privatim
Konferenz der schweizerischen Datenschutzbeauftragten
Conférence des préposé(e)s suisses à la protection des données
Conferenza degli incaricati svizzeri per la protezione dei dati

Aide-mémoire sur les risques et les mesures spécifiques à la technologie du Cloud

1 Introduction

Dans le cadre du traitement des données, les organes publics utilisent de manière très variée de prestations de tiers. Pour ce qui est de la sous-traitance du traitement de données à des tiers, la législation sur la protection des données (et sur l'information) comporte régulièrement des normes qui, de manière générale, maintiennent la responsabilité totale des organes publics pour des données traitées par des tiers. La manière d'assumer cette responsabilité, dans le cas de sous-traitant en matière de traitement de données, a été précisée par diverses autorités de protection des données dans des circulaires ou des check-lists[1].

Les traitements de données sont toujours plus fréquemment basées sur l'utilisation de la **technologie du Cloud** :

> *Les ressources pour le traitement de données sont mises à disposition de façon dynamique et une localisation concrète du traitement de données et des données n'est pas prévue : celles-ci se trouvent dans le « Cloud ».*

Lorsque les traitements de données mettent à contribution de tels services du Cloud, l'organe public reste globalement responsable.

privatim, la conférence des préposé(e)s suisses à la protection des données, a pour objectif d'indiquer, dans le présent aide-mémoire, les risques découlant de l'utilisation de la technologie du Cloud. Ceux-ci **s'ajoutent ou s'accentuent par rapport aux risques causés par la sous-traitance du traitement de données** à des tiers. Enfin, il s'agira de montrer comment les organes publics peuvent concrètement assumer leur responsabilité.

Dès lors, il convient d'abord d'analyser dans quelle mesure une sous-traitance du traitement de données est licite au regard des normes générales de la protection des données. En cas de licéité, il convient d'analyser l'utilisation de la technologie du Cloud et les risques spécifiques liés à cette technologie pour la sous-traitance du traitement de données.

[1] Voir les liens dans l'annexe no 2.

privatim
c/o Datenschutzbeauftragter des Kantons Basel-Stadt
Postfach 205, CH-4010 Basel
Tel. +41 (61) 201 16 40
praesident@privatim.ch, www.privatim.ch

L'aide-mémoire se concentre sur les risques spécifiques liés à la protection des données. Les organes publics doivent eux-mêmes gérer les autres risques concernant leurs activités légales, notamment ceux liés au respect des dispositions contractuelles.

2 Des risques accentués ou supplémentaires liés au traitement de donnés dans le Cloud

Lorsque l'on se sert de la technologie du Cloud de sous-traitants, les risques suivants existent ou s'accentuent dans des domaines spécifiques :

- détermination de la localisation des serveurs ;
- moyens de contrôle (quels sont les traitements de données concrets qui interviennent dans l'infrastructure du Cloud ?) ;
- liberté de modifier des offres standards (droit applicable, for, quantité des prestations, mesures de sécurité, contenu contractuel en général) ;
- mise en œuvre des prétentions liées à la protection des données (prétentions de l'effacement respectivement de la correction des données) ;
- confidentialité (cryptage et protection des secrets);
- droit d'accès des autorités nord-américaines fondé sur le CLOUD Act[2];ou d'autres organes étrangers en raison d'autres décrets juridiques[3] ;
- maîtrise des mesures de sécurité des informations (perte et abus des données) ;
- maîtrise des autres intervenants (contrats de sous-traitance, maintenance de l'infrastructure informatique) ;
- disponibilité des services et
- transparence en cas de dissolution des relations contractuelles (portabilité des données, destruction des données).

3 Responsabilité de l'organe public en cas d'utilisation de services du Cloud

L'organe public doit exclure ou réduire les risques spécifiques à un niveau acceptable par des mesures adéquates, s'il utilise des services du Cloud. Lors de l'analyse générale des risques pour le traitement concret des données, les risques spécifiques au Cloud doivent être considérés et des mesures correspondantes doivent être prises.

Trois questions particulières doivent être traitées de manière prioritaire :

---

2 Clarifying Lawful Overseas Use of Data Act (CLOUD Act), H.R. 4943, <https://www.congress.gov/bill/115th-congress/house-bill/4943>.

3 Dans ce qui suit, compris dans le CLOUD Act.

- droit applicable et for (chiffre 3.1) ;
- lieu du traitement des données (situation des serveurs ; chiffre 3.2) et
- protection des secrets et gestion des clés (chiffre 3.3).

Le risque lié à la technologie du Cloud est principalement déterminé par ces trois risques. Il faut y ajouter d'autres risques qui sont au moins accentués par l'utilisation d'une infrastructure du Cloud (chiffres 3.4-3.10).

3.1 Droit applicable, for

En principe, une relation contractuelle doit être soumise au droit suisse (notamment à la loi sur la protection des données) et les conflits résultant du contrat devraient être soumis à la juridiction suisse.

