# Choix d'outils non-institutionnels et RGPD

Fiche information

## Pourquoi ?

En dehors des outils numériques fournis par l'institution dans le cadre professionnel (*Big Blue Button*, *File Sender*, *Tribu* …), les enseignants sont régulièrement amenés à les compléter par des outils (ou ressources) en ligne dont ils perçoivent un fort potentiel pédagogique.

**Il faut s'assurer que ces solutions restent garantes de la protection des données des élèves**.

Adaptée du travail du DPD de l'académie d'Aix-Marseille, nous vous proposons cette fiche qui vous permettra d'évaluer, en première approche, la conformité des applications non-institutionnelles utilisées dans le cadre du numérique éducatif par rapport au RGPD.

## Comment ?

**Une vision globale des différentes étapes de la démarche vous est proposée en annexe, sous la forme d'une infographie.**

Cette méthode, simple, permettra d'identifier assez rapidement les points où la protection des données porte problème. Quelques outils seront proposés (traceur de cookies, base de donnée de conditions de service analysées …)

Des explications et lexiques sont proposés ci-dessous. Des exemples sont souvent utilisés pour illustrer les différentes étapes du processus.

## 1 Données à caractère personnel … Quid ?

Au cœur du Règlement Général pour la Protection des Données : les fameuses Données à Caractère Personnel (DCP) :

> DCP : *informations qui se rapportent à une personne, identifiée ou identifiable directement ou indirectement (par croisement de données par exemple).*

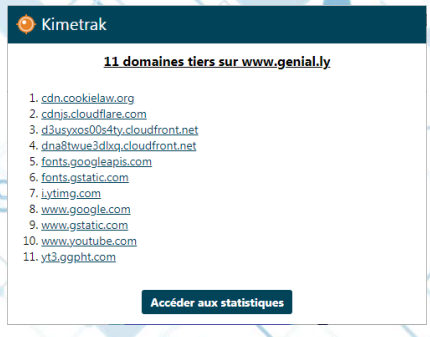
- nom, prénom, pseudonyme, date de naissance;
- photos, enregistrements sonores de voix;
- numéro de téléphone fixe ou portable, adresse postale, adresse email;
- adresse IP, identifiant de connexion informatique ou identifiant de cookie;
- empreinte digitale, réseau veineux ou palmaire de la main, empreinte rétinienne;
- numéro de plaque d'immatriculation, de sécurité sociale, d'une pièce d'identité;
- données d'usage d'une application, commentaires, etc.

Attention aux cookies, ces petits fichiers générés lors de la consultation de nombreux sites, bien souvent gourmands et peu respectueux des DCP, et aux Pixels espions (ou ‹‹pixel tab››, pixel invisible etc.).

Il est possible d'utiliser des extensions de navigateurs (*Kimetrak*, *Cookieviz* …) permettant de visualiser la « galaxie » de cookies créés sur le navigateur du client. Plus la liste est longue, moins le diagnostic sera bon.

**Vérifier le moyen, le cas échéant, de s'opposer au dépôt des cookies**. Notamment via la présence d'un bandeau permettant de refuser tous les cookies, ou de paramétrer à la seule utilisation des cookies strictement nécessaires.

*Exemple* : *Cookies* déposés sur Genially




*Exemple* : *Pixel Tags* sur Kahoot !

> Using pixel tags and other similar technologies: Pixel tags (also known as web beacons and clear GIFs) may be used in connection with some Services to, among other things, track the actions of users of the Services (including adult accountholders that may receive emails from us), measure the

success of marketing campaigns and compile statistics about usage of the Services and response rates.

## 2 Où sont stockées/traitées les DCP ?

Les données restent elles dans un pays adéquat (stockage, traitement, transfert, accès extraterritoriaux)?

Les pays au travers du monde n'offrent pas les mêmes garanties en termes de protection des données et des droits fondamentaux des personnes concernées.

