Règlement de traitement de la plateforme Cryfe™

1. Désignations

Les désignations suivantes sont utilisées dans les réponses du présent document :

- **Système** : Solution algorithmique traitant les entretiens filmés de façon automatique (machine learning et règles métier pour la désignation d'indices) pour en extraire les analyses
- **Utilisateur** : Personne (Coach, DRH, Recruteur…) utilisant la solution via un accès sécurisé (**compte**) et pour laquelle le système fournira des analyses de l'entretien (**analyses**) - Il s'agit de l'interviewer
- **Interlocuteur** : Personne filmée lors d'un entretien et sur laquelle reposera essentiellement le traitement de la vidéo par le système (analyse des signaux visuels et audio) - Il s'agit de l'interviewé, du coaché, etc.
- **Administrateur** : Personne (CEO CM Profiling ; CTO CM Profiling disposant d'un accès au backoffice de la solution avec des droits de lecture et d'édition des informations de par la plateforme (liste des utilisateurs, interviews…).
- **MVP (Minimum Viable Product)** : Il s'agit d'une version du produit avec juste assez de fonctionnalités pour satisfaire les premiers clients afin de fournir un retour d'information sur le développement futur du produit.
- **Entretien** : S'entend toute communication qu'elle soit interpersonnelle ou intrapersonnelle (dans le cas d'une préparation par exemple), interview.

2. Nom et adresse du responsable

Caroline Matteucci, CM Profiling Sàrl, Haldenweg 56, 3074 Muri b. BERN

3. Nom et dénomination complets de la plateforme

CRYFE

4. But de la plateforme et du traitement (fichier)

Mise à disposition d'une solution traitant toute forme de communication interpersonnelle, passant par des entretiens d'embauche, entretien ou de préparation en body impact pour permettre l'analyse de différents signaux audio et visuels (voix, gestuelles, confort, pacificateur, inconfort…) afin de remonter les indices nécessaires à l'évaluation de la congruence / incongruence.

Le fichier traité en entrée de la solution est un flux vidéo, incluant donc des données de l'utilisateur et de l'interlocuteur (visuel et audio de l'entretien filmé).

5. Situation de départ

CRYFE™ SAAS, software as a service:

L'objectif du système est de fournir un outil permettant d'accompagner et d'épauler les utilisateurs lors d'entretiens aux fins d'analyse de la congruence, soit la relation positive entre ce que je pense, dis et fais et son contraire l'incongruence. Pour ce faire, l'outil lit les signaux audio et visuels de manière automatisée afin de remonter les indices comportementaux clés. Cela permet à l'utilisateur d'être soutenu à la lecture comportementale de son interlocuteur, car il peut revenir sur chaque signal lu et analysé par les algorithmes. L'utilisateur peut donc voir les moments de congruence (impact) de son interlocuteur, identifier les différentes émotions ressenties (visuelles et audio) ou encore revenir sur des gestuelles de confort, pacificateurs ou inconfort.

L'upload d'une vidéo d'un entretien est nécessaire dans un premier temps (MVP), à terme il s'agira de traiter le flux vidéo de l'entretien en temps réel.

Dans un premier temps (MVP), l'outil est réservé aux utilisateurs (Coach, DRH, Recruteur…) via un accès sécurisé à la plateforme. Les interlocuteurs ne disposent pas d'un compte utilisateur leur permettant d'accéder à l'outil.

À terme, en cas de réussite du MVP, il est prévu que les interlocuteurs puissent aussi accéder à la plateforme avec un accès sécurisé en se créant eux-mêmes un compte.

La solution sera disponible dans différents pays (hors Suisse et hors Europe).

6. Catégories de données personnelles traitées

Sphère intime, caractéristiques personnelles, identité, adresse courrielle, voix, image, gestuelle

Pour l'utilisateur :

- Informations personnelles liées au compte utilisateur
    - Adresse courrielle
    - Nom / Prénom
    - Informations de paiement et abonnement
        - Adresses de facturation
        - Type/Plan de souscription

À noter que les informations relatives aux coordonnées bancaires (numéro de carte, cryptogramme…) ne sont pas stockées sur les serveurs de la plateforme.

- Voix (conversations lors de l'entretien)
- Image (potentiellement lors de l'entretien)

Pour l'interlocuteur :

- Voix (conversations lors de l'entretien)
- Image (postures et gestuelles lors de l'entretien)
- Adresse courrielle (saisi par le recruteur pour permettre de communiquer la vidéo brute – sans les analyses CRYFE™ – au candidat s'il le souhaite)

À terme (pour les interlocuteurs) :

- Informations personnelles liées au compte utilisateur
    - Adresse courrielle
    - Nom / Prénom

7. Catégories des destinataires des données

Les données – entretien filmé et audio, sans analyses du système – peuvent être remises au l'interlocuteur à sa demande. Les données analysées sont destinées aux utilisateurs.

Les destinataires des données sont uniquement des membres de la plateforme CRYFE™ (Utilisateur, Admin, Développeurs).

8. Catégories de participant au fichier

Aucune mutation des fichiers vidéo sources n'est envisagée.

L'utilisateur de CRYFE™ peut entrer des notes personnelles dans le flux de l'analyse de la communication interpersonnelle, il s'agit dans ce cas de métadonnées (ne mutant pas la vidéo originale).

