INFORMATIQUE EN NUAGE : Enjeux et risques

FICHE INFO DU PPDT

PREAMBULE

L'avènement des solutions dites "cloud" ces dernières années ont poussé toutes les organisations, y compris les administrations fédérales et cantonales, à adopter ces nouvelles technologies, soit pour les avantages qu'elles présentent (évolutivité, coût, sécurité), ou simplement parce que les fournisseurs ne proposent plus d'autres modèles de déploiement.

L'adoption de ce type de technologie devrait reposer sur une analyse des risques détaillée permettant, d'une part, d'évaluer les risques inhérents aux différentes solutions par rapport aux typologies de données traitées (données personnelles, données personnelles sensibles ou données soumises au secret de fonction) et, d'autre part, d'évaluer l'effet des mesures techniques, organisationnelles et contractuelles sur la réduction des risques à un niveau acceptable.

LES DISPOSITIONS LEGALES CANTONALES

Au niveau cantonal, les dispositions légales principales sont:

Art. 37 LIPAD Sécurité des données personnelles

[1] Les données personnelles doivent être protégées contre tout traitement illicite par des mesures organisationnelles et techniques appropriées.

[2] Les institutions publiques prennent, par le biais de directives ainsi que de clauses statutaires ou contractuelles appropriées, les mesures nécessaires pour assurer la disponibilité, l'intégrité et la confidentialité des données personnelles qu'elles traitent ou font traiter.

[3] Les institutions publiques sont tenues de contrôler le respect des directives et clauses visées à l'alinéa 2. S'il implique l'exploitation de ressources informatiques et le traitement de données personnelles, ce contrôle doit s'exercer conformément à des procédures spécifiques que les instances mentionnées à l'article 50, alinéa 2, doivent adopter à cette fin, après consultation du préposé cantonal.

Art. 13A RIPAD Sous-traitance (art. 37, al. 2, de la loi)

[1] Le traitement de données personnelles peut être confié à un tiers pour autant qu'aucune obligation légale ou contractuelle de garder le secret ne l'interdise.

[2] L'institution demeure responsable des données personnelles qu'elle fait traiter au même titre que si elle les traitait elle-même.

[3] La sous-traitance de données personnelles fait l'objet d'un contrat de droit privé ou de droit public avec le prestataire tiers, prévoyant pour chaque étape du traitement le respect des prescriptions de la loi et du présent règlement ainsi que la possibilité d'effectuer des audits sur le site du sous-traitant.

[4] Le recours par un sous-traitant à un autre sous-traitant (sous-traitance en cascade) n'est possible qu'avec l'accord préalable écrit de l'institution et moyennant le respect, à chaque niveau de substitution, de toutes les prescriptions du présent article.

[5] S'il implique un traitement à l'étranger, le recours à un prestataire tiers n'est possible que si la législation de l'Etat destinataire assure un niveau de protection adéquat.

[6] Le préposé cantonal publie une liste des Etats qui disposent d'une législation assurant un niveau de protection adéquat.

Il sied également de s'interroger sur les dispositions particulières en matière de secret applicables à la question de l'utilisation d'une infrastructure d'informatique en nuage pour le traitement de données d'une institution publique.

LA QUESTION DU SECRET DE FONCTION, DU SECRET PROFESSIONNEL ET DES SECRETS QUALIFIES

La violation du secret de fonction est punissable selon l'art. 320 CP:

1. Quiconque révèle un secret à lui confié 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, est puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.
   La révélation demeure punissable alors même que la charge ou l'emploi ou l'activité auxiliaire a pris fin.
2. La révélation n'est pas punissable si elle est faite avec le consentement écrit de l'autorité supérieure.

Au niveau cantonal il sied également d'évaluer les dispositions spéciales auxquelles sont soumises les institutions cantonales. A titre d'exemple, on peut citer l'art. 9A al. 1 de la loi générale relative au personnel de l'administration cantonale, du pouvoir judiciaire et des établissements publics médicaux, du 4 décembre 1997[1], qui dispose que les membres du personnel de la fonction publique sont soumis au secret de fonction pour toutes les informations dont ils ont connaissance dans l'exercice de leurs fonctions dans la mesure où la LIPAD ne leur permet pas de les communiquer à autrui (selon l'art. 26 LIPAD).

