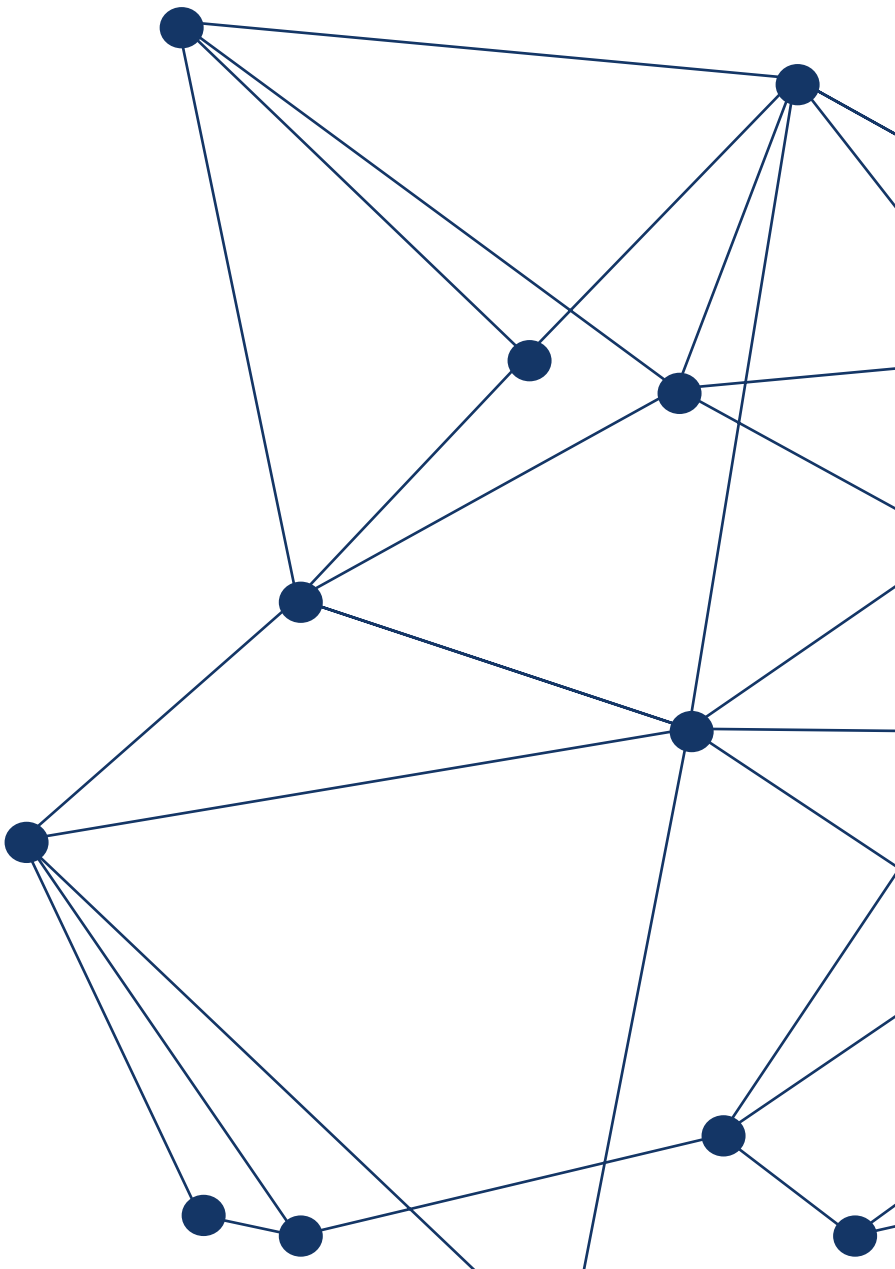
Le réseau éthique d'échange de données

Livre Blanc - VISIONS

