

**4 Décembre 2024**

|  |
| --- |
| Université Savoie Mont Blanc |
| Rapport de droit |
|  |

|  |
| --- |
|  |

**Année Universitaire 2024 – 2025**

**Réalisé Par :**

* AMARAL Nathan
* BEKHOUCHE Mohamed Amir
* CETINKAYA Melih
* MASHOVETS Nazar
* TINASTEPE FEYZA

**Encadré Par :**

* M Y. GAILLARD



*D*

*ans le cadre de cette SAE S3.01, notre groupe s’est penché sur l’étude et la mise en œuvre des mesures nécessaires pour assurer la conformité juridique et technique d’un site internet. Ce projet nous a permis de comprendre les implications du RGPD, d’explorer les solutions techniques disponibles pour renforcer la sécurité des données et de proposer des outils adaptés pour répondre aux attentes réglementaires et aux exigences des utilisateurs.*

**SOMMAIRE**

[1 - La réglementation relative aux cookies 3](#_Toc183697292)

[1.1. Les bandeaux cookies d’Uber non-conformes : 3](#_Toc183697293)

[1.2. Nos bandeaux cookies conformes : 4](#_Toc183697294)

[2 - Politique de protection des données personnelles 6](#_Toc183697295)

[2.1 Introduction 6](#_Toc183697296)

[2.2 Données personnelles 6](#_Toc183697297)

[2.3 Les données transmises directement 6](#_Toc183697298)

[2.4 Les données collectées automatiquement 6](#_Toc183697299)

[2.5 Base légale 7](#_Toc183697300)

[2.6 Durée de conservation 7](#_Toc183697301)

[2.7 Cookies 7](#_Toc183697302)

[2.8 DPO (Délégué à la Protection des Données) 7](#_Toc183697303)

[2.9 Contact délégué à la protection des données 8](#_Toc183697304)

[2.10 Analyse d’Impact relative à la Protection des Données (AIPD) 8](#_Toc183697305)

[3 - Excel 10](#_Toc183697306)

[3.1 Registre de traitement de gestion de la paie 10](#_Toc183697307)

[3.2 Registre de traitement de commande client 11](#_Toc183697308)

[3.3 Registre de traitement de course client 12](#_Toc183697309)

[4 - Note Explicative 13](#_Toc183697310)

# La réglementation relative aux cookies

## Les bandeaux cookies d’Uber non-conformes :



**NON-CONFORME**

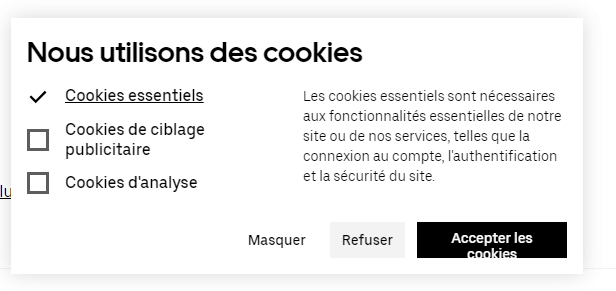
**POURQUOI ?**

* Non-respect du principe d’équilibre entre le bouton Accepter et Refuser :

Le bouton Accepter est mis en avant avec sa couleur tandis que le bouton Refuser est moins visible.

* La position des boutons :

Ils sont positionnés en petit dans le coin



**NON-CONFORME**

**POURQUOI ?**

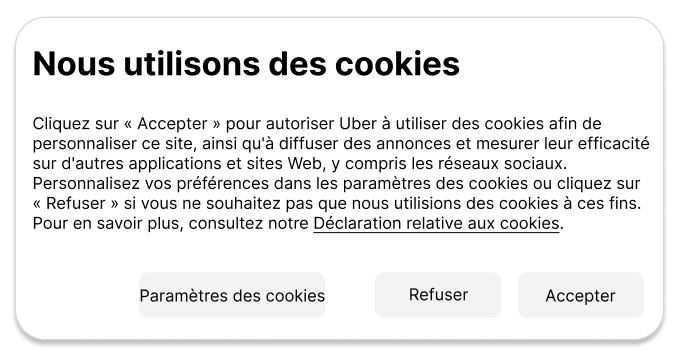
* Non-respect du principe d’équilibre entre le bouton Accepter et Refuser :

Le bouton Accepter est mis en avant avec sa couleur tandis que le bouton Refuser est moins visible.