Il convient donc de qualifier les sous-traitants (ici les services d'informatique en nuage) d'auxiliaires afin de reporter l'obligation de secret de fonction (ces derniers seront donc punissables en cas de violation du secret). Ceci s'applique également à un prestataire de service à l'étranger[2]. Il y a également un consensus sur le fait que si les données sont chiffrées et que le prestataire ne dispose d'aucun moyen de déchiffrement, rien ne s'oppose à leur externalisation[3]. Il est toutefois important de noter que les possibilités de chiffrement dépendent du type d'infrastructure d'informatique en nuage. Il n'est ainsi pas toujours techniquement possible de chiffrer les données en transit ("*in transit*"), en cours d'utilisation ("*in use*") et au repos ("*at rest*").

Il sied de s'assurer qu'aucune disposition en lien avec un secret particulier n'empêche expressément l'externalisation ou le transfert à l'étranger (ex. art. 17 LStat[4]).

En conclusion, si l'institution publique envisage d'externaliser des données soumises au secret, elle doit répondre aux questions suivantes:

- Peut-elle divulguer des informations secrètes à un prestataire de droit privé et, si tel est le cas, à quelles conditions?

[1] LPAC; RS/GE B 5 05.
[2] Intervention de Karin Keller-Sutter, BOCN 2022 354.
[3] Montavon, p. 498.
[4] Loi sur la statistique publique cantonale, du 24 janvier 2014; RS/GE B 4 40.

- Quel est le risque admissible en matière de protection du secret de fonction?
- Est-ce qu'il y a des exigences supplémentaires dans des lois spéciales ? (ex.: art. 17 al. 6 LStat, qui interdit le transfert à l'étranger)

LA QUESTION DES ACCES PAR LES AUTORITES ETRANGERES

L'utilisation de service d'informatique en nuage pose également la question de l'accès aux données sur requête des autorités étrangères. Il sied d'évaluer ce risque par exemple eu égard aux dispositions américaines découlant du Cloud Act ou du FISA (*Foreign Intelligence Surveillance Act*)[5].

Le rapport sur le US Cloud Act publié par le Département fédéral de justice et police précise que le Cloud Act oblige les Communication service providers (CSPs) dont le siège est aux USA et qui gèrent des centres de stockages de données hors des USA, de conserver les données hébergées sur leurs serveurs et de les communiquer sur demande aux autorités judiciaires américaines. Cette loi s'applique indépendamment du lieu d'enregistrement de ces données, que ce soit aux USA ou à l'étranger. Sont concernées les sociétés de droit américain, c'est-à-dire celles qui sont soumises à la juridiction américaine. Dans ce cadre, des contacts minimaux (*minimum contacts*) avec les USA sont une condition nécessaire ; l'interprétation et la qualification de ces contacts relèvent toutefois de la compétence des tribunaux américains. Les entreprises détenant des holdings, filiales ou succursales aux USA peuvent également être concernées, tout comme des prestataires étrangers qui font de la publicité pour leurs services de cloud aux USA. Seuls les CSPs étrangers qui n'entretiennent pas ces contacts minimaux avec les USA ne sont pas soumis à de nouvelles obligations[6].

En ce qui concerne le FISA, l'application peut-être plus problématique. Le Comité européen de la protection des données (*European Data Protection Board* – EPDB) s'est prononcé sur l'application des nouvelles dispositions de la section 702 et indique que les importateurs de données américains qui relèvent de l'article 1881a du 50 U.S.C. (FISA 702) sont directement tenus d'accorder l'accès aux données à caractère personnel importées en leur possession, sous leur garde ou sous leur contrôle, ou de les livrer. Cette obligation pourrait s'étendre à toutes les clés cryptographiques nécessaires pour rendre les données intelligibles[7].

Si les dispositions américaines figurent parmi les plus documentées à ce jour, la question doit être posée de manière systématique en fonction des fournisseurs et des lieux de stockage des données[8]. En effet, des lois d'autres pays peuvent trouver le même type d'application.

INFORMATIQUES EN NUAGE: AVANTAGES VS. RISQUES

L'informatique en nuage

Une infrastructure en nuage est l'ensemble du matériel et des logiciels qui permettent de réaliser les cinq caractéristiques essentielles de l'informatique en nuage (Libre-service à la demande, large accès au réseau, mise en commun des ressources, élasticité rapide et service mesuré).

