

# GESTE

Les éditeurs de contenus et services en ligne

Webinar Q&R CNIL / GESTE - 19 janvier 2022

\*Document réservé aux seuls membres du GESTE\*

# SOMMAIRE

|  |    |
|--|----|
| TRANSFERTS DE DONNÉES HORS UE                          | 3  |
| MESURE D'AUDIENCE                                      | 11 |
| RESPONSABILITÉ DES ACTEURS ET QUALIFICATION (RT/ST/RC) | 15 |
| COOKIES ET TRACEURS                                    | 18 |
| TCF  | 26 |
| AUTRES   | 28 |



## TRANSFERTS DE DONNÉES HORS UE

*Les réponses apportées sont générales et doivent systématiquement faire l'objet d'une analyse casuistique.*

***En présence de transferts de données personnelles à encadrer, la réponse négative du sous-traitant (ST) à l'existence de transferts est-elle suffisante pour écarter la responsabilité du responsable de traitement (RT) en cas de réponse erronée ? Sinon, comment se prémunir de ce risque ?***

- ❖ Le RT doit documenter par écrit, l'ensemble des éléments communiqués par son ST. L'objectif est de se prémunir du risque, et de bien comprendre ce que fait le ST ultérieur du ST initial.
- ❖ L'article [28.3.h du RGPD](#) prévoit la réalisation d'audits (qui peut être documentaire), y compris des inspections par le RT ou un autre éditeur qu'il a mandaté. Dans ce cadre → mise à disposition par le ST de toutes les informations nécessaires pour démontrer le respect des obligations, y compris en matière de transfert.
- ❖ Il y a souvent un déséquilibre entre RT et ST ou entre plusieurs RT, il est donc complexe d'obtenir toutes les informations nécessaires de la part d'un ST surtout lorsqu'il est en position de force. L'article 28 vise à redonner du pouvoir au RT pour le mettre en mesure d'obtenir les informations qu'il est en droit d'obtenir.

→ Voir le guide de l'Autorité danoise de protection des données qui donne une grille de lecture aux responsables de traitement dans leur relation avec les ST en fonction de plusieurs paramètres, et notamment du risque de chaque traitement (approche par les risques): <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2021/okt/ny-vejledning-saadan-kan-du-foere-tilsyn-med-dine-databehandlere->

*Lorsqu'un sous-traitant ultérieur importe des données personnelles dans un pays non membre de l'EEA et ne faisant pas l'objet d'une décision d'adéquation, le responsable de traitement doit-il signer des CCT ou bien celles-ci doivent être signées entre le sous-traitant et le sous-traitant ultérieur ? Si le responsable de traitement doit les signer, doit-il les signer avec son sous-traitant ou bien avec les sous-traitants ultérieurs ?*

### Cas de figure 1 :

- ❖ Le RT est dans l'UE ;
  - ❖ Le ST initial est dans l'UE et soumis au RGPD et décide de transférer les données UE vers un ST ultérieur hors UE
- Dans ce cas, le transfert a lieu entre le ST initial et le ST ultérieur. L'outil contractuel est le module 3 des [CCT](#) de la commission. Le ST initial sera l'exportateur, le ST ultérieur sera l'importateur. Ce module précise bien la notion "d'instructions documentées" du RT.

### Cas de figure 2 : le ST initial est hors UE

- ❖ C'est au RT de signer avec le ST initial (clause 09 des CCT)

En tout état de cause, c'est toujours le RT qui doit autoriser le recours à des ST ultérieurs. La protection doit être assurée sur tout le trajet de la donnée. Il est important de bien cartographier les flux ([voir doc CNIL sur la cartographie des flux.](#))

***Que faire si un partenaire/ST situé hors UE refuse de communiquer ses mesures techniques et organisationnelles (MTO) ou refuse de modifier ses conditions générales ? (contrat d'adhésion)***

- ❖ Voir les [lignes directrices du CEPD RT/ST](#) sur les contrats d'adhésion (paragraphe 30) : Le contrat d'adhésion ne déresponsabilise par le RT, qui reste libre de choisir avec qui il contractualise.
- ❖ Si le ST refuse de partager ses MTO dans ce cas le RT n'est pas en mesure de s'assurer que son ST présente des garanties suffisantes.

