RECOMMANDATIONS AUX OPÉRATEURS DE SOLUTIONS NUMÉRIQUES POUR L'ENSEIGNEMENT ET LA RECHERCHE

(Suite arrêt de la Cour de justice de l'Union Européenne du 16 juillet 2020, affaire C-311/18 invalidant la décision 2016/1250)

Sommaire

Contextualisation

SupDPO accompagne les structures de l'Enseignement Supérieur, de la Recherche et de l'Innovation (ci-après "Établissements" et "ESRI") qui font le choix de prestations ou solutions numériques propriétaires en ligne. **Ce document est un guide permettant de conseiller sur l'analyse de conformité à mener mais ne constitue en aucun cas une recommandation d'usage ni une garantie de conformité des solutions en ligne hébergées par des prestataires de "solution propriétaire".**

Lorsqu'un Établissement choisit une plateforme de services numériques, une attention particulière doit être portée sur la compatibilité des mesures techniques, logiques et organisationnelles offertes par le service avec la réglementation européenne sur la protection des données. Parmi les options possibles, l'une consiste à chercher des services sous "Juridiction RGPD". La Juridiction RGPD recoupe l'ensemble des pays au sein desquels l'exportation de données se déroule dans les mêmes conditions légales qu'au sein même de l'Union Européenne. Dans les cas où le fournisseur du service n'est pas localisé sur le territoire de l'Union européenne, il est en effet nécessaire d'analyser les mécanismes juridiques permettant de lui voir appliquer la réglementation relative à la protection des données. La réglementation prévoit ainsi la mise en oeuvre de de mécanismes de reconnaissance d'adéquation[1] ou d'adhésion[2], lesquels permettent d'assurer le transfert de données personnelles vers des États hors de l'Union Européenne où la réglementation européenne ne s'applique pas par défaut. La mondialisation des échanges de données engendre une incertitude juridique et technologique pour les structures de l'ESRI.

SupDPO souhaite rappeler que dans le contexte juridique actuel, suite à l'invalidation de l'instrument juridique permettant le transfert de données personnel de l'UE vers les USA, ces cas de transferts font peser :

[1]Liste des États reconnus comme offrant un niveau de protection adéquat au 10/05/2021 : Japon, Argentine, Uruguay, Suisse, Nouvelle-Zélande, Royaume-Uni, adéquation partielle pour le Canada; (ci-après "Juridiction RGPD")
[2]le RGPD s'applique à l'Espace Économique Européen

- **Un risque d'accès illégal aux données par les prestataires états-uniens :** La CNIL précise[3] que *"indépendamment de l'existence de transferts, les législations américaines s'appliquent aux données stockées par les sociétés états-uniennes en dehors de ce territoire. Il existe donc un risque d'accès par les autorités américaines aux données stockées. Cet accès, s'il n'est pas fondé sur un accord international, constituerait une divulgation non autorisée par le droit de l'Union, en violation de l'article 48 du RGPD."*
- **Un risque de sanctions[4] par les autorités de contrôle en cas de choix de prestataires étasuniens** (filiale et maison mère, où que soient situés les serveurs, y compris dans l'Espace Économique Européen) si les recommandations émises par le Comité européen à la protection des données (CEPD) ne sont pas suivies.

Différentes prises de positions ont pu questionner la légalité intrinsèque du choix d'opérateurs de solutions numériques étasuniens :

- les sanctions des grands opérateurs Internet par la CNIL et ses homologues en Europe fondant leurs décisions sur l'opacité de l'administration des données et la non maîtrise de ces données par les utilisateurs et les personnes concernées
- la décision de certaines autorités européennes à la protection des données d'interdire dans un premier temps Office 365 dans les Établissements d'enseignement (eg. Décision du Land de Hesse)
- la décision de la Cour de Justice de l'Union Européenne dans l'affaire SCHREMS II du 16 juillet 2020[5] imposant aux responsables de traitements la vérification effective des conditions d'exportation des données hors du territoire de l'Union et la mise en œuvre de mesures supplémentaires de sécurité
- la position de la CNIL dans ses conclusions concernant le Health Data Hub hébergé chez Microsoft[6]
- l'ordonnance en référé du 13 octobre 2020 du Conseil d'Etat[7], mettant en demeure Microsoft sous contrôle de la CNIL de mettre en place des mesures de sécurité supplémentaires conformément à la décision Schrems II
- la faisabilité technique et juridique de mise en œuvre des recommandations du comité européen pour la protection des données suite à l'arrêt SCHREMS II[8]