---

[5] PUBL261.PS (congress.gov) (dernière consultation: 26.09.2023).

[6] Office fédéral de la justice, Rapport sur l'US CLOUD Act – Avis de droit de l'Office fédéral de la justice du 17 septembre 2021: https://www.bj.admin.ch/bj/fr/home/publiservice/publikationen/berichte-gutachten/2021-09-17.html (dernière consultation: 25.09.2023).

[7] EPDB, Public consultation regarding Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Adopted on 10 November 2020: https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/public_consultation_regarding_recommendations_01.pdf.

[8] Cadre juridique pour l'utilisation de services d'informatique en nuage public au sein de l'administration fédérale (version 1.1, compris annexe A et B), chapitre 1.7 Accès des autorités étrangères, p. 21. (https://www.bk.admin.ch/dam/bk/fr/dokumente/dti/themen/cloud/rechtsrahmen.pdf.download.pdf/Cadre%20juridique%20pour%20l'utilisation%20de%20services%20d%E2%80%99informatique%20en%20nuage%20public%20au%20sein%20de%20l'administration%20f%C3%A9d%C3%A9rale%20(version%201.1,%20compris%20annexe%20A%20et%20B).pdf).

L'infrastructure en nuage peut être considérée comme contenant à la fois une couche physique (composants de serveur, de stockage et de réseau) et une couche d'abstraction (logiciel déployé sur la couche physique)[9].

Les modèles d'informatique en nuage

Il existe 3 modèles de services informatiques en nuage:

1. *Infrastructure as a Service*[10]

Le modèle d'infrastructure en tant que service correspond à la fourniture au consommateur d'une capacité de traitement, de stockage, de réseaux et d'autres ressources informatiques fondamentales où le consommateur est en mesure de déployer et d'exécuter des logiciels de son choix (systèmes d'exploitation et applications).

Le consommateur ne gère pas et ne contrôle pas l'infrastructure cloud, mais il a le contrôle des systèmes d'exploitation, du stockage et des applications déployées et éventuellement un contrôle limité de certains composants de réseau (par exemple, les pare-feu de l'hôte).

2. *Platform as a Service* (PaaS)[11]