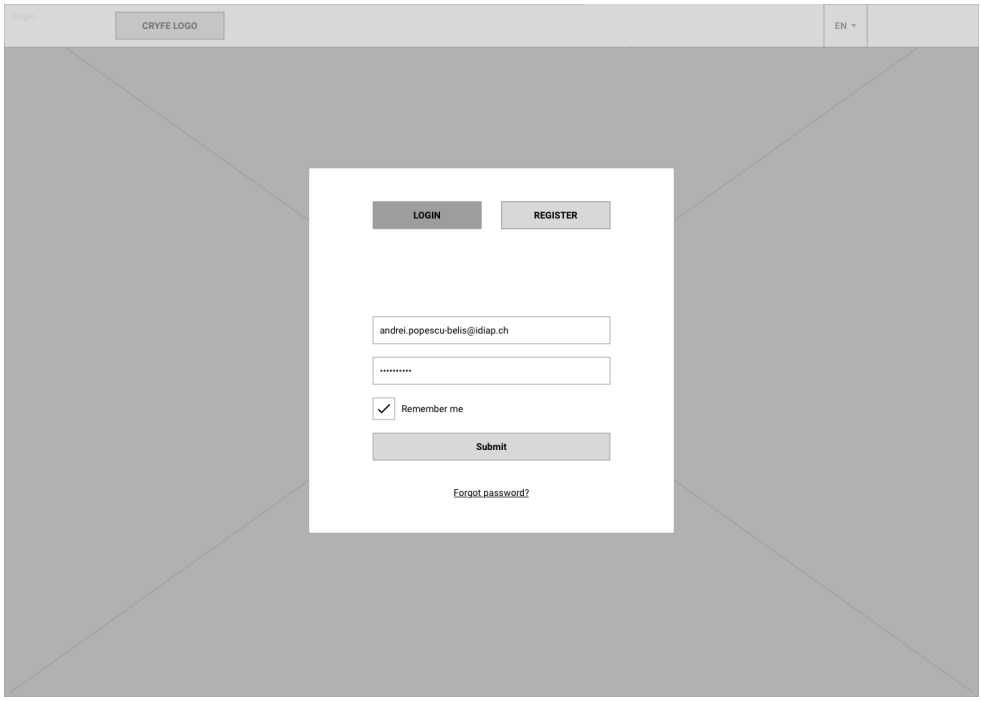
Il est envisagé que certaines vidéos puissent être utilisées par une personne de la société CM Profiling à des fins d'annotations (association manuelle de tels signaux à un moment T d'une vidéo) pour performer le système (amélioration des modèles de machine learning pour mieux détecter les signaux automatiquement par la suite). Dans l'optique de ce scénario, la solution prévoit que l'accord de « Partager sa vidéo et les analyses en découlant à des fins d'amélioration du système » soit donné explicitement par l'interlocuteur.

9. Description des interfaces

Écrans du scénario principal

Avant le sign to account, le client, futur utilisateur, doit renseigner son email et il a ainsi accès à une démo de la plateforme.

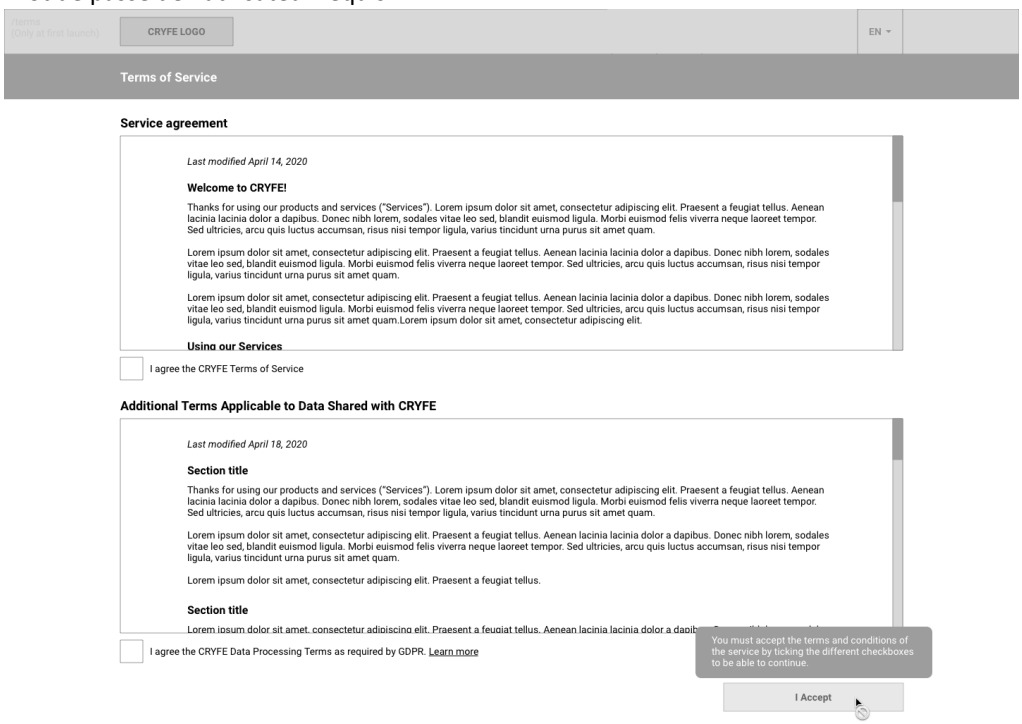
Ensuite, en cas d'intérêt :



