Communiqué de presse – 04 Janvier 2022

L'AFCDP dévoile les préoccupations des DPO liées aux outils collaboratifs

L'usage massif des outils collaboratifs, favorisé par la crise sanitaire, pose de multiples préoccupations aux DPO dans leur quotidien, d'autant plus depuis la décision de la Cour de justice de l'Union européenne (CJUE) à l'été 2020, d'invalider le dispositif d'autorégulation dit « Privacy Shield » permettant aux acteurs situés dans l'Union européenne d'exporter des données personnelles aux États-Unis, et aux acteurs américains d'en importer.

L'AFCDP a étudié les publications dédiées à ce sujet sur le réseau social privé de l'association, et partage les 5 préoccupations majeures des DPO relatives aux outils collaboratifs.

Des préoccupations concernant le transfert des données vers les États-Unis depuis l'invalidation du Privacy Shield

On rappelle qu'un transfert de données peut s'effectuer par l'envoi de fichiers contenants des données personnelles vers un pays tiers, mais aussi, par exemple, par la collecte de données de connexion à l'insu de l'expéditeur. Ainsi, lorsqu'un salarié utilise un outil collaboratif américain pour communiquer à sa DRH les heures de travail effectuées par les membres de son équipe, il transfère sur un serveur américain les données personnelles de ses collègues et parallèlement, le logiciel collecte des données sur sa connexion et celle de sa DRH.

Les transferts de données personnelles hors Union européenne (UE) sont autorisés tant qu'ils s'inscrivent dans un des cadres légaux proposés par le RGPD. L'un de ces cadres est le transfert vers un pays reconnu comme « adéquat » par l'UE. Or, depuis l'invalidation du bouclier juridique dit « Privacy Shield » par la CJUE (arrêt du 16 juillet 2020 « Schrems II) jugeant que le fait de transférer les données personnelles depuis l'UE vers les États-Unis n'offre pas un niveau de protection adéquat, tous les recours aux services et offres s'appuyant sur des infrastructures ou des éditeurs situés aux États-Unis sont remis en question.

Depuis, les échanges des DPO de l'AFCDP s'orientent sur :

- la mise en place de nouvelles clauses contractuelles types (CCT) de la Commission européenne afin d'encadrer légalement le transfert de données entre les deux continents. Mais la mise en œuvre de ces CCT pose de nombreux problèmes d'interprétation juridique, notamment, pour les CCT établies unilatéralement par les grands acteurs américains (les « GAFAM ») ;

- l'utilisation des outils collaboratifs proposés par les GAFAM, soit gratuitement, soit à prix préférentiels. Outre les problématiques d'espionnage industriel quand ces outils sont utilisés par le secteur de l'enseignement et de la recherche, des problématiques de transferts non autorisés des données personnelles de celles et ceux qui les utilisent en toute confiance sont à éclaircir ;

- l'usage d'outils collaboratifs américains par les Collectivités : les DPO du secteur public s'interrogent sur les moyens collaboratifs comme Microsoft Office 365, mais également sur les outils de communication. Des solutions alternatives sont proposées, mais utilisées avec réticences, soit parce que leurs interfaces sont moins attractives que leurs concurrentes des GAFAM, soit parce qu'elles ne jouissent pas du même support commercial. Par exemple, les échanges s'orientent sur des alternatives certifiées, proposées par l'État

(recommandées ou qualifiées par l'Agence Nationale de la Sécurité des Systèmes d'Information – ANSSI), tel que Tchap (messagerie instantanée), Tixeo (visioconférence).

Recherche d'outils respectueux de la vie privée, conformes au RGPD ou alternative aux outils américains

De façon récurrente, les DPO s'interrogent sur la mise en place d'outils au sein de leurs structures, respectueux de la vie privée ou de façon plus ambitieuse, conformes au RGPD.

Les outils particulièrement visés concernent les questionnaires/sondages en ligne (alternatives à Microsoft Form, Survey Monkey), les systèmes de stockage sécurisés (alternatives à DropBox), les outils d'envoi de fichiers employant du chiffrement (alternatives à Wetransfer), les agendas intégrés (Outlook, Doodle), des fichiers partagés (MS Office, Google), etc.

