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 «Risques et mesures spécifiques à la technologie de Cloud computing»

1 Introduction

Dans le cadre du traitement des données, les organes publics se servent 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 complètement la responsabilité des organes publics pour des données traitées par des tiers. La manière d'assumer cette responsabilité, en 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-listes[1].

Les prestations de traitement de données sont toujours plus fréquemment basées sur l'utilisation de la **technologie de Cloud computing**:

> *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 des prestations de traitements de données mettent à contribution de tels service de Cloud computing, 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 de Cloud computing. 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 et de volonté de se servir de cette technologie, il convient d'analyser l'utilisation du Cloud computing 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 de Cloud computing de sous-traitants, les risques suivants existent ou s'accentuent dans des domaines spécifiques:

- transparence liée à 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 (au droit applicable, au for, à la quantité des prestations, aux mesures de sécurité, au 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);
- transparence concernant les mesures de sécurité des informations (perte et abus des données);
- transparence sur l'existence d'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 de Cloud computing

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

Trois questions particulières doivent être traitées de manière prioritaire:

- 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 de Cloud computing est principalement déterminé par ces trois points. Il faut y ajouter d'autres risques qui sont 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 au niveau cantonal) 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 de services de Cloud computing; voir chiffre 3.3) ou

- lorsque les données ne sont pas sensibles et que l'Etat en question dispose d'une législation assurant un niveau de protection adéquat sur le plan de la protection des données (p.ex. les pays de l'UE).

3.2 Lieu du traitement des données

Le fournisseur de services de Cloud computing 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 adéquat de protection des données (sécurité juridique).

3.3 La protection des secrets et la gestion des clés

Les données (‹data at rest› *et* ‹data in transit›) doivent être cryptées.

En cas de données personnelles sensibles (y compris les données soumises à un secret professionnel ou à un secret de fonction particulier), il convient d'édicter des conditions supplémentaires pour la gestion des clés et l'évaluation des risques:

- Les clés doivent être exclusivement mises à la disposition de l'organe public.

- Si cela n'est pas possible, le fournisseur de services de Cloud computing peut conserver les clés s'il s'engage par contrat à les utiliser qu'avec le consentement exprès de l'organe public et s'il protège les clés contre une perte, une soustraction et contre une utilisation voire une communication abusive. Il faut tenir un protocole des accès.

3.4 Contrat

L'organe public doit conclure un contrat écrit avec le fournisseur de services de Cloud computing. 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 de services de Cloud computing 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 de services de Cloud computing 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 de Cloud computing puissent être prises à temps.

3.7 Droit et possibilités de contrôle

Lorsque l'organe public se sert de la technologie de Cloud computing, il ne peut – en fait – pas contrôler la sécurité des services. Il doit donc obliger le fournisseur de services de Cloud computing 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 soient garanties. Pour ce faire, il doit obliger le fournisseur de services de Cloud computing 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 de services de Cloud computing 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

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 de Cloud computing fournie par un tiers. A cet effet, il est nécessaire de tenir compte des risques spécifiques liés aux services de Cloud computing. 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 de Cloud computing 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 de Cloud computing est totalement, partiellement ou pas du tout licite.

Les organes publics qui se servent de services de Cloud computing pour accomplir leurs tâches restent complètement responsables pour le traitement des données. L'organe public (resp. sa direction) doit confirmer par écrit qu'il a compris les risques et qu'il est prêt à assumer les risques résiduels. 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 fasse saisir régulièrement 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 resp. consultation préalable). Ces autorités conseillent les organes publics par rapport à des questions juridiques, organisationnelles et techniques.

Annexe no 1: exemples d'une évaluation globale des risques de la technologie de Cloud computing en relation avec le droit applicable et le for, le lieu du traitement des données et la protection du secret et la gestion des clés

Cas	Droit appplicable / for (3.1)	Lieu du traitement des données (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	auprès de l'organe public
	Evaluation privatim:	*Risques spécifiques à la technologie de Cloud computing réduits*	
	Recommandation privatim:	*L'utilisation de la technologie de Cloud computing dépend du résultat de l'analyse globale du risque en cas de sous-traitance.*	
2	Droit suisse (sur la protection des données) / for suisse	dans un (ou plusieurs) Etat(s) étrangers sans législation assurant un niveau de protection adéquat sur le plan de la protection des données	auprès du fournisseur de services de Cloud computing, qui s'oblige par contrat à utiliser la clé qu'avec l'accord exprès de l'organe public
	Evaluation privatim:	*Risques spécifiques à la technologie de Cloud computing élevés*	
	Recommandation privatim:	*L'utilisation de la technologie de Cloud computing est possible pour le traitement de données personnelles («ordinaires»).* *L'utilisation de la technologie de Cloud computing pour le traitement de données personnelles sensibles resp. pour des données soumises à un 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 adéquat.* *Ce point doit être pris en considération dans l'analyse globale du risque.*	
3	Pas de droit suisse (sur la protection des données) / pas de for suisse	dans un (ou plusieurs) Etat(s) étrangers sans législation assurant un niveau de protection adéquat sur le plan de la protection des données	auprès du fournisseur de services de Cloud computing
	Evaluation privatim:	*Risques spécifiques à la technologie de Cloud computing très élevés*	
	Recommandation privatim:	*Il convient de renoncer à l'utilisation de telles technologies de Cloud computing 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