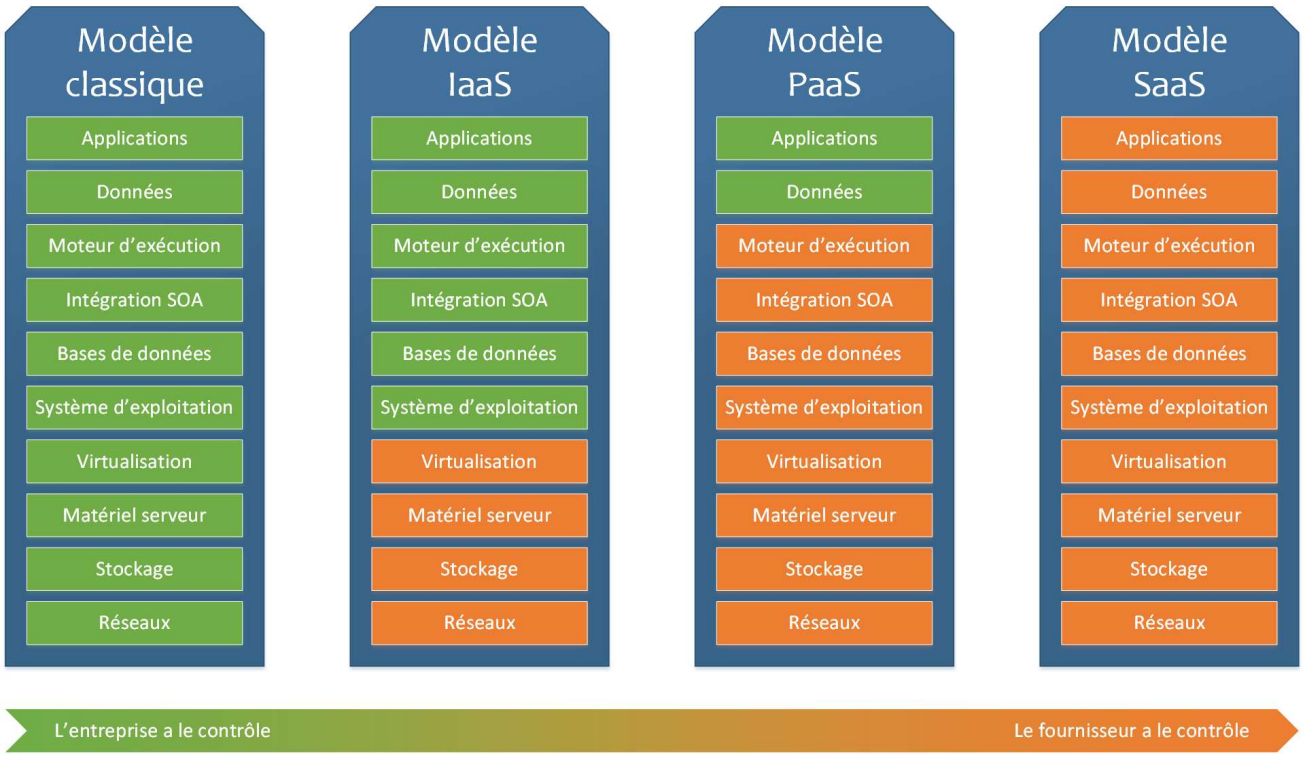
Le modèle de plateforme en tant que service correspond à la capacité fournie au consommateur à déployer sur l'infrastructure en nuage des applications créées ou acquises par le consommateur à l'aide de langages de programmation, de bibliothèques, de services et d'outils pris en charge par le fournisseur. Le consommateur ne gère ni ne contrôle l'infrastructure en nuage sous-jacente, y compris le réseau, les serveurs, les systèmes d'exploitation ou le stockage, mais il a le contrôle sur les applications déployées et éventuellement sur les paramètres de configuration de l'application hébergée et potentiellement les paramètres de configuration de l'environnement d'hébergement des applications.

3. *Software as a Service* (SaaS)[12]

Le modèle de logiciel en tant que service correspond à la possibilité offerte au consommateur d'utiliser les applications du fournisseur fonctionnant sur une infrastructure en nuage. Les applications sont accessibles à partir de divers dispositifs clients par l'intermédiaire d'une interface client légère, telle qu'un navigateur web (par exemple, le courrier électronique basé sur le web), ou d'une interface de programme. Le consommateur ne gère ni ne contrôle l'infrastructure en nuage sous-jacente, y compris le réseau, les serveurs, les systèmes d'exploitation, le stockage ou même les capacités des applications individuelles, à l'exception peut-être des paramètres limités de configuration des applications spécifiques à l'utilisateur.

L'étendue du contrôle des composants du service informatique en nuage est donc différente en fonction du modèle choisi[13]:

[9] NIST Special Publication 800-145 – The NIST Definition of Cloud Computing.
[10] NIST Special Publication 800-145 – The NIST Definition of Cloud Computing.
[11] NIST Special Publication 800-145 – The NIST Definition of Cloud Computing.
[12] NIST Special Publication 800-145 – The NIST Definition of Cloud Computing.
[13] https://blog.blaisethirard.com/qu-est-ce-que-le-cloud-computing/ (dernière consultation: 13.09.2023).



Le choix du modèle de service informatique en nuage aura une influence sur les mesures techniques (par ex. le chiffrement des données), organisationnelles et contractuelles qui devront être mise en œuvre afin de réduire les risques liés à l'utilisation des différents services d'informatique en nuage à un niveau acceptable.

Les modèles de déploiement

1. Cloud privé[14]

L'infrastructure en nuage est mise à disposition pour une utilisation exclusive par une seule organisation comprenant plusieurs consommateurs (par exemple des services). Elle peut être détenue, gérée et exploitée par l'organisation, par un tiers ou par une combinaison des deux, et elle peut exister dans les locaux de l'organisation (dit "*on premise*") ou à l'extérieur.

2. Cloud communautaire[15]

L'infrastructure en nuage est réservée à l'usage exclusif d'une communauté spécifique de consommateurs issus d'organisations ayant des préoccupations communes. Elle peut être détenue, gérée et exploitée par une ou plusieurs organisations de la communauté, par un tiers ou par une combinaison d'entre eux et elle peut exister dans des locaux ou à l'extérieur de ceux-ci.