* La position des boutons :

Ils sont positionnés en petit dans le coin

## Nos bandeaux cookies conformes :



**CONFORME**

**POURQUOI ?**

* Respect du principe d’équilibre entre le bouton Accepter et Refuser :

Le bouton Accepter et le bouton Refuser sont similaires et aucun n’est mis en avant plus que l’autre.

* La position des boutons :

Ils sont positionnés sur toute la partie basse du bandeau et sont moins compressés.





****

**CONFORME**

**POURQUOI ?**

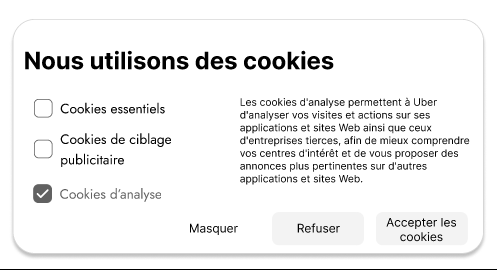
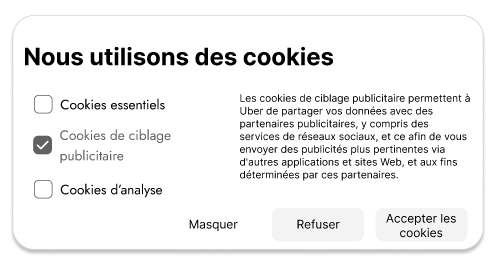
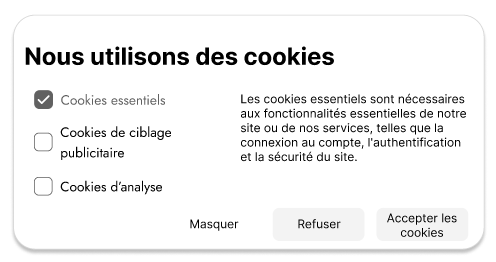
* Les cookies essentiels sont cochés par défaut car cela sert au bon fonctionnement du site et ne peuvent pas être décocher sinon le site ne fonctionne pas.
* Respect du principe d’équilibre entre le bouton Accepter et Refuser :

Le bouton Accepter et le bouton Refuser sont similaires et aucun n’est mis en avant plus que l’autre.

* La position des boutons :

Ils sont positionnés sur toute la partie basse du bandeau et sont moins compressés.

Lorsque l’on coche un type de cookies il est explicitement décrit en quoi consiste ces cookies :

****​ 

# Politique de protection des données personnelles

## Introduction

Dans le cadre de ses activités, la société Uber, dont le siège social est situé à San Francisco en Californie, est amenée à collecter et à traiter des informations dont certaines sont qualifiées des « données personnelles ». Uber attache une grande importance au respect de la vie privée, et n’utilise que des données de manière responsable et confidentielle et dans une finalité précise.

## Données personnelles

Sur le site web Uber, il y a plusieurs types de données personnelles susceptibles d’être recueillies :

* Les données fournies par les utilisateurs ou chauffeurs par des formulaires d’inscription ou de contact. Les informations fournies sont le prénom, le nom, l’adresse e-mail, le numéro de téléphone, et des informations concernant les chauffeurs du type permis de conduire, assurance, et d’autres informations professionnelles nécessaires pour valider leur profil et leur éligibilité à conduire pour Uber.
* Les données fournies lors d’une configuration des profils comme le moyen de paiement, les adresses fournies pour le départ/arrivée d’une course en favoris.
* Les données collectées lors des demandes d’aide grâce aux formulaires de contact sur le site ou par email comme le motif de la demande, les détails du problème concerné et toute autre information nécessaire pour résoudre le problème.

## Les données transmises directement

Ces données sont celles que vous nous transmettez directement, via un formulaire de contact ou bien par contact direct par email. Sont obligatoires dans le formulaire de contact les champs « prénom », « nom », « entreprise ou organisation » et « email ».

## Les données collectées automatiquement

Lors de vos visites, une fois votre consentement donné, nous pouvons recueillir des informations de type « web Analytics » relatives à votre navigation, la durée de votre consultation, votre adresse IP, votre type et version de navigateur. La technologie utilisée est le cookie.