Connexion

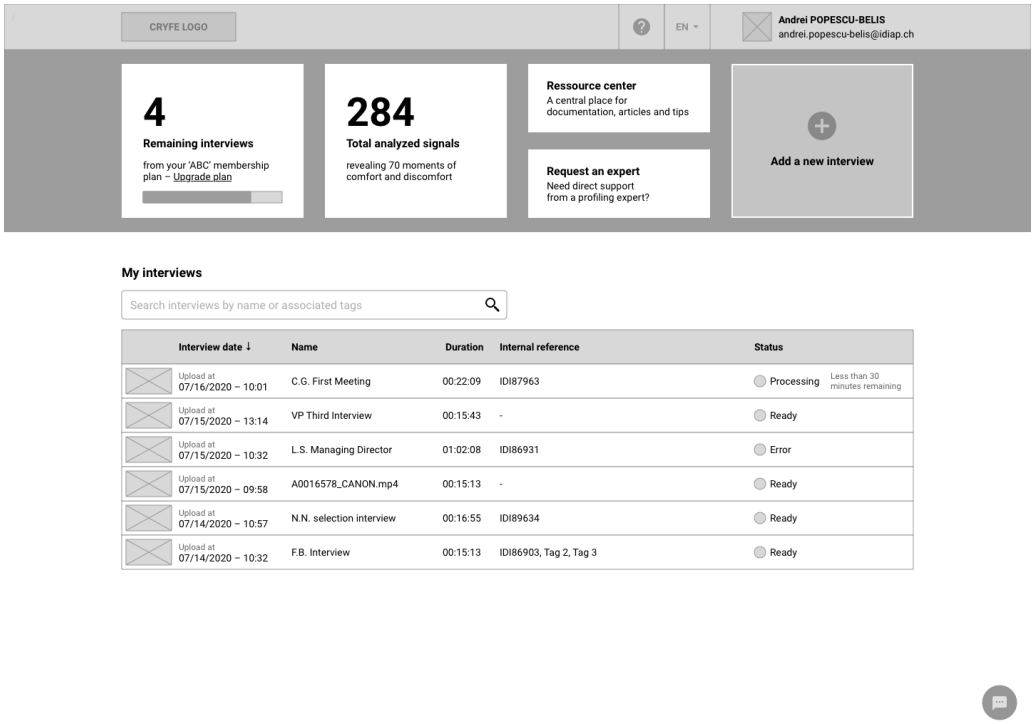
Email de l'utilisateur requis

Mot de passe de l'utilisateur requis



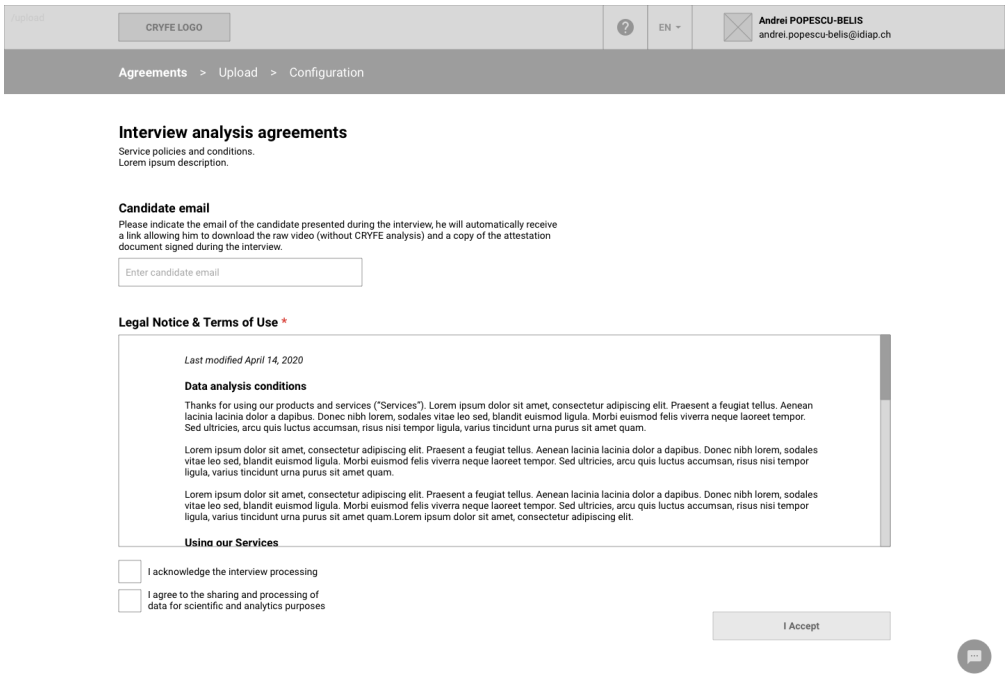
T&C de la plateforme

Exposés à la première connexion



Dashboard

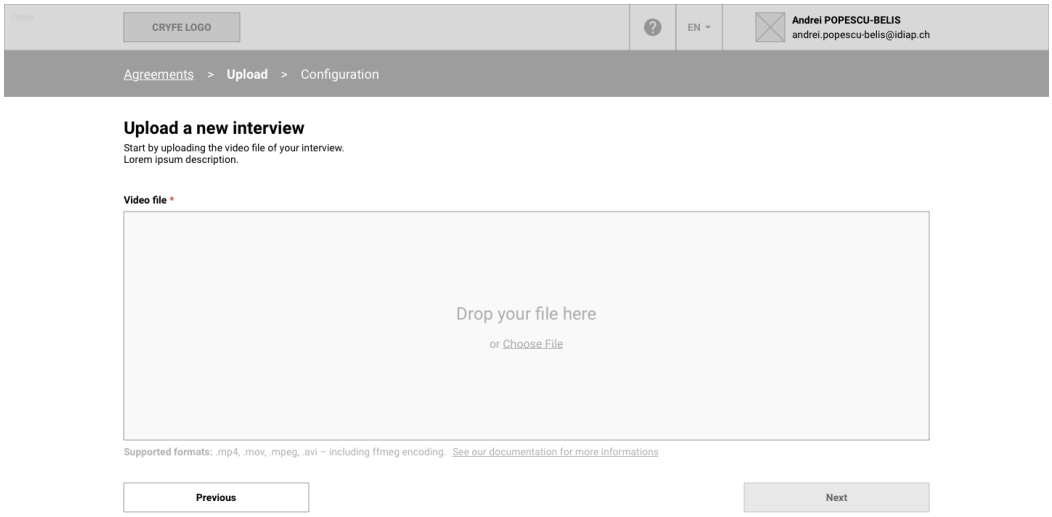
Consultation et accès à la liste des entretiens déjà uploadée sur CRYFE™



