Checklist générale d'éléments à analyser dans le cadre des services cloud

1 Fournisseur

☐ Y a-t-il des informations publiquement disponibles sur le fournisseur et ses pratiques en matière de protection des données ?

☐ Le fournisseur détient-il des certifications ou accréditations d'intérêt ?

☐ Le fournisseur a-t-il fait l'objet d'une attention médiatique négative particulière durant les derniers mois, notamment concernant la sécurité et la gouvernance ?

☐ Le fournisseur est-il disposé à remettre une copie des rapports d'audit qu'il a fait réaliser sur ses services, voire ceux de ses sous-traitants ?

☐ A quel droit le fournisseur est-il soumis ?

☐ Le fournisseur a-t-il du personnel qualifié en matière de sécurité et de protection des données ?

2 Sous-traitants (ultérieurs) du fournisseur

☐ Le fournisseur mandate-t-il des sous-traitants (ultérieurs) ?

☐ Où sont-ils localisés ?

☐ Quelles sont leurs tâches ?

☐ Ont-ils accès aux données ? Si oui, dans quels buts et depuis quels pays ?

☐ A quelles obligations contractuelles sont-ils soumis ? En particulier, ces obligations sont-elles au moins équivalentes à celles imposées par l'entreprise au fournisseur ?

☐ Comment le fournisseur sélectionne-t-il et gère-t-il ses sous-traitants ?

☐ Est-il disposé à fournir de la documentation sur ses sous-traitants à l'entreprise ?

☐ Le fournisseur est-il en mesure d'informer l'entreprise d'un changement de sous-traitant (ultérieur) ?

3 Traitements

☐ Quelles sont les catégories de données personnelles qui seront traitées dans le *cloud* ?

☐ Quelles sont les catégories de personnes concernées dont les données seront traitées dans le *cloud* ?

☐ Quels sont les traitements qui seront mis en œuvre par l'entreprise dans le *cloud*, y compris par le fournisseur sur instruction du responsable du traitement ?

☐ Quels sont ceux qui seront mis en œuvre par le fournisseur dans son propre intérêt (en tant que responsable du traitement), et ont-ils été analysés par l'entreprise ?

☐ Où les données personnelles (y compris les sauvegardes) seront-elles stockées ?

☐ Combien de temps sont-elles conservées et pour quelles raisons ?

4 Droits des personnes

☐ Le fournisseur collaborera-t-il à la gestion de l'exercice des droits par les personnes concernées ?

☐ Le fournisseur transmettra-t-il sans délai au responsable du traitement les demandes d'exercice des droits ?

5 Sécurité

☐ Quelles mesures de sécurité organisationnelles et techniques sont en place ?

☐ En regard des risques détectés et évalués par l'entreprise, le fournisseur met-il en place les mesures de sécurité adéquates ?

☐ Le fournisseur a-t-il établi des plans pour maintenir son activité en cas d'incident, pour revenir à une activité normale après un incident ?

☐ Des sauvegardes des données sont-elles effectuées ? Combien sur une période considérée ? Combien de temps sont-elles conservées ? Des tests de restauration sont-ils effectués ?

☐ Les paramètres par défaut sont-ils « *privacy-friendly* » pour les utilisateurs ?

6 Contrat

☐ Le contrat de service contient-il des clauses de protection des données, voire un DPA en annexe ?

☐ Le contrat et le DPA respectent-ils les exigences de l'art. 9 LPD et de l'art. 28 RGPD sur la sous-traitance ?

☐ Les données seront-elles restituées ou détruites à l'échéance du contrat ? Si elles sont restituées, dans quel format le seront-elles ? Dans quel délai ?

☐ En cas de litige avec l'entreprise, le fournisseur garantit-il à celle-ci un accès aux données ?

☐ Est-il prêt à fournir des certifications et rapports basés sur des normes internationalement reconnues ?

☐ Le fournisseur est-il prêt à se faire auditer, aux frais de l'entreprise ?

☐ Le fournisseur est-il prêt à corriger les manquements constatés lors de l'audit, à ses propres frais ?

☐ Le fournisseur est-il au bénéfice de polices d'assurance contre des risques particuliers (not. événements naturels), et quel est le montant couvert ?

☐ Le fournisseur tient-il un registre des traitements mis en œuvre pour le compte de l'entreprise ? Est-il disposé à en remettre une copie à celle-ci ?

☐ Quels sont le for et le droit applicable en cas de litige ?

7 Transferts

☐ L'utilisation du *cloud* implique-t-elle des transferts de données à l'étranger ? Si oui, quel mécanisme régit les transferts ?

☐ Les risques ont-ils été évalués ?

☐ Le fournisseur a-t-il reçu pour instruction de transférer les données dans un ou plusieurs pays spécifiques ?

☐ Y a-t-il un transfert de données lors du recours par le fournisseur à des sous-traitants ?

8 Performance

☐ L'entreprise dispose-t-elle d'outils ou indicateurs pour surveiller les performances du fournisseur ?

☐ Quel est le taux de disponibilité minimum que le fournisseur garantit, ainsi que ses plans de capacités ?

☐ Quelles sont les disponibilités du support technique ? Le fournisseur garantit-il une durée maximale de résolution des problèmes ?

☐ Le fournisseur détaille-t-il quels niveaux de service il est prêt à supporter en temps normal et lorsque survient une violation de la sécurité des données ?

9 Violations

☐ Le fournisseur s'engage-t-il à informer l'entreprise si des autorités accèdent ou tentent d'accéder aux données personnelles traitées ?

☐ Le fournisseur s'engage-t-il à notifier l'entreprise de la découverte d'une violation (potentielle) de la sécurité des données, dans les 24 heures suivant ladite découverte ?

☐ Le fournisseur s'engage-t-il à prêter assistance à l'entreprise pour la notification aux autorités ou aux personnes concernées de la violation de la sécurité des données ?

10 Gouvernance

☐ De manière générale, est-ce que les processus de gouvernance (not. informatique) de chaque partie parviennent à s'aligner ?

☐ L'entreprise a-t-elle prévu une stratégie de sortie (« *exit strategy* ») pour changer de fournisseur et migrer les données ?

☐ L'entreprise a-t-elle mis en place une politique ou des procédures pour assurer le respect de ses obligations légales lors de l'utilisation du *cloud* ?

☐ L'entreprise a-t-elle diligenté une analyse de risques, respectivement une analyse d'impact ou un *Transfer Impact Assessment* (TIA), avant d'utiliser le *cloud* ?

☐ L'entreprise a-t-il mis en place un processus de revue régulière (annuelle) des fournisseurs, y compris leurs sous-traitants ?

☐ L'entreprise a-t-elle un plan pour gérer avec le fournisseur les éventuels écarts par rapport à la loi, au contrat et au DPA ?

☐ Le fournisseur prévoit-il une information suffisamment en avance en cas de changements à venir dans la fourniture de ses services, et propose-t-il une alternative ?