Toutefois, contrairement à l'ère pré-RGDP, le ST a une part de responsabilité (article 28 du RGPD). Dans ses contrôles, la CNIL analysera dans le chef de quel acteur le manquement pourrait être retenu (notamment au regard de l'article 28 du RGPD), en tenant compte de la pratique et des rapports de force.

*Une liste identifiant le niveau de risque par pays va-t-elle être élaborée au niveau européen ? (ex : risque élevé si les autorités publiques ont accès aux données des entreprises nationales)*

- ❖ Non pas à ce stade.
- ❖ Analyse au cas par cas réalisée par le RT (principe de responsabilisation) : Cette analyse dépend de données factuelles (types de données (sensibles ou non), types de traitements..).
- ❖ Cependant de nombreuses ressources existent (cnil.fr, site de l'EDPB)
  - L'EDPB a détaillé les mesures supplémentaires susceptibles d'être mises en oeuvre pour encadrer les transferts de données à destination d'Etat n'assurant pas un niveau de protection suffisant ([Recommandation 01/2020](#)).
  - L'EDPB a récemment publié une étude externe qui [analyse la législation de la Chine, de l'Inde et de la Russie](#).
  - La CNIL a publié une [carte de la protection des données dans le monde](#).
- ❖ Le GESTE, en tant que tête de réseau avec des entreprises ayant les mêmes problématiques (même traitements, finalités similaires, même pays concernés), pourrait mener un travail de centralisation.

Pour le moment les autorités ont priorisé leurs travaux sur les mesures complémentaires plutôt qu'une analyse de toutes les législations.

*Quelles sont les recommandations de la CNIL pour limiter l'impact extraterritorial des lois américaines sur les données traitées par des sociétés dans l'UE (Cloud Act, programmes de surveillance fondés sur l'article 702 du "Foreign Intelligence Surveillance Act" (FISA) et l' "Executive Order (EO) 12333") ?*

- ❖ Pour limiter le risque : recourir à des prestataires qui entreposent les données au sein de l'UE, exclusivement soumis au droit de l'UE et qui ne les transfèrent pas vers un pays qui ne présente pas les garanties suffisantes OU recourir à des mesures supplémentaires (voir la liste de l'EDPB qui n'est pas exhaustive : d'autres solutions peuvent être présentées aux autorités de protection des données).
- ❖ A noter, l'EDPB n'a pas encore identifié de solution quand le prestataire doit impérativement accéder aux données en clair (lorsqu'il possède la clef de déchiffrement) comme par exemple dans des opérations de maintenance.
- ❖ Cloud act : Voir la [position de l'EDPB](#).



## *Jusqu'à quel niveau le RT doit-il contrôler les MTO mises en place par ses partenaires ?*

- *Est-ce que la signature d'un contrat de sous-traitance listant les MTO et dans lequel le ST s'engage à répercuter le niveau de sécurité sur ses sous-traitants ultérieurs suffit ?*
- *Ou est-ce que le RT doit lui-même s'assurer des MTO mises en place par toute la chaîne de traitement ? (ST + ST ultérieurs)*
- ❖ Audits / inspections prévus dans l'article 28(3)(h) du RGPD : le RT doit garder la main sur toute l'étendue du transfert.
- ❖ [Lignes directrices RT/ST](#) paragraphe 152 qui précisent comment le RT doit autoriser les ST ultérieurs.

*Les questionnaires adressés par les RT ne sont pas harmonisés, leur complétude est donc très chronophage. Est-ce qu'une documentation harmonisée est prévue par la CNIL ?*

- ❖ Non, pas à ce jour, car il s'agit d'une analyse casuistique et le sujet n'est pas spécifique à la protection des données.
- ❖ Peut être réalisé au niveau du GESTE (car activités / traitements / finalités similaires) en sollicitant, le cas échéant, la CNIL.