*Pays adéquats :* *Pays membre de L'UE ou de l'EEE , Grande Bretagne, Andorre, Argentine, les îles Féroé, Guernesey, Israël, l'île de Man, Japon, Jersey, Nouvelle-Zélande, Suisse et Uruguay. Le Canada est en adéquation partielle.*

*Pays non adéquats :* *Les transferts de données vers des pays non adéquats nécessitent la mise en place de mesures techniques, organisationnelles et contractuelles spécifiques.*

Comment obtenir ce genre de renseignements ?

- **Rechercher le nom de la société/ressource dans un moteur de recherche**

  *Exemple* : « Quizlet » saisi dans un moteur de recherche
  ⇨ Siège social : San Francisco, Californie, États-Unis *(pays non adéquat)*

- **Rechercher dans les Conditions Générales d'Utilisation (CGU) les éléments faisant références à l'hébergement et aux transferts.**

  *Exemple de non-conformité* : CGU de Quizlet

  Transferts internationaux de données

  Bien que Quizlet opère à l'échelle internationale, bon nombre de nos systèmes sont basés aux États-Unis *(pays non adéquat)*, où les normes de protection des données sont différentes de celles de l'Union européenne.

  *Exemple de non-conformité* : CGU de Padlet

  15. Special Provisions for Subscribers Located Outside of the United States

  Padlet provides global products and services and enables a global community for individuals to share and follow the things they love. Padlet's operations are, however, located in the United States, and Padlet's policies and procedures are based on United States law. As such, the following provisions apply specifically to Subscribers located outside of the United States: (1) you consent to the transfer, storage, and processing of your information, including but not limited to Subscriber Content and any personal information, to and in the United States and/or other countries;[…]

  *Exemple de non-conformité* : CGU de Kahoot!

  CROSS-BORDER TRANSFER

  Your Personal Information may be stored and processed in any country where we have facilities or in which we engage service providers, and by using the Services you understand that your information will be transferred to countries outside of your country of residence, which may have data protection rules that are different from those of your country.

  If you are located in the European Economic Area ("EEA"): Some of the non-EEA countries are recognized by the European Commission as providing an adequate level of data protection according to EEA standards (the full list of these countries is available here). For transfers from the EEA to countries not considered adequate by the European Commission, we have put in place adequate measures, such as standard contractual clauses *(Privacy Shield invalidé en août 2020)* adopted by the European Commission to protect your Personal Information. You may obtain a copy of these measures by contacting us (see below under Contacting Us).

**Attention,** un hébergement en UE n'est pas forcément gage de sécurité. En effet :

- l'accès à des données hébergées en Europe à partir d'un pays non européen est un transfert hors UE.
- Si l'hébergement dans un pays adéquat est opéré par une société non européenne, celle-ci ne doit pas être soumise à une législation avec une portée extraterritoriale, comme c'est le cas pour les sociétés américaines.

## 3 CGU modifiables unilatéralement ?

**Rechercher dans les conditions générales les modalités de leur mise à jour.**

Si les conditions d'utilisation de la solution sont modifiables unilatéralement, il faut vérifier que l'utilisateur en sera notifié et qu'il aura la possibilité, soit de refuser des modifications impliquant les DCP des élèves, soit de stopper leur traitement afin de rester en conformité avec le RGPD.

*Exemple de non-conformité* : CGU de Kahoot !

> The current Acceptable Use Policy is available here: https://kahoot.com/terms-and-conditions/#acceptable-use. We reserve the right to change the Acceptable Use Policy at any time without notice.

*Exemple de non-conformité* : CGU de Genially

> GENIALLY se réserve le droit de modifier ou de mettre à jour les Conditions Générales d'Utilisation à tout moment et sans préavis, en raison d'obligations légales, de motifs techniques, de changements dans les services offerts par GENIALLY ou de décisions stratégiques de la société, en modifiant ou en mettant à jour le texte accessible aux Utilisateurs dans les présentes Conditions Générales d'Utilisation. C'est la raison pour laquelle il est conseillé aux Utilisateurs de les lire régulièrement.

