grande majorité de ces déploiements n'ont aucun impact sur les utilisateurs finaux. PlayPlay communique pour certaines de ces évolutions directement sur l'application grâce à du contenu contextualisé ou via des release notes disponibles auprès de tous les utilisateurs.

En cas d'évolution majeure ou de changement radical qui peut résulter d'une incapacité de modifier des anciennes vidéos, une communication spécifique est envoyée à tous les utilisateurs avec une notification de 3 mois minimum.

Tous les changements bénéficient de l'intégration continue et de notre pipeline de déploiement qui réduit de manière significative les actions manuelles pour la release des nouvelles versions.

Tous les changements passent par la même procédure:

- Pair-review des spécifications (incluant l'évaluation des impacts)
- Le code est poussé dans une branche dédiée et validé dans notre pipeline DevOps qui inclut des vérifications automatiques diverses: qualité de code, analyses de sécurité,...
- Un environnement de test est déployé
- Une revue de code par un pair est obligatoire avant l'intégration de la branche dans la branche master
- Toutes les mises à jour (majeures, mineures et les patches) suivent la même pipeline de validation
- Promotion en production suivant une pipeline automatique
- Le processus de rollback est également automatique en cas de problèmes pendant et après le déploiement

Après une nouvelle release, les problèmes ou erreurs potentiels ainsi que les retours clients sont attentivement scrutés pour assurer l'intégration réussie de la release.

Environnements et données

Différents environnements sont utilisés selon le besoin.

L'environnement de production, qui ne contient que les services requis pour la plateforme accédée par les clients.

L'environnement de pré-production, pour simuler des tests avec un environnement similaire à l'environnement de production.

Les environnements de test sont principalement utilisés par les équipes de développement.

Les données utilisées en pré-production et en environnements de test sont des données fausses ou anonymisées.

Logging et surveillance

Les logs sont envoyés en temps réel dans notre outil de monitoring.

Nous récupérons les logs applicatifs (audit logs) dans Big Query. Ces logs tracent les actions réalisées par les utilisateurs sur notre produit PlayPlay. Nous construisons et maintenons une liste d'alertes de sécurité basées sur ces logs pour détecter des activités potentiellement suspectes.

Nous récupérons également les logs de niveau infrastructure pour détecter des activités suspectes de bas niveaux. Nous utilisons la solution Datadog pour effectuer ce monitoring.

La détection des activités suspectes et malicieuses peut aboutir à un incident de sécurité qui est par la suite géré via notre processus de gestion des incidents de sécurité défini dans ce document.

17. Sécurité sur les communications

Echange des informations

Toutes les communications sont sécurisées via SSL, TLS 1.2+.

Les seuls échanges passant par internet sont les appels à l'API PlayPlay (playplay.video) et les uploads et récupérations de fichiers via le service de stockage Google Cloud Storage (storage.googleapis.com). Tous les services utilisés par PlayPlay sont isolés au sein d'un réseau privé virtuel (VPC) Google Cloud. Celui-ci est doté d'un pare-feu proxy permettant d'en restreindre l'accès.

Les bases de données et les autres services utilisés sont uniquement accessibles depuis le réseau privé Google Cloud Platform. L'accès au VPC est protégé par un proxy Firewall.

Les différents environnements (test, pré-production et production) sont cloisonnés au niveau réseau de manière à éviter toute porosité.

L'utilisation du pare-feu fourni par Google Cloud permet de garantir le respect de ces principes ainsi que l'accès aux ressources sensibles uniquement à certaines adresses IP.

Protection contre les attaques DDOS

PlayPlay bénéficie de la protection native contre les attaques DDOS via l'utilisation des instances de Load Balancer Google Cloud.

18. Acquisition, développement et maintenance des systèmes d'information

Secure Software Development Life Cycle

Nos équipes de développement emploient une attention particulière sur les bonnes pratiques de sécurité.

Les spécifications techniques sont créées par les équipes de développement pour éviter au maximum les erreurs.

Dans le but de garantir un niveau de qualité excellent, la pratique de revue de code est au centre de notre processus de développement. Ainsi, toutes les lignes de code envoyées en production sont revues par au moins 2 membres de l'équipe. Cette phase est cruciale pour identifier des potentielles erreurs et vulnérabilités de sécurité. Nous utilisons bien entendu également des outils pour détecter automatiquement des vulnérabilités sur le code.

Les critères clés de notre approche sont l'intégration de nos outils de sécurité dans notre pipeline DevOps et l'adoption de la suite d'outils par les développeurs PlayPlay.

Toutes ces pratiques sont intégrées dans la pipeline CI/CD qui nous permet d'assurer une conformité au standard de développement et d'application sécurisée.

