GUIDE DES DATA PROTECTION AGREEMENT

DPA & RGPD : COMMENT RÉDIGER ET NÉGOCIER SON DPA ? L'EXEMPLE DU RESPECT DES INSTRUCTIONS DU CLIENT : QUELLES CONDITIONS ? LIMITES ? QU'EN PENSENT LES ACTEURS IT ?

Ce guide à l'usage des négociateurs de DPA présente les solutions concrètes et opérationnelles proposées par les membres de cet observatoire du DPA : les Prestataires IT les éditeurs, les Clients, l'ANSSI et les représentants de achats IT, pour aider les partenaires à mieux aborder les questions relatives à ces instructions et considérées comme adaptées et respectueuses des intérêts de chacun.

La signature des contrats de sous-traitance, encore nommés DPA, pour « Data Processing Agreement », est désormais, pour toute entreprise, le passage incontournable de sa mise en conformité au RGPD.

Destiné à régir la relation entre un responsable de traitement et son sous-traitant de données personnelles, le DPA est le contrat ou l'acte juridique « ad hoc » qui fixe les obligations respectives des parties, plus particulièrement du sous-traitant, à l'égard de son client.

Le prestataire, défini par le RGPD comme « *agissant sous l'autorité du responsable de traitement et ne pouvant traiter les données, excepté sur instruction de ce dernier* » est normalement dépourvu d'autonomie dans le traitement des données.

L'obligation première du prestataire IT est de mener à bien la prestation qui lui incombe et, pour ce faire, de respecter les instructions de son client.

Le texte européen précise que le DPA prévoit, notamment, que le sous-traitant « *ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement* ». En conséquence, toute initiative du prestataire dans la détermination des finalités et des moyens d'un traitement est susceptible de le faire « basculer » dans le rôle de responsable de traitement (Fiche 1 – Qualification des acteurs). Cette absence d'autonomie s'illustre notamment lorsque le prestataire décide de recourir aux services d'un sous-traitant ultérieur, cas qui le contraint à demander l'autorisation écrite, générale ou spécifique, de son client (Fiche 5 – Flux hors UE).

Le prestataire IT est pourtant tenu à des contraintes liées au respect du RGPD qui lui sont propres, notamment en matière de sécurité (Fiche 4 – Sécurité) ou d'accompagnement du client dans sa conformité au RGPD : l'aider à garantir le respect des obligations qui lui incombent, l'assister dans le respect des droits de personnes, lui faire remonter au plus vite un incident de sécurité « Data breach ». Il doit en outre mettre à la disposition de son client toute information nécessaire pour démontrer le respect des obligations relevant de cette relation de sous-traitance, obligation complétée par celle d'informer immédiatement le responsable de traitement d'une instruction que celui-ci aurait donnée en violation du règlement (article 28 2 h).

Ainsi, tenu de réaliser la prestation qui lui incombe, le prestataire IT doit :

- **être en mesure d'identifier les instructions de son client pour les mener à bien ;**
- **alerter son client d'une instruction non respectueuse du RGPD.**

Face au respect de telles contraintes, le prestataire IT est parfois confronté à des difficultés dans le suivi des instructions documentées du responsable de traitement.

Les participants de l'Observatoire des DPA ont mis en avant deux situations particulièrement délicates.

I. LE PRESTATAIRE IT CONFRONTÉ À DE MULTIPLES INSTRUCTIONS DE SON CLIENT.

Ce sont les instructions données par une partie (le client) à l'autre (le prestataire IT) qui contribuent à la qualification des acteurs (Fiche 1), au périmètre de la prestation (Fiche 2 – Description du traitement) et, de ce fait, à leurs responsabilités respectives (Fiche 6 – Responsabilités).

Aussi, le prestataire IT se doit d'identifier et de bien appréhender les instructions relevant de la prestation.

Sur ce sujet, certaines questions font débat chez les professionnels, tant clients que prestataires, dont les réponses sont fondamentales au regard des enjeux pour les parties au DPA.

- **Quelle forme doit revêtir l' « instruction documentée » ?**

On l'a vu, l'instruction doit être documentée. Les lignes directrices du G29 précisent que leur « documentation » nécessite un écrit, mais n'apportent pas de précisions quant à leur nature :

simple courriel ? nécessité d'une traçabilité des envois et des réceptions des instructions ?