Il peut être convenu d'un droit applicable et d'un for étranger, lorsque

- les données peuvent être protégées de manière efficace, par le biais du cryptage, contre l'accès de tiers (et même du fournisseur du service Cloud ; voir chiffre 3.3) ou
- lorsque les données ne sont pas sensibles et que l'Etat en question dispose d'une législation équivalente sur la protection des données (p.ex. les pays de l'UE).

3.2 Lieu du traitement des données

Le fournisseur du service Cloud doit déclarer le lieu de l'infrastructure du Cloud, afin de pouvoir prendre cet élément en considération dans le cadre de l'évaluation des risques.

- On doit privilégier des traitements de données qui s'effectuent en Suisse (sécurité de l'infrastructure, p.ex. en relation avec les objectifs de protection comme la disponibilité, l'intégrité des données, l'imputabilité ou la traçabilité).
- Lorsque les traitements de données ont lieu à l'étranger, il faut privilégier les Etats pour lesquels il existe un niveau de protection des données équivalent (sécurité juridique).

Le fournisseur du service soumis au CLOUD Act[4] doit accorder un droit d'accès aux données enregistrées aux autorités nord-américaines. Celui-ci doit être accordé même si la sauvegarde n'intervient pas aux USA mais par exemple dans un Etat de l'union européenne ou en Suisse.

---

[4] Pour savoir qui est soumis au CLOUD Act, voir le Whitepaper du département de justice américain du mois d'avril 2019, en particulier la p. 8 : <https://www.justice.gov/opa/press-release/file/1153446/download>.

3.3 La protection des secrets, le cryptage et la gestion des clés

Les données (data at rest *et* data in transit) doivent être cryptées selon l'état actuel de la technologie.

En cas de données personnelles sensibles (y compris les données soumises au secret professionnel ou à un secret de fonction particulier), il convient d'édicter des conditions supplémentaires pour le cryptage et la gestion des clés, qui doivent être pris en compte dans la gestion des risques :

- le cryptage doit être réalisé par l'organe public. Les clés doivent être en principe exclusivement mises à la disposition de l'organe public. Les clés doivent être protégées en cas de perte, soustraction tout comme utilisation et prise de connaissance abusives ;

- si cela n'est pas possible, le fournisseur du service du Cloud peut conserver les clés s'il s'engage par contrat à ne les utiliser qu'avec le consentement exprès de l'organe public. Il faut tenir un procès-verbal des accès. De plus, le fournisseur du service du Cloud doit protéger les clés en cas de perte, soustraction tout comme utilisation et prise de connaissance abusives. Il doit aussi garantir que les données ne peuvent pas être compromises lors du processus de cryptage.

3.4 Contrat

L'organe public doit conclure un contrat écrit avec le fournisseur du service du Cloud. Alternativement, il conclut un contrat cadre ou accepte des conditions générales (CG) qui respectent les exigences indiquées dans le présent aide-mémoire et qui ne peuvent pas être modifiées de manière unilatérale.

3.5 Sous-traitance (Subcontracting)

Le fournisseur du service du Cloud doit annoncer d'éventuels contrats de sous-traitance, afin qu'il soit possible d'évaluer les risques en relation avec tous les prestataires de service.

3.6 Devoirs d'annonce

Le fournisseur du service Cloud doit annoncer toute modification dans la manière de traiter les données (lieu du traitement, sous-traitance) et tout événement lié à la sécurité à l'organe public, afin que des mesures en relation avec les services du Cloud puissent être prises à temps.

3.7 Droit et possibilité de contrôle

L'organe public doit conserver le droit d'effectuer des contrôles : le fournisseur doit s'engager à procéder à des contrôles réguliers de l'infrastructure du Cloud, compte tenu des standards internationaux. En outre, il doit exiger que les rapports des contrôles soient, sur demande, remis à lui-même et à l'autorité de la protection des données compétente.

3.8 Mesures de sécurité de l'information

L'organe public doit s'assurer que ses exigences de protection sont garanties. Pour ce faire, il doit obliger le fournisseur du service Cloud à déclarer les objectifs de sécurité et les mesures avec lesquelles il entend les atteindre.

3.9 Exploitation de l'infrastructure du Cloud

Le fournisseur du service Cloud doit exploiter son infrastructure Cloud selon les standards internationaux et le prouve, cas échéant, avec les certificats usuels (ISO).

3.10 Obligations en cas de résiliation

Le processus à respecter en cas de résiliation du contrat de service doit être convenu au moment de sa conclusion (en particulier la restitution des données et leur suppression).

4 Conclusions pour les organes publics

Dans la mesure où ils respectent les règles qui leur sont imposées pour une sous-traitance du traitement des données (voir les documents référencés dans l'annexe no 2 ci-dessous), les organes publics peuvent aussi se servir de la technologie du Cloud fournie par un tiers. A cet effet, il est nécessaire de tenir compte des risques spécifiques liés aux services du Cloud. L'analyse du risque doit être faite de manière différenciée pour tous les traitements de données. Elle doit démontrer les risques spécifiques à la technologie du Cloud et les mesures concrètes avec lesquelles on entend exclure la réalisation du risque, respectivement avec lesquelles on diminue le risque dans une mesure acceptable. Une telle analyse des risques doit établir si, pour un traitement donné, l'utilisation des services du Cloud est globalement, partiellement ou pas du tout licite.

