privatim
die schweizerischen datenschutzbeauftragten
les commissaires suisses à la protection des données
gli incaricati svizzeri della protezione dei dati

Aide-mémoire

LE CLOUD COMPUTING DANS LE DOMAINE SCOLAIRE

1 Introduction

Cet aide-mémoire s'adresse aux écoles qui évaluent l'utilisation des services Cloud, comme par exemple Dropbox, Microsoft Office 365 ou Google Drive ou qui utilisent déjà ces services.

Si le traitement des données a lieu dans un Cloud, il s'agit d'un « traitement de données sur mandat », aussi appelé « externalisation » ou « outsourcing ». Dans un cas pareil, les risques sont considérablement plus élevés que lors d'un traitement de données sur mandat conventionnel. C'est pour cette raison qu'il faut particulièrement veiller aux facteurs inhérents aux Cloud comme par exemple la sauvegarde des données à plusieurs endroits et le traitement dans des situations de sous-traitance. En outre, avant l'utilisation de telles prestations, il faut répondre à diverses questions juridiques. Il est, par exemple, possible que des règles de confidentialité ou le secret professionnel s'opposent au traitement des données dans un Cloud.

Cet aide-mémoire traite des conditions juridiques, des questions à poser en amont d'une utilisation de tels services Cloud et des mesures à mettre en oeuvre.

2 Conditions juridiques

Pour l'utilisation d'un service Cloud, les conditions de la législation sur la protection des données (et sur la transparence), particulièrement concernant le « traitement de données sur mandat », s'appliquent. Dans ce contexte, il importe peu de savoir si le service Cloud est utilisé pour la sauvegarde des données, pour la simplification de la communication ou pour la collaboration. L'école qui se sert d'une telle prestation doit en toute circonstance être en mesure d'assumer ses responsabilités par rapport à la protection des données et la sécurité informatique, car c'est elle qui est responsable du traitement des données.

privatim
die schweizerischen datenschutzbeauftragten
les commissaires suisses à la protection des données
gli incaricati svizzeri della protezione dei dati
c/o Datenschutzbeauftragter des Kantons Zürich
Postfach, CH-8090 Zürich
Tel. +41 (43) 259 39 99, Fax +41 (43) 259 51 38
geschaeftsstelle@privatim.ch, www.privatim.ch

En partant du choix d'un service Cloud jusqu'à son utilisation, il convient de distinguer principalement cinq étapes :

- Vérifier si les données peuvent être traitées par le mandataire
- Vérifier si les données traitées peuvent l'être dans un service Cloud
- Sélectionner le service Cloud et un éventuel fournisseur
- Rédiger un contrat ou vérifier les conditions générales d'utilisation / CG
- Mettre en œuvre les mesures nécessaires

3 Démarche

3.1 Vérifier si les données peuvent être traitées par le mandataire

Si l'on prend en considération l'utilisation des services Cloud, il faut tout d'abord vérifier si des normes légales ou conventionnelles s'opposent à un tel traitement de données sur mandat. Il convient notamment de tenir compte des devoirs de confidentialité particuliers, comme par exemple le secret professionnel des psychologues scolaires.

Les données soumises à des devoirs de confidentialité particulières ne peuvent être traitées dans un Cloud que si la confidentialité est garantie et que les données sont protégées par cryptage, afin que le fournisseur du Cloud ne puisse pas y accéder.

3.2 Vérifier si les données traitées peuvent l'être dans un service Cloud

Lorsqu'on vérifie si les données traitées peuvent l'être dans un service Cloud, il faut principalement se préoccuper de leur sensibilité.

L'école doit évaluer le potentiel de menace et les buts de la protection, notamment au niveau de la confidentialité, de la disponibilité et de l'intégrité des données. Cela signifie qu'il faut éviter la perte des données, il faut les rendre inaccessibles pour des tiers non autorisés et il faut les protéger d'une manipulation non autorisée. Cette évaluation permet de déterminer les exigences relatives au service Cloud respectivement à son fournisseur.

En principe, les exigences sont échelonnées selon le type de données traitées (allant des données impersonnelles, aux données personnelles puis aux données sensibles). Plus les données sont délicates sur un plan du droit de la personnalité, plus les exigences liées à l'organisation, à la technique et aux règlements contractuels du service Cloud sont élevées. Souvent ce sont justement des produits standardisés qui ne peuvent pas être adaptés afin de répondre aux conditions cadres de l'école.

3.3 Sélectionner le service Cloud et une éventuel fournisseur

Si aucun devoir de confidentialité ne s'oppose au traitement des données dans un Cloud, si le niveau de protection a été déterminé et que les mesures à prendre sont définies, il est possible de choisir le service Cloud.

On peut demander à un fournisseur de Cloud de démontrer que les conditions cadres de l'école peuvent être satisfaites, respectivement d'exposer les conditions cadres juridiques, organisationnelles et techniques de la prestation proposée. Le choix peut être facilité par certificats ou des rapports d'audit indépendants.

Toutefois, l'utilisation de produits standards est souvent mise en échec par le fait qu'il est impossible de conclure des contrats ou des conditions d'utilisation répondant aux exigences de la protection des données. Fréquemment, les prestataires de service n'acceptent pas de dérogation à leurs dispositions contractuelles.

3.4 Rédiger un contrat ou vérifier les conditions d'utilisation / CG

En règle générale, il convient d'exiger un contrat écrit entre l'école et le fournisseur de Cloud. Pour pouvoir prendre en compte les évolutions technologiques, il est aussi possible de convenir des conditions d'utilisation, respectivement des CG. Par contre, la modification unilatérale des conditions d'utilisation voire des CG par le fournisseur ne peut pas être admise.

Les exigences liées au contenu du contrat ou des conditions d'utilisation sont concrétisées par la législation sur la protection des données (et sur la transparence). Notamment, il faut régler :

- l'objet du traitement de données et son intensité
- la responsabilité (qui est responsable de quoi)
- le pouvoir de disposer (doit être réservé à l'école)
- la finalité du traitement (les données peuvent uniquement être traitées pour des buts scolaires)
- les devoirs de confidentialité
- les droits des personnes concernées (le droit d'accès ainsi que la mise en oeuvre des droits à la rectification et à l'effacement des données doivent être garantis dans le contrat).
- la possibilité d'exercer un contrôle par l'institution scolaire ou une institution spécialisée externe
- les mesures de sécurité informatique (pour la garantie de la confidentialité, de l'intégrité, de la disponibilité, de l'authenticité et de la vérifiabilité).
- les éventuels contrats de sous-traitance (devoir de déclarer de tels contrats et modification soumise à l'accord de l'école)

- lors d'un traitement de données à l'étranger (soit il y a un niveau de protection des données identique ou alors il faut convenir de mesures additionnelles)
- les lieux du traitement des données (les lieux doivent être connus et un changement de localité doit être signalisé et accepté par l'école)
- le droit applicable (il faut convenir le droit suisse)
- le for (il faut convenir d'un for suisse)

3.5 Mettre en œuvre les mesures nécessaires

L'école doit vérifier constamment la mise en œuvre des conditions organisationnelles, techniques et juridiques convenues par contrat ou dans les conditions d'utilisation. Comme mentionné, le recours à des institutions spécialisées ou à des certificats est admissible.

4 Informations supplémentaires

privatim – Aide-mémoire Cloud Computing (Juillet 2013)

V 1.0 / Octobre 2013