FAQ concernant le rapport « Cadre juridique pour l’utilisation de services d’informatique en nuage public au sein de l’administration fédérale »

Table des matières

1 Introduction

Le rapport « Cadre juridique pour l'utilisation de services d'informatique en nuage public au sein de l'administration fédérale » de la Chancellerie fédérale donne un aperçu des principales questions juridiques qui se posent au sein de l'administration fédérale en rapport avec l'externalisation de données dans un nuage (étranger). Les présentes FAQ les complètent et répondent aux questions pratiques en relation avec l'externalisation des données dans un nuage. Elles seront régulièrement vérifiées et adaptées afin de correspondre à l'état actuel des connaissances. Elles sont classées par thème et renvoient au rapport précité[1].

2 Questions générales

2.1 Solution nuagique ou solution sur site, quelle est la différence ?

Question : Qu'est-ce qui change lorsque les données sont transférées vers un nuage plutôt que gardées sur site ? En d'autres termes, quelle est la différence entre le traitement des données dans le nuage et le traitement sur site ?

Réponse : Hormis le fait que l'unité administrative compétente n'a plus elle-même le contrôle physique des moyens informatiques en cas d'externalisation de données et d'applications dans un nuage, trois facteurs en particulier contribuent à la complexité juridique, mais aussi technique, des solutions nuagiques par rapport aux solutions sur site et doivent être pris en compte lors de l'évaluation des risques :

- À l'heure actuelle, les services issus de nuages publics des grands fournisseurs (fournisseurs hyperscalaires), en particulier, sont potentiellement fournis en tout ou partie à l'étranger (emplacements des serveurs, accès au support). La tendance à la diminution du contrôle sur l'environnement juridique (par ex. en ce qui concerne l'adéquation de la législation sur la protection des données dans le pays de destination et le risque d'accès par les autorités) doit donc être compensée par des mesures contractuelles, techniques et organisationnelles.
- Recours à des sous-traitants : pour l'exécution du mandat, les fournisseurs de services nuagiques (pour les solutions en nuage privé aussi) font généralement appel à des sous-traitants qui accomplissent certaines tâches. Par ailleurs, ces sous-traitants exécutent parfois leurs tâches à partir de pays tiers.
- Dépendance vis-à-vis de tiers : les solutions nuagiques peuvent entraîner une dépendance importante vis-à-vis de certains fournisseurs, notamment en ce qui concerne la disponibilité des services.

Décider quels sont les risques résiduels acceptables par rapport au traitement des données dans des centres de calcul de la Confédération (sur site) — dans les limites du droit applicable — est une question de conduite qui doit être prise par l'unité administrative et sollicitée par les responsables du projet. Cette décision doit être prise en fonction de la nature des données à transférer sur la base d'une analyse du cadre juridique et des risques. L'analyse des risques doit tenir compte des facteurs de risque existants dans le cas d'application concret et des mesures prises pour les atténuer. L'utilisation du nuage est toutefois interdite pour les informations classifiées « secret », conformément aux règles de la protection des informations.

Renvoi : partie 1 (ch. 3.1 et 3.2 et annexes C à E), partie 2 (ch. 1.4 à 1.7 et 4)

2.2 Secret de fonction

Question : Qu'est-ce qui change avec la modification de l'art. 320 CP (version du 1.1.2023) ?

Réponse : En vertu du nouvel art. 320, ch. 1, CP, les fournisseurs de services nuagiques sont soumis au secret de fonction lorsqu'ils traitent des données de l'administration. Le fournisseur est punissable lorsqu'il ne respecte pas les mesures techniques éventuelles ou ses obligations contractuelles et lorsqu'il révèle des informations couvertes par le secret de fonction.

[1] Informatique en nuage (admin.ch).

L'externalisation de la conservation des données dans le nuage ne constitue pas en soi une violation du secret de fonction.

Renvoi : partie 2 (ch. 2)

2.3 Mesures contractuelles

Question : Quelles mesures contractuelles peuvent contribuer à réduire les risques généraux liés à l'externalisation des données ? Pourquoi de telles mesures sont-elles nécessaires ?