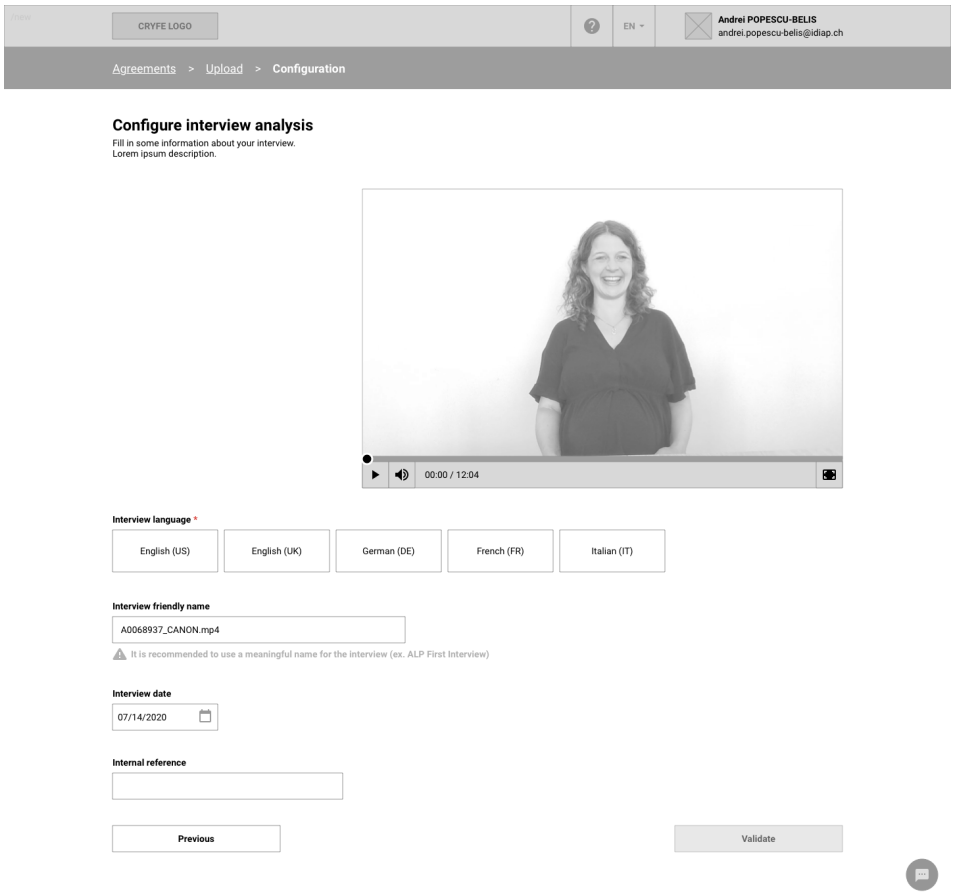
Ajout d'un nouvel entretien (Étape 1)

Acceptation des T&C

Renseignement de l'email de l'interlocuteur (dans l'optique que lui soit envoyée la vidéo brute de son entretien) – Dans le cadre du MVP cette fonctionnalité pourrait aussi être gérée manuellement.

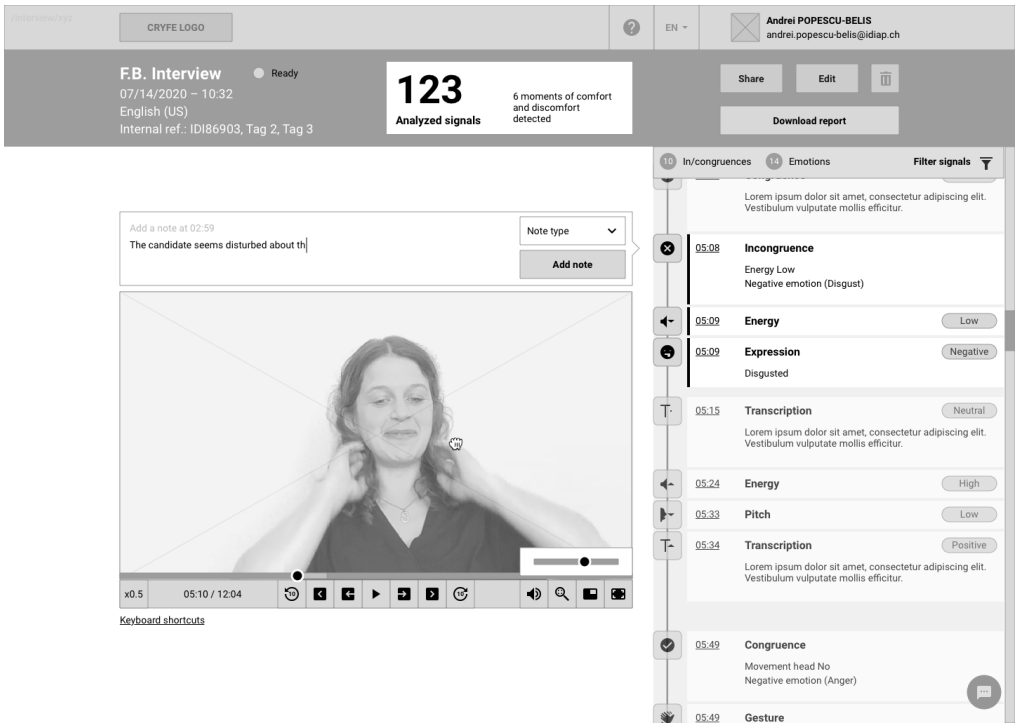


Ajout d'un nouvel entretien (Étape 2)
Upload de la vidéo d'entretien



Ajout d'un nouvel entretien (Étape 3)
Configuration de l'entretien et information sur l'entretien
Langue de l'entretien requis

Nom de l’entretien (apparaissant sur CRYFE™) optionnel
Date de l’entretien optionnelle
Références internes optionnelles (Champ libre permettant à l’utilisateur d’ajouter des labels à l’entretien)



Consultation de l’entretien
Après traitement par le système CRYFE™, l’utilisateur peut revisionner l’entretien et consulter les analyses du système

D’où proviennent les données ?

Source vidéo d’un entretien filmé et uploadé dans la solution par un utilisateur

Qui reçoit les données ?

Seul un utilisateur pourra disposer des entretiens vidéo et analyses associés à son compte pour le MVP. Par la suite, nous envisageons de permettre une gestion des comptes par plusieurs personnes pour une société (outil de gestion de projet avec attribution de comptes et partage des différents entretiens et analyses).

Dans quel but les données sont-elles communiquées ?

Elles sont communiquées à l’utilisateur dans le but de l’épauler à l’analyse comportementale de l’entretien qu’il a filmé et effectué avec son interlocuteur. Soit de revenir sur les points clés de l’entretien afin de comprendre la réalité de l’interlocuteur et éviter ainsi les biais cognitifs.

À terme, un accès pourra être proposé à la personne en entretien, interlocuteur, dans le cadre d’apprentissage sur elle-même. Exemple : lors d’un coaching en outplacement, le coach peut filmer son client et ensuite ils regardent la vidéo analysée par CRYFE™ ensemble.

Également, selon la politique / positionnement d’une société RH, l’entretien pourrait être revu avec le l’interlocuteur.