*Que risque un responsable du traitement qui n'est pas en mesure de produire l'analyse/ évaluation du droit américain en cas de contrôle CNIL relatif à un traitement des données opéré vers les Etats-Unis ou autre pays ne bénéficiant pas de décisions d'adéquation, prévue au point 2.3 "Step 3 Assess whether the article 46 GDPR [...]" des recommandations du CEPD 01/ 2020, version 2.0 adoptées le 18 juin 2021 ?*

- ❖ Focus sur la [décision de la DPA Autrichienne](#) qui indique en substance que le recours à Google Analytics entraîne un transfert illégal de données vers les USA en violation du RGPD. Cette décision s'intègre dans un contexte plus large de 101 plaintes déposées devant les DPA européennes.



## MESURE D'AUDIENCE

*Google aurait déposé plusieurs dossiers afin de faire certifier des versions de Google Analytics au titre de la mesure d'audience exemptée. A quelle date pouvons-nous espérer une réponse sur ces dossiers ?*

- ❖ Google a déposé un unique dossier dans le cadre du programme d'identification des solutions de mesure d'audience pouvant se passer de consentement.
- ❖ Les dossiers sont traités dans l'ordre de la réception, et celui de Google fait partie des derniers soumis.
- ❖ Le dossier sera traité de la même manière que les autres dossiers et sera le cas échéant inscrit sur la liste des outils exemptés lorsque les garanties nécessaires auront été apportées.

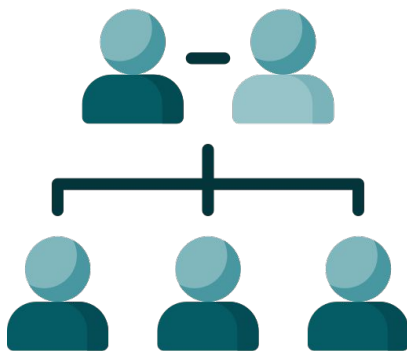
### *Quid du traitement par la CNIL des tiers de confiance mesureurs (comme l'ACPM / Médiamétrie), un régime dérogatoire est-il prévu ?*

- ❖ Pas de régime dérogatoire, mais un travail d'accompagnement pour déterminer les mesures qui permettent de préserver la capacité à fournir des métriques fiables sans sortir du cadre de la mesure d'audience exemptée.
- ❖ La CNIL envisage deux pistes:
- ❖ Première: s'assurer du statut de ST des tiers mesureurs, sans destinataire de données centralisées à travers le web (donc pas de traçage à travers différents sites).
- ❖ Seconde: méthode d'anonymisation des données (qui doit dans le même temps permettre d'assurer une certification fiable) → [les guidelines de 2014 de l'EDPB](#) relatives à l'anonymisation sont en cours de révision.
- ❖ Les travaux sont en cours, il revient à ces acteurs le soin d'informer leurs clients des éventuelles mises à jour qui permettent de rentrer dans ce cadre.

**Quelles actions/démarches l'éditeur doit-il entreprendre si son sous-traitant utilise un cookie multi-finalités pour la mesure d'audience exemptée ?**

- ❖ La question posée semble être celle des "mesures hybrides" qui fonctionnent différemment en cas de consentement ou en son absence.
- ❖ Il s'agit d'un choix technique du prestataire (pas d'obligations particulières de la CNIL), mais qui présente certains risques de mauvaise configuration, notamment du fait de la difficulté du contrôle du respect de l'absence de consentement si un unique traceur est utilisé sans signal facilement lisible par le RT sur la typologie de mesure d'audience.

→ Ce cas se présente notamment sur l'environnement mobile où il y a un identifiant pour plusieurs finalités : il faut donc soit avoir la capacité à désactiver les usages le nécessitant en l'absence de consentement, soit soumettre l'usage de l'identifiant au consentement.



