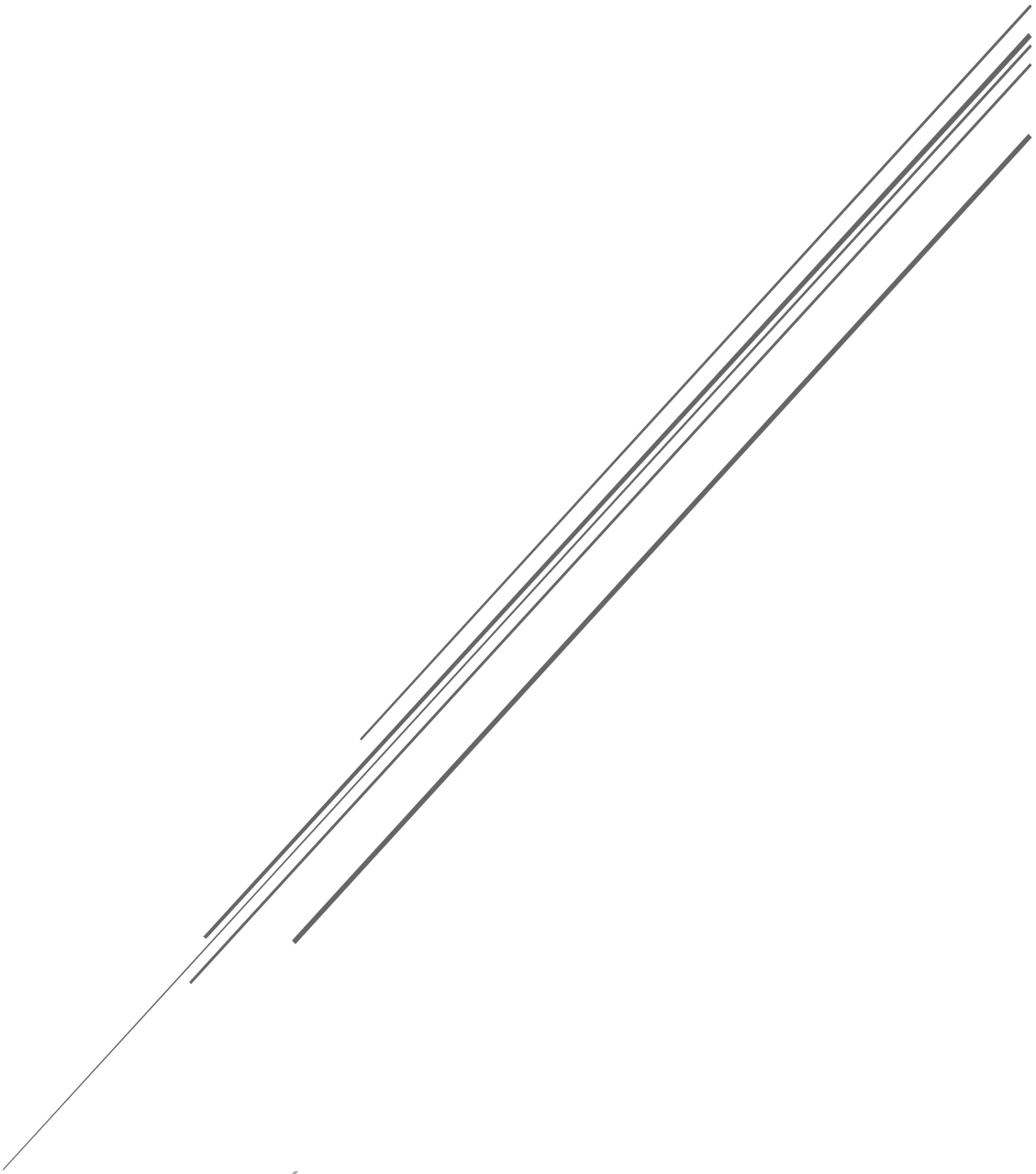
ÉTUDE D'IMPACT SUR LA VIE PRIVEE



Équipe 03 – On a pas de nom d'équipe
Nuit de l'info 2016

Contents

1 But de ce document

Le présent document a pour but de faire un état des lieux de l'impact de notre application sur la protection de la vie privée. Nous tentons ensuite d'identifier les risques pour finir par trouver des axes d'amélioration.

2 Définition des termes utilisés

Les définitions des termes suivant sont issues d'un document de la CNIL (Commission Nationale de l'Informatique et des Libertés). Le lien est donné est annexe.