Réponse : Les risques peuvent être limités par des mesures contractuelles, en plus des mesures techniques et organisationnelles. Des mesures contractuelles peuvent être utiles dans les domaines suivants :

- **Risques de conformité** : en particulier, réglementation des obligations du fournisseur de services nuagiques et de ses sous-traitants, réglementation du recours à des sous-traitants, pouvoirs de contrôle du client, obligations d'information du fournisseur en cas d'incidents liés à la sécurité, garantie d'un niveau de protection des données adéquat et du fait que les données ne peuvent être traitées que dans un pays étranger donné, obligation du fournisseur de se conformer au droit suisse pertinent et d'accepter la Suisse comme for, réglementation de la procédure en cas de demande d'accès par des autorités étrangères, réglementation de la défense en cas d'attaque, exclusion des modifications unilatérales du contrat, droits de résiliation en cas de modifications du contrat, responsabilité adéquate en cas de violation du contrat.
- **Risques de continuité des activités** : en particulier, réglementation en cas de modification du service par le fournisseur, option de sortie en cas de modification des conditions, réglementation de l'exportation et de la migration des données, réglementation de la procédure de récupération, peines conventionnelles pour les interruptions de service imprévues particulièrement critiques, réglementation claire des compétences des administrateurs, réglementation des procédures et des contrôles de sécurité des collaborateurs du fournisseur.
- **Risques politiques** : en particulier, accord sur des sites de traitement stables sous l'angle juridique et politique, accord sur des clauses de sortie.
- **Risques techniques** : notamment rapports d'audit du fournisseur documentant la sécurité des données, obligation du fournisseur d'annoncer les cyberattaques graves, obligation du fournisseur de respecter les normes ISO, accès du service fédéral responsable aux résultats des audits, garanties contractuelles concernant la détection des points faibles et la communication précoce par le fournisseur, directives concernant la sécurité des personnes chez le fournisseur.

Les mesures contractuelles sont en outre importantes pour garantir un traitement des données dans le nuage compatible avec le droit suisse. Elles sont en particulier essentielles et absolument nécessaires du point de vue de la protection des données lorsque, exceptionnellement, les données sont traitées dans un État qui ne dispose pas d'une législation adéquate en matière de protection des données.

Renvoi : partie 1 (ch. 3), partie 2 (ch. 1.3 à 1.7), annexe C

2.4 Protection des données

Question : Existe-t-il des recommandations et des directives générales concernant la protection des données d'un point de vue juridique ?

Réponse : Dans la mesure où les bases juridiques nécessaires au traitement existent et que le devoir de diligence est respecté lors du choix du fournisseur de services nuagiques, aucune précaution juridique particulière n'est nécessaire. Le traitement de données personnelles au moyen de services en nuage public présente toutefois un risque particulier, selon le PFPDT, et nécessite une analyse d'impact relative à la protection des données personnelles. Par ailleurs, la loi fédérale sur la protection des données fixe des exigences visant à garantir la sécurité des données.

L'évaluation des risques d'un point de vue commercial ainsi que les directives et les prescriptions internes jouent aussi un rôle, au-delà du cadre juridique, dans l'appréciation

globale de l'admissibilité du traitement des données par les fournisseurs de services en nuage public. La directive Si001 « Protection informatique de base dans l'administration fédérale » est essentielle : elle fixe, de manière contraignante, les exigences organisationnelles, personnelles et techniques minimales en matière de sécurité. La protection informatique de base est la norme minimale pour les objets informatiques à protéger.

L'analyse des besoins de protection (directive P041) est le point de départ de ce processus. Elle sert notamment à analyser si les données à externaliser sont en principe accessibles ou si elles sont soumises à des exigences de confidentialité particulières, fondées sur des bases juridiques spécifiques. Il convient par ailleurs de vérifier si des données personnelles sont traitées et s'il faut par conséquent procéder à une analyse d'impact relative à la protection des données personnelles. Celle-ci évalue en particulier les risques, définit des mesures et décrit leur mise en œuvre. Il convient également de vérifier si les fournisseurs de services en nuage public doivent fournir des données à leur gouvernement conformément au système juridique de leur pays d'origine et quelles sont les régions de conservation des données qu'ils proposent.

Sur cette base, on déterminera les mesures de protection appropriées, notamment les mesures techniques et organisationnelles de protection des données et des informations (cf. p. ex. art. 11 OTNI).

Si l'analyse des besoins de protection révèle un besoin de protection accru, un concept de sécurité de l'information et de protection des données (concept SIPD) et une analyse des risques doivent être établis en plus de la documentation relative à la mise en œuvre de la protection informatique de base (directive P042). Le concept SIPD décrit les mesures nécessaires au maintien et à l'amélioration de la sécurité de l'information et de la protection des données et résume ces deux aspects dans le projet.