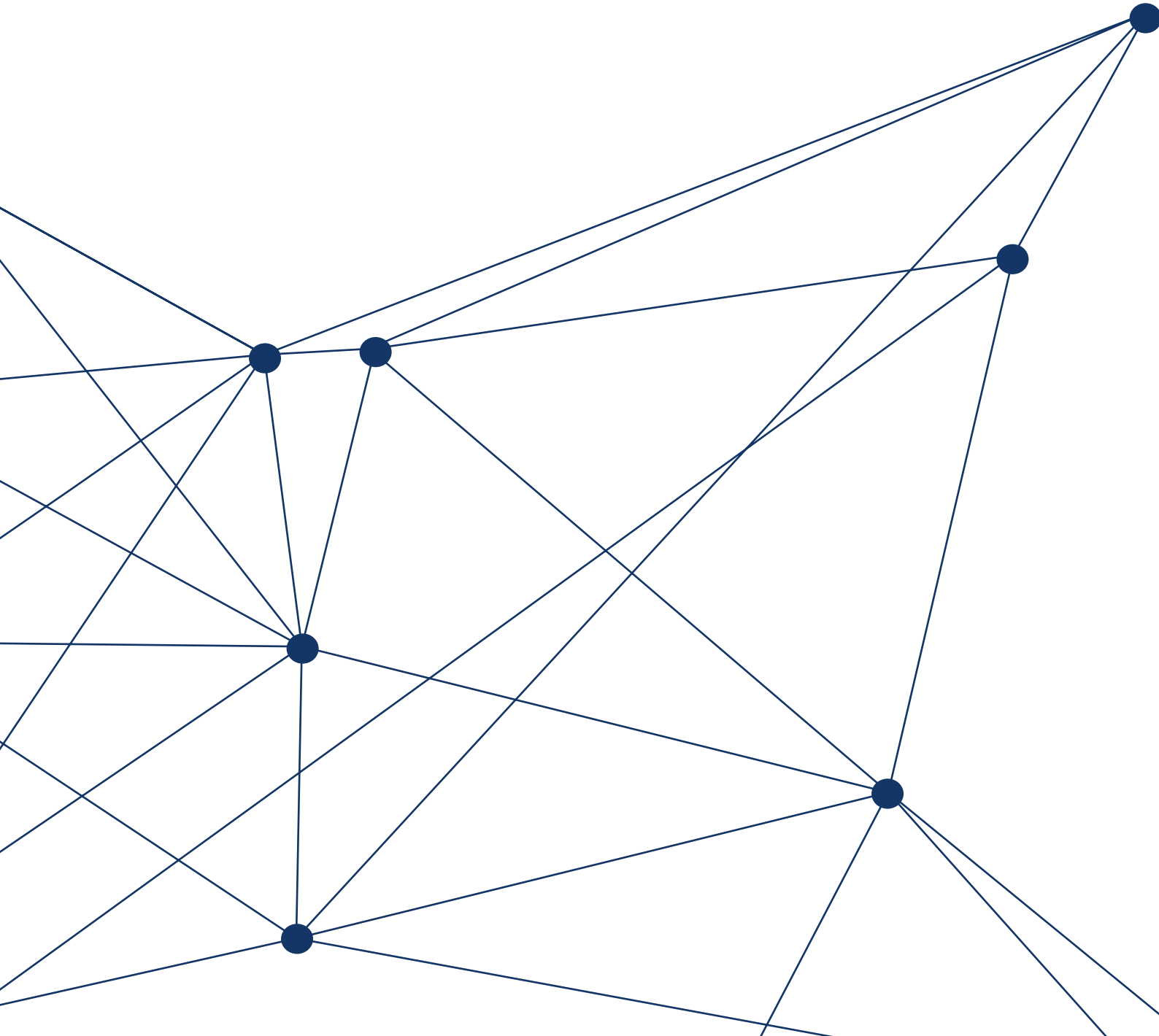


VISIONS

VISIONS : contrôler ses données, les récupérer, les partager et les échanger.

