Annexe D : Cadre juridique pour l'utilisation de services d'informatique en nuage public au sein de l'administration fédérale (liste de contrôle)

La présente liste de contrôle a pour but de vous aider à vous poser les bonnes questions avant de « passer au nuage ». En d'autres termes, les données de votre unité administrative doivent-elles être transférées dans le nuage et, si oui, quelles mesures techniques doivent être prises pour les protéger ?

Les destinataires de la liste sont donc en premier lieu les collaborateurs des unités administratives qui, dans le cadre de projets, se posent pour la première fois la question de l'externalisation des données dans le nuage. La liste de contrôle peut toutefois aussi être utile aux collaborateurs expérimentés pour se remémorer les questions importantes concernant l'externalisation.

Elle vise en outre à ce que l'externalisation ou la non-externalisation de données dans le nuage soit documentée de manière à pouvoir être prouvée et retrouvée.

Important :

- La liste de contrôle peut être complétée par d'autres questions si nécessaire et en fonction de la situation.
- La classification des réponses nécessite une connaissance approfondie de la thématique et devrait donc être effectuée en concertation avec les services compétents.
- La liste de contrôle ne remplace PAS la documentation qui doit être établie dans le cadre, par exemple, l'analyse des besoins de protection ou du concept SIPD.
- Elle n'aborde pas non plus les questions relatives au contenu des contrats et ne fournit pas de réponses aux problèmes juridiques de fond liés à l'externalisation des données dans le nuage.

Instructions pour l'utilisation de la liste de contrôle

Dans un *premier temps*, il s'agit de répondre aux questions ci-dessous et de les classer en fonction de la barre qui se trouve sous chaque catégorie de questions. L'idée est de réfléchir, pour chaque question, à la zone dans laquelle la réponse doit être classée : plus les données à externaliser ou les réponses aux questions sont délicates/critiques/importantes, etc., plus leur classement dans la zone orange/rouge s'impose.

Les réponses doivent être classées en fonction du point de vue (subjectif) de l'office. Elles doivent être clarifiées avec différents experts ou services spécialisés (par ex. le service de communication pour les questions intéressant les médias).

Le but de l'exercice est d'obtenir une vue d'ensemble des questions ou des classifications qui permettent de classer schématiquement les possibilités et les défis d'une externalisation des données dans un nuage.

La *deuxième étape*, « Atténuation des risques », consiste à examiner comment les risques identifiés peuvent être minimisés sur le plan technique/organisationnel. Ce n'est qu'à l'issue de la deuxième étape qu'on pourra décider, dans le cadre d'une évaluation finale, si les données seront externalisées ou non.

La troisième étape consiste à procéder à l'évaluation finale et à documenter la décision d'externaliser ou non les données dans un nuage.

I. Étape : Questions concernant l'externalisation dans le nuage

1.1 Protection des données (voir partie 1 du rapport)

a) Questions possibles

1. Faut-il externaliser des données personnelles dans le nuage ? Si oui, lesquelles et à quoi servent-elles dans le cadre de l'exécution des tâches ?
2. Faut-il externaliser des données sensibles dans le nuage ? Si oui[1], lesquelles et à quoi servent-elles dans le cadre de l'exécution des tâches ?
3. Faut-il procéder à une analyse d'impact relative à la protection des données ? Celle-ci doit être effectuée lorsque le traitement de données prévu est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée.
4. Si nécessaire ou souhaité : les données personnelles peuvent-elles être anonymisées (dans ce cas, on ne parle plus de données personnelles) ou pseudonymisées (dans ce cas, il existe encore des données personnelles d'un point de vue juridique) ? Qui détient la clef en cas de pseudonymisation ?
5. Si nécessaire ou souhaité : les données peuvent-elles être cryptées ? Si oui, qui détient la clef (bring your own key; hold your own key) ?

b) Classification des réponses

1.2 Obligation de sauvegarder le secret (voir partie 2, ch. 2, du rapport)

a) Questions possibles

6. Existe-t-il une base légale spéciale interdisant l'externalisation dans un nuage ?
7. Les données sont-elles soumises à des dispositions légales spéciales en matière de secret ?
8. Si nécessaire ou souhaité : les données peuvent-elles être protégées adéquatement, conformément à leur besoin de protection ?

