Bonjour,

Pour la SAE S3.01 en droit (partie livrable intitulée "Sécurité et protection des données" dans votre sujet + contrat OVH), vous devez rendre **2 documents :**

1) Un **document rédigé sous word** (paginé, avec sommaire, 10 à 20 pages hors les annexes) qui répond aux 4 questions juridiques de la SAE.

Ce document peut comporter des annexes, des captures d'écran, des maquettes si votre développement est en cours, etc.

Vous devez justifiez vos choix techniques au regard des contraintes juridiques.

Ne vous limitez pas à présenter vos travaux mais argumentez, expliquez vos choix (notamment en matière de RGPD, PBD/PBD, mdp, hébergement, limitation de la collecte, finalités, consentement, droit des personnes sur leurs données, cryptage ?, rapport d'outils de contrôle des cookies type cookiebot et cookieviz ou d'autres, durée de conservation et effet sur votre traitement automatisé des données, DPO, sécurité, choix de votre éventuel outils analytics selon les recommandations CNIL -->google analytics ? ou Matomo ?, chiffrage de mdp, base légale des traitement, etc.).

Pour ce travail, utilisez le site de la CNIL, de l'ANSSI et les 2 supports de cours qui vous permettront de ne rien oublier (et de réviser pour le DS) --> 1 support papier distribué et 1 à venir sur U:/

Pensez aussi aux formulaires de collecte des données personnelles avec toutes les mentions obligatoires (capture d'écran ou maquette).

Le registre des traitement sera dans ce document et vous commenterez les éléments que vous y faites figurer (même chose pour le contenu de la page "protection des données personnelles" et "cookies").

Ce document sera paginé, avec un sommaire, et relu pour l'orthographe.  
La lecture de ce document doit nous permettre de vérifier que vous êtes en conformité avec le RGPD **(sans que nous ayons besoin de consulter votre site**).  
Votre travail sera évalué via ce document. Nous ne devons pas avoir à visiter votre site. Pensez à mettre vos noms et votre groupe en page de garde.

2) Un **support powerpoint** qui vous permettra de présenter vos travaux à **l'oral la semaine 48 ou 49 selon les groupes** lors de la séance R3.11-S3.01 avec M. Thabuis ou moi-même. Durée de la présentation **15 minutes maximum**, 2 à 3 min de questions. Répartissez-vous la parole. Cet oral reprend les éléments du dossier word (les 4 questions) et vous permet d'insister sur les points que vous souhaitez mettre en avant pour valoriser votre travail. Si vous souhaitez afficher votre site web pendant l'oral ou faire une démonstration, limitez les risques techniques (enregistrez votre démo ou travaillez en local). Pour cet oral, c**haque groupe viendra avec son PC** pour réaliser la présentation. Pensez à mettre vos noms et votre groupe en page de garde.

Ces 2 documents sont à rendre AVANT la séance 3/3 qui a lieu fin novembre - début décembre.

Créer un dossier que vous nommerez "N°groupeTD\_Nom sujet" --> Exemple : "1\_Vinted"

Dans ce dossier vous déposerez : votre fichier word (point 1 ci-avant) + votre powerpoint (point 2)

Adresse du casier pour les dépôts : '[\\iut-acy.local\Public\Documents\Casier\Info2\_SAE301\_\_Droit\_2024](file://iut-acy.local/Public/Documents/Casier/Info2_SAE301__Droit_2024)'

**QUESTIONS DROIT**

1) Afin de respecter la réglementation relative aux cookies (bandeau, paramétrage, information détaillée des cookies), mettez en place les outils nécessaires (bandeau d’acceptation, gestion des préférences cookies, et pages web d’informations relatives aux cookies). Vous communiquerez l’URL de votre site afin d’évaluer vos travaux en ligne et documenterez avec des captures d’écrans ou des maquettes

-> réaliser bandeau cookies maquette figma

2)Proposer un contenu pertinent pour la page web du site “Politique de protection des données personnelles” du site internet. Vous communiquerez l’URL de votre site afin d’évaluer vos travaux en ligne et documenterez avec des captures d’écrans ou des maquettes

