Le *cloud* à la lumière du droit de la protection des données

Barbara Widmer, docteur en droit, LL.M.,
CIA (Certified Internal Auditor)

15 juin 2018

Journée des avocats 2018 à Schaffhouse

Marc Zuckerberg :

«Autrefois, nous vivions à la campagne. Nous nous sommes ensuite déplacés en ville. Aujourd'hui, nous habitons dans un vaste réseau»

Sommaire

I. Fondements

Définition de l'informatique en nuage, du *cloud*

Mise à disposition

- d'une **capacité de traitement informatique**

- d'un **espace de stockage**

- de **logiciels**

proposés sous la forme de **services en ligne** ⇨ via des navigateurs

I. Fondements

Caractéristiques du *cloud*

Particularités des services proposés :

- Disponibilité qui s'adapte aux **besoins particuliers**
- Coûts liés à la **consommation**

⇨ grande **flexibilité** et efficacité **des coûts**

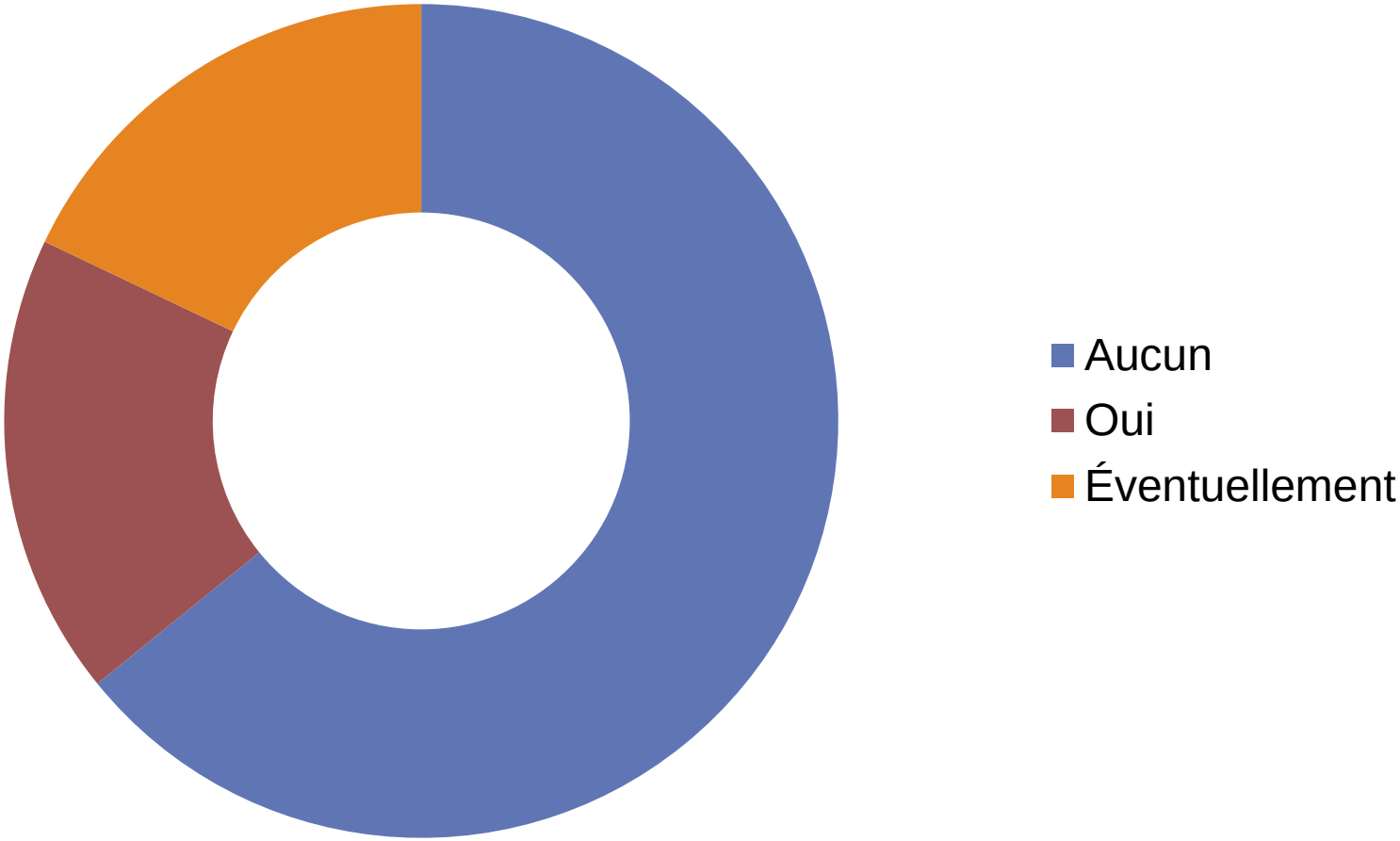
I. Fondements

Utilisation du *cloud* (cf. en 2016 pour les entreprises allemandes)