Renvoi : art. 8 LPD ; art. 14b ss OPCy, partie 2 (ch. 2.2.2), directive Si001 (Protection informatique de base dans l'administration fédérale), directive P041 (Analyse des besoins de protection), directive P042 (concept SIPD), SB020 — SB020- Stratégie d'informatique en nuage de l'administration fédérale.

2.5 Types de données à externaliser

Question : Quels types de données relèvent de la LPD, de la LSI ou du secret de fonction ?

Réponse : Ces bases juridiques visent des objectifs différents.

La LPD vise à garantir l'autodétermination informationnelle.

La LSI, par contre, règle la protection des informations, qu'il s'agisse ou non de données personnelles. C'est la classification en fonction des intérêts de la Confédération qui est déterminante.

Le secret de fonction s'applique dans le contexte de la révélation d'une certaine catégorie d'informations, notamment pour assurer le bon fonctionnement de l'administration.

Les objets à protéger peuvent être décrits sommairement comme suit :

LPD	LSI	Secret de fonction (art. 320 CP)
Données personnelles : toutes les informations concernant une personne physique identifiée ou identifiable	Informations classifiées : • « secret » : susceptibles de nuire gravement aux intérêts du pays si elles sont portées à la connaissance d'une personne non autorisée • « confidentiel » : susceptibles de nuire considérablement aux intérêts du pays si elles sont portées à la connaissance d'une personne non autorisée • « interne » (RESTRICTED ou classification équivalente d'informations provenant de l'étranger) : susceptibles de nuire aux intérêts du pays si elles sont portées à la connaissance d'une personne non autorisée	Informations confiées à une personne en sa qualité de membre d'une autorité ou de fonctionnaire, ou dont il a eu connaissance à raison de sa charge ou de son emploi ou en tant qu'auxiliaire d'une autorité ou d'un fonctionnaire On notera que le principe de la transparence limite la portée du secret de fonction (cf. explications dans le rapport).

Renvoi : art. 5, let. a, et 2, al. 2 à 4, LPD, partie 2 (ch. 1), art. 5 à 7, OPrI, partie 2 (ch. 4), art. 320 CP, art. 3, 4, 7 et 8, LTrans, partie 2 (ch. 2).

2.6 Sous-traitance du traitement des données

Question : Qu'est-ce qu'un auxiliaire ? À quelles conditions un sous-traitant peut-il à faire appel à un auxiliaire ?

Réponse : La notion d'auxiliaire est pertinente dans le contexte du secret de fonction. Par analogie avec le secret professionnel visé à l'art. 321 CP, les « auxiliaires » sont les personnes qui assistent le détenteur du secret dans son activité professionnelle et qui ont ainsi connaissance des faits. Les auxiliaires tels que les fournisseurs de services nuagiques et leurs sous-traitants sont donc inclus dans le cercle des détenteurs du secret de fonction visés au nouvel art. 320, ch. 1 CP.

Le traitement de données personnelles peut être confié à un sous-traitant si seuls sont effectués les traitements que le responsable du traitement serait en droit d'effectuer lui — même et qu'aucune obligation légale ou contractuelle de garder le secret n'interdise leur transfert. La sécurité des données, en particulier, doit être garantie. Si le sous-traitant fait appel à des sous-sous-traitants, le mandant doit s'assurer, par des clauses contractuelles appropriées et, le cas échéant, par des mesures techniques, que ces derniers sont liés par les mêmes règles que le fournisseur de services nuagiques lui-même. Le sous-traitant doit obtenir l'autorisation préalable du responsable du traitement. Il peut faire valoir les mêmes motifs justificatifs que pour une sous-traitance simple.

Renvoi : art. 9 LPD, art. 11 OTNI, partie 2 (ch. 1.5 et 2), art. 320 CP, PK StGB-TRECHSEL/VEST (art. 321, note 13)

2.7 Responsabilité de la protection informatique de base

Question : Qui assure le respect de la protection informatique de base pendant l'exploitation ?

Réponse : La mise en œuvre des consignes et des mesures de sécurité doit être documentée et contrôlée par les unités administratives responsables. La documentation doit être contrôlée et signée au moins par :

a) le responsable de l'objet à protéger,

b) le délégué à la sécurité informatique de l'unité administrative responsable,

c) le mandant (dans le cas d'un projet), et

d) le responsable du processus d'affaires

En outre, les signataires confirment que, selon leur évaluation, tous les fournisseurs de prestations (FP) participant à l'exploitation de l'objet à protéger répondent aux exigences les concernant.