Données à Caractère Personnel (DCP) : Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou tout autre personne.

Évènement redouté : Atteinte à la sécurité de DCP pouvant mener à des impacts sur la vie privée des personnes concernés.

Gravité : Estimation de l'ampleur des impacts potentiels sur la vie privée des personnes concernées. Elle dépend essentiellement du caractère préjudiciable des impacts potentiels.

Menace : Mode opératoire utilisé volontairement ou non par des sources de risques et pouvant provoquer un évènement redouté.

Risque : Scénario décrivant un évènement redouté et toutes les menaces qui le rendent possible. Il est estimé en termes de gravité et de vraisemblance.

Source de risque : Personne ou source non humaine qui peut être à l'origine d'un risque, de manière accidentelle ou délibérée.

Vraisemblance : Estimation de la possibilité qu'un risque se réalise. Elle dépend essentiellement des vulnérabilités exploitables et des capacités des sources de risques à les exploiter.

3 Présentation de notre application web

Le but de notre application web est d'apporter aux migrants arrivants en France un portail unique d'accès aux aides disponibles. Ces aides peuvent être de natures matérielle, par le don de nourriture ou l'hébergement par exemple, de nature médicale ou encore juridique par l'aide dans les démarches administratives. L'objectif est ici de simplifier pour les migrants l'accès aux ressources mises à leur disposition en les informant sur celles-ci et les redirigeant si besoin.

Notre solution se décompose en 3 parties distinctes :

- une partie accueil pour la recherche d'aide ;
- une partie pour que les acteurs de la solidarité puissent partager la mise à disposition de ressources ;
- une partie discussion pour que les migrants puissent échanger entre eux dans différents salons ;

Un bandeau est disponible sur toutes les pages pour que les administrateurs puissent faire passer des messages importants et ponctuels, comme l'annonce de mauvaises conditions météorologiques (locales ou nationales).

La page d'accueil permet ainsi à un migrant de trouver les aides disponibles près de lui s'il le souhaite en se focalisant sur un type en particulier (nourriture, logements, soins, aide juridique). Ces ressources s'affichent sur une carte selon un code couleur particulier.

La partie pour que les acteurs de la solidarité partagent leurs actions est accessible seulement aux utilisateurs disposant d'un compte. Sur cette partie ils peuvent partager des détails sur leur action. Ces détails sont ensuite consultable quand un utilisateur sélectionne l'action sur la carte.

La partie de discussion se regroupe en plusieurs salons. Ces salons sont :

- un salon de discussion générale
- un salon par type d'aide (nourriture, soins, logement, aides pour les démarches)
- un salon de discussion générale réservé aux utilisateurs disposant d'un compte.

3.1 Types d'utilisateurs

Il y a trois types d'utilisateurs de notre applications : les invités, les acteurs de la solidarité (abrégés AS dans la suite du document) et les administrateurs.

Les invités n'ont pas de compte et peuvent utiliser les services de notre site pour trouver des ressources, consulter les détails d'une mise à disposition de ressources et parler dans les salons de discussions.

Les AS peuvent faire la même chose que les invités mais ils peuvent également partager une mise à disposition de ressources et accéder à un salon réservés aux AS et aux administrateurs. Les AS utilisent un compte qui est obligatoirement créé par un administrateur.

Les administrateurs sont les gérants du site. Ils affichent les informations ponctuelles sur le bandeau et créent les comptes pour les autres administrateurs et les AS.

3.2 Niveaux de risques

Nous considérons qu'il existe pour les données 4 niveaux de risques différents : négligeable, limité, important et maximal. Chacun de ces niveaux est découpés en 2 parties, une pour la gravité de la menace et une pour sa vraisemblance.

4 Données conservées

DCP	Catégorie	Personnes pouvant y accéder	Durée de conservation
Position	Donnée de localisation	Administrateurs	Conservé en mémoire durant la session de l'utilisateur puis perdue.
Nom et prénom	État civil	Administrateurs	Conservé dans la base de données tant que le compte existe.

4.1 Utilisateurs invités

Dans le cas des invités, il n'y a qu'une seule DCP utilisée dans notre application. Il s'agit de la position de l'utilisateur. En effet, cette position est utilisée pour chercher les ressources mises à disposition dans une zone autour de cette position. Cette DCP est conservée en mémoire par l'application et est propre à la session. Elle disparaît donc de notre application en cas de fermeture de l'onglet ou de rafraîchissement de la page.

