Annexe

Points sur lesquels les formulations de la charte pourraient être améliorées ou clarifiées[1].

Point 1

La charte pourrait indiquer expressément que les fournisseurs de services doivent veiller à ce que soient traitées les seules données pertinentes et proportionnées à la finalité poursuivie par le service numérique. Une telle stipulation permettrait de rappeler les dispositions de l'article 6-3° de la loi du 6 janvier 1978 modifiée, ainsi que le fait que le ministère lui-même dans certains actes réglementaire relatifs aux traitements qu'il met en œuvre, tels que, par exemple, le « gestionnaire d'accès aux ressources » (GAR) dont l'objet est de limiter, aux seules données nécessaires, la transmission des données personnelles des élèves et des enseignants aux fournisseurs de services numériques.

Point 2

Le point 2 est relatif à l'information des personnes concernées et renvoie, par une note de bas de page, à l'article 32 de la loi « Informatique et Libertés ». Au titre de cette information sont visées la nature des données recueillies et la nature de leur utilisation. L'article 32 de la loi du 6 janvier 1978 modifiée prévoit pourtant d'autres éléments devant figurer dans la mention informative destinée aux personnes concernées par un traitement de données à caractère personnel (par exemple, les catégories de destinataires, la durée de conservation des données, l'existence de transfert hors de l'Union Européenne). La rédaction de cette stipulation pourrait dès lors être complétée afin de renvoyer plus clairement à l'ensemble de ces mentions informatives.

Point 4

Conformément à l'article 34 de la loi « Informatique et Libertés », le point 4 de la charte précise que le fournisseur de service doit mettre en œuvre des mesures de sécurité correspondant, d'une part, à l'état de l'art des risques et des solutions et, d'autre part, aux instructions données par le responsable de traitement. La charte précise que l'état de l'art s'entend des standards et normes en vigueur.

A titre illustratif, la charte cite les normes ISO 27001 et 27018, respectivement relatives au management de la sécurité des informations et à la protection des données personnelles pour le fournisseur de *cloud* agissant en qualité de sous-traitant. Ces standards, pertinents en matière de sécurité des données personnelles, seraient néanmoins utilement complétés par des normes ISO axées sur la protection de la vie privée, telles que les normes 29100 concernant les principes à appliquer et la norme 29151 concernant les bonnes pratiques en matière de protection des données personnelles.

Point 5

Le point 5 de la charte recommande que l'hébergement en France ou dans l'UE soit privilégié. Le fait de s'engager à privilégier un tel hébergement constitue une mesure protectrice des droits des personnes concernées et en particulier des mineurs. La réflexion sur cette question

---

[1] Sans être exhaustif :

- la formule « *rappelant au respect des règles nationales et européennes en vigueur* » pourrait être précisée pour faire explicitement référence aux textes européen et nationaux relatifs à la protection des données ;
- la rédaction du point 5 sur les mesures de sécurité pourrait être simplifiée ;
- la définition des « *services grand public* » pourrait être clarifiée.

pourrait utilement être poursuivie en concertation avec la CNIL. A cet égard, il doit être relevé que la note d'information du 5 avril 2016 relative à l'informatique en nuage, le ministère de l'intérieur (DGCL) et celui de la culture (direction des archives de France) préconisent le recours à un *cloud* souverain pour toute institution produisant des archives publiques[2].

Dans ces conditions, se pose la question de savoir si l'hébergement hors UE de données de mineurs traitées par une administration dans le cadre de ses missions de service public est opportun.

Règles d'engagement

La charte précise en outre que « *tout manquement aux engagements pris dans la charte sera notifié au signataire défaillant* [...], *celui-ci aura trois mois pour se mettre en conformité ou pour contester les griefs. Dans ce dernier cas, la Commission de suivi sera saisie par les promoteurs de la Charte, elle fera part de son avis motivé* ». Si la dénonciation de l'adhésion d'un fournisseur de service peut avoir un impact indéniable en termes d'image et donc en termes économiques, les sanctions d'un non-respect des stipulations de la charte pourraient être renforcées. A l'instar des codes éthiques des entreprises qui prévoient généralement que l'inobservation d'un engagement constitue une faute susceptible de sanction, le manquement aux stipulations de la charte devrait pouvoir permettre une sanction autre que la simple dénonciation de l'adhésion.

[2] http://circulaires.legifrance.gouv.fr/pdf/2016/05/cir_40948.pdf?wb48617274=7BA80F4A.