Les DPO pèsent le pour et le contre et partagent des documents recensant des critères pour les aider à prendre une décision. Les critères concernent notamment, l'hébergement des données, la lecture des Conditions Générales d'Utilisation et/ou de la politique de confidentialité, la gratuité ou non d'un outil.

L'usage d'outils collaboratifs pour le télétravail

Outre les questions de conformité « globale » au RGPD, la pandémie a mis en évidence d'autres interrogations précises. En particulier, lors de la mise en place d'outils de visioconférence (utilisation de Zoom, Webex, Teams, Tixeo, Hangout…). Les DPO s'interrogent en particulier sur ces questions :

- Le fait d'utiliser un système de visioconférence constitue-t-il un traitement de données personnelles ?

- Comment gérer et/ou formaliser le consentement des personnes (droit à l'image) en cas d'enregistrement ?

- Comment fournir les informations relatives à leurs droits quant aux traitements de leurs données, aux personnes s'inscrivant et participant aux webinaires ?

- Peut-on imposer aux salariés d'activer leur caméra ?

L'information et la gestion d'exercice des droits des personnes concernant l'usage d'outils collaboratifs en préservant la confidentialité des informations contenues

À l'occasion de la mise en place d'un tableau de présence des salariés lors du contexte sanitaire, se sont également posées des questions autour de la visibilité de ces informations par tous les salariés.

Des principes fondamentaux sont également mentionnés : la base légale du traitement choisie, la gestion des droits (confidentialité) et le principe de minimisation des données. Des solutions telles que Google Docs, Excel, Wimi-teamwork sont mentionnées.

Les mesures de sécurité mises en œuvre, en particulier pour les systèmes de messagerie et les fichiers partagés

Une question constante des DPO concerne les garanties de sécurité mises en œuvre. Outre les questionnements autour de la confidentialité des informations, les garanties « techniques » et non organisationnelles sont soulevées.

Tel est le cas notamment de la mise en place d'un système de chiffrement, notamment pour échanger par email ou partager des fichiers (Zone Central, ZED !, Veracrypt, 7-zip), la traçabilité des accès, ou encore des moyens d'anonymisation.

Les outils collaboratifs relèvent de la sphère informatique et sont souvent choisis par les DSI, en méconnaissance du RGPD, et souvent surtout pour leur coût attractif. Une fois ces solutions déployées, il est difficile de faire changer les mauvaises habitudes et de modifier un SI dont la plupart des autres applicatifs s'interopèrent avec ces outils mondialement distribués.

Pour un certain nombre de cas, des alternatives existent bel et bien. Il appartient aux décisionnaires et aux DPO de travailler en collaboration pour les identifier et les déployer en toute sérénité.

Pour les autres situations, "*les DPO sont aux prises avec de nombreux défis et interrogations autour de l'usage des outils collaboratifs dans leurs organisations et, pour le moment, il semble que ni la législation ni les instances ne sont en mesure de les résoudre »* souligne Paul-Olivier Gibert, Président de l'AFCDP.

À propos de l'AFCDP - www.afcdp.net

L'AFCDP, créée dès 2004, regroupe plus de 6 000 professionnels de la conformité au RGPD et à la Loi Informatique & Libertés – dont les Délégués à la Protection des Données (DPD ou DPO, pour *Data Protection Officer*).

Si l'AFCDP est l'association représentative des DPD, elle rassemble largement. Au-delà des professionnels de la protection des données et des DPD désignés auprès de la CNIL, elle regroupe toutes les personnes intéressées par la protection des données à caractère personnel. La richesse de l'association réside – entre autres – dans la diversité des profils des adhérents : DPD, délégués à la protection des données, juristes et avocats, spécialistes des ressources humaines, informaticiens, professionnels du marketing et du e-commerce, RSSI et experts en sécurité, qualiticiens, archivistes et Record Manager, déontologues, consultants, universitaires et étudiants.

Contact Presse : Maëlle Garrido, NASKAS RP, Relations Presse, 06 12 70 77 30, maelle@naskas-rp.com