3. Cloud Public[16]

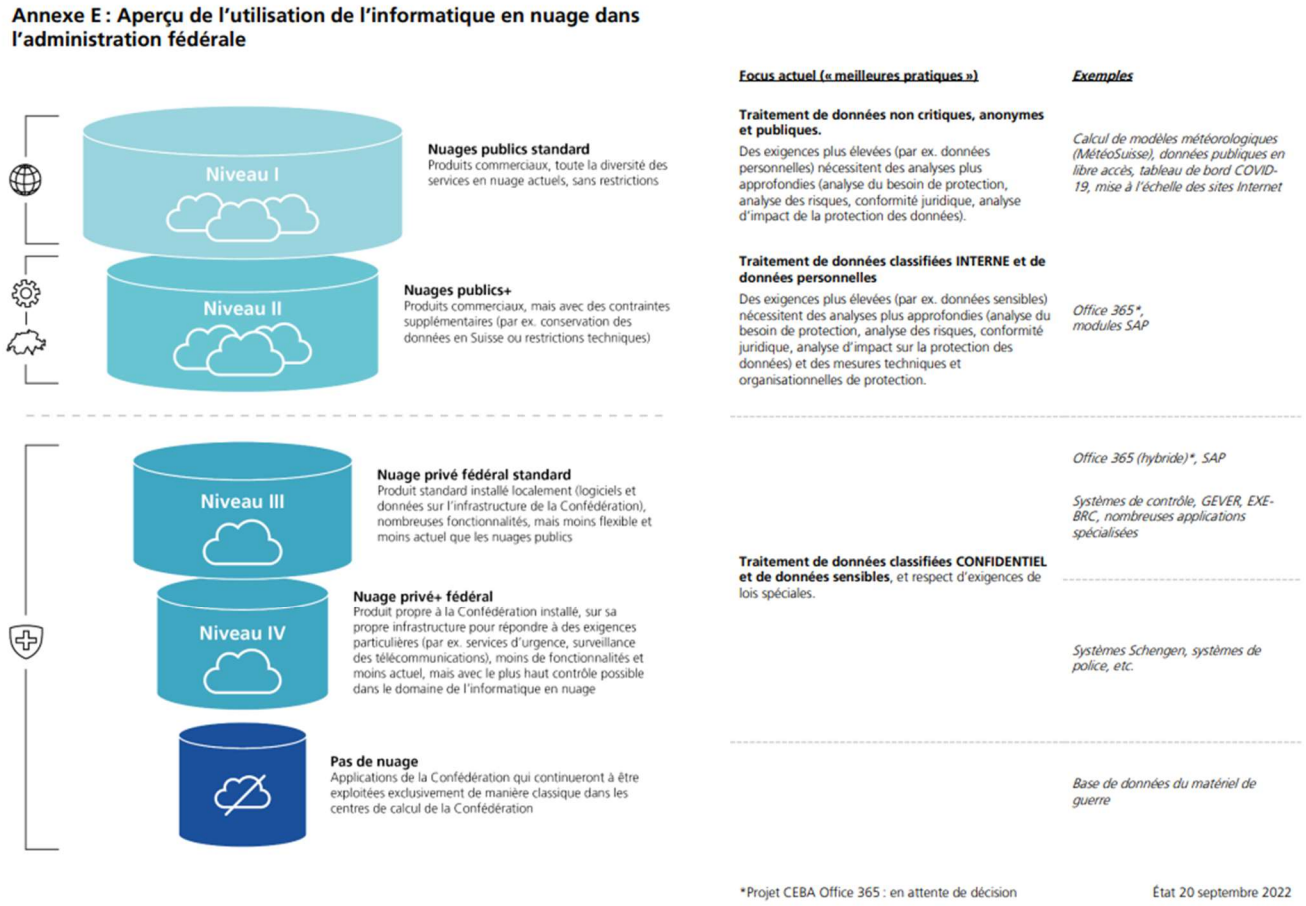
L'infrastructure cloud est prévue pour une utilisation ouverte par le grand public. Elle peut être détenue, gérée et exploitée par une entreprise, un universitaire ou un organisme gouvernemental, ou une combinaison de ceux-ci. Elle existe chez le fournisseur de cloud.