Si un formalisme poussé à l'extrême pourrait être un frein au bon déroulé de la prestation, il convient, pour le prestataire, d'être à même d'identifier aisément, voire « d'authentifier » l'instruction documentée qu'il est tenu de respecter.

• Le cas d'une nouvelle instruction donnée au cours de la prestation

La rédaction du DPA implique la description précise de la prestation, mais cela s'avère parfois difficile en amont de sa réalisation (cf fiche 2) et une certaine souplesse est de mise.

Le principe de suivi des instructions tout au long de la prestation par le responsable de traitement est d'ailleurs conforme à l'esprit du RGPD et aux différentes délibérations de la CNIL, dont il ressort que le client « garde la main » sur les traitements opérés par le sous-traitant, l'inverse pouvant d'ailleurs lui être reproché. Cette souplesse ne saurait cependant permettre au client d'élargir le périmètre de ses instructions au cours de la prestation.

Un avis récent[1] du Comité européen de protection des Données (CEPD, ancien groupe dit du G29), consulté sur un projet de clauses contractuelles de l'autorité de contrôle danoise, envisage la possibilité, pour le client, de donner des instructions supplémentaires pendant toute la durée du contrat, sous réserve qu'elles soient documentées.

Sur ces deux aspects, les membres du groupe de travail proposent, comme pour les autres thématiques, des solutions concrètes.

Le récent projet de lignes directrices du CEPD, ouvertes à consultation en septembre 2020, s'oriente, à l'identique, vers des propositions pragmatiques qui présentent le bénéfice d'une certaine souplesse, dans le respect de la sécurité juridique.

• Le cas d'une instruction émanant d'un nouvel interlocuteur

Tenu de rester dans son rôle de subordination, le prestataire IT doit s'assurer, en amont de leur réalisation, que les instructions émanent légitimement de son client.

Or, dans le cadre de l'exécution de la prestation, nombre d'instructions sont données par différents interlocuteurs de la société cliente ce qui et implique, pour le sous-traitant, de s'interroger sur leur bien-fondé : doit-il les prendre en considération ? Ne risque-t-il pas d'être confronté à des injonctions contradictoires ? Ne risque-t-il pas de se voir reproché une prise d'initiative, voire d'être requalifié en responsable de traitement ?

Autant de questions, sources d'inquiétudes, pour les prestataires IT qui pourraient se voir reprocher d'avoir suivi à tort des instructions qui n'émaneraient pas de leur client « stricto sensu ».

Au-delà de ces questions opérationnelles, une obligation inquiète particulièrement les prestataires IT : celle qui consiste à alerter son client d'une instruction non respectueuse du RGPD. La question fait d'autant plus débat qu'aucune réponse n'est apportée par les instances officielles à ce jour. Le présent guide, là encore, tentera d'y répondre par des solutions opérationnelles.

II. LE PRESTATAIRE IT CONFRONTÉ À UNE INSTRUCTION EN VIOLATION DU RGPD.

Cette obligation du prestataire de signaler au responsable de traitement tout risque de violation du RGPD qu'il aurait identifié, le positionne dans un rôle, non plus seulement d'accompagnant, mais de conseil.

Elle pose aussi la question de sa responsabilité, plus spécifiquement dans deux hypothèses (Fiche 6 – Responsabilités des acteurs) :

- Le cas de la suspension de l'exécution de sa prestation face à une instruction qu'il estime illicite ;
- Le cas de l'application d'une instruction illicite (soit qu'il ne l'a pas identifiée comme telle, soit qu'il l'a identifiée et signalée et en a poursuivi l'exécution).

EN SAVOIR PLUS

Ce guide, auquel l'ANSSI a pris une part active et dont l'avancée a été suivie avec intérêt par la CNIL, est présenté sous forme de fiches pédagogiques, une par thème abordé. Après un bref rappel du dispositif juridique, chaque fiche retrace ces échanges sous forme de « regards croisés » et propose des réponses concrètes et opérationnelles.

Tous les professionnels amenés à mettre en place, piloter ou négocier des DPA dans le cadre de projets technologiques trouveront dans ce guide un véritable instrument de travail et de conformité.

Un ouvrage conçu par des professionnels avocats, juristes, DPO, experts SI, Acheteurs IT pour les professionnels amenés à mettre en place et négocier des DPA.

> Collection Création Information Communication Pratique

Édition 2020 • 130 p. • 45,00 €

1 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_201914_dk_scc_fr.pdf