Renvoi : directive Si001 (Protection informatique de base dans l'administration fédérale).

2.8 Configuration

Question : Existe-t-il des recommandations générales en matière de sécurité pour les paramètres, les autorisations, etc.

Réponse : Avant sa première mise en service, l'objet à protéger doit être configuré et paramétré de façon à être protégé contre tout accès non autorisé, être renforcé, si cela est techniquement possible, être exploité dans une configuration minimale nécessaire à l'accomplissement des tâches qui ne peut pas être modifiée par un utilisateur (en d'autres termes, les interfaces, modules et fonctions non utilisés doivent être désactivés) et permettre un enregistrement et une évaluation rapide des activités et événements importants pour la sécurité (avec horodatage). L'activation, la modification, la désactivation et la désinstallation des configurations et des paramètres de sécurité requièrent une autorisation. Le cercle des personnes autorisées à traiter les données est restreint et contrôlé par des outils de gestion des identités.

Renvoi : directive Si001 (Protection informatique de base dans l'administration fédérale).

2.9 Procédures en cas d'incident de sécurité

Question : Existe-t-il une procédure réglementée en cas d'incident de sécurité (par ex. perte de données, attaque par rançongiciel) ?

Réponse : Lorsqu'un incident de sécurité se produit (par ex. fuite de données, attaque par rançongiciel, etc.), la sécurité des données a été violée au regard du droit de la protection des données. Lorsque des données personnelles sont concernées, l'art. 24 LPD prévoit en outre une obligation d'annonce qui s'applique explicitement aux sous-traitants (fournisseurs de services nuagiques compris).

Le responsable du traitement (ou son sous-traitant) annonce dans les meilleurs délais au PFPDT les cas de violation de la sécurité des données entraînant vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. La violation peut souvent atteindre cette intensité lorsque des données sont perdues. L'annonce doit en particulier indiquer les mesures prises ou envisagées. Le responsable du traitement doit en outre informer la personne concernée lorsque cela est nécessaire à sa protection ou lorsque le PFPDT l'exige.

Par ailleurs, l'incident doit être annoncé au NCSC même si aucune donnée personnelle n'est concernée.

Renvoi : art. 24 LPD, partie 2 (ch. 1.3) ; Cyberattaque — que faire ? Informations et aide-mémoire.

2.10 Accès du sous-traitant aux données

Question : Le sous-traitant peut-il accéder aux données (en clair) ? Si oui, dans quels cas ?

Réponse : Les fournisseurs externes de prestations peuvent obtenir l'accès à des données qui ne sont pas accessibles au public si les conditions de l'art. 9 LPD et de l'art. 11 OTNI sont remplies :

- l'accès doit être *nécessaire* pour fournir une prestation (en d'autres termes, les données doivent impérativement être disponibles pour que le prestataire puisse exécuter son mandat) ou la fourniture de la prestation nécessiterait un effort disproportionné sans accès aux données (ou avec un accès limité à des données dépersonnalisées ou cryptées) ;

- l'autorité responsable des données a donné son accord par écrit ;
- des mesures contractuelles, organisationnelles et techniques appropriées ont été prises pour éviter que les données soient accessibles à des tiers.

Le sous-traitant ne peut donc accéder à des données en clair et les traiter lui-même que dans des cas très précis et convenus à l'avance (par ex. aux fins du support). L'accès aux données secondaires, en particulier, fait exception à cette règle, car elles sont généralement collectées et traitées par le fournisseur de services nuagiques pour la facturation de ses services.

Renvoi : art. 9 LPD, art. 11 OTNI, partie 2 (ch. 1.2.2, 1.5, 2.2.2.2), annexes C à E

3 Communication de données à l'étranger

3.1 Possibilité de communiquer des données à l'étranger

Question : Quand des données peuvent-elles être communiquées à l'étranger ?

Réponse : Des données personnelles peuvent être communiquées à l'étranger si le Conseil fédéral a constaté que l'État concerné dispose d'une législation assurant un niveau de protection adéquat (art. 16, al. 1, LPD). C'est le cas des États mentionnés dans l'annexe 1 de l'ordonnance sur la protection des données (OPDo). Les États membres de l'UE, le Royaume-Uni, l'Argentine et la Nouvelle-Zélande remplissent aujourd'hui cette condition, contrairement aux États-Unis et à la Chine, par exemple.