Les organes publics qui utilisent un Cloud pour accomplir leurs tâches restent responsables du traitement des données. L'organe public (resp. sa direction) doit confirmer par écrit qu'il a compris les risques (résiduels) et qu'il est prêt à les assumer. La prise en compte des risques résiduels peut avoir une conséquence sur la comptabilité, ce qui devrait être vérifié par le contrôle des finances. Il est conseillé que l'exécutif prenne régulièrement connaissance de ces risques résiduels car c'est lui qui répond face au parlement et à la population du respect des droits fondamentaux des citoyennes et des citoyens et des agissements financiers de l'administration.

L'organe public doit procéder à une analyse d'impact sur le plan de la protection des données. Il convient de soumettre une analyse des risques et un plan des mesures aux autorités de la protection des données compétentes (contrôle préalable et consultation préalable). Ces autorités conseillent les organes publics par rapport à des questions juridiques, organisationnelles et techniques.

Annexe no 1 : exemples

Cas	Droit applicable / for (3.1)	Emplacement de l'infrastructure Cloud (3.2)	Protection du secret et la gestion des clés (3.3)
1	Droit suisse (sur la protection des données) / for Suisse	(exclusivement) en Suisse	1a. auprès de l'organe public 1b. auprès du fournisseur du service Cloud, qui s'est engagé par contrat à n'utiliser les clés qu'avec le consentement exprès de l'organe public
	Evaluation privatim :	*1a. risques spécifiques à la technologie du Cloud réduits* *1b. risques spécifiques à la technologie du Cloud élevés pour un fournisseur du service soumis au CLOUD Act*	
	Recommandation privatim :	*1a. L'utilisation de la technologie du Cloud est possible.* *1b. Les risques sont élevés lorsque le fournisseur du service cloud est soumis au CLOUD Act. De tels fournisseurs doivent accorder l'accès aux données enregistrées aux autorités nord-américaines, même si les données ne sont pas sauvegardées aux USA, mais dans un Etat de l'Union européenne ou en Suisse. Pour le traitement de données personnelles sensibles, p.ex. des données soumises au secret professionnel ou à un secret de fonction particulier, il faut renoncer à la mise en œuvre d'une telle solution de Cloud. Le risque ne pourrait être réduit que par un cryptage par l'organe public (→ 1a).*	
2	Droit suisse (sur la protection des données) / for en Suisse	dans un (ou plusieurs) Etat(s) étrangers sans niveau équivalent dans la protection des données	2a. auprès de l'organe public 2b. auprès du fournisseur du service Cloud, qui s'oblige par contrat à n'utiliser la clé qu'avec l'accord exprès de l'organe public
	Evaluation privatim :	*2a. risques spécifiques à la technologie du Cloud élevés* *2b. risques spécifiques à la technologie du Cloud plus élevés lorsque le fournisseur du service Cloud est soumis au CLOUD Act*	
	Recommandation privatim :	*2a. L'utilisation de la technologie du Cloud est possible pour le traitement de données personnelles («ordinaires»).* *L'utilisation de la technologie du Cloud pour le traitement de données personnelles sensibles, resp. pour des données soumises au secret professionnel ou à un secret de fonction spécial, comporte des risques élevés. Ceux-ci peuvent être réduits si l'infrastructure du Cloud se trouve en Suisse ou du moins dans un pays avec un niveau de protection des données équivalent. Ce point doit être pris en considération dans l'analyse globale du risque.* *2b. Les fournisseurs du service Cloud soumis au CLOUD Act doivent toutefois aussi accorder l'accès aux données enregistrées aux autorités nord-américaines, même si les données ne sont pas sauvegardées aux USA. Pour le traitement de données personnelles sensibles, p.ex. des données soumises au secret professionnel ou à un secret de fonction particulier, il faut renoncer à la mise en œuvre d'une telle solution de Cloud. Le risque ne pourrait être réduit que par un cryptage par l'organe public (→ 2a)*	

3	Droit Suisse (sur la protection des données) / for Suisse	dans un (ou plusieurs) Etat(s) étranger(s) sans niveau équivalent dans la protection des données	auprès du fournisseur du service Cloud
	Evaluation privatim :	*Risques spécifiques à la technologie du Cloud très élevés*	
	Recommandation privatim :	*Il convient de renoncer à l'utilisation de telles technologies du Cloud dans le cadre du traitement de données personnelles.*	

Annexe no 2 : guides sur la sous-traitance du traitement des données par des préposé(e)s cantonaux à la protection des données

Canton de Bâle-campagne	Merkblatt Outsourcing
Canton de Bâle-ville	Website «Handreichungen» Leitfaden Auftragsdatenbearbeitung
Canton de Genève	Fichier «Cloud Computing et protection des données personnelles au sein des institutions publiques genevoises»
Canton de St. Gall	Website «Informatik» Checkliste «Vereinbarungsinhalt beim Outsourcing»
Canton de Zurich	Website «Outsourcing» Leitfaden Bearbeiten im Auftrag Leitfaden Verschlüsselung der Datenablage im Rahmen der Auslagerung