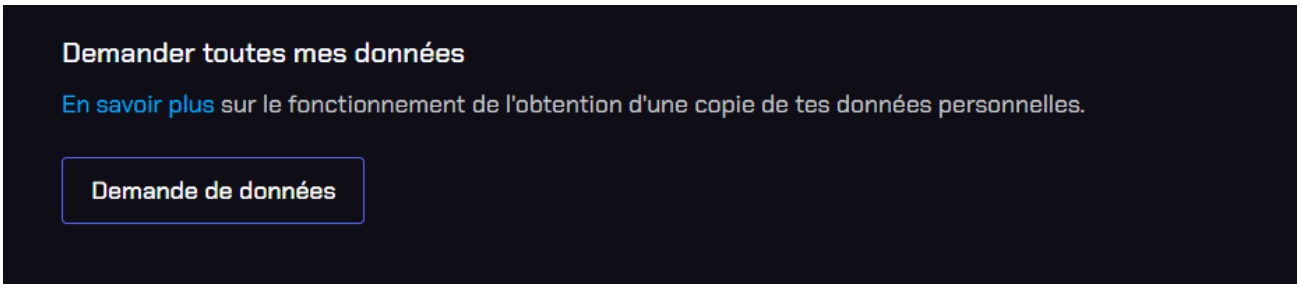
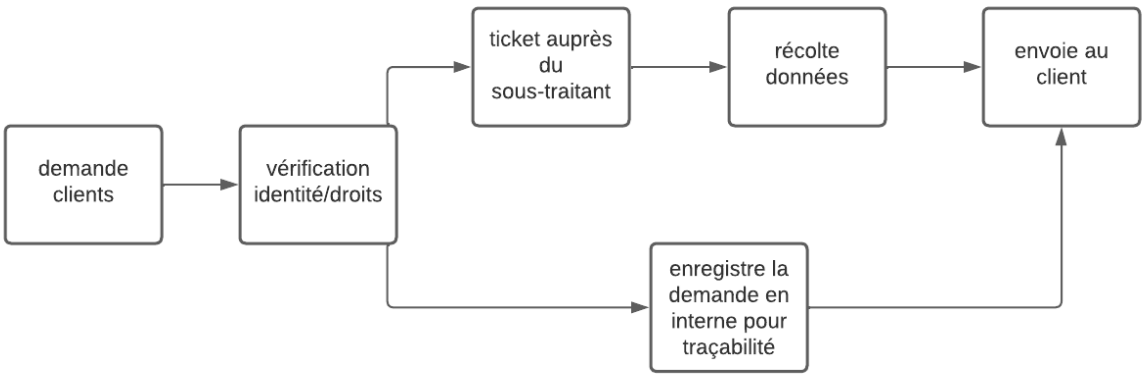
Etape 1: Les éléments considéré comme étant des DCP dans le fichier `customer_data.csv` sont les suivants :

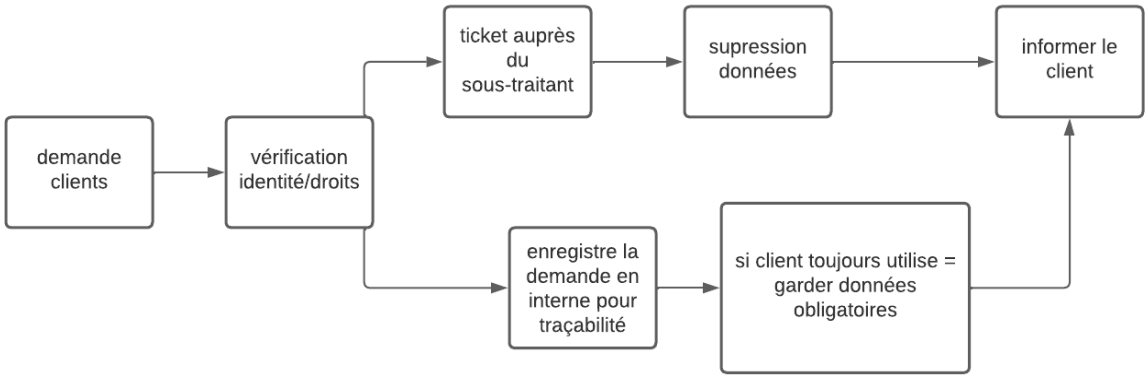
- Prénom
- Nom
- E-mail
- Adresse postale.
- En nous appuyant sur la législation RGPD à l'égard des données à caractères personnels. Comme mentionné dans ce site : "D'un côté, la donnée à caractère personnel correspond à toute information relative à une personne physique susceptible d'être identifiée, directement ou indirectement. Dans ce cadre, n'importe quel nom, prénom, photographie, empreinte, courriel, adresse postale, numéro de téléphone, matricule interne, numéro de sécurité sociale, adresse IP, identifiant de connexion informatique, enregistrement vocal sont des données à caractère personnel." (loi n°78-17 du Réglement Général sur la Protection des Données) Etape 2: 1- Afin de permettre aux clients de consulter leurs données à caractères personnels, nous pouvons mettre en place un bouton visible uniquement sur leur page "confidentialité et sécurité" après la connexion à leur compte permettant d'accéder et modifier ses données si besoin. Ces données seront chiffrés dans un zip avec un mot de passe prédéfini par l'utilisateur ce qui évitera d'avoir des données sensibles en clair avant afin de le recevoir sur son mail de connexion. Ci joint l'exemple de discord :