En outre, dans certains cas exceptionnels, des données peuvent être transmises à des États qui ne disposent pas d'un niveau de protection des données adéquat, notamment lorsque la personne concernée a expressément consenti à leur communication (art. 17, al. 1, let. a, LPD).

Si, exceptionnellement, un traitement de données est nécessaire dans un État qui ne dispose pas d'une législation adéquate en matière de protection des données, il convient de prévoir une garantie contractuelle appropriée, par exemple au moyen de clauses standard approuvées ou mises à disposition par le PFPDT ou des garanties spécifiques élaborées par l'unité administrative compétente et communiquées au préalable au PFPDT. En outre, des mesures techniques et organisationnelles appropriées doivent être prises.

Renvoi : art. 16 ss LPD, annexe 1 OPDo, partie 2 (ch. 1.6)

3.2 Questions concernant l'US CLOUD Act et le FISA

Question : FISA et US CLOUD Act , de quoi s'agit-il ?

Réponse : Le FISA (Foreign Intelligence Surveillance Act) et le CLOUD Act (Clarifying Lawful Overseas Use of Data Act) sont des lois américaines qui permettent, dans certains cas, aux autorités américaines d'accéder à des données traitées ou hébergées hors des États-Unis, notamment par des entreprises ayant leur siège aux États-Unis ou ayant d'autres liens juridiques avec les États-Unis (*incorporated in the United States*).

- FISA : le FISA a des finalités de prévention et de surveillance à l'étranger. Il permet à certaines autorités américaines d'exiger l'obtention d'informations étrangères concernant certaines cibles. Les garanties procédurales sont limitées en cas d'accès aux données fondé sur le FISA. En outre, la transparence n'est pas garantie dans la mesure où les fournisseurs de services nuagiques ne sont pas autorisés à fournir des informations sur le fait qu'une autorité demande l'accès aux données (*gag order*) même s'ils disposent de moyens juridiques pour contester les ordres de surveillance.
- US CLOUD Act : dans le cadre d'une procédure judiciaire, cette loi permet aux autorités de poursuite pénale d'accéder aux données stockées chez le fournisseur de services nuagiques, sans procédure d'entraide judiciaire. Les mesures prises par les autorités en vertu de l'US CLOUD Act sont soumises à certaines conditions : seules les autorités de poursuite pénale peuvent se fonder sur cette base pour poursuivre des infractions

graves et les données ne doivent être communiquées par les fournisseurs de services nuagiques concernés que s'ils exercent un contrôle effectif ou juridique sur elles. Les fournisseurs de services nuagiques peuvent contester les mesures prises en vertu de l'US CLOUD ACT devant un tribunal américain, mais le recours n'est pas possible en Suisse.

Renvoi : partie 2 (ch. 1.7.2)

Question : Les filiales de sociétés américaines sont-elles aussi soumises à l'US CLOUD Act et au FISA ?

Réponse : En principe, les filiales européennes de sociétés américaines sont également soumises à ces dispositions. Toutefois, une injonction de production des autorités de poursuite pénale américaines qui leur est directement adressée ne peut pas être exécutée par la contrainte pénale en dehors du territoire américain. Il est donc fort probable que les autorités de poursuite pénale américaines adresseront leurs injonctions de production aux sociétés mères sises aux États-Unis. Une remise conforme au droit (américain) n'est possible que dans certaines conditions, notamment si la société mère a déjà accès aux données.

Renvoi : partie 2 (ch. 1.7.2)

Question : Comment peut-on réduire les risques liés à l'US CLOUD Act ou au FISA par des mesures contractuelles ?

Réponse : En ce qui concerne l'US CLOUD Act, on peut partir du principe suivant : les données des autorités suisses bénéficient d'une certaine protection contre l'accès par les autorités américaines, compte tenu des mécanismes procéduraux prévus par l'US CLOUD Act. Le risque d'accès — non conforme au droit du point de vue suisse — sur la base du FISA peut également être réduit à un niveau juridiquement acceptable si les mécanismes déjà prévus par le droit américain sont complétés contractuellement (en particulier l'obligation de contester une production de données). Dans la mesure où la loi le permet, des accords doivent notamment être conclus sur la manière dont le fournisseur de services nuagiques répond aux demandes des autorités ou à des procédures en rapport avec la production ou la transmission d'informations protégées (devoir d'informer, rapport, accès aux résultats de l'audit).

Dans tous les cas, les mesures contractuelles doivent donc être combinées avec d'autres mécanismes de protection. La situation doit toujours être examinée en fonction des circonstances concrètes.