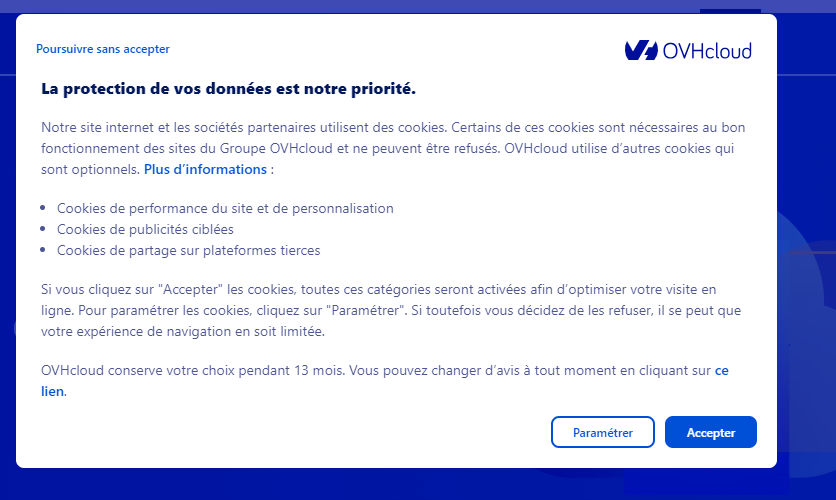
DPO ? Y'en a un ou pas obligatoire ou pas, justifier

Analyse d’impact aipd obligatoire ou pas, ne pas faire d’analyse juste expliquer.

<https://www.uber.com/legal/th/document/?country=canada&lang=fr-ca&name=privacy-notice>

-> réaliser bloc cookies accepter refuser maquette figma

<https://www.uber.com/global/en/privacy/overview/>



L'obligation d'une Analyse d'Impact relative à la Protection des Données (AIPD) dans le contexte d’Uber :

Dans l’article 35 du Règlement Général sur la Protection des Données (RGPD) -->

### Article 35 - Analyse d'impact relative à la protection des données

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 seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires.

Lorsqu'il effectue une analyse d'impact relative à la protection des données, le responsable du traitement demande conseil au délégué à la protection des données, si un tel délégué a été désigné.

L'analyse d'impact relative à la protection des données visée au paragraphe 1 est, en particulier, requise dans les cas suivants:

a) l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire;

b) le traitement à grande échelle de catégories particulières de données visées à l'article 9, paragraphe 1, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10; ou

c) la surveillance systématique à grande échelle d'une zone accessible au public.

L'autorité de contrôle établit et publie une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise conformément au paragraphe 1. L'autorité de contrôle communique ces listes au comité visé à l'article 68.

L'autorité de contrôle peut aussi établir et publier une liste des types d'opérations de traitement pour lesquelles aucune analyse d'impact relative à la protection des données n'est requise. L'autorité de contrôle communique cette liste au comité.

Avant d'adopter les listes visées aux paragraphes 4 et 5, l'autorité de contrôle compétente applique le mécanisme de contrôle de la cohérence visé à l'article 63, lorsque ces listes comprennent des activités de traitement liées à l'offre de biens ou de services à des personnes concernées ou au suivi de leur comportement dans plusieurs États membres, ou peuvent affecter sensiblement la libre circulation des données à caractère personnel au sein de l'Union.

L'analyse contient au moins:

a) une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement;

b) une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités;

c) une évaluation des risques pour les droits et libertés des personnes concernées conformément au paragraphe 1; et

d) les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées.

Le respect, par les responsables du traitement ou sous-traitants concernés, de codes de conduite approuvés visés à l'article 40 est dûment pris en compte lors de l'évaluation de l'impact des opérations de traitement effectuées par lesdits responsables du traitement ou sous-traitants, en particulier aux fins d'une analyse d'impact relative à la protection des données.

Le cas échéant, le responsable du traitement demande l'avis des personnes concernées ou de leurs représentants au sujet du traitement prévu, sans préjudice de la protection des intérêts généraux ou commerciaux ou de la sécurité des opérations de traitement.

Lorsque le traitement effectué en application de l'article 6, paragraphe 1, point c) ou e), a une base juridique dans le droit de l'Union ou dans le droit de l'État membre auquel le responsable du traitement est soumis, que ce droit règlemente l'opération de traitement spécifique ou l'ensemble des opérations de traitement en question et qu'une analyse d'impact relative à la protection des données a déjà été effectuée dans le cadre d'une analyse d'impact générale réalisée dans le cadre de l'adoption de la base juridique en question, les paragraphes 1 à 7 ne s'appliquent pas, à moins que les États membres n'estiment qu'il est nécessaire d'effectuer une telle analyse avant les activités de traitement.