**Utilisation des données**

Les données que vous nous transmettez directement sont utilisées dans le but de vous recontacter et/ou dans le cadre de la demande que vous nous faites. Les données « web Analytics » sont collectées de forme anonyme (en enregistrant des adresses IP anonymes) par Google Analytics, et nous permettent de mesurer l'audience de notre site web, les consultations et les éventuelles erreurs afin d’améliorer constamment l’expérience des utilisateurs. Ces données sont utilisées par Uber ainsi que par le responsable du traitement des données, et ne seront jamais cédées à un tiers ni utilisées à d’autres fins que ceux détaillés ci-dessus.

## Base légale

Les données personnelles collectées par Uber ne sont collectées qu’après consentement obligatoire de l’utilisateur. Ce consentement est recueilli de manière valable (boutons et cases à cocher), libre, clair et sans équivoque.

## Durée de conservation

Des données des utilisateurs seront sauvegardées pour une durée maximale de 3 ans en cas d'inactivité.

Des données des chauffeurs peuvent être conservée pour une durée de 5 ans après la fin de leurs activités selon les obligations légales.

Des données anonymisées peuvent être conservées indéfiniment pour effectuer des analyses statistiques ou des mesures de performance de la plateforme.

## Cookies

Voici la liste des cookies utilisés et leurs objectifs :

**Cookies Google Analytics (liste exhaustive) : Web analytics**

**Cookies de consentement :** Permet de garder en mémoire le fait que vous acceptez les cookies afin de ne plus vous importuner lors de votre prochaine visite.

Vos droits concernant les données personnelles

Vous avez le droit de consultation, demande de modification ou d’effacement sur l’ensemble de vos données personnelles. Vous pouvez également retirer votre consentement au traitement de vos données.

**Cookies strictement nécessaires :** Permet le fonctionnement du site, comme la gestion des comptes utilisateurs, la connexion ou la validation des transactions.

**Cookies personnalisés :** Permet d’enregistrer les préférences des utilisateurs comme les langues, choix de région, mode de navigation pour simplifier les prochaines expériences des utilisateurs lors de la prochaine utilisation du site.

**Cookies publicitaires :** Permet de personnaliser les annonces publicitaires en fonction des historiques de recherche, des trajets effectués, ou de la localisation. Ces cookies sont activés uniquement si vous nous avez donné votre consentement.

## DPO (Délégué à la Protection des Données)

**Définition d’un DPO :**

Personne désignée au sein d'une organisation pour veiller à la conformité au Règlement Général sur la Protection des Données (RGPD) et à la protection des données personnelles. Le DPO est doit s'assurer que l'entreprise respecte les règles relatives à la collecte, au traitement et à la sécurisation des données personnelles des utilisateurs, employés et autres parties prenantes.

Comme explicité dans l’article 37 de la CNIL :

* **Article 37 :**

« Le responsable du traitement et le sous-traitant désignent en tout état de cause un délégué à la protection des données lorsque :

a) le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle ;

b) les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ; où

c) les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l’article 9 ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l’article 10. »

Un DPO est nécessaire car les activités principales d’Uber consistent à suivre régulièrement des personnes à grande échelle par l’utilisation de la géolocalisation. Certaines données traitées présentent des risques élevés pour les droits et libertés des personnes, ce qui nécessite un suivi juridique et organisationnel.

## Contact délégué à la protection des données

Feyza Tinastepe

N° téléphone : 06 47 29 12 07

Email : [feyza.tinastepe@etu.univ-smb.fr](mailto:feyza.tinastepe@etu.univ-smb.fr)

## Analyse d’Impact relative à la Protection des Données (AIPD)

**Définition d’une AIPD :**

Processus qui permet d’identifier les risques associés au traitement des données personnels et mettre en place des solutions pour garantir la protection des droits et libertés des personnes concerné.

Comme dit dans l’article 35 de la CNIL :

* **Article 35, paragraphe 1 :**

« Lorsqu’un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. »

Une AIPD est nécessaire lorsque les traitements envisagés représentent des dangers pour la vie privée des individus. Elle a pour objectif d’évaluer ces risques de manière approfondie et de proposer des mesures adaptées garantissant une meilleure protection des droits et libertés des personnes concernées.