Renvoi : partie 2 (ch. 1.7.2), annexe C

3.3 Relation entre le droit suisse et le droit étranger

Question : Est-il possible d'empêcher contractuellement l'application d'un droit étranger à des données d'une autorité suisse qui se trouvent à l'étranger ?

Réponse : Même si l'applicabilité du droit suisse peut être convenue entre les parties, elle ne concerne que les éléments du contrat. Le principe de territorialité s'applique toujours. Par exemple, une entreprise américaine ne peut pas se soustraire totalement à son obligation légale de divulguer des données dans le cadre d'une procédure aux États-Unis simplement parce qu'elle a signé un contrat par lequel elle s'engage à ne pas le faire. Les mesures contractuelles doivent donc toujours être combinées avec d'autres mécanismes de protection.

Mais le principe de territorialité signifie également qu'une injonction de production d'une autorité de poursuite pénale adressée directement à une filiale européenne d'une entreprise américaine ne peut pas être exécutée par la contrainte pénale en dehors du territoire américain.

Renvoi : partie 2 (ch. 1.6 à 1.7)

4 Questions techniques à caractère juridique

4.1 Cryptage de données

Question : Quand est-il judicieux de crypter les données ? Existe-t-il des recommandations en la matière ?

Réponse : La LPD impose aux personnes qui traitent des données de les protéger aussi par des mesures techniques. Le cryptage est judicieux lorsque l'analyse des risques montre, dans le cas d'espèce, que c'est la mesure de protection la plus appropriée pour les données concernées et qu'elle contribue à garantir une protection adéquate et conforme à la loi. C'est notamment le cas lorsqu'il s'agit de données personnelles (sans possibilité d'anonymisation) ou d'informations classifiées et qu'il existe un risque d'accès par des autorités à des données se trouvant à l'étranger.

La gestion des clefs est cruciale s'agissant des mesures de cryptage. Il convient de clarifier qui gère effectivement les clefs, si elles sont partagées, comment éviter leur perte ou comment les récupérer (*Key Recovery*).

- En principe, il faut adopter des solutions dans lesquelles les sous-traitants n'ont pas accès aux clefs, ou seulement un accès très limité (par ex. « Bring Your own Key » ou « Keep your own Key »). D'autres approches visant à protéger les données contre une consultation non autorisée, par exemple en limitant les droits d'accès et en utilisant des systèmes de sécurité ou d'authentification complémentaires, doivent aussi être examinées.
- Les technologies de cryptage évoluent constamment, il faut donc veiller à ce la solution de cryptage choisie corresponde toujours à l'état actuel de la technique.
- Il faut notamment vérifier si les normes de cryptage utilisées ainsi que les mesures de protection des clefs sont suffisantes. Le stade du traitement des données (*données en transit, données en cours d'utilisation* ou *données au repos*) doit aussi être pris en compte.
- Les nouvelles techniques de cryptage (par ex. le cryptage homomorphe) promettent de nouvelles possibilités, mais ne sont toutefois pas encore commercialisables partout.

Renvoi : partie 2 (ch. 1.2.2), annexes B à D, directive Si001 (Protection informatique de base dans l'administration fédérale), art. 7 et 9 LPD

4.2 Règles en matière de disponibilité des données

Question : Existe-t-il des dispositions légales ou contractuelles (par ex. de l'UE) qui règlent la disponibilité des données ?

Réponse : L'art. 2, let. b, OPDo dispose que le responsable du traitement veille à ce que les données soient accessibles en cas de besoin. Cette exigence est d'autant plus élevée lorsque les informations doivent être disponibles en permanence pour l'accomplissement de tâches essentielles, voire de tâches légales. L'art. 3, al. 2, OPDo prévoit à cet effet que le contrôle des supports de données, de la mémoire et du transport ainsi que la restauration des données doivent être garantis. Les mesures doivent être appropriées afin que la disponibilité soit assurée. La sécurité du système doit toujours être à jour.

La disponibilité des informations importantes pour les affaires doit être garantie à tout moment, conformément au besoin de protection. L'unité administrative responsable des informations doit disposer d'une stratégie de sauvegarde et la mettre en œuvre. Cette stratégie doit prévoir un principe multigénérationnel et un stockage hors ligne des principaux jeux de données afin que celles-ci puissent être récupérées même en cas de maliciels chiffrant les informations (rançongiciel).

L'unité administrative peut en outre exiger contractuellement que le fournisseur de services nuagiques respecte les normes et les meilleures pratiques en matière de disponibilité ou convenir de peines conventionnelles qui seront dues si certains objectifs de disponibilité ne sont pas atteints.

