

Université Savoie Mont Blanc

Rapport de droit



Réalisé Par :

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

Encadré Par :

- M Y. GAILLARD

Dans 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
1.1. Les bandeaux cookies d'Uber non-conformes :.....	3
1.2. Nos bandeaux cookies conformes :.....	4
2 - Politique de protection des données personnelles.....	6
2.1 Introduction.....	6
2.2 Données personnelles.....	6
2.3 Les données transmises directement.....	6
2.4 Les données collectées automatiquement.....	6
2.5 Base légale.....	7
2.6 Durée de conservation.....	7
2.7 Cookies.....	7
2.8 DPO (Délégué à la Protection des Données)	7
2.9 Contact délégué à la protection des données.....	8
2.10 Analyse d'Impact relative à la Protection des Données (AIPD).....	8
3 - Excel	10
3.1 Registre de traitement de gestion de la paie.....	10
3.2 Registre de traitement de commande client.....	11
3.3 Registre de traitement de course client.....	12
4 - Note Explicative.....	13

1 - La réglementation relative aux cookies

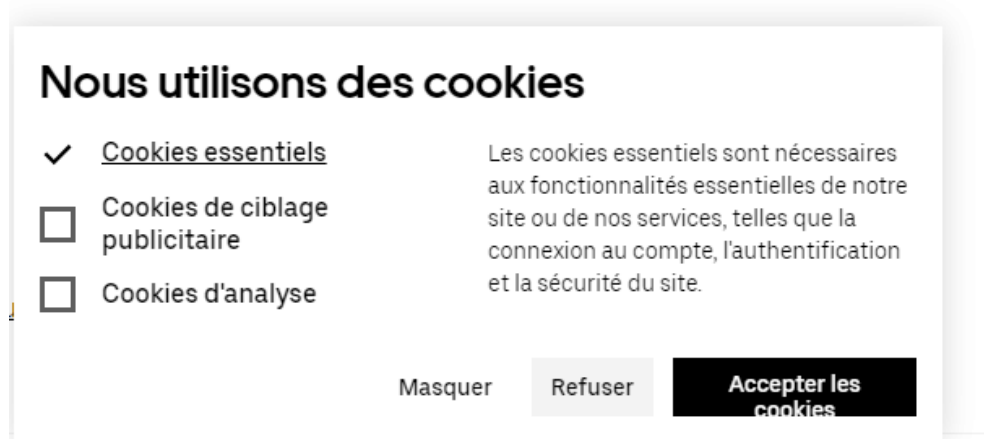
1.1. Les bandeaux cookies d'Uber non-conformes :



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 ?

- Les cookies essentiels sont cochés par défaut et ne peuvent pas être décocher.
- 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

1.2. Nos bandeaux cookies conformes :

Nous utilisons des cookies

Cliquez sur « Accepter » pour autoriser Uber à utiliser des cookies afin de personnaliser ce site, ainsi qu'à diffuser des annonces et mesurer leur efficacité sur d'autres applications et sites Web, y compris les réseaux sociaux. Personnalisez vos préférences dans les paramètres des cookies ou cliquez sur « Refuser » si vous ne souhaitez pas que nous utilisions des cookies à ces fins. Pour en savoir plus, consultez notre [Déclaration relative aux cookies](#).

[Paramètres des cookies](#)[Refuser](#)[Accepter](#)

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.

Nous utilisons des cookies

☐ Cookies essentiels☐ Cookies de ciblage publicitaire☐ Cookies d'analyse

Nous traitons vos données pour fournir du contenu ou des publicités. Nous analysons la diffusion de ce contenu ou de ces publicités pour en tirer des informations sur notre site web. Nous partageons ces informations avec nos partenaires sur la base d'un consentement.

[Masquer](#)[Refuser](#)[Accepter les cookies](#)

CONFORME

POURQUOI ?

- Les cookies essentiels sont décochés par défaut et peuvent être cocher/décocher.
- 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 :

Nous utilisons des cookies

- ☐ Cookies essentiels
- ☐ Cookies de ciblage publicitaire
- ☒ Cookies d'analyse

Les cookies d'analyse permettent à Uber d'analyser vos visites et actions sur ses applications et sites Web ainsi que ceux d'entreprises tierces, afin de mieux comprendre vos centres d'intérêt et de vous proposer des annonces plus pertinentes sur d'autres applications et sites Web.

