Lignes directrices 07/2020 sur les notions de responsable de traitement et de sous-traitant dans le RGPD

Contribution de l'AFCDP

Note: This document has been originally written in French. An English version is provided below. It should be read with care, due to partially automatic translation.

L'Association Française des correspondants à la protection des données personnelles (AFCDP) a constitué en son sein un groupe de travail dédié à la relation de sous-traitance de données personnelles dont les travaux ont porté, en particulier, sur la qualification des acteurs et l'identification des difficultés au regard des retours d'expérience de ses membres.

Dans le cadre de l'ouverture à consultation publique des futures lignes directrices « responsable de traitement, sous-traitant, responsables de traitement conjoints », le présent document a pour objectif de transmettre au CEPD les principales questions soulevées par le groupe de travail de l'AFCDP.

I - La qualification des professions réglementées : si le CEPD conforte la position du G29 en ce que les prestataires de services demeurent des responsables de traitement (RT), ce principe ne comporte-t-il pas des limites dans certains cas spécifiques ? En effet, dans l'exemple visé par le CEPD, le cabinet d'avocats, pour mener à bien sa tâche, doit traiter les données personnelles liées à l'affaire, relevant de son mandat de conseil ou de représentation en justice, mais pas spécifiquement du traitement des données personnelles. Ne recevant pas d'instructions de son client dans le déploiement des traitements de données personnelles qu'implique la bonne réalisation de sa prestation, il revêt dans leur déploiement la qualification de responsable de traitement.

Les participants du groupe de travail relèvent des interrogations similaires s'agissant d'autres professions indépendantes réglementées tels que les notaires ou encore les experts comptables.

- Les membres du groupe de travail s'interrogent pour autant sur les limites de cette qualification : n'en serait-il pas autrement dans l'hypothèse où l'avocat serait amené, sur instructions précises de son client, à analyser à des fins spécifiques les bases de données qui lui sont fournies dans le cadre de sa prestation ? Ne deviendrait-il pas sous-traitant (ST) dans le cadre de cette prestation d'analyse de bases de données ?

II - La qualification des prestataires de services standardisés tels que les services CLOUD : cités en exemple par le CEPD, de tels services standardisés proposés par le prestataire ne le font pas basculer dans la qualification de responsable de traitement, en ce qu'il doit respecter les instructions spécifiques de son client : durées de conservation, éventuelles restrictions en matière de localisation…

À contrario cet exemple implique que, si les services sont standardisés au point notamment de ne pas permettre une souplesse dans l'exécution des instructions (ex. : la purge ou l'anonymisation des données), le prestataire emporterait la qualification de responsable de traitement alors même qu'il traite les données pour le compte de son client et ne les réutilise pas au-delà de la durée utile au RT. Ainsi, des services intégralement standardisés par le prestataire ne le rendraient-il pas RT, y compris lorsqu'il ne réutilise pas les données pour son propre compte ? La qualification de RT

conjoint doit-elle être envisagée en cas de services CLOUD standardisé ? (en gardant à l'esprit que les acteurs du CLOUD se présentent comme ST et que les liasses contractuelles – CGV/DPA – ne sont pas – ou sont peu – négociables et relèvent parfois du contrat d'adhésion).

III- La qualification des acteurs au sein d'un groupe de sociétés ou d'un réseau de franchises.

Plusieurs questions essentielles se posent aux DPO, chargés de l'organisation d'une gouvernance de la protection des données, claire et protectrice des droits des personnes :

- Quelle doit être la position des filiales par rapport à la société mère s'agissant de traitements exercés de manière distributive ? Relation RT-ST ? Relation de RT conjoints ? Relation de RT à RT entre simples destinataires ?
- Quelles positions doivent adopter les filiales vis-à-vis des prestataires/fournisseurs ? Sont-elles des clients à part entière qui assument une responsabilité de traitement ?
- Doit-il exister un lien contractuel (le DPA, article 28 du RGPD) entre les entités filiales et le prestataire/fournisseur ? DPA ?

Deux situations ont été mises en avant par le groupe de travail : elles portent sur la qualification au sein d'un groupe de sociétés ou d'un réseau de franchises.

A. **La qualification des acteurs en cas d'utilisation d'outils communs.** L'exemple présenté porte sur différentes sociétés au sein d'un groupe qui utilisent une base de données ou un outil centralisé (parfois hébergé) par la maison mère (ex. : logiciel de gestion prospects/clients, logiciel de réservation. SIRH, etc.) La société mère pourrait, selon son rôle dans les différents traitements opérés, être qualifiée de RT, de RT conjoint (car elle est souvent à l'initiative d'une telle mise en place de moyens techniques) ou encore de ST (en tant qu'hébergeur/fournisseur). Dans de nombreux cas, chaque société du groupe travaille en autonomie sur les données de ses propres clients et prospects (décidant parfois des accès des rectifications et suppressions) et ne reçoit pas d'instructions (ou en tout état de cause d'instructions exhaustives) de la maison mère.