b) Classification des réponses

1.3 Sécurité de l'information (voir partie 2, ch. 3 et 4 du rapport)

a) Questions possibles

9. La classification des informations conformément à l'OPrI (à l'avenir LSI) est-elle encore correcte, les critères de classification ont-ils été réexaminés ? En particulier :

[1] Attention, dans ce cas il faut informer le NCSC, le PFPDT et la CSG, conformément à la stratégie d'informatique en nuage.

9.1. Y a-t-il d'autres intérêts au maintien du secret à prendre en compte dans ce contexte ?
9.2. L'action des autorités peut-elle être compromise ou empêchée si les données sont connues ?
10. Les informations classifiées peuvent-elles être protégées de manière adéquate (par ex. cryptées), conformément à leur besoin de protection, en cas d'utilisation de l'informatique en nuage ? Les exigences en matière de protection informatique de base dans l'administration fédérale peuvent-elles être respectées malgré une externalisation ?

b) Classification des réponses

1.4 Intégrité (voir partie 2 du rapport)

a) Questions possibles

11. Est-il possible de garantir que, même en cas d'externalisation des données, les processus de traitement sont documentés de manière traçable, de sorte que les données ne soient pas modifiées sans qu'on le remarque ou illicitement ?
12. Quelles seraient les conséquences d'une modification des données passée inaperçue ?
13. Est-il garanti qu'aucune erreur ne se produira lors de la transmission des données et que celles-ci ne peuvent pas être modifiées ?
14. La récupération des données peut-elle être garantie en cas d'externalisation ?

b) Classification des réponses

1.5 Disponibilité/Résilience/Criticité opérationnelle

a) Questions possibles

15. Qui utilise les données ? Les citoyens doivent-ils y avoir accès ou « seulement » les collaborateurs ?
16. Quelles sont les exigences en matière de disponibilité ? 24/7 (pour les ambassades CH, les douanes, etc.) ? Heures de bureau (HEC) ?
17. Quelle est la durée maximale d'une interruption de l'accès ?
18. Existe-t-il des dispositions légales/contractuelles (par ex. de l'UE) réglant la disponibilité ?
19. Quelles seraient les conséquences de l'indisponibilité des données ?
20. Existe-t-il des solutions d'évitement (*Business Continuity Management*) ?

b) Classification des réponses

1.6 Souveraineté/bases juridiques étrangères (voir partie 2 du rapport)

a) Questions possibles

21. Y a-t-il des raisons pour que les données soient traitées exclusivement en Suisse ?
    21.1. Bases légales ?
    21.2. Raisons politiques ?
22. Existe-t-il des normes juridiques étrangères qui limitent ou interdisent certaines mesures nécessaires à la protection des données dans certains États/certaines régions ?
23. Quelles sont les conséquences pour l'administration fédérale si les données sont divulguées en vertu de bases juridiques internationales (par ex. saisie)
24. Quelles sont les conséquences d'une interdiction (temporaire) d'accès aux données en raison de sanctions étatiques ?
25. Quelles sont les conséquences d'une interdiction de cryptage des données en raison de sanctions étatiques ?

b) Classification des réponses

1.7 Acceptabilité politique d'une externalisation/intérêt des médias

a) Questions possibles

26. Quel est l'intérêt des médias pour les données à externaliser ?
27. Quel est l'intérêt des médias lorsque les données sont divulguées de manière illicite ?
28. Existe-t-il un risque de perte de données en cas d'externalisation des données dans un nuage ? Si oui, de quelle ampleur ? Conséquences ?

b) Classification des réponses

1.8 Stratégie de sortie du nuage

a) Questions possibles

29. Quelle pourrait être une stratégie de sortie du nuage ?

30. Quelles sont les solutions techniques ?
31. Quelles ressources une sortie du nuage exigerait-elle, que coûterait-elle ?