## RESPONSABILITÉ DES ACTEURS ET QUALIFICATION (RT/ST/RC)

***Une société-mère peut-elle être le sous-traitant d'une filiale dans le cadre d'un service commercialisé par la filiale ou est-ce que son statut de société-mère l'empêche-t-il de recevoir des instructions de sa filiale ?***

- ❖ Oui : rien ne l'interdit par principe, il faut faire une analyse au cas par cas (finalité, qui donne les instructions etc..). Dans les lignes directrices RT/ST, il y a un exemple qui reprend ce cas.
- ❖ Analyse capitalistique de la société mère du point de vue du droit des sociétés est différente de la grille de responsabilité en vertu du droit des données à caractère personnel.

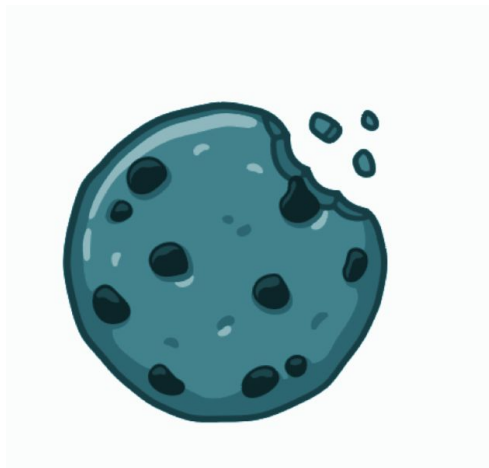
***Dans le cas où société-mère et filiale sont des responsables conjoints du traitement, le traitement doit-il figurer dans :***

- *le registre de la société-mère uniquement, dans la mesure où elle joue un rôle plus prépondérant que la filiale dans la détermination des moyens, ou*
- *le registre de la société-mère **et** le registre de la filiale?*
- ❖ Au terme de [l'article 30 du RGPD](#), le registre doit être tenu par "chaque responsable du traitement" donc par chaque RT conjoint ; ici tant par la société mère que par la filiale.
- ❖ Conjoint ne veut pas dire "solidaire".



*En cas de désaccord sur la qualification (RT / ST), peut-on prévoir uniquement un contrat définissant les obligations de chaque partie / La définition et la qualification des parties est-elle indispensable si les obligations de chaque partie sont bien définies dans un DPA ?*

- ❖ La CNIL soulève ce point: il n'est pas certain que ce contrat puisse satisfaire les critères de l'article 2. Quid par exemple de la désignation de ST ultérieur ? Qui peut le désigner si pas de qualification arrêtée ?
- ❖ Le strict minimum est de définir les obligations et les responsabilités de chacun. La limite et la complexité est qu'un ST ne peut agir que sur instruction. La CNIL va dûment tenir compte de la répartition des rôles de chacun des acteurs et voir si in fine les personnes concernées par le traitement sont bien protégées. Les contrôles peuvent parfois aboutir à des requalifications (impact sur les relations contractuelles, commerciales des acteurs) sans pour autant faire l'objet de sanction.
- ❖ Les guidelines de l'EDPB apportent des éléments de réponse.



## COOKIES ET TRACEURS

**Exemption AB test: Les derniers éléments fournis par la CNIL pouvaient laisser penser qu'il était possible de réaliser des AB tests basiques (ex: quelle version d'une page produit génère le plus de clics) sans avoir besoin du consentement des personnes pour le dépôt des cookies d'AB test. Pourrait-on avoir des éclaircissements à ce propos ?**

- ❖ Dans l'absolu, la CNIL n'exclue pas qu'une finalité strictement nécessaire puisse être poursuivie via un procédé technique tel que l'AB test.
- ❖ L'AB test doit permettre d'évaluer le fait qu'on puisse bien rendre le service demandé par la personne.
- ❖ A titre d'exemple:
  - si la finalité poursuivie consiste à tester les performances de deux solutions de paiement afin d'évaluer celle qui fonctionne le mieux (provoque le moins d'erreurs techniques), les traceurs de tests A/B pourraient être considérés comme strictement nécessaires à un service expressément demandé par l'utilisateur.
  - tester et comparer l'audience d'un site dans une version 1 vs. version 2 (avec mesure d'audience exemptée)? il faut analyser la finalité. S'il s'agit de mesurer la performance de contenu à des fins marketing : pas d'exemptions car ce n'est plus strictement nécessaire au service demandé par l'utilisateur.