- Quid si les entités du groupe reçoivent des consignes spécifiques de la maison mère et ne peuvent, en aucun cas, modifier les paramètres du logiciel exemple ?
- Quid si les entités du groupe ne peuvent paramétrer l'outil, mais ont la maîtrise de son utilisation, et en particulier de la collecte de données ?
- Quid si les entités tirent un bénéfice propre de l'utilisation de cet outil (aide à la gestion de leur propre clientèle, de leurs propres actions de prospections, etc.) ?
- Quid si la maison mère ou le franchiseur tire un bénéfice commercial des actions de prospection ou de commercialisation de ses entités et/ou franchisés ?

B. La qualification des acteurs dans le cadre de l'achat d'une solution. La qualification des acteurs souhaitant bénéficier d'une solution commune au sein d'un groupe (par exemple, après contractualisation par la centrale d'achat ou par la maison mère) est un sujet récurrent. Lorsqu'une seule entité contracte avec le prestataire/éditeur/fournisseur (le ST), la qualification des entités bénéficiaires utilisatrices de la solution achetée (ex. : filiales) se pose. Or, seule l'entité signataire donne des instructions écrites (dans le cadre du contrat de prestation de service, de ses annexes et du Data Processing Agreement). Autrement dit :

- Le fait de donner des instructions écrites positionne-t-il l'entité signataire (ex. : maison mère/centrale d'achat) en tant qu'unique RT ? Cette analyse est-elle transposable lorsque l'entité signataire n'est que simple signataire et n'agit qu'en tant qu'acheteur sans besoin réel d'utilisation ?

ou

- Le fait, pour les filiales, de bénéficier de la solution est-il de nature à les qualifier de RT conjoints ? Dans ce cas, les instructions seraient-elles considérées comme données « au fur et à mesure de l'exécution des services », hors de toute formalisation contractuelle ?
- Le fait pour une entité chapeau de signer et de financer le contrat n'est-elle pas le signe d'une qualification de RT ?

IV - le secteur bancaire : l'exemple présenté par le CEPD de la banque amenée à réaliser les paiements bancaires des salaires des employés dans le cadre des instructions de l'employeur implique sa parfaite autonomie quant au traitement des données qu'elle opère dans le cadre de sa mission.

Pour autant, au vu des remontées d'expérience des membres du groupe de travail, dont certains du secteur bancaire, les services bancaires se diversifient et certains établissements bancaires proposent des services complémentaires. Ainsi en est-il notamment des services SAAS, que le client est libre d'accepter, ou de faire réaliser par un autre prestataire. Pour de tels services complémentaires, la banque ne serait-elle pas amenée à endosser la qualification de sous-traitant de données personnelles ?

V - Sur les instructions complémentaires : le CEPD conforte l'idée de ce qu'elles peuvent intervenir au cours de la réalisation de la prestation, sous réserve qu'elles soient documentées. Il propose des procédures destinées à sécuriser le processus de l'instruction complémentaire et permet, notamment la prise en considération de courriels d'instructions sous réserve de leur conservation et/ou annexe au contrat.

Ne serait-il pas opportun d'envisager l'identification d'une ou des personnes à même de donner des instructions à prendre en considération par le ST ? Il s'agirait ainsi d'éviter des instructions émanant d'une multiplicité d'interlocuteurs qui pourraient, en outre être contradictoires.

VI - La notion de transparence inhérente à la qualité de sous-traitant : ce critère, présent dans les critères de qualification du ST par le G29, semble avoir disparu du projet des lignes directrices du CEPD. Qu'en est-il de la position du CEPD à ce sujet ?

Guidelines 07/2020 on the concepts of data controller and processor in the GDPR

Contribution of AFCDP

The French Association of Personal Data Protection Professionals (AFCDP) has set up a working group dedicated to the relationship of personal data subcontracting, whose work has focused, in particular, on the qualification of the actors and the identification of difficulties with regard to feedback from its members.

In the framework of the opening for public consultation of the future guidelines "controller, processor, joint controllers", the purpose of this document is to transmit to the EDPB the main issues raised by the AFCDP working group.

I - The qualification of regulated professions: while the EDPB supports the position of the G29 that service providers remain data controllers, does this principle not have limits in some specific cases? Indeed, in the example referred to by the EDPB, the law firm, in order to carry out its task, must process the personal data related to the case, falling within its mandate of legal advice or representation, but not specifically the processing of personal data. As it does not receive instructions from its client in the deployment of the personal data processing operations involved in the proper performance of its service, it assumes the qualification of data controller in their deployment.

The participants of the working group note similar questions with regard to other regulated independent professions such as notaries or accountants.