Cela inclut:

- Un outil d'analyse de code statique (**SAST**) qui identifie les vulnérabilités (notamment celles de l'OWASP Top 10) sur le code source de l'application. Nous utilisons à ce jour Sonar Cloud. Les vulnérabilités sont ensuite analysées pour en déterminer l'applicabilité et les corrections sont planifiées selon le niveau de criticité
- Un outil de scan de dépendances (**SCA** - Software Component Analysis) qui notifie en cas de nouvelles vulnérabilités connues - CVE - Nous utilisons l'outil dependabot intégré à GitHub
- Un outil de **détection des secrets** dans le code source - Nous utilisons GitLeaks

De plus, les développeurs ont tous accès à un ensemble de cours qui couvrent les bonnes pratiques de développement et les exploitations des vulnérabilités communes sur l'application.

Enfin, nous lançons régulièrement des campagnes de tests de pénétration via des experts d'entreprises tierces.

19. Gestion des incidents de sécurité

Notification dans le cas d'un incident

La transparence totale avec nos clients sur le sujet des incidents de sécurité est essentielle.

PlayPlay a défini un plan de communication transparent avec l'ensemble de ces clients pour les notifier rapidement sur une potentielle brèche de données. Ce plan de communication est continu jusqu'à la résolution de l'incident et une identification précise des conséquences.

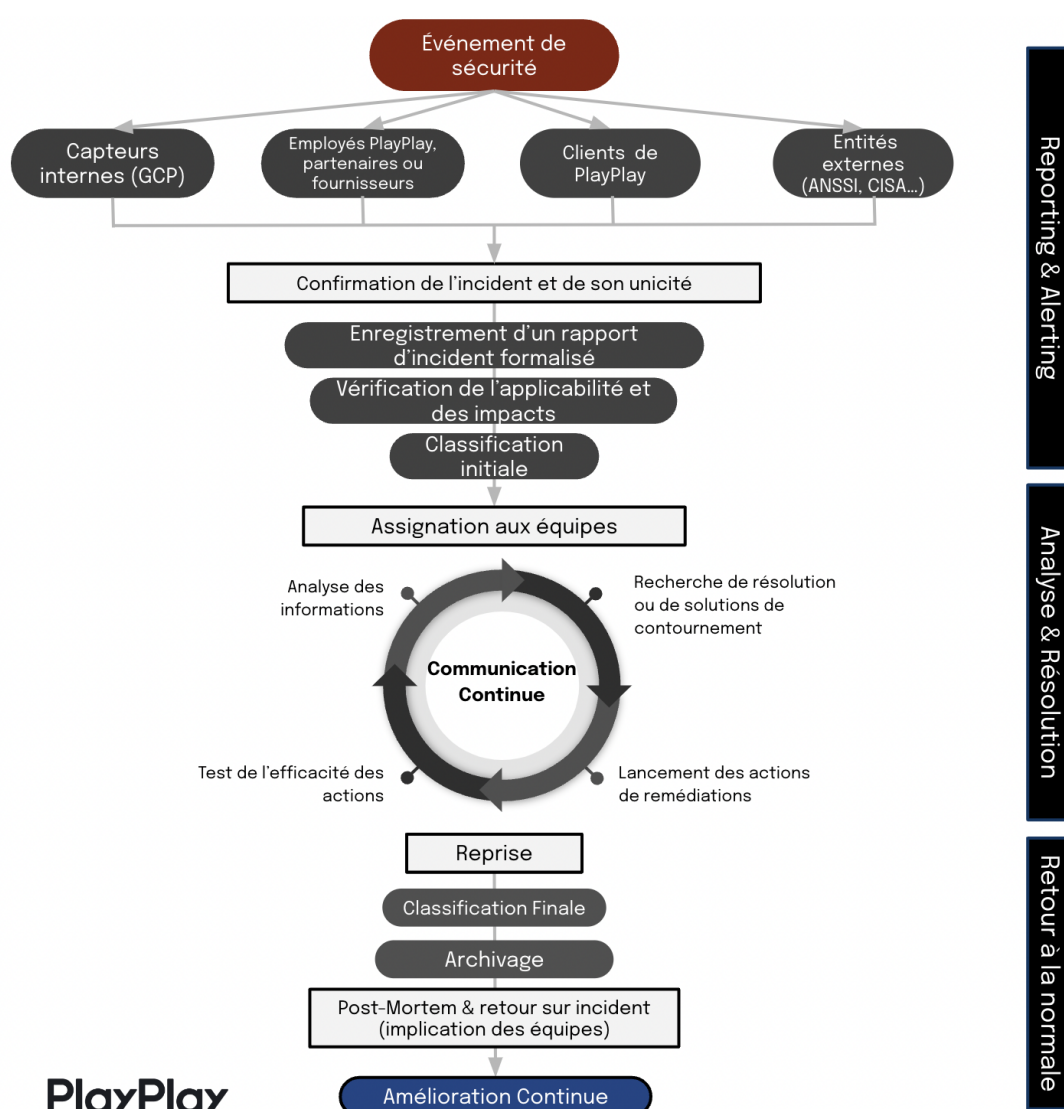
Nous demandons à nos clients d'identifier un contact sécurité (email et téléphone) qui peut être contacté en cas d'urgence. De plus, deux numéros de téléphone du support PlayPlay sont communiqués à nos clients et sont joignables en 24/7.