[14] NIST Special Publication 800-145 – The NIST Definition of Cloud Computing.
[15] NIST Special Publication 800-145 – The NIST Definition of Cloud Computing.
[16] NIST Special Publication 800-145 – The NIST Definition of Cloud Computing.

4. Cloud hybride[17]

L'infrastructure en nuage est une composition de deux ou plusieurs infrastructures en nuage distinctes (privées, communautaires ou publiques) qui restent des entités uniques, mais qui sont liées entre elles par une technologie standardisée ou propriétaire qui permet la portabilité des données et des applications (par exemple, "*cloud bursting*" pour l'équilibrage de charge entre des nuages).

Le choix du modèle de déploiement devrait s'effectuer en fonction de la nature des données qui seront traitées dans l'informatique en nuage. A ce titre, la Confédération suisse, dans sa démarche, envisage une utilisation de Cloud Public uniquement pour des données publiques (données météorologiques par exemple), tandis que les applications contenant des informations sensibles ou soumise au secret resteront sur l'informatique classique (données de l'armée par exemple)[18]:



Avantages vs risques

En dehors des avantages propres à l'informatique en nuage, les organisations sont souvent attirées par des modèles *Cloud* dans l'optique de réduire les coûts et améliorer la sécurité informatique. Toutefois, des exemples récents tendent à mitiger ces avantages.

[17] NIST Special Publication 800-145 – The NIST Definition of Cloud Computing.
[18] Informatique en nuage: https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud.html (dernière consultation: 19.09.2023).

La société Dropbox a expliqué en 2018 avoir économisé près de 75 millions en deux ans en abandonnant la solution Cloud Amazon AWS et en créant sa propre infrastructure technologique[19].

En août 2023, la société Danoise Cloud Nordic a subi une attaque en rançongiciel (*ransomware*) majeure avec des conséquences irrémédiables: « Les attaquants ont réussi à crypter tous les disques des serveurs, ainsi que les systèmes de sauvegarde primaires et secondaires, ce qui a entraîné le blocage de toutes les machines et la perte de l'accès à toutes les données. […] Malheureusement, il s'est avéré impossible de les restaurer et la majorité de nos clients ont donc perdu toutes leurs données stockées chez nous »[20].

L'utilisation d'informatique en nuage, au-delà de ses avantages, présente de nombreux risques qui devraient être évalués de manière rigoureuse.

On pensera notamment aux risques juridiques tels que la violation des prescriptions légales concernant la protection des données, la violation du secret (secret de fonction ou secret qualifié) ou aux risques en cas de rupture de contrat.

Les risques de sécurité et notamment de continuité d'activités tels que les accès indus, la perte ou la modification indue de données devront être évalués et une attention particulière devrait également être portée aux risques en lien avec les accès aux données par les autorités étrangères (ex. Cloud Act et FISA), mais aussi aux risques de communication transfrontière ou d'accès depuis un pays n'offrant pas les garanties suffisantes en matière de protection des données.

DONNEES PERSONNELLES, PERSONNELLES SENSIBLES ET DONNEES SOUMISES AU SECRET

Le choix de l'utilisation de l'informatique en nuage ne peut se faire que sur la base d'une évaluation détaillée des risques en fonction de la sensibilité des données.

Les mesures de réduction des risques seront plus importantes s'il s'agit de données personnelles sensibles ou de données soumises au secret de fonction ou à un secret qualifié.

ANALYSE DES RISQUES

Selon les normes et bonnes pratiques, une analyse des risques comporte en principe les étapes suivantes:

1. Etablissement du contexte:

   Cette première étape consiste à établir le contexte dans lequel s'inscrit l'analyse et permet notamment de définir le périmètre concerné: données, ressources informatiques, ressources humaines.

2. Identification des risques:

   Cette étape consiste à identifier les risques inhérents, c'est-à-dire les risques existants en l'absence de toute mesure visant à réduire l'impact ou la probabilité de survenance du risque.

[19] https://managedserver.fr/dropbox-a-%C3%A9conomis%C3%A9-pr%C3%A8s-de-75-millions-en-deux-ans-en-abandonnant-amazon-aws-et-en-cr%C3%A9ant-sa-propre-infrastructure-technologique/ (dernière consultation: 19.09.2023).