## 4 Données collectées vraiment nécessaires ?

Il est possible de collecter des données, lorsque la finalité l'impose, mais uniquement celles nécessaires.

Par exemple, un simple site proposant des exercices dans une matière demande le nom, prénom, numéro de téléphone, âge et adresse mail d'un élève avec l'astérisque rouge indiquant l'obligation de renseigner le champ lors de la création du compte utilisateur. La plupart de ces informations sont superflues, voire intrusives, et ne devraient pas être collectées.

- **Rechercher la liste des données collectées dans les CGU et dans la politique de protection des données.**

  La liste des données utilisées par l'application figure généralement dans les CGU ou dans la politique de confidentialité du site. Si elles sont en grand nombre ou si elles ne correspondent que très peu à l'objectif poursuivi, le pronostic n'est pas bon.

- **Consulter les différentes interfaces de l'application et les données obligatoires récoltées.**

## 5 Quel(s) traitement(s) des données ?

*Le(s) traitement(s) fait(s) sur les données collectées doivent se limiter à ce qui est strictement nécessaire du point de vue de l'utilisation pédagogique de l'outil en ligne.*

Il est possible d'utiliser le site http://tosdr.org ou son extension de navigateur, qui propose pour plusieurs ressources en ligne une note de confidentialité allant A à E. Le site propose une synthèse des analyses réalisées par des contributeurs éclairés.

- **Rechercher dans les conditions générales d'utilisations les traitements qui pourraient être effectués sur les données.**

La lecture des CGU peut parfois être très éclairante sur les traitements effectués sur les données récoltées, notamment sur l'éventuelle utilisation commerciale de ces données ou des traces laissées lors de la consultation de la ressource en ligne (cookies et pixels invisibles).

*Exemple de non-conformité* : CGU de Facebook

> We use the information we have to deliver our Products, including to personalize features and content including your News Feed, Instagram Feed, Instagram Stories and ads and make suggestions for you (such as groups or events you may be interested in or topics you may want to follow) on and off our Products. To create personalized Products that are unique and relevant to you, we use your connections, preferences, interests and activities based on the data we collect and learn from you and others […]

- **Consulter les différents modules et/ou interfaces de l'application en ligne et les fonctionnalités qu'ils proposent.**

## 6 Données conservées combien de temps ?

*La règle est que les données ne doivent pas être conservées au-delà de la durée nécessaire à l'activité pédagogique.*

La suppression doit être soit automatique, soit possible de façon manuelle. Dans ce dernier cas, ne pas omettre de le noter - pour renseigner le registre de traitement - et de relever la procédure de suppression pour être en mesure de la mettre en œuvre en temps utiles.

- **Rechercher les informations relatives aux durées de conservation dans les CGU et dans la documentation.**

  Porter attention notamment aux modalités de fermeture des comptes et aux engagements associés quant à la suppression des données.

## 7 Qui a accès aux données ?

*Seules les personnes définies dans le cadre du projet pédagogique et sur le domaine les concernant doivent pouvoir accéder aux données.*

- **Consulter la documentation de l'application, les CGU et les différentes interfaces proposées (selon le type d'utilisateurs).**

  Il est nécessaire que ces éléments soient en adéquation avec le projet pédagogique tel que vous l'avez défini.

# 1er niveau atteint !

Les analyses postérieures vont porter sur une analyse encore plus fine des CGU et de la politique de confidentialité de la ressource en ligne, et des conditions de sécurité des données. Vous pouvez vous rapprocher du DPD pour ces étapes.

**RAPPEL** toute utilisation de ressource numérique doit être faite avec l'accord des Responsables de traitements, c'est-à-dire le chef d'établissement dans les EPLE, selon les modalités d'organisation qu'ils ont définies.

# Fiche information