_swissprivacy.law

L’administration publique responsable dans l’utilisation de services en nuage

Pauline Meyer, le 22 mars 2023

Le Comité européen de la protection des données émet des points d’attention pour responsabiliser les administrations publiques et leur permettre d’assurer la protection des données lorsqu’elles recourent à des services en nuage.

Coordinated Enforcement Action adopted on 17 January 2023 on the Use of cloud-based services by the public sector

Le Comité européen de la protection des données (*European Data Protection Board,* EDPB) publie le 17 janvier 2023 un rapport contenant des points d’attention fondés sur la pratique de certaines autorités européennes de protection des données en matière d’utilisation de services en nuages (*Cloud Computing*) au sein de l’administration publique.

Les points soulevés par l’EDPB portent principalement sur les difficultés quant à la négociation de contrats entre administrations publiques et fournisseurs de solutions cloud (*Cloud Service Provider*, CSP), sur le respect des obligations fondées sur la législation en matière de protection des données par les administrations publiques et les CSP et sur les transferts de données à des États tiers. Les défis identifiés présentent régulièrement un lien avec le possible déséquilibre entre l’administration négociant avec un CSP détenant une position dominante.

Le contrat et la position de l’administration publique

Lors de l’utilisation de services en nuage, les administrations publiques sont en règle générale considérées comme les responsables du traitement, alors que les CSP sont considérés comme des sous-traitants. Il est important que les rôles soient clairement répartis contractuellement pour respecter le principe de responsabilité (art. 5 par. 2 et 24 RGPD), connaître les obligations à respecter de part et d’autre et savoir si une base légale est nécessaire ou non pour justifier les traitements. Pour les traitements dont le CSP détermine les moyens et les finalités et dans la mesure où les rôles dépendent de cette considération, ce dernier est considéré comme responsable du traitement au sens des art. 5 par. 2 et doit respecter le RGPD à ce titre (art. 28 par. 10 RGPD ; cf. www.swissprivacy.law/204/). D’autres situations

peuvent exister dans lesquelles l'administration et le CSP sont considérés comme co-responsables du traitement, à savoir lorsqu'ils déterminent ensemble les moyens et les finalités du traitement, ce qui doit se refléter dans le contrat.

L'objet, les données et les finalités des traitements doivent également être précisées dans le contrat (art. 28 par. 3 RGPD), bien que les administrations publiques peinent parfois à exercer une influence sur ces considérations, notamment en raison d'un déséquilibre des pouvoirs entre les cocontractants.

Problème à portée similaire : les autorités interrogées ont un contrôle limité et prennent le risque de perdre une importante part de service si elles objectent ou négocient l'utilisation par le sous-traitant d'un sous-traitant ultérieur. Cependant, l'administration publique doit avoir voix au chapitre lorsqu'il en va de sous-traitance en cascade (art. 28 par. 2 RGPD). Elle peut s'assurer d'une sous-traitance en cascade spécifique plutôt que d'accepter une telle délégation de manière générale, par exemple en prévoyant des critères à remplir pour tout nouveau sous-traitant ultérieur afin d'anticiper et diminuer les risques pour les personnes concernées.

Pour aider à compenser le déséquilibre dans les négociations, les autorités faisant appel à un même CSP doivent coopérer pour avoir un poids plus élevé. De même, leur délégué à la protection des données (DPO) doit être impliqué dans les négociations du contrat (comme dans d'autres processus, à l'instar des analyses d'impact relatives à la protection des données (AIPD) au sens de l'art. 35 par. 2 RGPD). Dans le prolongement de cette réflexion, nous estimons qu'il peut être bénéfique que l'État négocie pour l'ensemble de son administration l'utilisation de solutions en nuage (comme le fait actuellement la Confédération avec son projet « Public Clouds Confédération ») pour que les autorités puissent avoir plus de poids dans les négociations.