L'avis de la CNIL du 15 avril 2021, suite à la demande de conseil formulée par la Conférence Présidents d'Universités et la Conférence des grandes écoles apporte un éclairage clair et précis quant au recours aux solutions numériques étatsuniennes, en appelant à une évolution des choix numériques, tout en proposant deux solutions à suivre :

- *"soit confier la sous-traitance de ces données à un opérateur qui les entrepose sur le territoire de l'Union européenne, qui soit exclusivement soumis au droit européen, et qui ne transfère pas vers les Etats-Unis ;*

- *soit, peut-être, recourir à une forme particulière de service d'hébergement, dans lequel les données sont traitées dans les conditions mentionnées ci-dessus, tout en permettant d'utiliser les outils des sociétés étatsuniennes, par le biais d'un accord de licence ne leur donnant aucune prise sur les données. D'importants sociétés étatsuniennes ont annoncé vouloir développer ce type de solutions mais ces dernières ne sont pas commercialisées et leur conformité aux exigences de la CJUE devra être expertisée."*

[3] https://www.cnil.fr/fr/la-cnil-appelle-evolutions-dans-utilisation-outils-collaboratifs-etatsuniens-enseignement-superieur-recherche
[4] Ex: https://www.cnil.fr/fr/utilisation-de-google-analytics-et-transferts-de-donnees-vers-les-etats-unis-la-cnil-met-en-demeure
[5] http://curia.europa.eu/juris/document/document.jsf?docid=228677&doclang=FR
[6] https://www.cnil.fr/fr/la-plateforme-des-donnees-de-sante-health-data-hub
[7] https://www.cnil.fr/fr/le-conseil-detat-demande-au-health-data-hub-des-garanties-supplementaires
[8] https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en

Le gouvernement a annoncé, le 17 mai 2021, une stratégie nationale pour le cloud[9].

Le 18 juin 2021, le CEPD a également mis à jour ses recommandations[10] sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données personnelles de l'UE.

Ces éléments amènent SupDPO à rappeler que l'écosystème juridique européen et français permet d'asseoir et d'affirmer un modèle portant haut les valeurs de protection des données, de respect de la vie privée . En témoigne les textes et initiatives les plus récentes (cf. supra) et à venir[11].

Principales demandes de SupDPO aux Opérateurs de solutions numériques

1. DOCUMENTATION CONTRACTUELLE

    a. Les Opérateurs doivent privilégier et asseoir un socle juridique négocié avec le secteur au niveau national. Les modifications permanentes (possiblement mensuelles) des termes juridiques en ligne ne sont pas légitimes compte tenu de la dimension et de la portée des outils numériques dans l'Enseignement Supérieur et la Recherche, notamment concernant les Suites collaboratives.

    b. Les Opérateurs doivent exclure tout transfert de données vers les Etats-Unis.

    c. En cas de transfert dans un pays de protection adéquat, la documentation du traitement, à laquelle l'Opérateur contribue, rappelle la décision d'adéquation de la Commission européenne concernant le pays destinataire.

    d. En cas de transfert hors Juridiction RGPD, la documentation du traitement, à laquelle l'Opérateur contribue, doit rassembler le régime juridique applicable (notamment la base légale), les garanties appropriées mises en œuvre, mais également toutes les mesures complémentaires applicables, qu'elles soient techniques, logiques ou organisationnelles.

    e. Les Opérateurs doivent compléter et mettre à disposition des Établissements les grilles de synthèse des "Contacts et références utiles de l'Opérateur" (Annexe 1) et "Sous-traitance ultérieure" (Annexe 2). Ces documents doivent être tenus à jour pendant toute la durée du contrat.