Attention : bien que notre application ne conserve pas cette DCP sur le long terme, nous utilisons l'API Google pour notre carte. De ce fait, nous ne sommes pas en mesure de garantir que Google ne conserve pas cette information.

4.2 Utilisateurs AS

Chaque AS est utilisateur qui a créé un compte. De ce fait, nous conservons un nom d'utilisateur qui est composé de leur nom et de leur prénom séparé par un espace. Cet identifiant est utilisé pour les connexions suivantes et en tant que nom dans les salons de discussion.

4.3 Utilisateurs administrateurs

Nous gardons les mêmes informations pour les administrateurs que pour les AS.

5 Étude des mesures

Avec l'aide des outils mis à notre disposition par la CNIL, nous déterminons pour chacune des parties ci-dessous les points critiques et les mesures que nous prenons pour chacun d'entre eux.

5.1 Mesures de nature juridique

Point de contrôle	**Mesure et justifications**
Finalité : finalité déterminée, explicite et légitime	Nous utilisons la position pour afficher des résultats spécifiquement liés à leur position géographique parce que les migrants ne peuvent pas beaucoup se déplacer pour aller chercher des ressources. En ce qui concerne le nom et le prénom, nous nous en servons afin que les migrants aient un interlocuteur bien défini lors de leurs échanges sur les salons de discussions ou dans le partage de la mise à disposition de ressources.
Minimisation : réduction des données à celles strictement nécessaires	Nous n'utilisons que les données strictement nécessaires au fonctionnement du service.
Qualité : préservation de la qualité des DCP	La position est stockée en mémoire dans une variable locale au navigateur, et donc non modifiable par un navigateur non malveillant.
Durée de conservation : durée nécessaires à l'accomplissement des finalités, à défaut d'une autre obligation légale imposant une conservation plus longue	La position est conservée durant le temps de la session, donc jusqu'à ce que la page soit rafraîchie ou fermée. Le nom et le prénom des AS et des administrateurs sont conservés tant que les comptes associés existent.

Information : respect du droit à l'information des personnes concernées	Lors de la création d'un compte utilisateur, la personne associée à ce compte est informée par un moyen n'appartenant pas obligatoirement à l'application. Dans le cas où la demande de création a eût lieu par mail, les administrateurs informent la personne concernée en répondant à ce mail. Dans le cas où l'utilisateur à fait la demande par un autre moyen, nous supposons que les administrateurs utilisent un moyen approprié pour informer les personnes concernées.
Consentement : obtention du consentement des personnes concernées ou existence d'un autre fondement légal justifiant le traitement	En ce qui concerne la position, nous considérons que le navigateur demande ou a demandé le consentement de l'utilisateur. Pour ce qui touche à l'utilisation du nom et du prénom d'un AS ou d'un administrateur en tant que nom d'utilisateur, nous considérons que la création n'a lieu qu'en réponse à une demande par la personne concernée ou un tiers ayant son accord de la création d'un compte.
Droit d'opposition : respect du droit d'opposition des personnes concernées	De par l'acceptation des conditions de service, un utilisateur admet que nous pouvons utiliser sa position pour lui fournir un service (ici les ressources à sa disposition près de lui). En ce qui touche le nom et le prénom, un utilisateur peut faire opposition en envoyer un mail à l'adresse mail de contact de l'application. Dans ce cas, l'utilisateur accepte que le compte associé à ces nom et prénom soit détruit.
Droit d'accès : respect du droit des personnes concernées à accéder à leurs données	Un utilisateur ne peut pas accéder à sa position, tout comme nous ne pouvons pas y accéder. La donnée étant conservée en mémoire dans une variable, et ayant une durée de vie liée à celle de la session, nous ne pouvons pas nous en servir en dehors de la fourniture du service en question. Cela ne couvre pas les usages que Google pourrait faire de cette position. Pour les noms et prénoms, un utilisateur authentifié accède à ces données à chacune de ses actions sur le site puisqu'il s'agit de son nom d'utilisateur.

Droits de rectification : respect du droit des personnes concernées de corriger leurs données et de les effacer.	Parce que nous utilisons la position que nous fournit le navigateur, un utilisateur peut théoriquement utiliser des outils pour modifier cette position. En revanche, ni lui ni aucune autre personne ne peut altérer sa position une fois que notre application l'a récupérée. Les noms et prénoms peuvent être modifiés par les administrateurs. Pour cela, il suffit que l'utilisateur en question envoie un mail à l'adresse mail de contact en détaillant sa demande.
Transferts : respect des obligations en matière de transfert de données en dehors de l'Union Européenne	Les noms et prénoms de nos utilisateurs inscrits sont stockés en France et n'en sortiront pas. En revanche, en ce qui concerne la position, nous ne pouvons pas garantir l'endroit où les données vont aller. Nous effectuons un appel à une API de Google sans pouvoir garantir la destination effective de cet appel. Nous nous basons sur le fait que Google respecte les accords de transferts de données vers l'extérieur de l'Europe.