Les critères pour l’obligation d’une AIPD pour Uber sont :

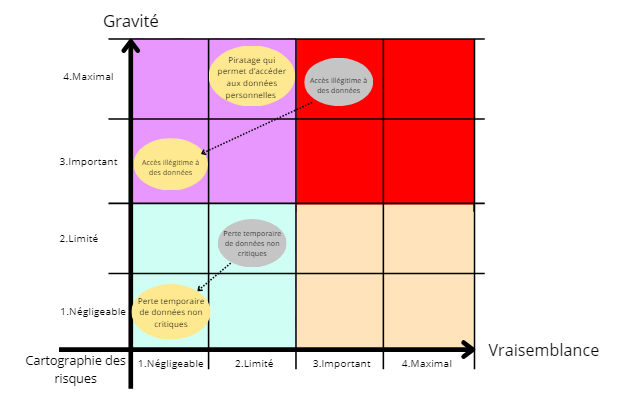
Le profilage :

* Attribution des courses aux chauffeurs en fonction des critères du client
* Evaluation des chauffeurs par les utilisateurs avec le système de notation
* Tarif des courses en fonction des lieux du client / Historique des trajets

Les courses :

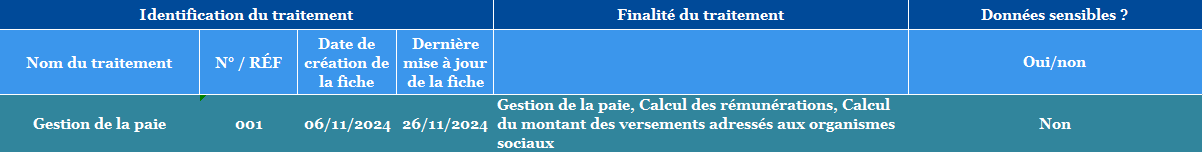
* Géolocalisation des clients/chauffeurs lors d’une course ou d’une commande
* Mode de paiement

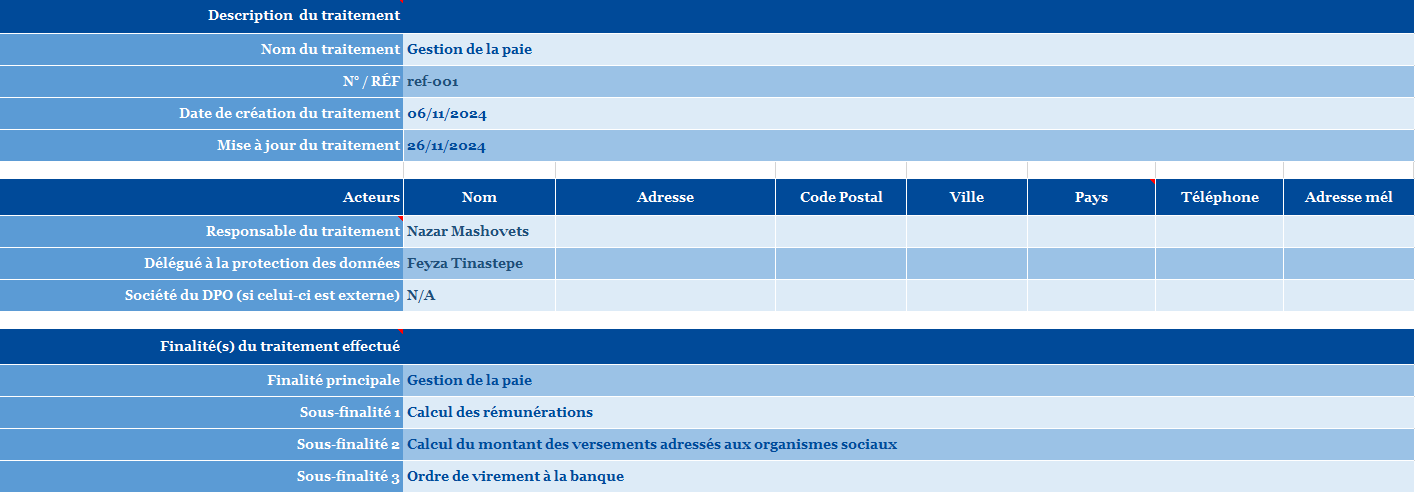
## Élaboration de la cartographie des risques liés à la sécurité des données