- However, the members of the working group wonder about the limits of this qualification: would it not be different if the lawyer were to be led, on precise instructions from his client, to analyze for specific purposes the databases provided to him in the framework of his service? Wouldn't he become a processor in the context of this database analysis service?

II - The qualification of providers of standardized services such as CLOUD services: cited as an example by the EDPB, such standardized services proposed by the provider do not make him qualify as a data controller, in that he must comply with the specific instructions of his client: retention periods, possible restrictions in terms of location, etc.

Conversely, this example implies that, if the services are standardized to the point of not allowing flexibility in the execution of instructions (e.g. purging or anonymizing data), the provider would carry the qualification of data controller even though it processes the data on behalf of its client and does not reuse it beyond the useful life of the controller. Thus, would fully standardized services by the provider not make him a controller, even when he does not reuse the data for his own account? Should the qualification of joint controller be considered in the case of standardized CLOUD services? (bearing in mind that CLOUD actors present themselves as processors and that the contractual bundles - contract/DPA - are not - or only slightly - negotiable and sometimes fall under the membership contract).

III- The qualification of the actors within a group of companies or a franchise network.

Several essential questions arise for the DPOs, who are responsible for organizing a data protection governance system that is clear and protects the rights of individuals:

- What should be the position of subsidiaries in relation to the parent company with regard to processing carried out in a distributive manner? Controller-Processor relationship? Joint Controller-Porcessor relationship? Controller to Controller relationship between simple recipients?
- What positions should subsidiaries adopt with respect to providers? Are they full-fledged customers who assume responsibility for processing?
- Must there be a contractual relationship (the DPA, Article 28 of the GDPR) between the subsidiary entities and the provider?

Two situations were put forward by the working group: they concern qualification within a group of companies or a franchise network.

A. The qualification of the actors in case of use of common tools. The example presented relates to different companies within a group that use a database or a centralized tool (sometimes hosted) by the parent company (e.g.: prospect/customer management software, reservation software. HRIS, etc.) Depending on its role in the various processes carried out, the parent company could be qualified as an controller, a joint controller (as it is often the initiator of such a technical means implementation) or a processor (as a host/provider). In many cases, each company in the group works autonomously on the data of its own customers and prospects (sometimes deciding on access to corrections and deletions) and does not receive instructions (or in any case exhaustive instructions) from the parent company.

- What if group entities receive specific instructions from the parent company and cannot, under any circumstances, modify the parameters of the example software?
- What if the group entities cannot configure the tool, but are in control of its use, and in particular of the data collection?
- What if the entities derive their own benefit from the use of this tool (help in the management of their own customers, their own prospecting actions, etc.)?
- What if the parent company or the franchisor derives a commercial benefit from the prospecting or marketing actions of its entities and/or franchisees?

B. The qualification of the actors in the context of the purchase of a solution. The qualification of actors wishing to benefit from a common solution within a group (for example, after contractualization by the central purchasing unit or by the parent company) is a recurring subject. When only one entity contracts with the service provider/publisher/supplier (the processor), the qualification of the beneficiary entities using the purchased solution (e.g. subsidiaries) arises. However, only the signatory entity gives written instructions (within the framework of the service provision contract, its annexes and the Data Processing Agreement). In other words :

- Does giving written instructions position the signatory entity (e.g. parent company/purchasing center) as the sole controller? Is this analysis transposable when the signatory entity is only a signatory and only acts as a buyer with no real need for use?
or
- Does the fact that subsidiaries benefit from the solution qualify them as joint controllers? In this case, would the instructions be considered as given "as the services are performed", without any contractual formalities?
- Is the fact that a parent entity signs and finances the contract not a sign of controller qualification?

V - The banking sector: the example presented by the EDPB of a bank that is required to make bank payments of employees' salaries in the context of the employer's instructions implies its complete autonomy with regard to the data processing it carries out in the context of its mission.

However, in view of the experience feedback from the members of the working group, some of whom come from the banking sector, banking services are diversifying and some banking institutions offer complementary services. This is particularly true of SAAS services, which the client is free to accept or to have carried out by another service provider. For such additional services, would the bank not have to qualify as a personal data processor?

VI - On the additional instructions: the EDPB supports the idea that they may intervene during the performance of the service, provided that they are documented. He proposes procedures designed to secure the process of the complementary instruction and allows, in particular, the consideration of instruction e-mails subject to their conservation and/or annex to the contract.
Would it not be appropriate to consider the identification of a person or persons able to give instructions to be taken into consideration by the processor? This would avoid instructions from a multiplicity of interlocutors that could, moreover, be contradictory.

VI - The notion of transparency inherent to the status of subcontractor: this criterion, present in the G29 criteria for the qualification of the processor, seems to have disappeared from the draft EDPB guidelines. What about the EDPB position on this issue?