Pour cela nous devons assurer la protection de ces données, la garantie que les autorisations des utilisateurs soient respectées et la possibilité de les échanger facilement entre services.

Ce livre blanc détaille comment nous assurons cela au niveau technique.



1 Libérez leurs données, Respectez vos utilisateurs

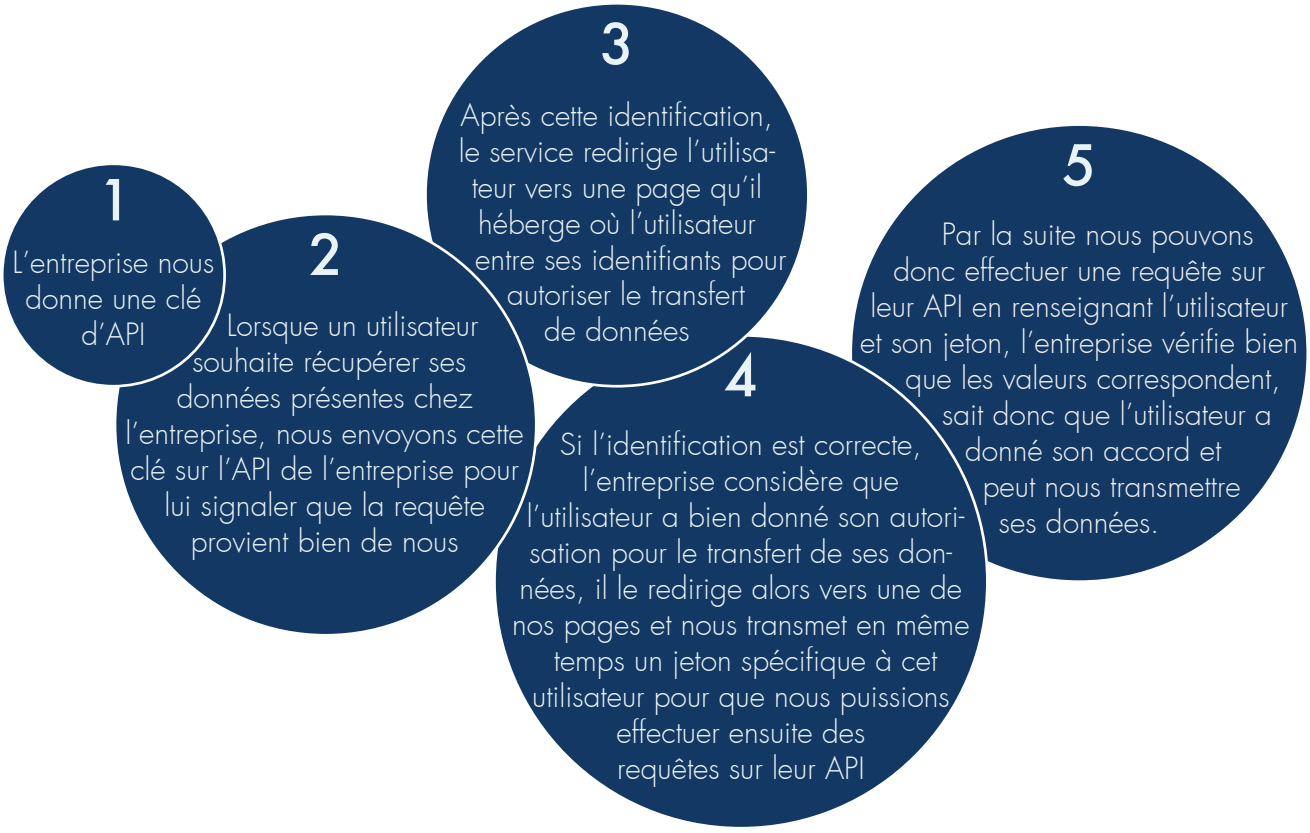
Les entreprises partenaires nous donnent un **accès sécurisé** à leur base de données. Elles nous informent des différentes catégories de données qu'elles renseignent sur leurs utilisateurs et autorisent nos serveurs à effectuer des **requêtes de lecture** de ces données au nom d'un utilisateur.