Quelles données sont communiquées ?

La vidéo et les analyses découlant de son traitement par le système (détection de signaux et indices comportementaux) sont communiquées à l'utilisateur.

La vidéo transmise à l'interlocuteur s'il fournit son adresse courrielle.

À quelle fréquence les données sont-elles communiquées ?

Dans le cas où la vidéo est uploadée (scénario actuel en temps différé), les données d'analyse sont communiquées après la finalisation du traitement par le système, une seule fois. Toutefois l'utilisateur peut revoir ces données durant la période fixée par le système CRYFE™ (12 mois)

À terme, dans le cas où l'entretien est filmé directement (scénario temps réel) les données d'analyses seront communiquées en direct ou avec un court temps de latence et une seule fois.

Toutefois l'utilisateur pourra décider, en informant son interlocuteur, de filmer l'entretien et également procéder à son analyse en temps différé.

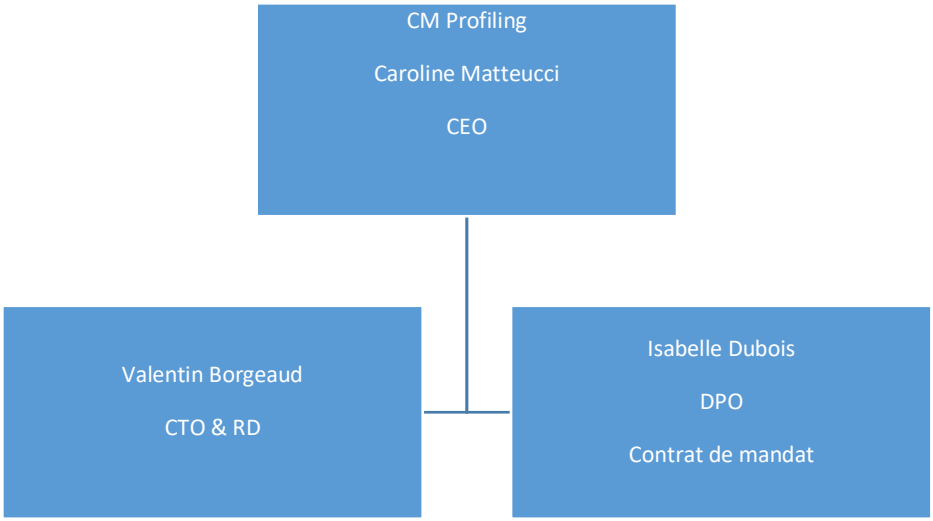
Qui initie la communication ?

L'utilisateur en créant un nouvel 'entretien' dans la solution CRYFE™.

Au moyen de quel support (média) les données sont-elles communiquées ?

Les données enregistrées lors de l'entretien peuvent l'être via tout support disposant d'une caméra et d'un microphone (se référer au setting). Elles sont communiquées via la plateforme web sécurisée.

10.Organigramme et Responsabilités



Sites internet :