Masquer

Refuser

Accepter les cookies

Nous utilisons des cookies

- ☒ Cookies essentiels
- ☐ Cookies de ciblage publicitaire
- ☐ Cookies d'analyse

Les cookies essentiels sont nécessaires aux fonctionnalités essentielles de notre site ou de nos services, telles que la connexion au compte, l'authentification et la sécurité du site.

Masquer

Refuser

Accepter les cookies

Nous utilisons des cookies

- ☐ Cookies essentiels
- ☒ Cookies de ciblage publicitaire
- ☐ Cookies d'analyse

Les cookies de ciblage publicitaire permettent à Uber de partager vos données avec des partenaires publicitaires, y compris des services de réseaux sociaux, et ce afin de vous envoyer des publicités plus pertinentes via d'autres applications et sites Web, et aux fins déterminées par ces partenaires.

Masquer

Refuser

Accepter les cookies

2 - Politique de protection des données personnelles

2.1 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.

2.2 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.

2.3 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 ».

2.4 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.

2.5 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.

2.6 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.

2.7 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.

2.8 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 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.

2.9 Contact délégué à la protection des données

Feyza Tinastepe

N° téléphone : 06 47 29 12 07

Email : feyzat.inastepe@etu.univ-smb.fr

2.10 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 personnelles et mettre en place des solutions pour garantir la protection des droits et libertés des personnes concernées.

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 :

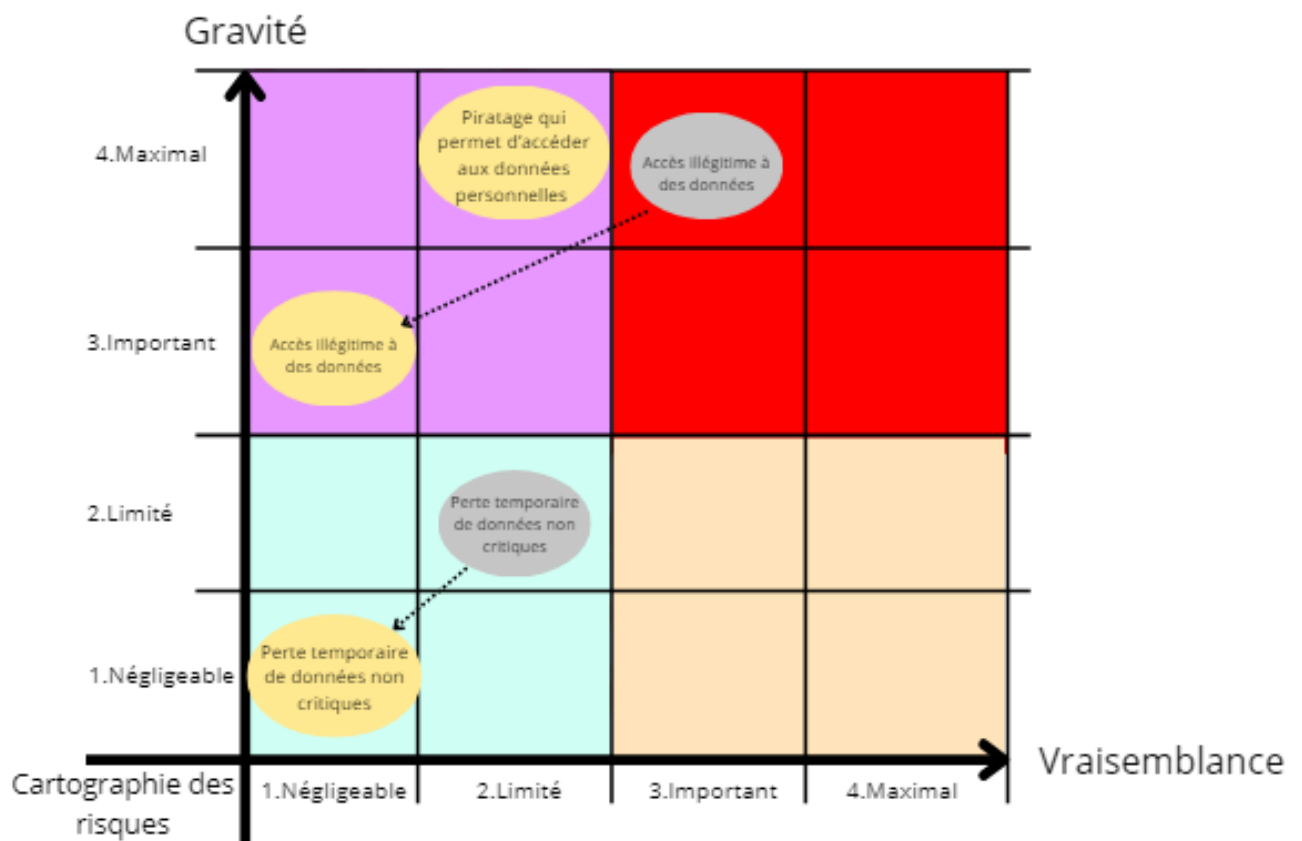
Le profilage :