Chaque utilisateur peut ainsi récupérer et stocker ses données dans son compte VISIONS afin de pouvoir ensuite les contrôler et les échanger.

Cela suppose que le service ait construit **une API** ou un autre moyen pour permettre l'accès aux données. Nous suggérons de mettre en place un système simple qui permette de récupérer un **fichier JSON** sur un utilisateur en renseignant l'identifiant et le mot de passe, **VISIONS** se charge ensuite de séparer les catégories de données. Cela permet ainsi à l'entreprise de s'assurer que seuls ses utilisateurs identifiés puissent récupérer leurs données et elle reste maître de l'accès à sa base de données et des authentifications, par le paramétrage de son API.

Nous proposons également de sécuriser ces requêtes vers l'API de l'entreprise par **protocole OAuth 2**.

Voici comment se déroule ce protocole :



Une explication plus détaillée du protocole :
http://www.bubblecode.net/fr/2016/01/22/comprendre-oauth2/

Il existe de nombreuses librairies dans de nombreux langages pour implémenter facilement ce protocole : **https://oauth.net/code/**

Cette **API** servira dans un premier temps **à interagir avec le service VISIONS** mais sera également plus **largement bénéfique à l'entreprise** par la suite car elle facilitera son intégration par et dans d'autres services.
Ce moyen nécessite ainsi un **effort limité** de la part de l'entreprise partenaire et lui permet de **respecter simplement** et de façon automatique le droit à la portabilité des données et le droit d'accès instaurés par **le RGPD**.

Nous avons donc **un serveur** qui se charge de **traiter les demandes de récupération** des individus et d'interagir avec les systèmes des différents services, appelons-le **« serveur de gestion» (SG)**. Ce n'est pas ce serveur qui stocke les données.
Le **SG** se charge de récupérer les données, **il les chiffre en utilisant le protocole AES** (Advanced Encryption Standard) – 128 bit - qui est le protocole de **chiffrement symétrique le plus avancé**, utilisé par armées et banques. Il les envoie ensuite pour stockage à un autre serveur : **le serveur de stockage**.

Pour les fournisseurs de serveurs nous privilégions ceux qui garantissent des **protections physiques et biométiques** afin d'assurer une **haute protection du matériel.**

Nous installons sur ces serveurs des **pare-feux** et **systèmes de détection d'intrusion**. Seules des requêtes provenant de nos utilisateurs identifiés ou de services partenaires renseignés seront autorisées.

La connexion entre le navigateur de l'utilisateur et notre **SG** est **sécurisée par HTTPS**, seules des **informations peu sensibles circulent** ainsi : l'utilisateur a décidé d'accorder cette autorisation ou d'échanger cette donnée. Par exemple, une information ainsi passée serait : « Sarah accepte d'échanger son emploi avec Meetup ». Les données elles-même circulent entre les serveurs des partenaires et les nôtres, **les échanges sont authentifiés par Oauth** et **les données sont chiffrées par AES**.

Tous les procédés de chiffrement et déchiffrement se passent sur nos serveurs, ainsi les entreprises comme les usagers interagissent avec notre système sans jamais avoir accès à notre algorithme de chiffrement. **La connexion entre les services partenaires et notre SG est sécurisée et authentifiée par HTTPS et par le protocole Oauth2 pour les interactions avec notre API.**

Séparer ainsi le processus de récupération et de stockage correspond à **une stratégie de protection** qui fait qu'aucun élément extérieur à **VISIONS** n'interagit avec le serveur de stockage et que le serveur de stockage ne contient que **des données chiffrées et inexploitables sans contenir l'algorithme de déchiffrement**. Ainsi, si un des deux serveurs s'avère être corrompu, nous pouvons sécuriser et régler le problème sans qu'aucune donnée ne soit compromise.