Source : Statista.com

I. Fondements

Problèmes de sécurité (en 2016 pour les entreprises allemandes)



Source: Statista.com

II. Cadre juridique

Le fournisseur d'un *cloud* **traite les données** de l'utilisateur

- en exploitant des logiciels
- en mettant à disposition une infrastructure et une capacité de stockage

= traitement régulier de **données personnelles**

⇨ le **droit de la protection des données** s'applique

II. Cadre juridique

Terminologie en **droit de la protection des données**

«Traitement de données par un tiers» (art. 10a LPD)

deviendra «*sous-traitance*» (art. 8 P-LPD)

Base légale :

Art. 10a DSG et art. 8 P-DSG

III. «Sous-traitance»

Base légale

Art. 10a LPD:

Le traitement de données personnelles peut être confié à un tiers pour autant qu'une convention ou la loi le prévoie et que les conditions suivantes soient remplies :

a. Seuls les traitements que le mandant serait en droit d'effectuer lui-même sont effectués ;

b. Aucune obligation légale ou contractuelle de garder le secret ne l'interdit.

[2]…

Art. 8 P-LPD:

1 Le traitement de données personnelles peut être confié à un sous-traitant pour autant qu'un contrat ou la loi le prévoie et que les conditions suivantes soient réunies:

a. Seuls sont effectués les traitements que le responsable du traitement serait en droit d'effectuer lui-même;

b. Aucune obligation légale ou contractuelle de garder le secret ne l'interdit.

[2]…

[3]…

III. «Sous-traitance»

Let. a – Traitements que le mandant serait en droit d'effectuer lui-même

Les **traitements** que le mandant est en droit d'effectuer lui-même découlent

- du **droit de la protection des données** en vigueur
- de **directives spéciales** applicables en la matière

III. «Sous-traitance»

Let. a – Traitements que le mandant serait en droit d'effectuer lui-même

La let. a nécessite que

1. Le «sous-traitant» **connaisse** les règles applicables

2. Le «sous-traitant» les **applique** en s'y engageant contractuellement

⇨ convention séparée sur la protection des données ou partie intégrante du contrat de services

3. Le mandant en **vérifie** l'application

III. «Sous-traitance»

Let. a – Traitements que le mandant serait en droit d'effectuer lui-même

Difficultés à mettre en œuvre les **chiffres 2 et 3** précités dans l'informatique en nuage:

- Contexte souvent **international** → risque de conflits de lois
- **Position de force** du «sous-traitant» sur le marché → difficulté à négocier
- Données ventilées sur **plusieurs serveurs** ou à des **emplacements inconnus**

III. «Sous-traitance»

Let. b – Obligation de garder le secret

Légalement ou contractuellement :

- **Légalement :** secret de fonction, secret professionnel, secret des télécommunications, etc.

- **Contractuellement** : clauses de confidentialité

III. «Sous-traitance»

Let. b – Obligation de garder le secret

…Examen de chaque cas d'espèce:
L'obligation au secret vise-t-elle à empêcher la «sous-traitance» de données personnelles ?

…NON : au regard de la protection des données, le secret ne s'oppose pas en soi à l'externalisation de données.

…MAIS, il subsiste toujours une obligation de garder le secret à l'égard de tiers.

III. «Sous-traitance»

Législation européenne sur la protection des données

Les dispositions particulièrement exhaustives du droit européen… Ici, l'art. 28 du *Règlement général sur la protection des données* (RGPD) :

Artikel 28

Auftragsverarbeiter

(1) Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

(2) Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

(3) Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind. Dieser Vertrag bzw. dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter

a) die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen — auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation — verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;

b) gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;

c) alle gemäß Artikel 32 erforderlichen Maßnahmen ergreift;

d) die in den Absätzen 2 und 4 genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;

e) angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen;

f) unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützt;

g) nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht;

h) dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen — einschließlich Inspektionen —, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt.

Mit Blick auf Unterabsatz 1 Buchstabe h informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen diese Verordnung oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

(4) Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in dem Vertrag oder anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter gemäß Absatz 3 festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden muss, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen dieser Verordnung erfolgt. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.