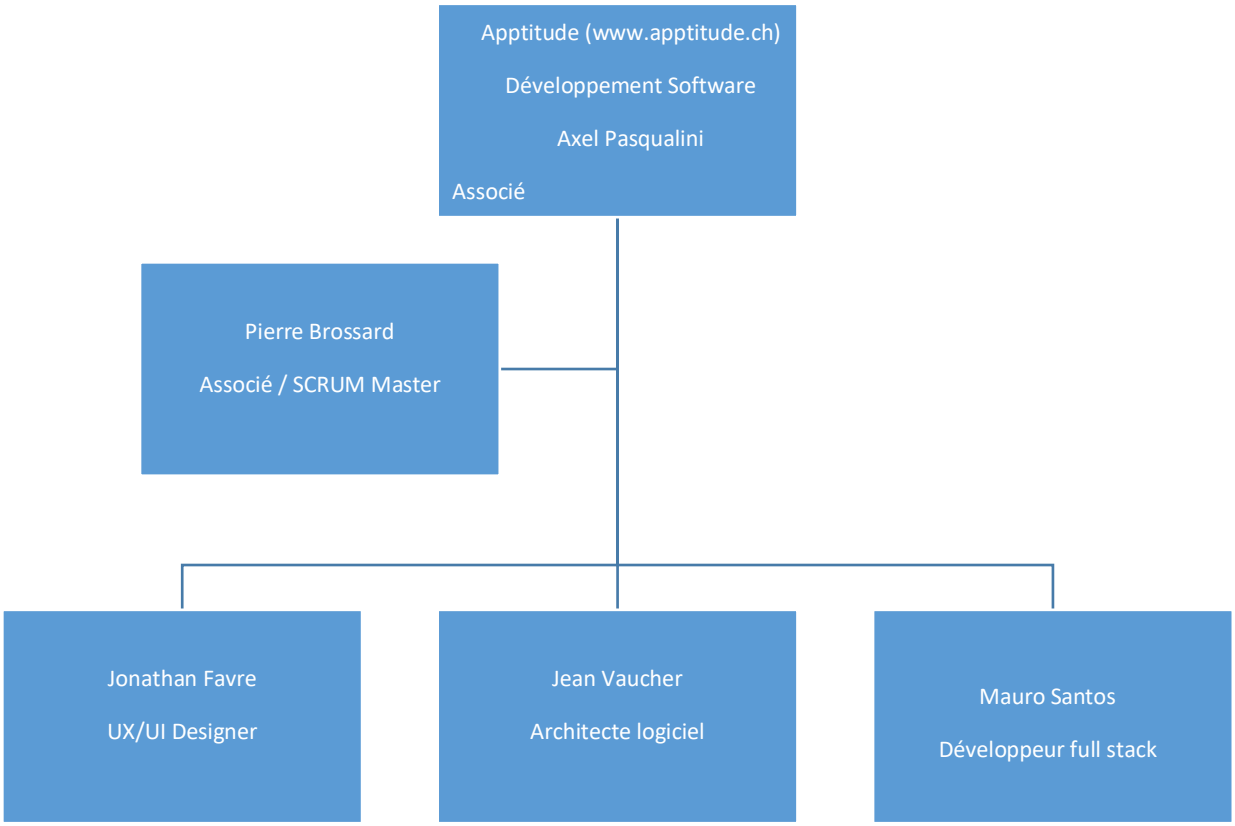
CM Profiling

Webmaster Gilles Scherlé www.impressions.name

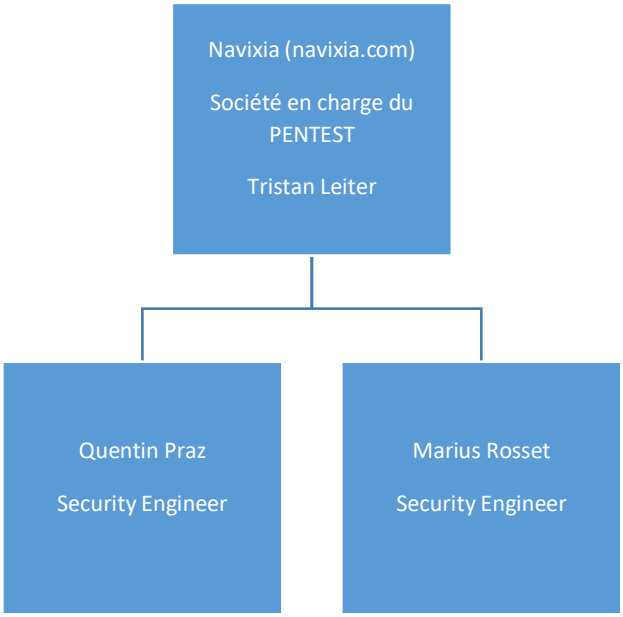
CRYFE™

Webmaster Lucas Georges & Jonathan Juste https://pixelpirate.fr/lab & https://www.behance.net/LucasGeorges

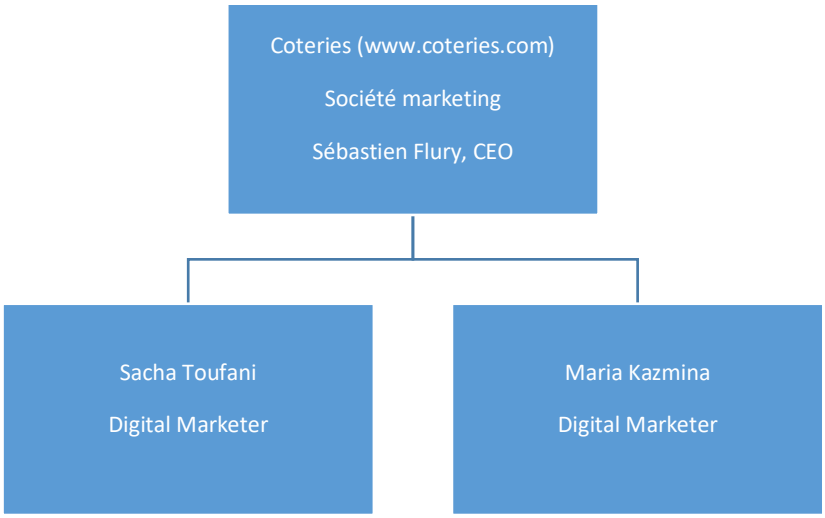
Développement de la plateforme :



Société en charge des PENTEST :



Société en charge du marketing



11. Dossier de la documentation de planification, réalisation et exploitation du fichier

Il est prévu que les vidéos et analyses d'un entretien soient effacées automatiquement de la plateforme après une durée donnée (12 mois).

Il est laissé au choix de l'utilisateur de pouvoir supprimer un entretien manuellement (vidéo et analyse) depuis la plateforme en ligne.

12. Déclaration du fichier au PFPDT : faite en septembre 2020, voir annexe à la fin du document

13. Processus

Le processus d'acquisition et traitement des données est celui développé au travers des écrans de la question 9 (Description des interfaces).

Une destruction des données (vidéo et analyses du système) de l'utilisateur est prévue automatiquement après une période donnée (12 mois). L'utilisateur peut également effectuer cette opération manuellement (supprimer un entretien) au sein de la plateforme pour un entretien donné (ce qui supprimera la vidéo et ses analyses).

14. Personne (s) responsable (s) de la protection et de la sécurité des données

Caroline Matteucci : CEO CM Profiling / CRYFE™

Isabelle Dubois, AD HOC RESOLUTION : DPO

Apptitude : développant la plateforme CRYFE™, Axel Pasqualini, associé & directeur

Navixia, société spécialisée en sécurité informatique, interviendra sur le projet concernant ses aspects de sécurité (mise en place de bonnes pratiques en termes de sécurité, pentest/audit de la solution développée). Tristan Leiter, responsable projet Cryfe™

15.La provenance des données

Elles proviennent de l'entretien entre un utilisateur et son interlocuteur filmé lors de celui-ci.

En temps différé : notre client (l'utilisateur) télécharge l'entretien qu'il a filmé sur la plateforme CRYFE™.

En temps réel : les données seront directement traitées par CRYFE™.

16.Les Buts dans lesquels les données sont régulièrement communiquées

Pour un utilisateur dans le but d'être soutenu et épaulé à l'analyse comportementale de son interlocuteur grâce à nos algorithmes (CRYFE™).

Nos clients disposeront également de support vidéo leur permettant d'apprendre la VIP©(validation des incongruences perçues) afin de revenir sur les incongruences analysées, en temps différé, lors du prochain entretien avec leur interlocuteur. Mais également de revenir directement sur les incongruences perçues lorsque CRYFE™ sera disponible en temps réel.

Dans le cas où l'accord est donné par un interlocuteur de « Partager son entretien et analyse à des fins d'amélioration du système » le but est pour CRYFE™ / la personne en charge des annotations (CM Profiling) de performer le système en annotant diverses vidéos d'entretien.

17.Procédures de contrôle et en particulier mesures techniques et organisationnelles visées à l'art. 20 OLPD

Gestion des droits d'accès

La gestion des droits d'accès est administrée par une personne de l'équipe CRYFE™ disposant d'un rôle administrateur (CEO, CTO). Les accès aux informations sont segmentés par utilisateur (client). Il n'aura accès qu'au contenu qu'il a lui-même uploadé. Les membres de l'équipe CRYFE™ disposant d'un rôle administrateur peuvent disposer d'un accès à l'ensemble des données recueillent sur la plateforme.