Par ce système nous assurons que chacun puisse récupérer et stocker ses données sans les rendre plus vulnérables. En plus d'assurer la sécurité de leurs données, nous permettons **aux utilisateurs d'échanger leurs données** et **aux services de leur demander davantage de données**.

2 Demandez poliment, Tout le monde y gagne

Nous permettons aux utilisateurs d'également **autoriser l'accès à leurs données par d'autres services** et de **choisir l'utilisation qui en sera faite**.
Notamment, nous permettons de choisir si une donnée est utilisée pour la **personnalisation** du service, des **études statistiques** ou **marketing**, de la **recherche**, de la **revente** ou de la **publicité ciblée**.

Comment pouvons-nous à la fois permettre d'échanger ses données et garantir que les données échangées soient utilisées de la manière autorisée par l'utilisateur ?

Prenons un exemple :

Sarah a récupéré différentes données comme son emploi, sa formation, sa religion et son adresse dans un réseau social.
Un service de vente privée, appelons-le « Vente Privée », **souhaite utiliser son emploi et sa formation** pour lui faire de meilleures recommandations (personnalisation) et son adresse pour faire des statistiques sur ses utilisateurs et où ils se trouvent (marketing).
Vente Privée peut **directement demander ces données à ses utilisateurs** depuis notre interface qui lui indique quels types de données sont disponibles sur ses utilisateurs.
Une **notification est alors envoyée à Sarah**, si elle a choisit le traitement automatique (DataProfile) cela est fait automatiquement (voir plus bas).

Si **elle accepte**, c'est très simple.
Nous renseignons dans le profil de Sarah qu'elle a accordé à Vente Privée l'autorisation d'utiliser son emploi et sa formation pour personnaliser le service et son adresse pour faire des études statistiques. Ces informations sont stockées sur le **SG**.
Ces informations sont structurées de la sorte : Vente privée a un fichier avec tous ses utilisateurs, chaque utilisateur a **5 catégories** : Personnalisation/Marketing/Revente/Recherche/Publicité ; et dès que l'utilisation est accordée on renseigne la catégorie avec le type de donnée (ici « Emploi », « Formation » pour Personnalisation).

Les entreprises accèdent aux données **en envoyant des requêtes sur notre serveur** intermédiaire pour interagir avec notre **API**. Ce sont des requêtes POST qui contiennent :
1. l'**ID du service** auprès de nous
2. le **code secret du service** que nous lui avons fournit
3. l'**identifiant de l'utilisateur** dans ce service
4. le **type de donnée demandée**
5. le **type d'utilisation souhaitée**

Tout d'abord le **SG** vérifie que le service qui effectue la requête est bien celui qu'il indique être grâce à l'identifiant unique et au code secret que nous lui avons fournit lorsque nous avons paramétré son compte, paramètres qui sont passés dans chaque requête et renouvelés régulièrement (3 mois).

Ensuite, le **SG** vérifie si pour ce type de donnée de cet utilisateur, l'autorisation est renseignée.
Si oui, le **SG** récupère cette donnée dans le serveur de stockage, la déchiffre et l'envoie à Vente Privée pour qu'elle l'utilise.

Cela assure que la donnée est disponible à l'entreprise si et seulement si Sarah a autorisé l'utilisation, car si l'autorisation n'est pas renseignée dans le **SG**, la requête n'est jamais envoyée au serveur de stockage pour récupérer la donnée.

Nous **renseignons la mise ou la levée d'autorisation avec des dates précises** pour pouvoir fournir à l'entreprise les différentes **preuves que le consentement a bien été donné**.

Nous rendrons public le code qui traite les demandes des entreprises vis-à-vis des autorisations des utilisateurs.