Si nécessaire, le responsable du traitement procède à un examen afin d'évaluer si le traitement est effectué conformément à l'analyse d'impact relative à la protection des données, au moins quand il se produit une modification du risque présenté par les opérations de traitement.

Comme dit dans l’article 35 de la cnil, une aipd reste obligatoire lors des traitements de données personnels car cela peut engendrer un danger important pour les droits et libertés des individus.

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.

Une AIPD est nécessaires lorsque les traitements envisagés représentent des dangers pour la vie privée des individus. Elle a pour objectifs d’évaluer ces risques de manières approfondie et de proposer des mesures adaptées pour atténuer, garantissant ainsi une meilleure protection des droits et libertés des personnes concernée.

Les critères pour l’obligation d’une aipd pour uber :

Le profilage :

- Attribuer des courses aux chauffeurs en fonctions des critères du client

- Evaluation des chauffeurs par les utilisateurs avec le système de notation

- Tarif des courses en fonction de lieu du client et le chauffeur

- Historique des trajets

Les courses :

- Géolocalisation des clients/chauffeurs lors d’une course/commande

-Mode de paiement

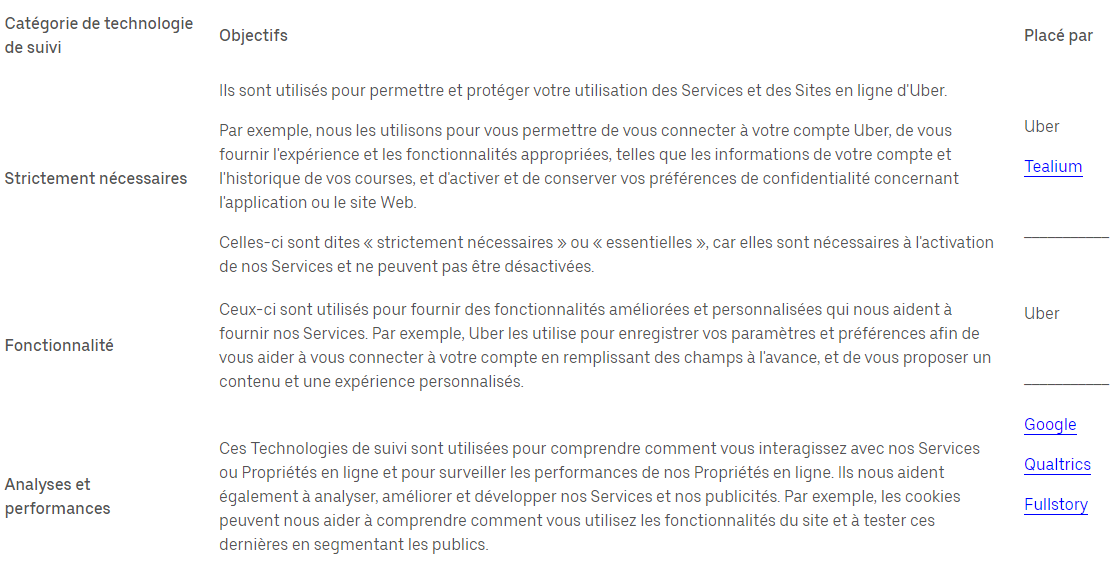
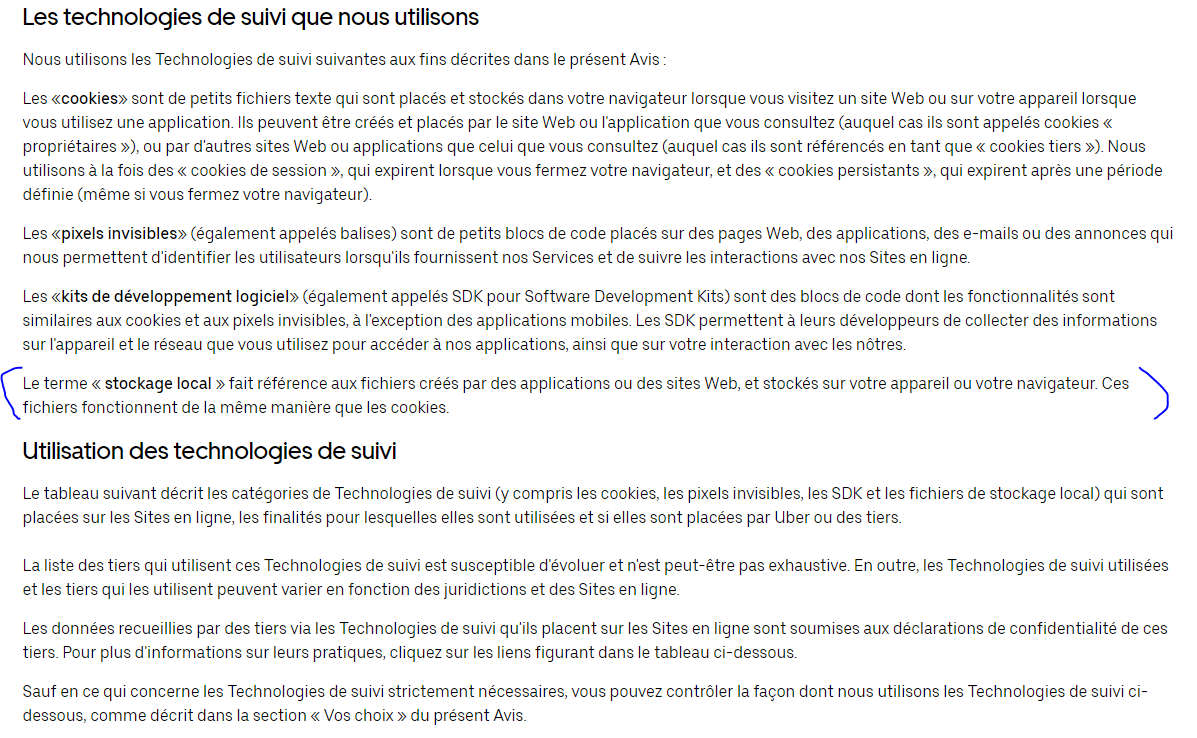
3)Complétez le registre des traitements proposé par la CNIL afin de décrire le traitement des données clients (traitement relatif à une vente en ligne).