Les analyses d'impact relatives à la protection des données (AIPD)

Une AIPD doit être conduite lors de traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques (art. 35 par. 1 RGPD). L'art. 35 par. 3 let. b RGPD dispose qu'une AIPD doit être menée notamment lors du traitement à grande échelle de catégories particulières de données en vertu de l'art. 9 par. 1 RGPD ou de données personnelles relatives à des condamnations pénales et à des infractions visées à l'art. 10 RGPD. Dans les cas où elle n'est pas nécessaire, les mesures techniques et organisationnelles doivent en tout état de cause être déterminées à la suite d'une analyse de risque (art. 32 RGPD).

Alors que l'administration est fréquemment amenée à traiter des catégories particulières de données à grande échelle ou des données relatives à des condamnations pénales et à des infractions, seule une part des autorités interrogées indiquent avoir réalisé une AIPD. Une AIPD doit être réalisée (ou son bienfondé vérifié) lors de la conclusion d'un contrat avec un CSP. Elle est nécessaire pour adopter les mesures techniques et organisationnelles identifiées et doit être régulièrement réexaminée, dans la mesure où les services en nuage sont dynamiques et évoluent en permanence.

Les audits

Rares sont les audits menés, durant le traitement, auprès des CSP, souvent en raison de ces derniers. Il est également difficile d'accéder aux résultats des audits menés au sein des CSP. L'EDPB rappelle néanmoins que l'art. 28 par. 3 let. h RGPD impose au sous-traitant de mettre à disposition du responsable du traitement les informations nécessaires aux audits et d'y contribuer.

Les transferts des données vers des pays tiers

Finalement, il est nécessaire que les transferts de données soient identifiés et que le Chapitre V RGPD soit respecté. De nombreux CSP sont basés dans des États hors de l'UE qui ne présentent pas un niveau adéquat de protection des données au sens de l'art. 45 RGPD. Les autorités doivent s'assurer en amont des catégories de données transmises, des finalités dudit transfert, de l'utilisation d'un outil sécurisé pour la transmission des données ou encore des entités susceptibles d'avoir accès aux données. Dans la mesure où de nombreux CSP sont basés dans des pays ne bénéficiant pas d'une décision d'adéquation, il nous semble également important que les administrations s'assurent de transférer les données sur la base de clauses contractuelles types, voire qu'elles privilégient des relations avec des CSP avec des règles d'entreprise contraignantes.

Ensuite, l'administration doit clarifier l'éventuelle application d'un droit étranger et l'éventuel accès par des autorités étrangères aux données transférées, et savoir si le droit étranger applicable pourrait imposer au CSP de ne pas respecter les instructions du responsable du traitement. L'administration doit examiner si, cas échéant, le CSP peut mettre la requête de l'autorité étrangère en attente et informer le responsable du traitement ou si ces actions peuvent faire l'objet d'une interdiction. L'administration doit savoir si les requêtes étrangères peuvent se faire moyennant le respect de la base de l'art. 48 RGPD ou si le CSP peut demander à l'autorité étrangère de suspendre l'interdiction en raison de ses obligations RGPD.

Si aucune solution n'est satisfaisante, l'administration doit être certaine que des mesures appropriées au sens de l'art. 28 RGPD sont mises en place et le CSP doit informer les autorités compétentes de protection des données par un rapport annuel au sujet de telles requêtes.

En Suisse

En Suisse, la question de l'utilisation de solutions cloud par des autorités fait également du chemin. Alors que le PFPDT estimait en 2022 que la SUVA devait réexaminer son projet de faire appel au service cloud Microsoft 365 de Microsoft Irlande (cf. www.swissprivacy.law/165/), il va bientôt prendre position sur le projet Microsoft 365 de la Confédération. Les circonstances factuelles semblent avoir permis au Conseil fédéral d'approuver un crédit d'engagement pour cette migration, mais il s'agit maintenant d'attendre la prise de position du PFPDT au sujet de sa conformité aux règles de protection des données. À noter que ce projet prend forme dans le cadre du projet « Public Clouds Confédération », dans lequel la Confédération tente de trouver les compromis pour permettre l'externalisation de services de l'administration en respectant les droits en présence.

Proposition de citation : Pauline Meyer, L'administration publique responsable dans l'utilisation de services en nuage, 22 mars 2023 *in* www.swissprivacy.law/210