Renvoi : art. 8 LPD, art. 2, let. b, et 3, al. 2, OPDo, art. 32, al. 1, let. b et c, RGPD, annexe C, directive Si001 (Protection informatique de base dans l'administration fédérale), directive P041 (Analyse des besoins de protection), directive SD100 (Catalogue des services standard).

5 OMC 20007

5.1 Contrats de l'appel d'offres OMC 20007

Question : Quelles sont les dispositions contractuelles convenues dans le cadre de l'appel d'offres OMC 20007 et où puis-je consulter les contrats-cadres pour vérifier ce qui est couvert par cet appel d'offres ?

Réponse : Des contrats-cadres pour l'utilisation de services en nuage public ont été négociés avec les cinq adjudicataires de cloud Ali Baba, Amazon, IBM, Microsoft et Oracle, sur la base des conditions de l'appel d'offres OMC 20007. Il a notamment été convenu de manière contraignante avec les cinq fournisseurs que le droit suisse est applicable et que le for est la Suisse. Les contrats contiennent parfois des accords différents, aussi convient-il, en cas de besoin concret, de vérifier au préalable si ce besoin est couvert par l'objet de la prestation et les autres exigences de fond et de forme de l'appel d'offres et de consulter les contrats. Les contrats-cadres sont disponibles auprès des secrétariats généraux des départements. Pour les consulter, les unités administratives doivent s'adresser à leur département.

5.2 Questions concernant Power BI et Power Apps

Question : Power BI (serveur) et Power Apps sont-ils couverts par l'appel d'offres OMC 20007 ?

Réponse : L'objet du marché de l'appel d'offres OMC 20007 est décrit concrètement aux ch. 3.1 s. du cahier des charges et dans les annexes correspondantes de l'appel d'offres. La délimitation prévue au ch. 3.2.1 ne doit pas être comprise comme une énumération exhaustive. Dans la mesure où un besoin déterminé n'est pas concrètement décrit dans l'objet de la prestation, il convient de déterminer, par l'interprétation des documents d'appel d'offres, si un contenu non explicitement mentionné peut — du point de vue des spécialistes — être considéré comme étant couvert par l'objet du marché (la volonté subjective de l'adjudicateur n'entre pas en ligne de compte).

Ce processus d'examen permet de déterminer, au cas par cas, s'il existe une base suffisante en matière de droit des marchés publics pour l'établissement d'un cahier des charges dans le cadre d'une procédure de fourniture sur demande au titre de l'appel d'offres OMC 20007 ou si, dans le cas contraire, une autre base d'acquisition doit être créée.

Dans la mesure où un besoin concret entre dans le champ d'application de l'appel d'offres OMC 20007, l'adjudicateur s'est formellement engagé dans l'appel d'offres à mettre en œuvre des procédures de fourniture sur demande au sens du cahier des charges (mise en concurrence des adjudicataires), telles que décrites dans le cahier des charges.

5.3 Déroulement de l'appel d'offres OMC 20007

Question : Doit-on toujours passer par la procédure de fourniture sur demande ou peut-on d'adresser directement à un fournisseur ?

Réponse : Oui, il faut toujours passer par une procédure de fourniture sur demande. Celle-ci est réglée dans les contrats-cadres conclus avec les fournisseurs de services nuagiques. L'unité administrative qui souhaite couvrir un besoin détermine d'abord si les services nuagiques peuvent être utilisés. Si oui, le service demandeur établit un cahier des charges indépendant des fournisseurs et un catalogue des exigences.

Il évalue les exigences sur la base des informations accessibles au public du fournisseur de services nuagiques. Le soumissionnaire le mieux noté lors de l'évaluation doit être choisi.

La procédure de fourniture sur demande est décrite plus en détail dans les principes relatifs à l'informatique en nuage de l'administration fédérale (AR010). L'OFIT, en qualité de CSB de l'administration fédérale, répond à d'autres questions et fournit des informations à l'adresse suivante : csb@bit.admin.ch.

Renvoi : AR010 — Principes relatifs à l'informatique en nuage de l'administration fédérale

5.4 Fournisseur de prestations / bénéficiaire de prestations

Question : Ai-je aussi besoin d'un fournisseur de prestations supplémentaire (interne) pour l'intégration et l'exploitation ?