- 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

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



3 - Excel

3.1 Registre de traitement de gestion de la paie

Identification du traitement				Finalité du traitement	Données sensibles ?
Nom du traitement	N° / RÉF	Date de création de la fiche	Dernière mise à jour de la fiche		Oui/non
Gestion de la paie	001	06/11/2024	26/11/2024	Gestion de la paie, Calcul des rémunérations, Calcul du montant des versements adressés aux organismes sociaux	Non

Description du traitement							
Nom du traitement	Gestion de la paie						
N° / RÉF	ref-001						
Date de création du traitement	06/11/2024						
Mise à jour du traitement	26/11/2024						
Acteurs	Nom	Adresse	Code Postal	Ville	Pays	Téléphone	Adresse mél
Responsable du traitement	Nazar Mashovets						
Délégué à la protection des données	Feyza Tinastepe						
Société du DPO (si celui-ci est externe)	N/A						

Finalité(s) du traitement effectué	
Finalité principale	Gestion de la paie
Sous-finalité 1	Calcul des rémunérations
Sous-finalité 2	Calcul du montant des versements adressés aux organismes sociaux
Sous-finalité 3	Ordre de virement à la banque

Catégories de données personnelles concernées	Description	Durée de conservation
Etat civil, identité, données d'identification, images, etc.	Nom, Prénom, Date de naissance, Genre, Email	5 ans à compter du versement de la paie
Vie personnelle (habitudes de vie, situation familiale, etc.)	X	
Informations d'ordre économique et financier (revenus, situation financière, situation fiscale, etc.)	RIB	5 ans à compter du versement de la paie
Données de connexion (adress IP, logs, etc.)	X	
Données de localisation (déplacements, données GPS, GSM, etc.)	X	
Numéro de Sécurité Sociale (ou NIR)	X	

Données sensibles	Description	Durée de conservation
Données biométriques aux fins d'identifier une	N/A	
Données concernant la santé	N/A	
Données relatives à des condamnations pénales ou infractions	N/A	

Catégories de personnes concernées	Description	Précisions
Catégorie de personnes 1	Salariés	

Mesures de sécurité	Type de mesure de sécurité	Précisions
Mesure de sécurité 1	Mesures de protection des logiciels	
Mesure de sécurité 2	Sauvegarde des données	
Mesure de sécurité 3	Contrôle d'accès des utilisateurs	

Transferts hors UE	Destinataire	Pays	Type de Garanties	Liens vers la documentation
Organisme destinataire 1	N/A			

3.2 Registre de traitement de commande client

Identification du traitement				Finalité du traitement	Données sensibles ?		
Nom du traitement	N° / RÉF	Date de création de la fiche	Dernière mise à jour de la fiche		Oui/non		
Effectuer une commande	002	06/11/2024	26/11/2024	Effectuer une commande, Choisir les articles, Valider le panier, Régler la commande	Non		

Description du traitement							
Nom du traitement							
Effectuer une commande client							
N° / RÉF							
ref-002							
Date de création du traitement							
06/11/2024							
Mise à jour du traitement							
26/11/2024							
Acteurs	Nom	Adresse	Code Postal	Ville	Pays	Téléphone	Adresse mél
Responsable du traitement	Nazar Mashovets	1 rue Rivoli	75001	Paris	France	01 XX XX XX XX	exemple1@ets.com
Délégué à la protection des données	Feyza Tinastepe	1 rue Rivoli	75001	Paris	France	01 XX XX XX XX	exemple2@ets.com
Société du DPO (si celui-ci est externe)	N/A						

Finalité(s) du traitement effectué	
Finalité principale	Effectuer une commande
Sous-finalité 1	Choisir les articles
Sous-finalité 2	Valider le panier
Sous-finalité 3	Régler la commande