[20] https://www.globalsecuritymag.fr/L-attaque-ransomware-catastrophique-sur-Cloud-Nordic-rappelle-l-importance-d.html (dernière consultation: 19.09.2023).

3. Analyse des risques:

   Cette étape consiste à analyser les effets des mesures techniques, organisationnelles ou encore contractuelles existantes sur la réduction soit de la probabilité soit de l'impact du risque afin de déterminer le risque résiduel et d'évaluer s'il celui-ci est acceptable. Dans le cas contraire, un plan de traitement des risques est défini.

4. Traitement des risques:

   Il s'agit de mettre en œuvre les mesures, techniques, organisationnelles ou contractuelles permettant d'accepter, réduire, éviter ou transférer le risque.

5. Evaluation en continu:

   Il s'agit d'évaluer, soit de manière continue ou, à tout le moins, selon une fréquence régulière, l'évolution des menaces et l'efficacité des mesures de traitement du risque.

Au vue de l'évolution rapide des technologies et des risques, une veille technologique et réglementaire devrait être mise en œuvre pour couvrir spécifiquement l'utilisation de l'informatique en nuage.

MESURES TECHNIQUES, ORGANISATIONNELLES ET CONTRACTUELLES

La réduction des risques en lien avec l'informatique en nuage dépend de la mise en place de mesures techniques, organisationnelles et contractuelles appropriées.

Mesures techniques

Au niveau technique, on s'assurera notamment que des mesures appropriées sont mises en place afin de garantir la confidentialité, l'intégrité, la disponibilité et l'authenticité des données.

Il faut considérer au moins les mesures suivantes:

- Chiffrement des données: En fonction de la sensibilité des données, un chiffrement des données devrait être réalisé au minimum "*in transit*" et "*at rest*" et idéalement également "*in use*" lorsque cela est possible et utile. Il est important de noter que les possibilités de chiffrement peuvent déprendre des modèles d'informatique en nuage choisi.
- La gestion des clés de chiffrement: Il s'agit également d'un aspect essentiel, notamment lorsqu'il est question de données soumises au secret de fonction. Afin de se prémunir d'un accès par les autorités étrangères, la clé de déchiffrement ne devrait en aucun cas être rendue accessible au fournisseur du service d'informatique en nuage.
- Pseudonymisation, anonymisation ou tokenisation: Si le chiffrement des données n'est pas possible, d'autres possibilités comme la pseudonymisation, l'anonymisation ou la tokenisation peuvent être évaluées en fonction de la criticité de la donnée.
- Gestion des accès, authentification et journalisation: Les solutions de sécurisation du cloud comme les outils CASB (*Cloud Access Security Brooker*) ou *Trusted Platform Modules* peuvent être évaluées pour la gestion des accès et la journalisation. On s'assura également du niveau approprié de sécurisation des interfaces (https par ex.), ainsi que de la gestion des sauvegardes.

Mesures organisationnelles

En ce qui concerne les mesures organisationnelles, on veillera à mettre en œuvre un cadre de gouvernance des solutions informatiques en nuage précisant les processus de fonctionnement avec le prestataire externe et en particulier en ce qui concerne:

- La gestion des accès
- La gestion des demandes d'accès aux données des personnes
- La gestion des demandes d'accès des autorités
- La gestion des incidents et notamment la communication en cas de cyberattaque réussie ou non
- La gestion du chiffrement et des clés de chiffrement
- Les droits de contrôle ou d'audit

En interne, l'organisation veillera également à l'information des personnes concernées, à la sensibilisation des utilisateurs et à la mise en œuvre d'un processeur de veille technique et réglementaire.