[9] https://www.numerique.gouv.fr/uploads/Strategie-nationale-pour-le-cloud.pdf
[10]https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf
[11] Le Digital Markets Act;
Le projet de règlement européen sur la gouvernance européenne des données ;
Le projet de règlement européen sur l'intelligence artificielle;
Le rapport Bothorel# sur la politique publique de la donnée;
La création d'une mission logiciels libres et communs numériques au sein de la direction interministérielle du numérique (Dinum) de l'Etat et faisant suite au rapport Bothorel;

f. Les opérateurs sont des sous-traitants des Établissements. Ils n'agissent que pour le compte des Établissements et en fonction des finalités définies par les Établissements. Au-delà, les opérateurs prennent leur responsabilité pleine et entière lorsqu'ils traitent pour leur propre compte des données initialement en sous-traitance. A ce titre, SupDPO recommande aux **Établissements de refuser de signer des accords de réutilisation / réexploitation des données par un Opérateur** (eg. machine learning, marketing digital, exploitation de données de recherche (via questionnaire et sondage)).

2. HEBERGEMENT - Les Opérateurs doivent proposer un hébergement des données conforme à la qualification SecNumCloud de l'ANSSI[12].

3. CHIFFREMENT - Les Opérateurs doivent proposer des outils de chiffrement, et une gestion externalisée des clés aux Établissements[13]. Les Opérateurs doivent permettre le recours à un dispositif tiers (voire certifié) de chiffrement des données par l'Établissement, en tant que mécanisme additionnel aux mécanismes de chiffrement natifs de la solution.

4. MINIMISATION - Les Opérateurs doivent minimiser les données collectées et restituées, y compris pour les services annexes. Par exemple, les tableaux de bord restituant en back-office les statistiques d'utilisation (avec la non-agrégation des données individuelles) doivent être rigoureusement minimisés et respecter la vie privée des utilisateurs. Les services proposés doivent être validés préalablement par l'Établissement, sur la base des conseils de son/sa Délégué.e à la protection des données.

5. CONSOLE D'ADMINISTRATION ET SUPERVISION DES BRIQUES APPLICATIVES - Les Opérateurs doivent améliorer les consoles d'administration/supervision des outils numériques :

   a. Proposer une console d'administration permettant de lister l'ensemble des briques / fonctionnalités de leur solution.

   b. Afficher la liste des services applicatifs inclus dans leur outil "For Education" et ceux activables de manière optionnelle, ou gérés par leurs prestataires externes et qui ne sont pas inclus dans les contrats passés avec l'Établissement (produits complémentaires). L'activation de ces services applicatifs externes doit rester à la main de l'Établissement et ne doit pouvoir être possible que lorsqu'un engagement juridique institutionnel est conclu.

   c. Améliorer la console d'administration de l'outil numérique afin que l'Établissement soit en mesure de limiter l'accès aux services "grands publics" enrichissant éventuellement leur solution.

   d. Faciliter la distinction entre :

      i. les interfaces techniques relatives aux processus de gestion informatique,
      ii. les interfaces engendrant un engagement juridique institutionnel explicite et éclairé,
      iii. les rôles des utilisateurs de ces interfaces

   e. Utiliser les terminologies de la protection des données dans leurs consoles d'administration et leurs fonctionnalités de gestion des droits des utilisateurs.

6. HABILITATIONS - Les Opérateurs doivent proposer des fonctionnalités de gestion des habilitations et de classification des données par profil, avec la possibilité de distinguer les services applicatifs proposés par la solution.

[12] https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-service-dinformatique-en-nuage-secnumcloud/
[13] point 79. des recommandations 01/2020 de l'EDPB

7. GESTION DES DROITS DE PROPRIÉTÉ - Les Opérateurs doivent proposer des solutions numériques pour l'enseignement et la recherche dont les "droits de propriété" des documents stockés sur les espaces d'hébergement proposés aux utilisateurs (e.g. Drive individuel) sont gérés par un ou plusieurs groupes de "propriétaires".