*Certains opérateurs nous imposent des pop in de consentement supplémentaires qui se superposent aux CMP et qui n'ont pas pour objectif de répondre à des obligations légales mais uniquement aux règles fixées dans leurs propres CGU. Ces pop in se déclenchent en général juste avant ou juste après la présentation de la CMP, ce qui revient à solliciter l'utilisateur de nouveau dans un laps de temps très court, en contradiction avec la doctrine de la CNIL sur l'enregistrement de la durée des choix et ses positions sur la consent fatigue. Qu'en pense la CNIL ?*

- ❖ Ces pop in ne sont pas stricto sensu des pop in de consentement, il n'y a donc pas de contradiction avec la recommandation de la CNIL.

***Cross-device : Pouvez-vous confirmer que les choix relatifs aux traceurs faits via une CMP peuvent être répercutés sur plusieurs terminaux où les utilisateurs sont logés tant qu'ils sont informés de la portée de leur consentement au moment du choix ? (i.e. qu'il ne faut pas demander un consentement distinct aux utilisateurs avec qui l'on a une relation contractuelle pour le cross-device).***

- ❖ Rappel principe : le fait que les utilisateurs soient authentifiés ne dispense pas de recueillir leur consentement conformément à l'article 82 de la loi « Informatique et Libertés », dès lors que des traceurs soumis au consentement sont utilisés ;
- ❖ La lettre de [l'article 82 de la LIL](#) : “un consentement par équipement terminal.”
- ❖ Dans la pratique un panneau de configuration associé au compte, si la portée en termes de terminaux est claire peut permettre une configuration cross-device des préférences. Cependant, les difficultés opérationnelles et d'interface d'un tel dispositif le rendent très complexe à mettre en œuvre de manière claire pour l'utilisateur.
- ❖ Exemple : Un utilisateur est logé sur son terminal, puis se connecte sur un autre device, établit une préférence et se loge. Quelle est la préférence exprimée qui va prendre le pas sur l'autre ? Cela peut être complexe pour l'utilisateur. Attention aux darks patterns.

## La CNIL envisage - t-elle de faire évoluer sa recommandation en matière de cookies/ traceurs du 17 septembre 2020 ?

- ❖ Pas à ce jour ;
- ❖ En revanche, la CNIL fait évoluer régulièrement sa [FAQ « cookies et autres traceurs »](#) qui vient compléter ses outils afin de mieux répondre aux questions les plus fréquemment posées par les professionnels et le grand public ;
- ❖ La CNIL s'investit sur ce sujet, à plusieurs égards :
  - Accompagnement : investissement de la CNIL au niveau national et au sein du collectif européen ;
  - Répressif : thématique du programme annuel des contrôles 2021 (nombreuses MED, sanctions, etc.).

→ L'exigence de permettre un refus aussi facile que l'acceptation implique qu'une modalité claire de refus soit proposée sur le même niveau d'interface que l'acceptation: le bouton « tout refuser » n'est pas une obligation (d'autres alternatives sont possibles) mais constitue un moyen clair pour l'utilisateur qui souhaite refuser. Attention aux « dark patterns ».

→ L'interprétation des [lignes directrices](#) et [recommandations](#) est constante. A titre de préconisation, la CNIL encourage les acteurs à mettre en place un bouton de refus au même niveau. La figure 5 (continuer sans accepter) est toujours autorisée par la CNIL. Attention toutefois aux darks patterns.

→ La task force sur les « dark patterns » de l'EDPB clarifiera ce point.