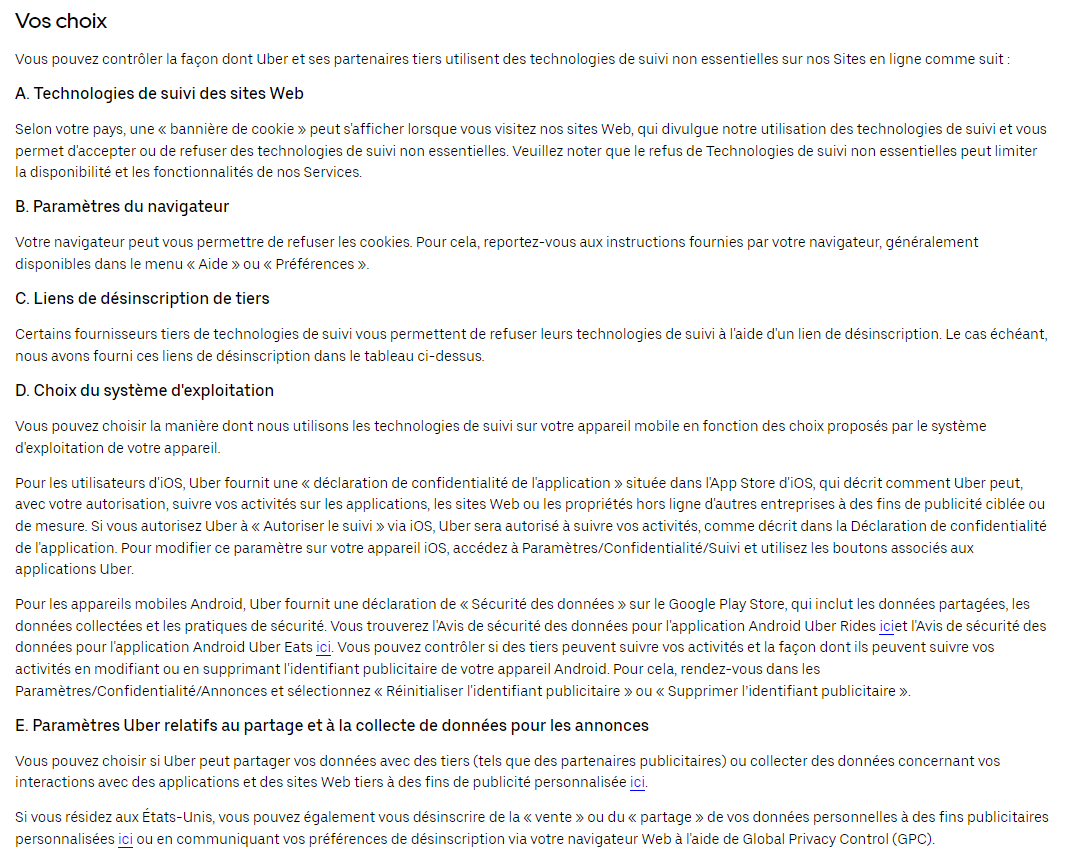
--> excel

4)A la lecture du contrat OVH de location d’un serveur dédié, le responsable juridique a besoin de vos compétences informatiques afin de bien comprendre les clauses les plus techniques. Il vous demande donc de lire attentivement le contrat en annexe et de rédiger une note explicative relative à l’un des articles ci- dessous. Choisissez un article au choix.

* + à l’article 6 : mitigation (votre note sera d’une page maximum, peut présenter des schémas, des définitions, des exemples, les avantages pour l’entreprise, les limites, etc.)
  + à l’article 7 : engagement de niveau de service (votre note sera d’une page maximum, peut présenter des schémas, des définitions, des exemples, les avantages pour l’entreprise, les limites, etc.)

**QUESTION 1**





**QUESTION 4**

**Note explicative relative à l'Article 6 : Mitigation (Protection contre les attaques DOS et DDOS) – OVH**

#### **Objet : Résumé des protections OVH contre les attaques DOS et DDOS**

OVH propose une protection pour ses clients contre les attaques DOS (Denial of Service) et DDOS (Distributed Denial of Service). Ces attaques cherchent à rendre un site ou service inaccessible en surchargeant les serveurs avec un trafic massif. Voici ce qu’il faut savoir sur cette protection :

### **1. Comment fonctionne cette protection ?**

OVH vérifie le trafic entrant vers votre service. Si le trafic provient d'une attaque (DOS ou DDOS), il est bloqué avant d'atteindre votre infrastructure. Cela permet aux utilisateurs légitimes d’accéder normalement au service, même pendant l’attaque.

### **2. Limites de la protection :**

* **Types d'attaques couvertes** : Cette protection ne protège que contre les attaques DOS et DDOS. Elle ne couvre pas d'autres attaques comme celles visant à exploiter des failles de sécurité (ex : injections SQL).