2-



3-



Etape 3:
1- Énumérez cinq questions à poser au fournisseur de services cloud pour s'assurer qu'il est en conformité avec le RGPD.

1. Ou stockez-vous physiquement les données ?
2. Comment gérez-vous le traitement des données personnelles ?
3. Quelles sont les mesures de sécurités mises en place par votre entreprise ?
4. Avez-vous une politique de conservation des données ?
5. Garantissez-vous la transparence et le consentement sur le traitement des données ?

2- Conformité au RGPD (Règlement général sur la protection des données) Responsabilités du Sous-Traitant : Le Sous-Traitant s'engage à respecter toutes les obligations imposées par le Règlement général sur la protection des données (RGPD) de l'Union européenne dans le cadre du traitement des données personnelles au nom du Responsable de traitement. Le Sous-Traitant garantit la mise en place de mesures techniques et organisationnelles appropriées pour assurer la sécurité, la confidentialité et l'intégrité des données personnelles conformément aux articles pertinents du RGPD. Traitement des Données : Le Sous-Traitant traitera les données personnelles uniquement conformément aux instructions documentées du Responsable de traitement, en garantissant que toute personne autorisée à traiter les données personnelles est soumise à des obligations de confidentialité appropriées. Assistance au Responsable de traitement : Le Sous-Traitant s'engage à fournir au Responsable de traitement l'assistance nécessaire pour répondre aux demandes d'exercice des droits des personnes concernées, à notifier les violations de données personnelles conformément aux obligations du RGPD, et à coopérer de manière transparente lors d'audits ou d'inspections par les autorités de contrôle. Transfert de Données Transfrontalier : Si le traitement des données personnelles implique le transfert de données en dehors de l'Union européenne, le Sous-Traitant s'engage à respecter les exigences du RGPD en matière de transfert de données internationales et à mettre en place des mécanismes de transfert appropriés. Durée de Conservation des Données : Le Sous-Traitant s'engage à ne conserver les données personnelles que pendant la durée

nécessaire à l'accomplissement des finalités du traitement, conformément aux obligations de conservation prévues par le RGPD. Audit et Inspection : Le Responsable de traitement se réserve le droit d'effectuer des audits ou des inspections pour s'assurer que le Sous-Traitant respecte ses obligations en vertu du RGPD. Ces audits ou inspections seront menés avec un préavis raisonnable et seront conformes aux lois et réglementations applicables. En signant ce contrat, les deux parties reconnaissent leur engagement envers la conformité au RGPD et acceptent de coopérer pleinement pour assurer la protection des données personnelles conformément aux exigences légales en vigueur.