En interne, nous avons un canal de communication dédié à la gestion des incidents.

Le processus de gestion des incidents de sécurité est divisé en 3 grandes étapes:

- Le **Reporting** et **l'Alerting**: Cela consiste à récupérer les détails via les différents canaux et de faire une première analyse pour déterminer l'applicabilité et le niveau de classification de l'incident
- **L'analyse** et la **résolution**: Les équipes impliquées dans l'incident vont identifier des résolutions ou des solutions de contournement et vont planifier les actions pour stopper la propagation potentielle et pour remédier de manière appropriée le plus rapidement possible. Pendant toute l'étape de résolution, une communication continue est entretenue avec les parties prenantes
- **Retour à la normale**: Une fois l'incident résolu et toutes les actions de remédiations implémentées, PlayPlay organise un rituel de Post-Mortem pour un retour d'expérience et pour identifier des actions potentielles dans le but d'améliorer le temps de résolution et pour éviter des cas similaires dans le futur

Le schéma suivant fournit une vue générale du processus:



Pour la notification d'incidents de sécurité avec des impacts potentiels sur les données ou les services des clients, PlayPlay s'engage à notifier dans les 48 heures suivants l'identification de l'incident.

La résolution de ces incidents est réellement dépendante de leurs natures mais PlayPlay s'engage à mettre en place tous les moyens nécessaires et les efforts requis pour revenir à une situation normale le plus rapidement possible.

De plus, tout événement suspicieux ou incidents de sécurité, ou pour toutes questions de sécurité, vous pouvez nous contacter sur security@playplay.com.

20. Gestion du plan de continuité de l'activité

Différents éléments nous permettent de garantir une continuité du service en cas de sinistres majeurs:

- L'utilisation de services redondés et des sauvegardes comme décrit précédemment dans ce document
- L'implémentation d'outils de déploiement automatique (Ansible, Terraform, Packer) pour nous permettre de redéployer un environnement complet dans une nouvelle infrastructure dans un délai raisonnable
- La non-adhérence à notre fournisseur de Cloud - en effet tous les services utilisés sont des services "génériques" (VM, MySQL database, Cloud File Storage...) qui trouvent leurs équivalents chez les autres fournisseurs

PlayPlay a également défini un **Plan de Reprise d'Activité** qui inclut des tests réguliers en conditions opérationnelles.

Le Plan de Reprise d'Activité est prévu pour décrire les actions nécessaires pour restaurer les accès à la donnée et aux services après un sinistre. Cela inclut les mesures immédiates prises pour remettre en place les opérations à un niveau acceptable dans un délai raisonnable et avec une perte minimum de données. Cela est possible grâce à un ensemble de mesures et de solutions comme le remplacement des services indisponibles et des mesures de restauration de données.

21. Conformité

Infrastructure

Google Cloud Platform est conforme avec les certifications principales (ISO 27001, 27017, 27018 and 27701, SOC 1, 2 et 3 ...). Toutes ces certifications et les pratiques de sécurité sont accessibles ici <https://cloud.google.com/security/>.



Règlement Général sur la Protection des Données - RGPD

PlayPlay est strictement conforme avec les législations applicables sur la data privacy et notamment le RGPD en Europe et le CCPA en Californie (USA).



Campagnes de tests de pénétration

Pour valider notre résilience continue et pour assurer que l'évolution constante de notre produit n'impacte pas notre posture de sécurité, nous lançons régulièrement des campagnes de tests de pénétration.

Ceci permet également d'améliorer la culture sécurité des équipes PlayPlay en illustrant les menaces et les risques avec des exploitations réelles.

En conséquence, une campagne de pentest est lancée au moins tous les 6 mois.

Les pentests se concentrent sur:

- Les nouvelles fonctionnalités et les évolutions de notre produit

- Les fonctionnalités sécurité de notre produit
- Les nouvelles techniques de cyber attaques et les nouvelles menaces
- La validation potentielle des corrections des vulnérabilités remontées par les derniers pentests

Les pentests peuvent être lancés selon différents scénarios:

- Black box - les pentesteurs n'ont accès à rien
- Grey box - les pentesteurs ont des comptes sur notre plateforme
- White box - Les pentesteurs ont accès au code source de notre application et tout document leur permettant d'avoir une vue précise de notre produit

Les pentests sont lancés sur notre environnement de production.

Les résultats des pentests sont gérés au travers de notre processus de gestion de vulnérabilités décrit plus haut dans ce document.