b) Classification des réponses

1.9 Vendor Lock-In

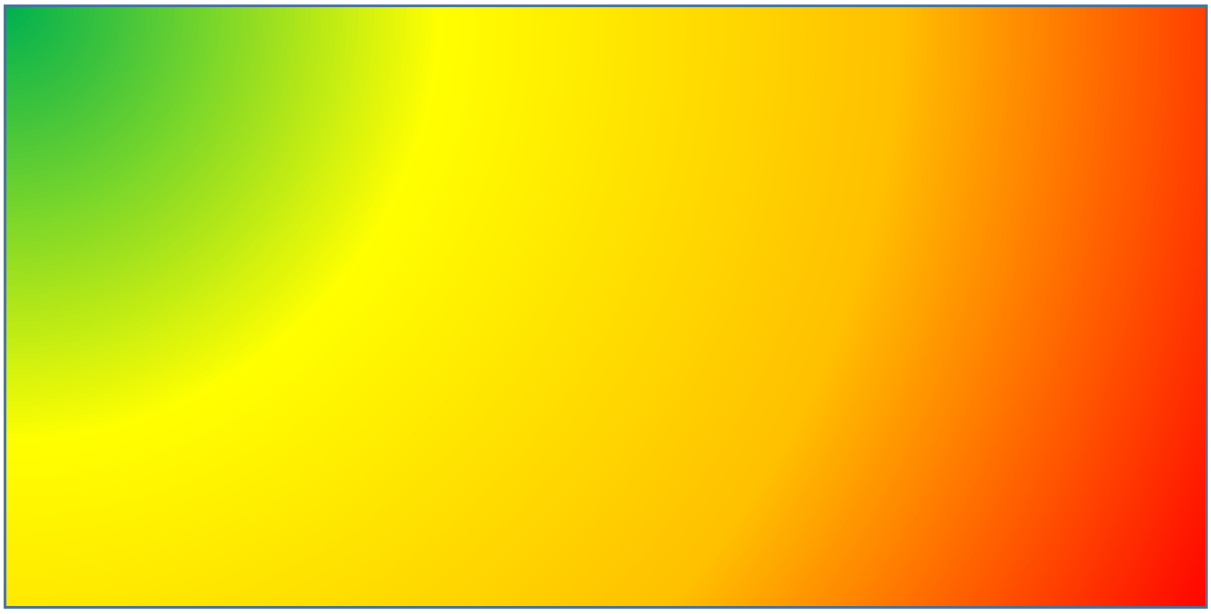
a) Questions possibles

32. Existe-t-il un concept de migration pour passer à un autre fournisseur de services nuagiques ?
33. Quelles ressources une migration exigerait-elle, que coûterait-elle ?
34. Le type de collecte de données permet-il d'externaliser les jeux de données séparément dans différents nuages ? Quelles seraient les charges, à combien s'élèveraient les coûts ?
35. Existe-t-il une possibilité de rendre la solution portable pour des normes ouvertes ?

b) Classification des réponses

2. Vue d'ensemble de l'évaluation des réponses

Les réponses données (barres) aux ch. 1 à 33 peuvent être regroupées ici.



II. Étape : Atténuation des risques (voir partie 2, ch. 1.4 du rapport)

Il convient d'évaluer les mesures possibles pour atténuer les risques identifiés à l'étape I (« que doit proposer un fournisseur de services informatiques en nuage pour que l'on puisse oser se tourner vers le nuage malgré la classification orange/rouge », « quelles mesures internes peuvent être prises »). Il convient également de déterminer quels risques peuvent/doivent être assumés.

[*Liens vers les documents suivants*] :

- Annexe C : Risques et mesures
- Analyses GAP des fournisseurs de services nuagiques
- Modèle d'analyse des risques OMC 20007

III. Étape : Évaluation finale et décision

Une fois que toutes les questions ont été posées et que les risques ont été évalués, il faut prendre une décision finale pour ou contre l'externalisation des données vers le nuage. Celle-ci doit se fonder sur les connaissances acquises et documenter les différentes considérations dans sa motivation.