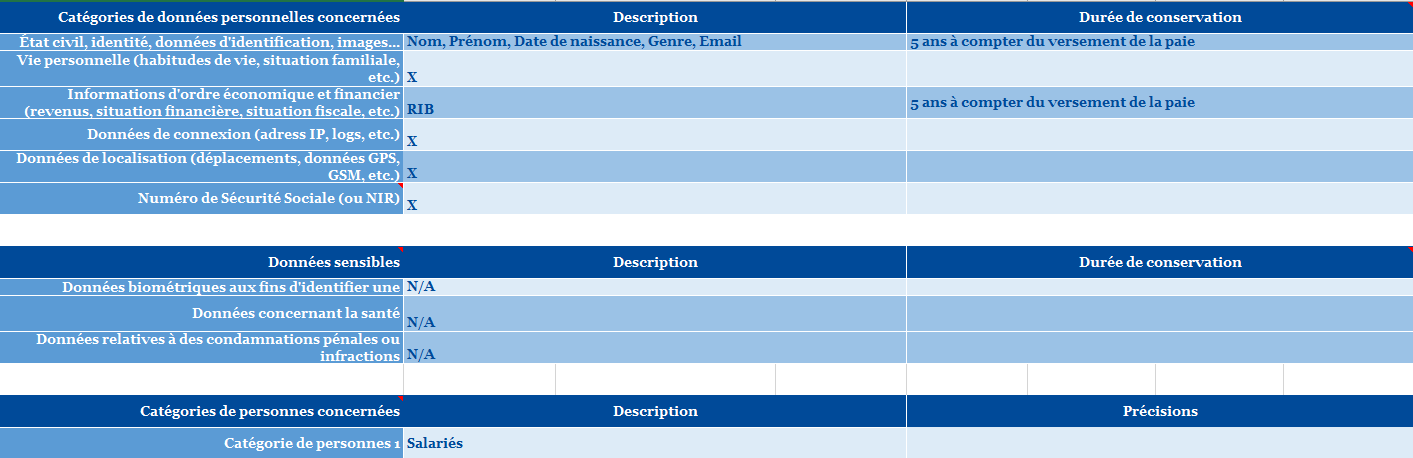


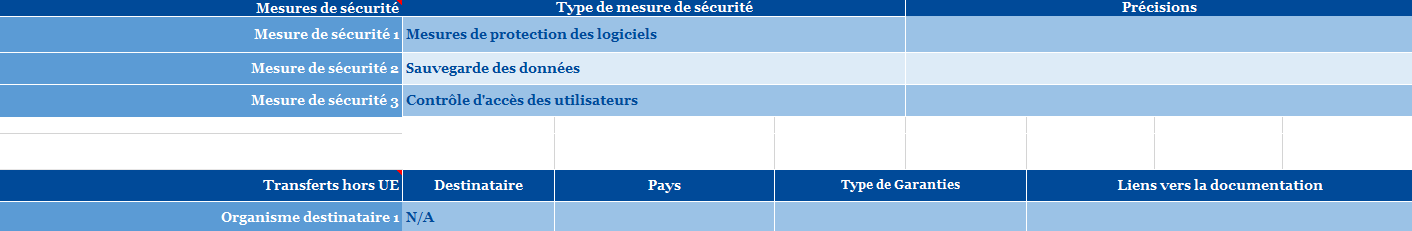
# Excel

## Registre de traitement de gestion de la paie

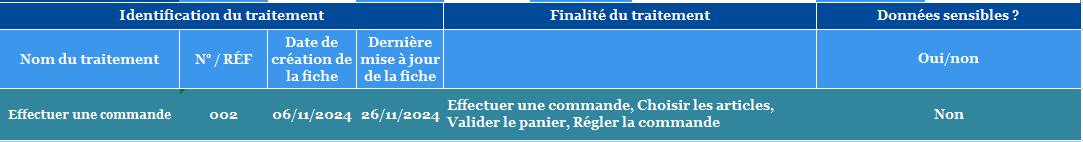




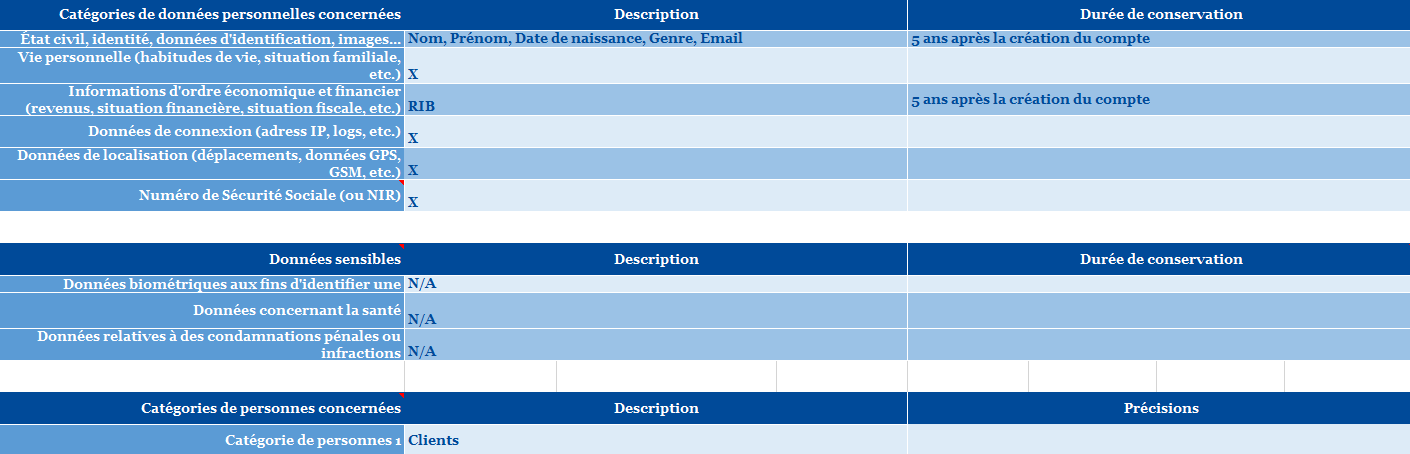


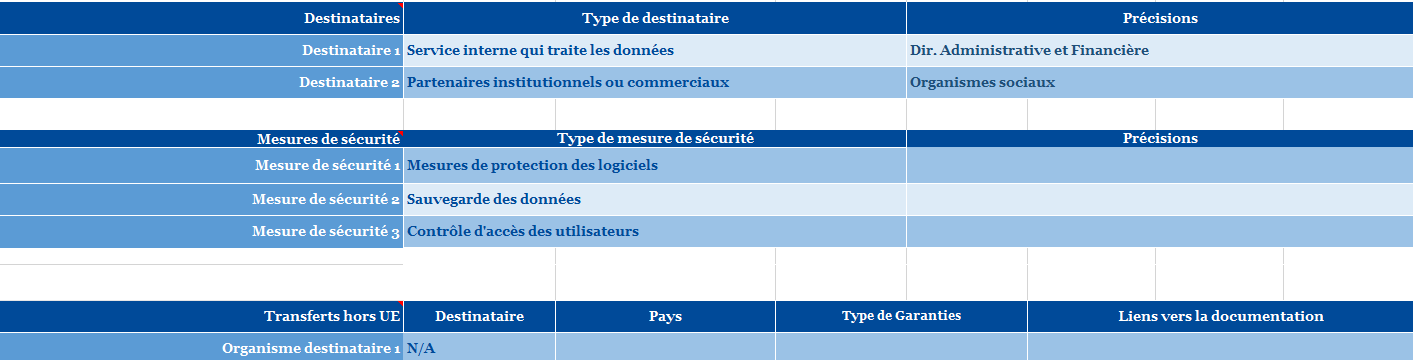


## Registre de traitement de commande client

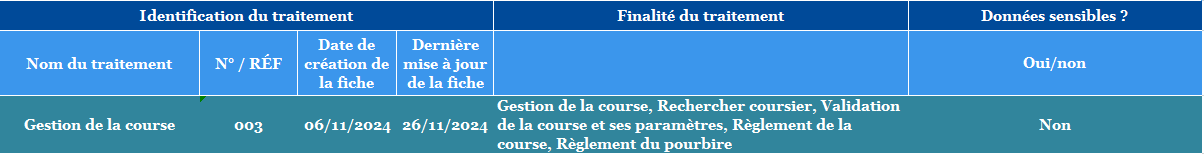




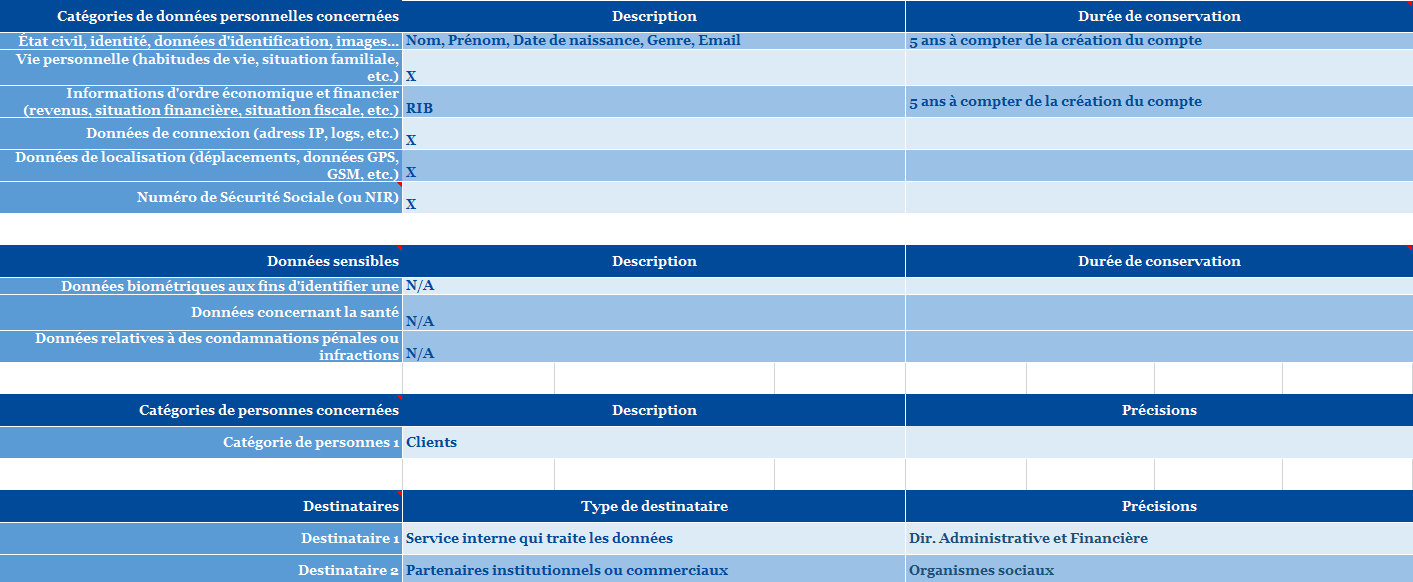


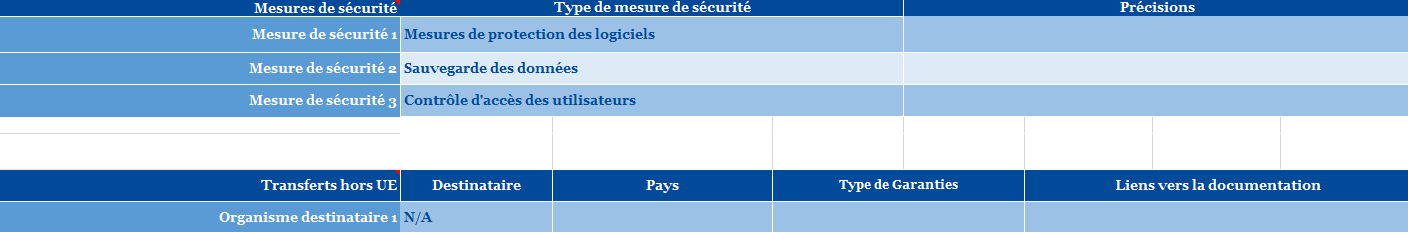


## Registre de traitement de course client









# Note Explicative

L’article 6 du contrat OVH aborde la protection contre les attaques DoS (Denial of Service) et DDOS (Distributed Denial of Service). Ces attaques ont pour objectif de rendre un service inaccessible en surchargeant les serveurs. C’est pour cela que OVH propose une fonctionnalité de mitigation qui permet de détecter et bloquer ce type de trafic avant qu’il n’atteigne les services du client.

OVH analyse en temps réel le trafic entrant vers le Service du Client et si un trafic suspect est détecté, il sera bloqué avant que cela n’atteigne le service. Cette protection reste activée jusqu’à ce que l’attaque soit terminée ou que le trafic ne soit plus suspecté.

La mitigation garantit un service protégeant la réputation de l’entreprise et réduisant les pertes économiques pendant l’indisponibilité du service.

L’article 7 se concentre sur la gestion de la disponibilité et les dédommagements après une défaillance du service par exemple pour signaler un problème et attendre une intervention. En cas de problème, le client a la possibilité de signaler l’incident et une intervention sera effectuée par OVH pour résoudre le problème.

Bien que cet article soit moins technique, il reste important pour assurer un suivi et une gestion efficaces des défaillances. Il établit une relation de confiance entre le fournisseur et le client en garantissant une bonne communication concernant la gestion des problèmes.