Etape 4: Pia (privacy Impact Assessment) 1- afin d'évaluer trois potentiel risques lié a la protection des données chez TechSavvy nous avons choisis de présenter les suivant, tous d'abord si jamais le sous traitant sois a l'origine d'une panne/erreur et renvoie la demande entière du client sous forme de requête slq qui pourrait permettre a des users mal intentionnés d'accéder au donnée d'autres user. Ensuite le cas d'une mauvaise traçabitilité, qui pourrait entrainer des données perdu ou entre de mauvaise main + des demande qui ne seront pas traité. Enfin si la gestion des droits est mal faites ou défaillante certaine demande pourrait être exécuter alors que les users n'ont pas les droits. 2- augmenter les étapes avant exécutions d'une demande de traitement de données afin de s'assurer que les personnes étant à l'origine de la demande sont bien légitime. Si il y'a une faille lors du process il doit y avoir des services ayant la possibilité de tracé les donnée pour savoir jusqu'ou la fuite s'étant et de pouvoir limiter la casse. Il faut proprement désigner qui est le propriétaire des données à protéger et leur niveau de sensibilité. Mettre en place des politiques de sécurités. évaluer notre exposition sur internet. Pour se qui concerne les mesures opérationnelles, nous pourrions réduire les droits d'accès des users classique. Pouvoir déployer un système correctifs de sécurité. Obligé les utilisateurs à opter pour des mots de passes sécurisé. Authentification à plusieurs facteurs. Effectuer régulièrement des pentest et des audits de sécu. Faire des campagnes de sensibilisations au sein de l'entreprise. 3- Pour la procédure a suivre en cas de fuite de données à caractère sensible, nous avons fait plusieurs recherche sur internet afin de cerner au mieux le sujet. La plupart des sources estime que la premiere étape lorsqu'il y a une fuite de données est, pour la partie entreprise victime/ responsable de la fuite, de réaliser une estimation des dégats en se basant sur plusieurs critères. Tous d'abords recontextualiser la fuite de données, ensuite essayer d'estimer la quantité de données qui ont fuitée et enfin de calculer les potentielles conséquences/ préjudices pourrait être causé suite à la fuite de données. Après les estimations, il faut désormais notifier les autorités ainsi que les utilisateurs de la fuite. L'entreprise victime de la fuite a 72h pour notifier les autorités et si l'entreprise dépasse se délai, ils devront justifié le dépassement. Si le retard n'est pas justifié, des sanctions peuvent être appliqué. Ensuite, l'entreprise doit travailler avec les autorités pour prendre les mesures nécessaires. Si jamais les données qui ont fuitée sont dangereuse pour les personnes touchées elles doivent être informées au plus vite suivant l'incident.

(voir PIA en pj sous format de fichier .json)

Étape 5 :

1. 2. Les trois types de cookies utilisés par TechSavvy sont :

- Les cookies de performances : ils doivent être acceptés par l'utilisateur afin d'être en règle avec le RGPD. Ils permettent de faire des statistiques de visites par page et interactions. Dans ce cas, nous n'avons pas l'information si ils sont uniquement des cookies liés au site ou si ils sont partagés avec des tiers, si le cas est vérifié, il est non-conforme suite à l'article 82 du RGPD.
- Les cookies de sécurité : également en règle avec le RGPD, ils permettent de sécuriser le site internet (comme par exemple le cookie X-XSS-PROTECTION), ils n'ont donc aucune information sur l'utilisateur.
- Les cookies de personnalisations : ils doivent être acceptés par l'utilisateur afin d'être conforme au RGPD. Ils permettent de savoir les préférences de l'utilisateur sur la navigation du site.

Actuellement, la politique de cookie n'est pas conforme au RPGD puisqu'il est difficile de les refuser. Cette politique explique qu'il est possible de les refuser par le navigateur, mais aucun bouton ou formulaire n'est proposé à la venue de ce site. Ceci est une violation des articles articles 4(11) et 7 du RGPD qui stipulent que l'utilisateur doit être en mesure de le retirer, à tout moment, avec la même simplicité qu'il l'a accordé. (modifié)
Gestion des cookies

1. 2. Les trois types de cookies utilisés par TechSavvy sont :
   - Les cookies de performances : ils doivent être acceptés par l'utilisateur afin d'être en règle avec le RGPD. Ils permettent de faire des statistiques de visites par page et interactions. Dans ce cas, nous n'avons pas l'information si ils sont uniquement des cookies liés au site ou si ils sont partagés avec des tiers, si le cas est vérifié, il est non-conforme suite à l'article 82 du RGPD.
   - Les cookies de sécurité : également en règle avec le RGPD, ils permettent de sécuriser le site internet (comme par exemple le cookie X-XSS-PROTECTION), ils n'ont donc aucune information sur l'utilisateur.
   - Les cookies de personnalisations : ils doivent être acceptés par l'utilisateur afin d'être conforme au RGPD. Ils permettent de savoir les préférences de l'utilisateur sur la navigation du site.

   Actuellement, la politique de cookie n'est pas conforme au RPGD puisqu'il est difficile de les refuser. Cette politique explique qu'il est possible de les refuser par le navigateur, mais aucun bouton ou formulaire n'est proposé à la venue de ce site. Ceci est une violation des articles articles 4(11) et 7 du RGPD qui stipulent que l'utilisateur doit être en mesure de le retirer, à tout moment, avec la même simplicité qu'il l'a accordé.

2. Afin de rendre la politique de cookie de TechSavvy conforme à la réglementation RPGD, nous pouvons modifier la section "Consentement" en expliquant qu'ils peuvent répondre au formulaire à la visite du site en n'utilisant que les cookies uniquement nécessaires au fonctionnement du site (cookies de sécurité). Nous devons aussi modifier qu'est ce que sont les cookies de performances car nous n'avons aucune information si ce sont des cookies tiers ou non.