*A la lecture combinée de la [décision « LE FIGARO »](#) et de la décision « GOOGLE », l'éditeur sera-t-il considéré comme responsable si un tiers continue à lire un cookie ayant pour finalité le partage sur réseaux sociaux par exemple, alors que l'utilisateur a retiré a posteriori son consentement ? Si oui, quelles démarches doit-il entreprendre ?*

- ❖ Rappel du périmètre de la responsabilité : obligation de moyen (renforcée) qui implique qu'une mise en conformité puisse être atteinte par la mise en œuvre d'un ensemble d'aménagements nécessaires (mesures juridiques ou techniques) ; (Ex : dépôt de cookie suite au refus de l'utilisateur, continuer à lire le cookie déposé suite à un retrait du consentement) → [Jurisprudence constante Croque Futur](#)
- ❖ La responsabilité des éditeurs sur les cookies tiers n'a pas pour conséquence d'alléger les obligations de ces derniers qui ont une obligation de résultat sur leurs propres cookies (aussi bien les acteurs nationaux, qu'internationaux).
- ❖ Sur les démarches que l'éditeur peut entreprendre :
  - Prévoir des clauses contractuelles pour rompre de manière temporaire ou permanente les relations avec les acteurs qui ne respectent pas leurs obligations RGPD.
  - Prévoir des outils techniques pour s'assurer de manière plus automatisée du dépôt conforme de cookie tiers et de l'absence de lecture des cookies post-retrait du consentement.

***La CNIL a fourni des bonnes pratiques sur la durée de conservation des cookies. A l'issue du délai retenu par l'éditeur, faut-il également supprimer l'ID Cookie dans la DMP ? Autrement dit, peut-il y avoir une dissociation des durées de conservation des cookies et des données ?***

- ❖ Oui, c'est possible. Voir notamment la partie Mesure d'audience de la [Recommandation Cookies et autres traceurs](#).
- ❖ Les délais de conservations dans la recommandation de la CNIL portent sur la conservation des choix des personnes ;
- ❖ Les informations collectées par l'intermédiaire de ces traceurs peuvent être conservées pour une durée différente : il appartient au RT de faire une analyse en tenant compte de la finalité poursuivie et d'être transparent à l'égard des personnes concernées.



*Alternatives d'accès : comment pouvons-nous assurer de la conformité de nos projets auprès de la CNIL ? « projet » = privacy by design : nous aimerions pouvoir interroger la CNIL dès la phase de conception. Quels seraient les modalités et les délais ?*

La CNIL a rappelé la nécessité d'une analyse au cas par cas:

<https://www.cnil.fr/fr/cookie-walls-et-monetisation-des-donnees-personnelles-les-enjeux-juridiques-et-ethiques>

La CNIL a précisé sa doctrine dans une charte d'accompagnement:

<https://www.cnil.fr/fr/la-cnil-publie-sa-charte-daccompagnement-des-professionnels>

→ La CNIL souhaiterait publier plus d'informations d'ici quelques semaines pour exposer les critères devant nécessairement rentrer en compte dans l'analyse de l'implémentation d'une alternative d'accès. Cette analyse restera, en tout état de cause, au cas par cas.



TCF

*Afin d'utiliser certains prestataires de publicité contextuelle, nous sommes techniquement contraints par notre prestataire d'autoriser l'intérêt légitime dans l'IAB TCF (pour l'utilisation de l'adresse IP). Or, les prestataires de CMP ne nous permettent pas d'activer l'intérêt légitime de manière granulaire par Vendors (activation ou désactivation pour tous). Si nous décidions de l'activer pour tous, serions-nous responsable de l'utilisation faite par les vendors IAB TCF de l'intérêt légitime ?*

- ❖ Le sujet est identifié depuis longtemps par la CNIL, qui avait commencé des actions en termes d'accompagnement.
- ❖ Cependant, dans la mesure où une action contentieuse est en cours, la CNIL ne peut pas donner d'éléments sur ce dossier. Les apports de la CNIL sur le sujet se feront dans le cadre des procédures de coopération, qui sont strictement confidentielles.
- ❖ Il n'est donc pas permis à l'Autorité de faire de retours sur les travaux de l'APD ou les éventuels débouchés de ceux-ci.