Cryptage

Les données sont cryptées de bout en bout via le protocole SSL (système de clés privé/public). Les données sont automatiquement chiffrées avant d'être écrites sur les disques du serveur où elles sont hébergées.

Résumé des éléments de sécurité et chiffrement de la solution de traitement/hébergement (Google Cloud Platform) :

- Google utilise plusieurs niveaux de chiffrement pour protéger les données client au repos dans les produits Google Cloud.
- Google Cloud chiffre automatiquement les contenus clients stockés au repos à l'aide d'une ou de plusieurs méthodes.
- Les données stockées sont divisées en fragments, et chacun d'entre eux est chiffré avec une clé de chiffrement unique. Les clés de chiffrement sont quant à elles stockées avec les données, et chiffrées (ou "encapsulées") à l'aide de clés de chiffrement de clés. Ces dernières sont stockées et utilisées

exclusivement dans le service de gestion des clés central de Google, qui est redondant et distribué à l'échelle mondiale.

- Toutes les données stockées dans Google Cloud Platform sont chiffrées au niveau de l'espace de stockage à l'aide de l'algorithme AES256, à l'exception d'un petit nombre de disques persistants créés avant 2015 qui utilisent l'algorithme AES128.
- Google utilise Tink, une bibliothèque de cryptographie commune qui inclut le module certifié FIPS 140-2 BoringCrypto, pour mettre en œuvre le chiffrement de manière cohérente dans presque tous les produits Google Cloud. L'utilisation systématique d'une bibliothèque commune signifie qu'une petite équipe de spécialistes du chiffrement peut assurer de manière adéquate la mise en œuvre et la gestion de ce code étroitement contrôlé et révisé.

Authentification

Dans le cadre du MVP, aucun système d'authentification **forte** n'est implémenté.

À terme ce type de système d'authentification multifacteurs (2FA) pourra être implémenté pour compléter la sécurité liée à l'accès de la plateforme en ligne.

18. Description des champs de données et des unités d'organisation qui y ont accès

Pour l'utilisateur :

- Informations personnelles liées au compte utilisateur
    - Adresse courrielle
    - Nom / Prénom
    - Informations de paiement et abonnement
        - Adresses de facturation
        - Type/Plan de souscription
- Voix (conversations lors de l'entretien)
- Image (potentiellement lors de l'entretien)

Pour l'interlocuteur :

- Voix (conversations lors de l'entretien)
- Image (postures et gestuelles lors de l'entretien)
- Adresse courrielle (saisi par le recruteur pour permettre de communiquer la vidéo brute – sans les analyses CRYFE™ – à l'interlocuteur)

À terme (pour les interlocuteurs) :

- Informations personnelles liées au compte utilisateur
    - Adresse courrielle
    - Nom / Prénom

19. Nature et étendue de l'accès des utilisateurs au fichier

La nature de l'accès aux fichiers (vidéos) et données est de type consultatif (l'utilisateur consulte ses propres entretiens et analyses proposées par le système par l'intermédiaire de la plateforme).
L'accès aux fichiers (vidéos) et données est limité à son utilisateur par un accès sécurisé à la plateforme.

20. Procédure de traitement des données, notamment les procédures de rectification, blocage, anonymisation (pseudonymisation), sauvegarde, conservation, archivage ou destruction des données

Il est prévu que les vidéos et analyses d'un entretien soient effacées automatiquement de la plateforme après une durée donnée (12 mois). Il est laissé au choix d'un utilisateur de pouvoir supprimer un entretien manuellement (vidéo et analyse) sur la plateforme.

Les vidéos sont sauvegardées durant une période donnée (12 mois) pour permettre :

- Leur traitement par le système
- Leur lecture avec les analyses découlant du traitement par l'utilisateur

Dans le cadre du MVP, la consultation des vidéos et de leurs analyses n'est accessible que pour un utilisateur donné (utilisateur ayant déposé la vidéo sur CRYFE™) et n'est pas partagée entre plusieurs utilisateurs.

Par la suite, il est possible que des comptes utilisateurs pour les sociétés soient créés. Un administrateur gérerait ainsi les utilisateurs de sa société et l'accès aux vidéos et analyse pourrait être partagé entre les utilisateurs. Dans ce cas, le présent règlement sera adapté.

Un utilisateur refusant les "Termes et conditions" exposés lors de sa première connexion sur la plateforme ne pourra pas accéder à l'outil et ne pourra donc pas bénéficier de ses services.

Il est envisagé que certaines vidéos puissent être utilisées par une personne de la société CM Profiling à des fins d'annotation (association manuelle de tels signaux à un moment T d'une vidéo) pour performer le système (amélioration des modèles de machine learning pour mieux détecter les signaux automatiquement par la suite). Dans l'optique de ce scénario, la solution prévoit que l'accord de « Partager sa vidéo et les analyses en découlant à des fins d'amélioration du système » soit donné explicitement par l'interlocuteur.

Un interlocuteur souhaitant que les données de son interview puissent être utilisées pour performer le système donnera son accord explicite lors de l'upload de la vidéo sur la plateforme (checkbox complémentaire lors de l'étape d'accord à l'ajout d'une vidéo).

L'usage prévu des vidéos est de pouvoir les annoter dans le but de 'Performer le système'. On entend par là l'utilisation d'un logiciel tiers (non-intégré à la plateforme en ligne CRYFE™) permettant d'ajouter manuellement des indications de comportement aux vidéos consenties (exemple : à un moment T de l'interview, on indique que le candidat hoche la tête horizontalement). Ces annotations servent à enrichir les données existantes (datasets) servant à rendre le système plus performant et précis dans ses analyses (trivialement pour reprendre l'exemple ci-dessus : plus le système disposera d'annotations manuelles précises sur un hochement de tête, plus il sera par la suite en mesure de les détecter automatiquement et avec précision sur une d'autres vidéos).

Seule une personne responsable de la société CM Profiling (CEO, CTO) pourra accéder à l'outil d'annotation et aux vidéos consenties à des fins d'annotation.