(5) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 durch einen Auftragsverarbeiter kann als Faktor herangezogen werden, um hinreichende Garantien im Sinne der Absätze 1 und 4 des vorliegenden Artikels nachzuweisen.

(6) Unbeschadet eines individuellen Vertrags zwischen dem Verantwortlichen und dem Auftragsverarbeiter kann der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 des vorliegenden Artikels ganz oder teilweise auf den in den Absätzen 7 und 8 des vorliegenden Artikels genannten Standardvertragsklauseln beruhen, auch wenn diese Bestandteil einer dem Verantwortlichen oder dem Auftragsverarbeiter gemäß den Artikeln 42 und 43 erteilten Zertifizierung sind.

(7) Die Kommission kann im Einklang mit dem Prüfverfahren gemäß Artikel 87 Absatz 2 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.

(8) Eine Aufsichtsbehörde kann im Einklang mit dem Kohärenzverfahren gemäß Artikel 63 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.

(9) Der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.

(10) Unbeschadet der Artikel 82, 83 und 84 gilt ein Auftragsverarbeiter, der unter Verstoß gegen diese Verordnung die Zwecke und Mittel der Verarbeitung bestimmt, in Bezug auf diese Verarbeitung als Verantwortlicher.

III. «Sous-traitance»

Législation européenne sur la protection des données

Art. 28 RGPD (sous-traitant)

Al. 1er :

Le responsable du traitement doit s'assurer que le sous-traitant présente des garanties suffisantes :

- le traitement doit **répondre aux exigences du présent règlement** et
- **garantir la protection des droits de la personne concernée**.

III. «Sous-traitance»

Législation européenne sur la protection des données

Al. 2:

En cas de sous-traitance du **sous-traitant** ⇨ il faut l'accord écrit du mandant responsable du traitement des données.

Al. 3:

L'objet et la durée du traitement doivent être définis dans un contrat entre le mandant responsable du traitement et le mandataire sous-traitant.

Al. 10:

Les sous-traitant tombent **sous le coup des amendes** prévues en droit européen.

III. «Sous-traitance»

Législation européenne sur la protection des données

Art. 3 al. 1er RGPD (champ d'application territorial)

La législation européenne s'applique à des **sous-traitants sur le territoire de l'UE**, également si

- le **traitement** n'a pas lieu dans l'UE ou que
- le **responsable du traitement** ne se trouve pas dans l'UE.

⇨ En cas de conflits de lois avec le droit suisse, celui-ci entend s'appliquer au sous-traitant.

III. «Sous-traitance»

Législation européenne sur la protection des données

Distinctions avec le droit suisse :

- **Pas de secret** destiné à s'opposer explicitement à une éventuelle sous-traitance
- **Sous-traitant qui fait appel à un autre sous-traitant** : n'est possible que si **consentement** écrit (condition légale)
- **Un sous-traitant** dans l'UE est soumis **au droit européen**

III. «Sous-traitance»

sous-traitant avec siège à l'étranger

… **c'est possible**, mais le **sous-traitant** doit traiter les données selon le droit suisse, où qu'il soit ⇨ conflits de lois avec le droit européen

ET le mandant responsable de traitement doit effectuer une analyse des risques soignée ⇨ critères à prendre en compte :

- nature et sensibilité des données
- importance de la protection des données dans le droit de l'Etat d'externalisation

III. «Sous-traitance»

Analyse du risque

Clauses contractuelles: nature et sensibilité des données

Données	Lieu du serveur	2e sous-contrat	Droit applicable	For
Très sensibles				
Moyennement sensibles				
Peu sensibles				

III. «Sous-traitance»

Analyse de risque

Choix de l'Etat de sous-traitance
selon l'importance que celui-ci accorde à la protection des donnée

Pays	Droit applicable	Sensibilité à la protection des données
UE		
USA		
Russie, Chine, Inde, etc.		

IV. Tendances

Comment évoluera le *cloud* ?

⇨ Le *cloud* est en pleine croissance et continuera d'être développé.

⇨ Cette évolution s'**explique** par :

- la globalisation
- l'utilisation accrue d'appareils mobiles (téléphones, tablettes, ordinateurs portables)
- la pression des coûts sur l'informatique
- l'amélioration de la compétitivité

V. Conclusions

Le *cloud* :

- Plus rien n'empêche sa progression
- Il s'agit d'un bon outil de travail
- Le droit de la protection des données ne s'oppose pas fondamentalement au *cloud*, mais pose des garde-fous.
- Le mandant doit s'assurer et est responsable que le «sous-traitant» respecte le droit de la protection des données.

Je vous remercie de votre attention.