* **Activation de la protection** : La protection se déclenche seulement après que l'attaque ait été détectée. Cela signifie qu’avant cette détection, votre service peut être temporairement **hors ligne**.
* **Efficacité variable** : OVH fait tout son possible pour bloquer l'attaque, mais il n'y a aucune garantie que l'attaque sera complètement stoppée. Le système de protection dépend aussi de la configuration de votre service.

### **3. Durée de la protection :**

La protection reste active **jusqu'à ce que l’attaque soit terminée** ou que OVH n’identifie plus de trafic suspect. Cependant, pendant cette période, OVH ne peut pas garantir que votre service restera **pleinement accessible**.

### **4. Impact sur le service :**

* **Possible dégradation du service** : Si l'attaque est trop forte ou menace les serveurs d'OVH, cela peut affecter la performance de votre service.
* **Partie du trafic non détectée** : Certains éléments de l’attaque pourraient ne pas être détectés, ce qui pourrait encore perturber votre service.

### **5. Responsabilité du client :**

* **Sécurisation de votre service** : La protection d'OVH ne remplace pas la nécessité pour vous de sécuriser votre propre service (pare-feu, mises à jour, sauvegardes, etc.).
* **Activation anticipée** : Vous pouvez activer cette protection avant même d'être attaqué, mais cela peut parfois **affecter la qualité** de votre service.

### **Conclusion :**

La protection contre les attaques DOS et DDOS fournie par OVH est utile pour maintenir la disponibilité de votre service en cas d'attaque, mais elle a des limites. Il est essentiel que vous continuiez à sécuriser votre propre infrastructure et que vous compreniez que la protection ne garantit pas une disponibilité totale pendant toute l'attaque.