8. GESTION DES FONCTIONNALITÉS APPLICATIVES - Des restrictions d'accès à certaines fonctionnalités sur les données (e.g. Exportation des données) doivent pouvoir être déterminées par les administrateurs en fonction des groupes d'utilisateur (rôles applicatifs).

9. GESTION DES DURÉES DE CONSERVATION - Les Opérateurs doivent proposer des fonctionnalités de paramétrage des durées de conservation par application par rôle applicatif.

10. ARCHIVAGE - Les Opérateurs doivent proposer des solutions d'archivage soit intégrées, soit compatibles et interopérables, avec les solutions numériques dédiées. Leurs solutions doivent être respectueuses des obligations d'archivage intermédiaire et définitif (définition des durées, définition de habilitations archivage et des supports d'archivage)

11. GESTIONS DES DROITS RGPD

    a. DROIT D'ACCÈS, SUPPRESSION ET SORT DES DONNÉES - Les Opérateurs doivent proposer une interface utilisateur permettant de consulter aisément :

        i. toutes les données personnelles collectées par l'outil sur un utilisateur (par service applicatif s'il y en a plusieurs), y compris les traces de connexion et d'activité
        ii. toutes les données et documents auquel l'utilisateur accède sur chaque service applicatif
        iii. tous les accès donnés à des utilisateurs et à des tiers sur les données et sur les documents

        L'utilisateur doit pouvoir supprimer directement ses données et ses historiques de traces (log et activité) dans le respect des règles de conservation mises en œuvre par la politique de sécurité des systèmes d'information de l'Établissement.

        L'utilisateur doit pouvoir définir le sort de ses données post-mortem dans le respect des règles de conservation minimale mises en œuvre par la politique de sécurité des systèmes d'information de l'Établissement (règles de conservation des archives privées et publiques).

        Cette interface utilisateur doit être accessible aux fonctions de Délégué à la protection des données (DPO) et Responsable de la sécurité des systèmes d'information (RSSI) uniquement.

    b. GESTION DES COMPTES - Les Opérateurs doivent proposer un outil de gestion du cycle de vie des comptes (création / modification / validation / suppression / transfert du compte et des données avec option de calibrage du périmètre de données transférés par application).

    c. Les Opérateurs doivent proposer des outils ergonomiques à la main des DPO et des utilisateurs permettant de suivre les exercices de droit.

12. GESTION DES VIOLATIONS DE DONNÉES - Les Opérateurs doivent proposer des outils ergonomiques à la main des DPO permettant de suivre les violations de données.

Annexe 1 - Grille de synthèse des contacts et références utiles

Grille à compléter par l'éditeur et mettre à disposition des Établissements

Contacts et références utiles de l'éditeur	
Nom de la société éditrice	(à compléter)
Contact dirigeant	(à compléter)
Pays de son siège social	(à compléter)
Droit ou pratique du pays tiers, si hors UE ou pays non adéquat (selon la CNIL)[14]	(à compléter)
Contact DPO	(à compléter)
Contact RSSI	(à compléter)
Contact Assistance informatique	(à compléter)
Contact juriste	(à compléter)
Lien.s vers la politique de protection des données	(à compléter)
Lien.s vers la politique de sécurité des systèmes d'information (PSSI)	(à compléter)
Liens. vers le niveau de certification / norme (eg. famille ISO27000, etc.)	(à compléter)
Lien.s vers des audits de vulnérabilité ou/et de test(s) intrusif(s)	(à compléter)
Lien vers une attestation de non-présence de backdoor délivré par un organisme qualifié en matière de sécurité des systèmes d'information ou tiers équivalent	(à compléter)
Lien vers l'analyse d'impact sur la protection des données (AIPD)	(à compléter)
Lien vers un rapport de transparence[15]	(à compléter)