Ce système permet aux entreprises de facilement demander aux utilisateurs davantage de données pour des utilisations précises et variées et de garantir que si une autorisation n'est pas donnée, le service n'a pas accès à la donnée.

Finalement l'entreprise accèdera aux données comme si elle utilisait une base de données sur le cloud. Les requêtes peuvent se faire directement par HTTP et **nous développons un SDK pour faciliter leur intégration**. L'authentification de l'entreprise auprès de notre serveur se fait par le protocole OAuth 2.

Les échanges de données sont donc entièrement décidés par l'utilisateur, authentifié avec son mot de passe. **Nous n'avons jamais accès aux mots de passe** car nous les conservons uniquement sous forme de hash et c'est cet hash qui est comparé pour assurer l'authentification.

Une limite pourrait être de dire : si un utilisateur autorise une donnée pour de la personnalisation mais pas pour de la publicité, pour y avoir accès l'entreprise n'a qu'à passer personnalisation au lieu de publicité dans la requête vers notre API et ainsi récupérer la donnée. En théorie c'est envisageable, en pratique c'est peu pratique car cela supposerait que l'entreprise ferait du cas par cas dans les requêtes alors que c'est un service automatique et identique pour tous les utilisateurs. Cela supposerait qu'en plus de connaître les autorisations de chacun pour chaque donnée (ce que seul VISIONS et l'utilisateur savent), l'entreprise fait tourner un code différent pour chaque utilisateur.
Même si l'entreprise parvient à automatiser et tester toutes les combinaisons possibles, nous le saurons car nous détecterons plusieurs requêtes pour un même utilisateur en quelques millisecondes. Nous pourrons alors désactiver le service si les explications ne sont pas satisfaisantes.
Cela fonctionne de la sorte : avant même qu'une requête ne soit traitée pour vérifier si l'autorisation de la part de l'utilisateur est donnée, nous enregistrons dans une base données le service, l'utilisateur et l'heure exacte.

Un programme tourne sur cette base de données pour signaler dès que plusieurs requêtes sont passées par un même service pour un même utilisateur à des intervalles rapprochés, si cela se répète régulièrement nous prenons les mesures nécessaires.

L'entreprise pourrait également théoriquement stocker dans une base de données propres toutes les données qu'elle récupère par VISIONS et ensuite en faire ce que bon lui semble. Mais cela aussi en pratique s'avère peu vraisemblable car, **par le RGPD**, toute utilisation autre que celle autorisée sera illégale et pourra être punie jusqu'à 20 millions d'euros ou 4% du C.A mondial de l'entreprise (en fonction de ce qui est plus élevé).

Pour les entreprises utilisant **des services tiers pour faire des études statistiques, marketing ou de la publicité**, elles peuvent **connecter ces services directement à la base de données VISIONS** prévue à cet effet.

C'est donc un moyen simple pour l'entreprise de s'assurer que toutes les données qu'elle utilise soient utilisées suite à l'accord de l'utilisateur. Et un moyen sûr pour l'utilisateur de faire confiance à l'entreprise et ainsi de lui transmettre davantage de données, sachant qu'il a contrôle sur ce qui en est fait et que ses données ne sont jamais stockées ailleurs que sur le serveur de stockage de VISIONS.

Cette solution permet aux entreprises de **facilement se conformer au RGPD** en utilisant **le consentement comme base légale de leurs traitements** et en pouvant facilement le prouver grâce à notre solution : nous mettons à disposition des entreprises partenaires **un registre qui détaille les consentements des utilisateurs** renseignés grâce à VISIONS.

Egalement cela permet aussi à l'entreprise de respecter le droit à la portabilité, le droit d'accès, le droit d'opposition et le droit d'information.

L'utilisateur n'est pas obligé de devoir autoriser le transfert à chaque demande : il peut constituer un **« DataProfile »** qui indique **ses préférences générales** et les demandes sont traitées en fonction de ce profile. Il peut toujours configurer des autorisations spécifiques à chaque service également.