*Actualisation : Décision de l'APD*

<https://www.autoriteprotectiondonnees.be/iab-europe-est-tenue-responsable-d-un-mecanisme-qui-viole-le-rgpd>

AUTRES

## Référentiels CNIL / Mooc

### *Quand le référentiel CNIL sur la gestion des données clients et des impayés sera-t-il publié ?*

- ❖ Publication des référentiels “gestion des activités commerciales” et “gestion des impayés” imminente;
- ❖ Le référentiel “gestion des activités commerciales” sera accompagné d’une mise à jour des contenus sur le site de la CNIL (notamment s’agissant des fiches relatives de la transmission des données à des partenaires commerciaux à des fins de prospection commerciale);
- ❖ La CNIL organisera des webinaires, sur le même modèle que ceux organisés suite à la publication des outils “cookies et autres traceurs” et continuera d’alimenter son site de fiche / FAQ pratiques.

Actualisation : <https://www.cnil.fr/fr/gestion-commerciale-et-gestion-des-impayees-la-cnil-publie-deux-nouveaux-referentiels>

## Référentiels CNIL / Mooc

*La CNIL prépare-t-elle actuellement un référentiel de durées de conservation, permettant de lier une activité de traitement à une durée et à un texte de référence? (le guide pratique sur l'archivage de juillet 2020 ne listant pas de durées).*

- ❖ La CNIL a publié, en parallèle du guide pratique sur les durées de conservation, certains référentiels de durées de conservation (dans le domaine de la santé ou encore RH);
- ❖ Elle poursuit ses efforts dans l'élaboration de référentiels spécifiques à certaines activités de traitements / certains acteurs;
- ❖ S'agissant des activités commerciales: référentiels "gestion des activités commerciales" projet de référentiel durée de conservation en matière de commerce / marketing (en cours);
- ❖ Ces référentiels doivent être vus comme des outils d'aide à la prise de décision qui orientent l'organisme vers les durées obligatoires ou recommandées pour les traitements couverts.

## Référentiels CNIL / Mooc

### *Quand sortira la nouvelle version du MOOC RGPD de la CNIL ?*

- ❖ Pas de calendrier à ce jour (remise à neuf, développement de nouveaux modules en cours);
- ❖ Disponible prochainement.

Projet de décision DPC

*Où en est la validation par l'EDPB du raisonnement et de la sanction appliqués à Facebook qui souhaite baser ses traitements de données de publicité ciblée sur le contrat plutôt que sur le consentement ?*

- ❖ Comme vous le savez, **les autorités de protection des données, au niveau européen, ont eu l'occasion de présenter leur(s) "objection(s) pertinente(s) et motivée(s)"** dans le délai prévu par le mécanisme de coopération ([article 60 du RGPD](#));
- ❖ **Le mécanisme de coopération** suit son cours au niveau européen sans qu'il ne soit possible aux services de la CNIL d'apporter des précisions complémentaires sur la procédure en cours.



Projet de décision DPC  
*Quel est l'avis de la CNIL sur le sujet ?*

- ❖ Sur la question de la validité de la base légale du contrat en matière publicitaire, la CNIL est en accord avec la position du Comité européen de la protection des données (EDPB) telle que formulée dans ses lignes directrices sur le contrat.
- ❖ Le consentement sera, en général, la base légale la plus appropriée dans le cadre des traitements mis en oeuvre à des fins publicitaires (notamment lorsque le traitement est intrusif, création d'un profil détaillé, croisement et enrichissement des données via des tiers, etc.)  
→ Plus large que l'utilisation des données collectée à partir de cookies.
- ❖ La CNIL estime que ces finalités ne peuvent pas être couvertes par l'exemption n°2 de l'article 82 de la LIL.
- ❖ En plus des travaux menés par les autorités de protection des données européennes, la CJUE a été saisie de questions préjudicielles sur des sujets similaires.