5.2 Mesures destinées à traiter les risques

Thème	**Point de contrôle**	**Mesures et justifications**
Mesures organisationnelles	Gestion des incidents et des violations de données	Une fois une altération des données détectée, nous utilisons une sauvegarde antérieure pour rétablir les données dans leur dernier état correct.
	Relation avec les tiers	Elles se résument à la communication de la position de l'utilisateur à l'API de Google. Le nom et le prénom de l'utilisateur ne sont jamais communiqués à des tiers.

Mesures de sécurité logique	Anonymisation	La position n'est pas associée à une information permettant d'identifier clairement une personne particulière. En revanche, nous ne pouvons pas anonymiser les couples noms-prénoms sans aller contre le concept d'identification claire des interlocuteurs.
	Chiffrement	La position n'est pas accessible de l'extérieur puisqu'il s'agit d'une variable locale. Les noms et prénoms des utilisateurs ne sont pas chiffrés puisqu'ils sont déjà visibles en tant que noms d'utilisateurs.
	Contrôle d'accès logique	Les noms et prénoms, tout comme les mots de passe, sont stockés dans une base de données dont l'accès n'est disponible que depuis la machine sur laquelle elle est stockée et avec une demande de mot de passe.
Mesures de sécurité physique	Éloignement des sources de risques (produits dangereux, zones géographiques dangereuses …)	La salle serveur est située dans une grande ville. Celle-ci se situe dans le Sud-Ouest de la France, loin des zones géographiques dangereuses, que le danger soit humain ou naturel.

	Sécurité des matériels	Le serveur contenant les DCP sont placés dans une salle fermée à clé. Seule la personne en charge de le maintenir dispose de cette clé.

6 L'étude des risques

6.1 Les sources de risques

Type de source de risques	Sources de risque pertinentes
Sources humaines internes agissant accidentellement	Administrateurs
Sources humaines internes agissant de manière délibérée	Administrateurs
Sources humaines externes agissant accidentellement	Concurrents, organisations sous le contrôle d'un État étranger
Sources humaines externes agissant de manière délibérée	Concurrents, organisations sous le contrôle d'un État étranger
Sources non humaines interne	Aucune
Sources non humaines externes	Aucune

6.2 Les évènements redoutés

Violations potentielles	Impacts potentiels	Gravité	Vraisemblance	Justification
Modification non désirée des DCP	Perte d'accès sur certains comptes ; Perturbation du service ;	Négligeable	Limité	Seule une perte de temps est engendrée et l'exploitation est difficile
Disparition des DCP	Perturbation du service ; Perte d'un compte ;	Négligeable	Limité	Seule une perte de temps est engendrée et l'exploitation est difficile

Il est à noter que les personnes externes à l'organisation nommées dans les sources humaines externes de risque peuvent effectuer les mêmes actions que les administrateurs suscités. La différence est que ces personnes doivent tout d'abord entrer dans la base et donc augmenter leurs privilèges au même niveau que les administrateurs.

6.3 Évaluation des risques

Dans les deux cas, la gravité des impacts est considérée comme négligeable, étant donné que les impacts sont une simple perte de temps, les utilisateurs devant effectuer les démarches une fois de plus. En ce qui concerne la vraisemblance des menaces, nous pensons que le niveau est limité. En effet, il nous semble difficile pour les sources de risque de mettre en pratiques de telles actions, d'une part parce que la sécurité de l'application par rapport aux menaces extérieures semble correcte. D'autre part parce que nous ne pensons pas plausible que les administrateurs en arrivent à faire de telles actions.
Nous considérons dès lors que le niveau de risque est limité.

7 Conclusion

Au vue de l'analyse présentée, nous pouvons dire que notre application présente une bonne approche quant à la quantité de données récoltée et à leur utilisation. En revanche, nous pouvons notre que des améliorations pourraient être apportées au stockage de ces données ainsi qu'aux processus de gestion des risques. Un des axes d'amélioration pourrait être de définir plus précisément une politique de gestion des risques, des projets et du personnel en y définissant plus précisément des processus

8 Annexe :

8.1 Bibliographie :

Document de la CNIL sur la vie privée