3 Irréprochables jusqu'au bout, Créez le numérique éthique

Tout cela garantit les conditions des utilisateurs sur les données qu'ils échangent mais quid de leurs données déjà présentes dans les services et stockées sur des bases de données non contrôlées par VISIONS ?

Pour cela nous mettons en place **un programme d'autorisation dans le système des entreprises** qui vérifie avant chaque requête sur la base de donnée de l'entreprise si l'utilisateur a bien donné son autorisation.

Par exemple Vente Privée veut accéder à l'historique de navigation de Sarah pour lui faire de la publicité ciblée mais Sarah a indiqué dans VISIONS qu'elle ne veut pas que cette donnée soit utilisée à cette fin ; lorsque le code de Vente Privée s'exécute pour aller chercher dans sa base de données cette donnée, une condition est mise à l'exécution de ce code. Une requête est envoyée sur le SG avec pareillement le service, la donnée, le traitement et l'utilisateur, le SG vérifie dans le DataProfile de Sarah si ce traitement est autorisé et retourne « vrai » ou « faux ». Si c'est « vrai » la requête est autorisée, sinon non.

L'implémentation de cette solution ne **demande aucun effort de développement** de la part de l'entreprise : **VISIONS se charge d'analyser le code source** pour déterminer où placer son programme d'autorisation. Nous adaptons le programme au langage utilisé ainsi qu'aux différentes spécificités techniques de l'entreprise.

Nous sommes en train d'effectuer un partenariat de recherche avec JOLLYCLICK pour évaluer précisément comment cela va se mettre en place.

Ce fonctionnement permet à l'entreprise de **continuer à renseigner des données sur ses utilisateurs** comme dans toute autre base de données, tout en respectant tous les droits des utilisateurs et donc en étant constamment **conforme au RGPD**.

4 Une opportunité Pour tous

Cette solution est un avantage pour toutes les parties prenantes. L'intégration pour les entreprises demande un effort de développement mais il s'agit uniquement de **changer la connexion avec la base de données** et de **développer une API simple** de transmission des données. Ensuite pour respecter les droits, il suffit d'appeler l'API et nous permettre d'analyser le code pour implémenter notre programme d'autorisation.

Cet effort est bien moindre comparé à l'effort nécessaire pour se conformer au RGPD sans cette solution : l'entreprise devrait alors développer elle-même des systèmes d'autorisations et de leur gestion alors qu'ici c'est VISIONS qui s'en occupe. Développer une API ou un moyen d'accès aux données depuis l'extérieur sera également de toute façon obligatoire pour respecter le droit à la portabilité.

Egalement au-delà de la simple conformité à la loi, **cette solution présente l'avantage de gagner la confiance des utilisateurs en leur donnant ce contrôle et donc de pouvoir accéder à plus de données** car ils sont alors davantage prêts à les partager.

VISIONS se considère également comme un label : les entreprises partenaires se démarqueront par ce contrôle et leur gestion éthique des données, elles seront mises en avant et seront facilement reconnaissables.

Dans l'économie numérique, la confiance de ses utilisateurs passe par ce contrôle sur les données et la confiance est la ressource indispensable pour fidéliser une base et créer une relation saine et durable.

Pour les utilisateurs les bénéfices sont multiples. Ils prennent **contrôle de leur vie numérique** et **en sont acteurs** alors qu'avant toutes ces transactions étaient faites à leur insu. **Ils en tirent de la valeur car l'entreprise payera l'utilisateur pour avoir accès à ses données** mais également **ils peuvent utiliser leurs données pour soutenir les causes qui leur sont chères** : en reversant l'argent issu de l'échange aux associations partenaires mais aussi en transférant leurs données à ces associations qui peuvent les utiliser pour faire de meilleures études, prendre de meilleures actions et faire profiter ainsi toute la société de la valeur générée par l'exploitation des données personnelles.


VISIONS
DATA
PROFILE