21.Configuration des moyens informatique

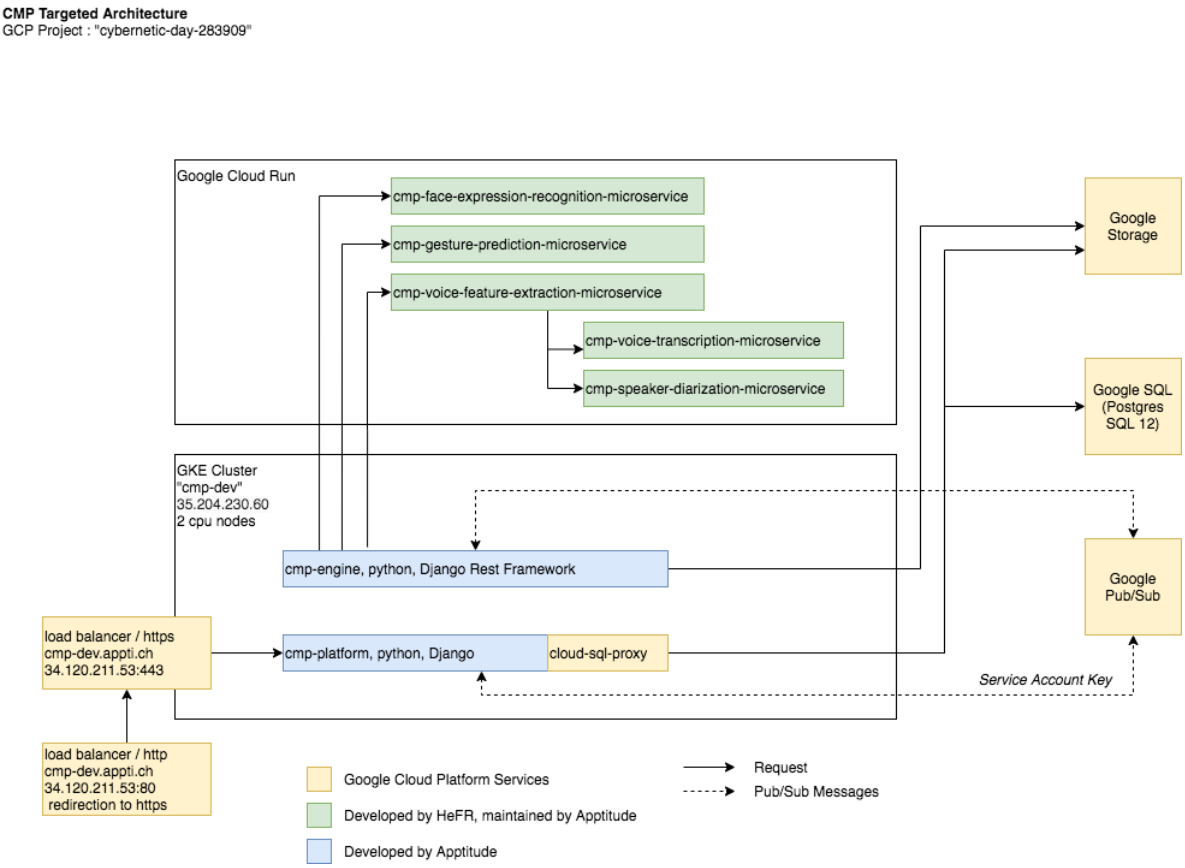


Schéma d'architecture de la plateforme CRYFE™

L'équipe technique de Cryfe™ a accès au backoffice et à la base de données du système. Des suppressions de données manuelles peuvent être prévues à la demande du candidat ou de l'utilisateur dans le cadre du MVP.

À terme et selon la croissance du système (nombre d'utilisateurs et de données traitées), des logiques de traitement automatisé et en lot pourront être implémentées pour répondre au besoin de suppression des données.

22.Procédure d'exercice du droit d'accès

L'utilisateur peut accéder aux fichiers (et analyses du système en découlant) directement sur la plateforme par l'intermédiaire de son compte. La finalité d'utilisation de ces données lui est exposée chaque fois à la création d'un "nouvel entretien" sur la plateforme (étape "interview agreement").

Il est prévu que les vidéos et analyses d'un entretien soient effacées automatiquement de la plateforme après une durée donnée (30 à 45 jours). Passée cette période les données sont donc détruites et ne sont plus accessibles pour l'utilisateur.

Une demande d'accès à ses données personnelles peut se faire par toute personne concernée auprès de la DPO, Isabelle Dubois, qui centralise les demandes et veille à leur suivi, par l'adresse courriel : dpo@cmprofiling.ch

Annexe :

Caroline Matteucci

CM Profiling Sàrl

Haldenweg 56

3074 Muri b. BERN

Préposé fédéral à la protection des données
et à la transparence
Feldeggweg 1
CH-3003 Berne

Berne, le 22 septembre 2020

Concerne : désignation d'un conseiller à la protection des données (DPO)

Monsieur le Préposé fédéral,

Notre société, inscrite au Registre du commerce, a pour but de fournir toutes prestations en matière de profiling (c'est-à-dire la lecture, l'analyse comportementale ainsi qu'établissement de profil de personnalité), notamment expertises, consulting, coaching, formations continues et spécialisées, création d'une académie, support psychologique, communication interpersonnelle, accompagnement de l'individu et des sociétés (instituts) dans les domaines du management, leadership, ressources humaines, assurances, juridiques, légal, médical, social (domaine du business) et du domaine politique, policier, sécurité, sûreté (domaine de la sécurité), ainsi que développement, réalisation, conception et vente de logiciels en relation avec le profiling.

Consciente des enjeux en matière de protection des données personnelles, notre société a désigné un Conseiller en protection des données personnelles en entreprise, en la personne de Madame Isabelle Dubois, AD HOC RESOLUTION, avenue du Général Guisan 46, 1800 VEVEY (contact : id@adhocresolution.ch) avec effet immédiat.

Nous vous remercions d'en prendre bonne note.

Veuillez recevoir, Monsieur le Préposé fédéral, nos salutations distinguées.

Pour CM Profiling Sàrl

Caroline Matteucci

Cc : Mme Isabelle Dubois