Réponse : La stratégie d'informatique en nuage de l'administration fédérale[2] prévoit que les unités administratives obtiennent en principe les services en nuage (public) par l'intermédiaire d'un courtier de services en nuage (CSB). Le CSB de l'administration fédérale est l'OFIT. Les services en nuage public doivent donc en principe être obtenus par l'intermédiaire de l'OFIT. Le secteur TNI de la Chancellerie fédérale peut prévoir des exceptions conformément à la stratégie d'informatique en nuage. Il a autorisé des exceptions pour MétéoSuisse et Swisstopo.

Renvoi : stratégie d'informatique en nuage de l'administration fédérale, principe 0-2, p. 11

5.5 Relation entre l'appel d'offres OMC 20007 et d'autres marchés publics

Question : J'ai acheté un logiciel. Le fournisseur utilise un composant qui est fourni par l'un des adjudicataires de l'appel d'offres OMC 20007 (par ex. IA/scanning) ; à quoi faut-il faire attention ?

Réponse : Ce scénario n'est pas pertinent sous l'angle de l'appel d'offres OMC 20007, car le fournisseur du logiciel fait appel au fournisseur de services nuagiques en tant que sous-traitant. L'adjudicataire du marché pertinent sous l'angle du droit des marchés publics est le fournisseur du logiciel (avec lequel le contrat a été conclu par la suite). La relation contractuelle n'existe qu'entre ce dernier et le fournisseur de services nuagiques. Dans ce cas également, il convient de prévoir les mesures contractuelles, organisationnelles et techniques nécessaires pour garantir la protection des informations, en particulier des données personnelles, ainsi que la continuité des activités.

Question : Que faire si j'ai fait obtenu une partie de mon application et que l'appel d'offres OMC 20007 arrive à son terme, mais pas celui de mon application ? Qui doit surveiller ces délais ?

Réponse : Les unités administratives sont responsables de leurs applications. Dans la mesure où l'objet du marché OMC 20007 est épuisé, en termes de volume ou de durée, il faut envisager une nouvelle base légale en matière de marchés publics.

Question : De quoi faut-il tenir compte si j'ai déjà acquis une application en nuage (auprès de l'un de adjudicataires de l'appel d'offres OMC 20007 ou d'un autre fournisseur proposant des offres équivalentes) ?

Réponse : Si des services nuagiques ont été achetés dans le cadre d'une procédure indépendante antérieure ou parallèle à l'appel d'offres OMC 20007, les contrats correspondants restent valables. Dans ce cas également, il faut prévoir les mesures contractuelles, organisationnelles et techniques nécessaires pour garantir la protection des informations, en particulier des données personnelles, et la continuité des activités.

Question : Que faut-il acheter en premier :

[2] Stratégie d'informatique en nuage de l'administration fédérale (admin.ch)

- la plateforme, ou
- le développeur/l'application métier ?

Est-ce que je dois passer d'abord par une procédure de fourniture sur demande au titre de l'appel d'offres OMC 20007 pour obtenir la plateforme et passer un autre marché pour me procurer les ressources ou les applications à développer/exploiter sur cette plateforme, ou dois-je d'abord passer un marché pour me procurer les ressources ou les applications et ensuite me procurer la plateforme correspondante au titre de l'appel d'offres OMC 20007 ?

Réponse : Il n'y a pas de règles concernant ce qui doit être acheté en premier, mais il est recommandé de commencer par la plateforme ou les services en nuage public. En fonction du fournisseur de services nuagiques, il est possible de se procurer les développeurs de l'application métier. Lors de l'acquisition de la plateforme, il faut garantir qu'un cahier des charges indépendant des fournisseurs est rempli. Si ce n'est pas le cas dès le départ, il n'est pas possible de s'approvisionner au titre de l'appel d'offres OMC 20007.

Question : Quelle est la procédure prévue si l'appel d'offres OMC 20007 désigne un fournisseur de services nuagiques pour lequel aucune ressource/compétence ne peut être obtenue par l'acquisition de services — soit parce qu'elle n'existe pas sur le marché, soit parce qu'elle n'est pas disponible en temps voulu ?

Réponse : La disponibilité des ressources/compétences peut être incluse dans le catalogue des exigences pour l'évaluation du fournisseur de services nuagiques qui convient. Les ressources/compétences appropriées peuvent être obtenues au moyen de différents appels d'offres (l'appel d'offres OMC 2007 n'est qu'une possibilité parmi d'autres). Une nouvelle évaluation peut être effectuée si aucune ressource ne peut être trouvée pour le fournisseur de services nuagiques choisi.