### **Pourquoi choisir l'article 6 ?**

1. **Importance croissante des attaques DDoS** :  
   Les attaques DoS et DDoS sont l'une des menaces majeures pour les services en ligne, affectant gravement la disponibilité des serveurs et l’expérience utilisateur. Expliquer comment OVH atténue ces attaques est crucial pour garantir la sécurité et la continuité des activités des entreprises clientes.
2. **Technologie complexe mais essentielle** :  
   La **mitigation** est un sujet technique qui peut être déroutant pour des non-experts. Une note claire avec des schémas et des exemples pratiques aiderait à illustrer comment OVH filtre le trafic malveillant tout en préservant l'accès légitime.
3. **Enjeux pour les entreprises** :
   * **Avantages** : La mitigation garantit un service continu, protégeant la réputation de l’entreprise et réduisant les pertes économiques liées à l’indisponibilité.
   * **Limites** : Le caractère réactif (activation après détection) peut entraîner des temps de latence. En outre, OVH n’assume qu’une obligation de moyens.
4. **Sensibilisation nécessaire** :  
   Cet article rappelle au client qu’il reste responsable de la sécurisation de son infrastructure (pare-feu, mises à jour). C’est un point clé pour éviter les malentendus sur les responsabilités respectives.

### **Proposition de contenu pour une note explicative**

Une note sur cet article pourrait inclure :

* **Définition et types d’attaques DoS/DDoS** : Explication des concepts pour clarifier les risques.
* **Principe de la mitigation** : Schéma simplifié du filtrage de trafic illégitime.
* **Exemple concret** : Cas où une entreprise subit une attaque et la manière dont OVH y répond.
* **Avantages pour les entreprises** : Maintien de l’activité malgré une attaque.
* **Limites et responsabilités du client** : Importance des mesures internes (pare-feu, monitoring).

En résumé, l'article 6 permet d’aborder un sujet stratégique pour les entreprises, combinant des aspects techniques et organisationnels. Cela le rend pertinent à développer dans une note explicative. Si ce choix vous convient, je peux rédiger cette note avec des schémas et des détails.

### **1. Sujet moins stratégique que la sécurité**

* L’article 7 concerne principalement la gestion de la disponibilité et les dédommagements liés aux incidents. Bien que cela soit important, ce sujet est moins critique que la gestion des attaques DDoS, qui représentent une menace directe à la continuité des activités.
* La sécurité (article 6) est un enjeu primordial dans le contexte actuel des cyberattaques croissantes. L'impact d’une attaque DDoS est plus immédiat et visible qu’un SLA légèrement non respecté.

### **2. Moins de technicité à expliquer**

* Les engagements SLA décrits dans l’article 7 sont surtout contractuels, avec des définitions claires et des calculs simples (par exemple, pourcentage de crédits appliqués en cas d’indisponibilité). Cela nécessite peu d'explications techniques.
* En revanche, l’article 6 implique des concepts complexes comme la mitigation, le filtrage de trafic et les techniques de défense réseau, qui nécessitent davantage de vulgarisation et de mise en contexte pour être bien compris.

### **3. Focus sur la prévention plutôt que sur la compensation**

* L’article 7 est réactif : il décrit des dédommagements après une défaillance du service, ce qui ne résout pas le problème initial.
* L’article 6 est proactif : il montre comment OVH anticipe et atténue des problèmes graves avant qu’ils n’impactent gravement le service.

### **4. Moins d’interaction directe avec les clients**

* Dans l’article 7, le client joue un rôle passif : signaler un problème et attendre une intervention ou un dédommagement.
* L’article 6 met en lumière une collaboration entre OVH et le client, notamment en insistant sur la configuration adéquate de son infrastructure et l’importance de ses propres outils de sécurité.

### **5. Complexité contractuelle de l’article 7**

* L’article 7 contient des notions juridiques précises (limites des dédommagements, exclusions, etc.), qui sont moins liées aux compétences informatiques. Une explication exhaustive nécessiterait davantage d’expertise juridique qu’informatique.
* En revanche, l’article 6 se concentre sur des mécanismes informatiques, où une compétence technique est plus utile.

### **Conclusion**

Bien que l’article 7 soit important pour établir une confiance contractuelle entre OVH et ses clients, l’article 6 aborde un enjeu technique et stratégique bien plus crucial : la protection contre les cyberattaques. Cela justifie mon choix de prioriser l’article 6 pour une note explicative.