[14] **Obligations de transparence -** L'importateur s'engage à fournir l'information utile sur les conditions d'accès aux données par les autorités publiques, y compris dans le domaine du renseignement : Il s'agit d'énumérer les lois et réglementations du pays de destination applicables à l'importateur ou à ses (sous) sous-traitants permettant aux autorités publiques d'accéder aux données à caractère personnel faisant l'objet du transfert, notamment dans les domaines du renseignement, de l'application de la loi, surveillance administrative et réglementaire applicable aux données transférées, production d'informations et statistiques basées sur l'expérience de l'importateur ou des rapports provenant de diverses sources (par exemple partenaires, sources ouvertes, jurisprudence nationale et décisions des organes de contrôle) sur l'accès du public autorités aux données personnelles, indication des mesures prises pour empêcher l'accès aux données transférées, production d'informations suffisamment détaillées sur toutes les demandes d'accès aux données à caractère personnel des autorités publiques que l'importateur a reçues au cours d'une période déterminée et comprenant des informations sur les demandes reçues, les données demandées, l'organisme demandeur et la base juridique de la divulgation et dans quelle mesure l'importateur a divulgué la demande de données.

[15] **Production d'un rapport de transparence -** L'importateur publie au moins une fois par an à l'exportateur un rapport de transparence résumant les demandes d'accès reçues des autorités publiques et la réponse fournie, ainsi que le raisonnement juridique et les acteurs impliqués.

Niveau de conformité au Référentiel Général de Sécurité (RGS)	(à compléter)
Accès aux données de l'Établissement	(cocher les cases utiles) ❑ Editeur ❑ Filiales de l'éditeur (si oui, préciser) ❑ Partenaire de l'éditeur (si oui, préciser) ❑ Sous-traitants de l'éditeur (si oui, préciser) ❑ Autres (si oui, préciser)

Annexe 2 - Grille des sous-traitants ultérieurs et autres tiers accédant aux données ou intervenant potentiellement dans la chaîne de traitement des données de l'Établissement

Grille à compléter par l'éditeur et mettre à disposition des Établissements

Sous-traitance ultérieure		
Nature de la prestation Exemple : Hébergement	Société.s	(à compléter)
	Pays de son siège social	(à compléter)
	Pays où sont localisés les serveurs d'hébergement des données de l'Établissement	(à compléter)
	Existence d'un contrat / clause sur la protection des données	OUI/NON + En cas d'export vers un pays tiers : ☐ Décision d'adéquation de la commission Européenne ☐ Clauses contractuelles type de la commission Européenne avec des clauses additionnelles (mesures supplémentaires post-Schrems II) ☐Binding Corporate Rules (BCR) ☐Clauses contractuelles spécifiques validé par une autorité de contrôle européenne
Nature de la prestation (à compléter[16]) *L'éditeur complète le tableau avec les natures de sous-traitance ultérieure qui le concerne*	Société.s	(à compléter)
	Pays de son siège social	(à compléter)
	Pays où sont localisés les serveurs	(à compléter)

[16] **L'éditeur complète le tableau avec les natures de sous-traitance ultérieure qui le concerne**. Par exemple : Maintenance Logiciel, Maintenance Matériel, Achat de licences de logiciels, Achat de matériel, Récupération de support de données/Mise au rebut, Télémaintenance/Administration à distance, Interconnexion réseau, Développement logiciel et/ou application, Installation/Integration/Déploiement, Infogérance, Monitoring, Cloud (PaaS, SaaS, IaaS), messagerie collaborative, visioconférence, etc

	d'hébergement des données de l'établissement	
	Existence d'un contrat / clause sur la protection des données	OUI/NON + En cas d'export vers un pays tiers : ☐ Décision d'adéquation de la commission Européenne ☐ Clauses contractuelles type de la commission Européenne avec des clauses additionnelles (mesures supplémentaires post-Schrems II) ☐Binding Corporate Rules (BCR) ☐Clauses contractuelles spécifiques validé par une autorité de contrôle européenne
etc.	etc.	etc.