Catégories de données personnelles concernées	Description	Durée de conservation
Etat civil, identité, données d'identification, images... Vie personnelle (habitudes de vie, situation familiale, etc.)	Nom, Prénom, Date de naissance, Genre, Email	5 ans après la création du compte
Informations d'ordre économique et financier (revenus, situation financière, situation fiscale, etc.)	X	
Données de connexion (adress IP, logs, etc.)	RIB	5 ans après la création du compte
Données de localisation (déplacements, données GPS, GSM, etc.)	X	
Numéro de Sécurité Sociale (ou NIR)	X	

Données sensibles	Description	Durée de conservation
Données biométriques aux fins d'identifier une	N/A	
Données concernant la santé	N/A	
Données relatives à des condamnations pénales ou infractions	N/A	

Catégories de personnes concernées	Description	Précisions
Catégorie de personnes 1	Clients	

Destinataires	Type de destinataire	Précisions
Destinataire 1	Service interne qui traite les données	Dir. Administrative et Financière
Destinataire 2	Partenaires institutionnels ou commerciaux	Organismes sociaux

Mesures de sécurité	Type de mesure de sécurité	Précisions
Mesure de sécurité 1	Mesures de protection des logiciels	
Mesure de sécurité 2	Sauvegarde des données	
Mesure de sécurité 3	Contrôle d'accès des utilisateurs	

Transferts hors UE	Destinataire	Pays	Type de Garanties	Liens vers la documentation
Organisme destinataire 1	N/A			

3.3 Registre de traitement de course client

Identification du traitement				Finalité du traitement	Données sensibles ?		
Nom du traitement	N° / RÉF	Date de création de la fiche	Dernière mise à jour de la fiche		Oui/non		
Gestion de la course	003	06/11/2024	26/11/2024	Gestion de la course, Recherche coursier, Validation de la course et ses paramètres, Règlement de la course, Règlement du pourboire	Non		

Description du traitement							
Nom du traitement	Gestion de la course						
N° / RÉF	ref-003						
Date de création du traitement	06/11/2024						
Mise à jour du traitement	26/11/2024						
Acteurs	Nom	Adresse	Code Postal	Ville	Pays	Téléphone	Adresse mél
Responsable du traitement	Nazar Mashovets	1 rue Rivoli	75001	Paris	France	01 XX XX XX XX	exemple1@ets.com
Délégué à la protection des données	Feyza Tinastepe	1 rue Rivoli	75001	Paris	France	01 XX XX XX XX	exemple2@ets.com
Société du DPO (si celui-ci est externe)	N/A						

Finalité(s) du traitement effectué	
Finalité principale	Gestion de la course
Sous-finalité 1	Recherche coursier
Sous-finalité 2	Validation de la course et ses paramètres
Sous-finalité 3	Règlement de la course
Sous-finalité 4	Règlement du pourboire

Catégories de données personnelles concernées	Description	Durée de conservation
Etat civil, identité, données d'identification, images,...	Nom, Prénom, Date de naissance, Genre, Email	5 ans à compter de la création du compte
Vie personnelle (habitudes de vie, situation familiale, etc.)	X	
Informations d'ordre économique et financier (revenus, situation financière, situation fiscale, etc.)	RIB	5 ans à compter de la création du compte
Données de connexion (adress IP, logs, etc.)	X	
Données de localisation (déplacements, données GPS, GSM, etc.)	X	
Numéro de Sécurité Sociale (ou NIR)	X	

Données sensibles	Description	Durée de conservation
Données biométriques aux fins d'identifier une	N/A	
Données concernant la santé	N/A	
Données relatives à des condamnations pénales ou infractions	N/A	

Catégories de personnes concernées	Description	Précisions
Catégorie de personnes 1	Clients	

Destinataires	Type de destinataire	Précisions
Destinataire 1	Service interne qui traite les données	Dir. Administrative et Financière
Destinataire 2	Partenaires institutionnels ou commerciaux	Organismes sociaux

Mesures de sécurité	Type de mesure de sécurité	Précisions
Mesure de sécurité 1	Mesures de protection des logiciels	
Mesure de sécurité 2	Sauvegarde des données	
Mesure de sécurité 3	Contrôle d'accès des utilisateurs	

Transferts hors UE	Destinataire	Pays	Type de Garanties	Liens vers la documentation
Organisme destinataire 1	N/A			

4 - 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.