Mesures contractuelles

Au niveau contractuel on veillera notamment:

- Au choix du droit applicable (idéalement suisse) et du for (idéalement en Suisse)
- A s'assurer de la soumission au secret de fonction du prestataire et de ses employés en cas de traitement de données soumises au secret de fonction.
- A interdire contractuellement la sous-traitance en cascade sans validation préalable.
- Se réserver un droit d'audit et de contrôle sur place ou à tout le moins un accès aux rapports détaillés d'audit du prestataire (ex. ISO 27001 OU 27701, SOC I et II).
- Prévoir la manière dont le prestataire répond aux demandes des autorités.
- Prévoir la portabilité des données et les dispositions de sortie de contrat[21].
- Formuler clairement les obligations du prestataire (par ex. le signalement de cyber attaque)

Il n'est pas possible de dresser une liste exhaustive des mesures techniques, organisationnelles et contractuelles à considérer. L'annexe C[22] de la stratégie d'informatique en nuage de la Confédération présente toutefois une liste, non exhaustive, de risques en lien avec l'informatique en nuage et des mesures techniques, organisationnelles et contractuelles pouvant réduire la survenance et/ou l'impact des risques. Ce document peut servir de base de réflexion pour les institutions que ne disposeraient pas des connaissances suffisantes en matière de gestion des risques de l'informatique en nuage.

CONCLUSION

L'adoption de service d'informatique en nuage doit être évaluée en fonction de la sensibilité de la donnée et reposer sur une analyse détaillée des risques inhérents et des mesures techniques, organisationnelles et contractuelles qui peuvent être mises en œuvre afin de réduire les risques résiduels à un niveau acceptable.

Dans un contexte juridique et technologique en constante évolution, la mise en œuvre de ce type de solutions devrait être accompagnée d'une veille réglementaire et technologique, ainsi que d'une évaluation continue ou au moins périodique de l'évolution des risques.

Dans tous les cas, une approche prudente devrait être favorisée en fonction de la criticité de la donnée.

---

[21] Sur la sortie des contrats de cloud, cf: JOTTERAND Alexandre, Contrats cloud: qualification, gestion des données et sortie de la relation, *in* Sylvain Métille (éd.), *L'informatique en nuage*, Berne 2022, pp. 7 ss.

[22] Annexe C: Aperçu des risques et des mesures: https://www.bk.admin.ch/dam/bk/fr/dokumente/dti/themen/cloud/rechtsrahmen_anhang_c.pdf.download.pdf/Annexe%20C%20Apercu%20des%20risques%20et%20des%20mesures.pdf.

LECTURES COMPLEMENTAIRES:

- ASB - Guide «Cloud» – Recommandations pour sécuriser le cloud banking: https://www.swissbanking.ch/_Resources/Persistent/7/b/7/e/7b7eab588cc461aa494d7b38b4c7281255ad71a8/ASB_Guide_Cloud_2020_FR.pdf
- ANSSI – Maîtriser les risques de l'infogérance: https://www.ssi.gouv.fr/uploads/IMG/pdf/2010-12-03_Guide_externalisation.pdf
- ANSSI – Guide des mécanismes cryptographiques: https://www.ssi.gouv.fr/uploads/2021/03/anssi-guide-mecanismes_crypto-2.04.pdf
- ANSSI – Guide de sélection d'algorithmes cryptographiques: https://www.ssi.gouv.fr/uploads/2021/03/anssi-guide-selection_crypto-1.0.pdf
- FINMA, Externalisations dans le secteur des banques, des entreprises d'assurance et de certains établissements financiers au sens de la LEFin: https://www.finma.ch/fr/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2018-03-01012021_de.pdf?la=fr
- ISO/IEC 27017:2015 – Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services: https://www.iso.org/standard/43757.html
- ISO/IEC 27018:2019 – Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors: https://www.iso.org/standard/76559.html
- NIST, NIST SP 800-210 – General Access Control Guidance for Cloud Systems: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-210.pdf
- NIST, NIST Special Publication 800-144 – Guidelines on Security and Privacy in Public Cloud Computing: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf
- PFPDT, Externalisation de données personnelles par la Suva vers un cloud de Microsoft: https://www.edoeb.admin.ch/edoeb/fr/home/kurzmeldungen/20220613_suva_cloud.html
- PPDT Canton de Vaud, Check-list pour contrat de sous-traitance: https://www.vd.ch/themes/etat-droit-finances/protection-des-donnees-et-droit-a-linformation/protection-des-donnees#c2074832
- Privatim, Nouvelle version révisée de l'aide-mémoire « Risques et mesures spécifiques au cloud » de Privatim: https://www.privatim.ch/wp-content/uploads/2022/02/privatim_Cloud-Merkblatt_v3_0_20220203_def._FR.pdf

PPDT – 11.12.2023