Analyse des recommandations du G29 sur la GDPR

Nous nous sommes intéressés aux recommandations du G29 sur la portabilité et les moyens de transmettre les données d'un responsable de traitement à un autre. Nous pensons que **les APIs sont, sauf dans de rares exceptions, le seul moyen d'être en conformité avec le texte de la GDPR.**

En effet, le texte impose que

> *« Lorsque la personne concernée exerce son droit à la portabilité des données en application du paragraphe 1, elle a le droit d'obtenir que les données à caractère personnel soient transmises directement d'un responsable de traitement à un autre lorsque cela est techniquement possible »*

Or, si cette transmission se fait **par voie numérique et sans intermédiaire, elle ne peut se faire que via une API.** En effet, par définition, la transmission automatisée et directe d'informations d'un responsable de traitement à un autre est une API, quelle que soit sa nature et le protocole qu'elle utilise (ftp, http, imap…).

D'autre part, les guidelines communiquées par le G29 insistent sur le fait que :

> *« Second, Article 20(1) provides data subjects with the right to transmit personal data from one data controller to another data controller « without hindrance » » (page 5)*

Le concept de « hindrance » réfère à une entrave, un frein, une gêne. « Without hindrance » signifie qu'il ne devrait pas y avoir de gêne inutile à la transmission de ces données d'un responsable de traitement à un autre. L'obstacle n'a pas besoin d'être infranchissable pour provoquer une gêne, et le fait de **ne pas ouvrir d'APIs induit une friction inutilement gênante pour le data subject. La généralisation et la banalisation des APIs dans l'état de l'art sont telles qu'un RT ne mettant pas en place une transmission par voie numérique - donc comme vu précédemment via une API - pour permettre la portabilité des données de ses utilisateurs ferait objectivement obstruction à l'exercice de ce droit,** qui est pensé dans les guidelines de la façon suivante :

> *« One specificity of data portability lies in the fact that it offers an easy way for data subjects to manage and reuse personal data themselves » (page 4)*

La portabilité a été pensée comme un droit de réutilisation de ses données personnelles : la commodité d'accès est donc déterminante dans l'exercice de ce droit.

Ainsi, nous pensons que le G29 pourrait insister sur la mise en place d'APIs qui sont presque toujours la solution adaptée pour permettre à l'individu d'exercer ses droits. Les recommandations du G29 pourraient être clarifiées en disant que :

> « For instance, they should offer a direct download opportunity for the data subject but should also allow data subjects to directly transmit the data to another data controller. ~~This could be implemented by making an API available~~ ; **In most cases, making an API available is the only way to guarantee a direct transmission and exceptions should be technically justified.**
> Data subjects may also with to use a personal data store or a trusted third party, to hold and store the personal data and grant permission to data controllers to access and process the personal data as required, so data can be transferred easily from one controller to another. If the data subject. **If the data subject wants his or her data transmitted without hindrance, APIs will be the expected mean to disclose his or her data and exceptions should be technically justified.** » (page 5)

Ces précisions nous paraissent d'autant plus importantes que **sans recommandations claires, les acteurs industriels risquent d'hésiter et de mettre en place des solutions diverses et non unifiées**, ce qui irait clairement contre l'esprit d'unification de la GDPR. Si les données sont dans

un format interopérable et machine readable mais qu'on ne peut pas ou difficilement les transmettre, l'intérêt de la portabilité risque d'être très limité… **Il faut donc clarifier la notion de « transfert direct » et d'« obstacle » pour qu'elles correspondent à la réalité du monde numérique d'aujourd'hui, où l'absence d'API pour un transfert direct de données est une aberration.**

Cosignataires publics :

Cozy Cloud

SNIPS

OpenDataSoft

MAIF

MEF - Mobile Ecosystem Forum

Meeco

Framasoft

Linxo

Budget Insight

Bankin

Fabernovel

PLOSS-RA (entreprises du numérique libre en Rhône-Alpes Auvergne)

Qwant - The search engine that respects your privacy

France Digitale

Innovacom

Digi.me

OVH

Antoine Petit (PDG d'INRIA et membre du CNNum)

Célia Zolynsky (Professeur à l'UVSQ - Paris Saclay, membre du CNNum)

Aevatar

Shopmium

CNLL

Benoit Thieulin (doyen de l'école du management et de l'innovation Science Po & DG de La Netscouade)

Nicolas Anciaux (responsable de l'équipe-projet PETRUS/INRIA)

UChange – Digital transformation platform

Yann Bonnet (Secrétaire Général du CNNum)

Inno3

Hugo Roy (co-auteur du User Data Manifesto)