ETAT DE FRIBOURG
STAAT FREIBURG

Service de législation SLeg
Amt für Gesetzgebung GeGA

Développements de la Cyberadministration dans le canton de Fribourg

—

Bases légales sur le recours au *cloud computing*

—

Chancellerie d'Etat **CHA**
Staatskanzlei **SK**

Plan de la présentation

1. Approche juridique du *cloud computing*
2. Stratégie d'informatique en nuage des autorités suisses 2012-2020
3. Appréhension et mise en œuvre à l'échelon de la Confédération
4. Appréhension et mise en œuvre à l'échelon du canton de Fribourg
5. Discussion

1. Approche juridique du *cloud computing*

Définition donnée dans la législation fribourgeoise

*Forme de **sous-traitance** impliquant la **délocalisation** du traitement de données ou de la gestion d'outils informatiques sur les infrastructures du sous-traitant / Form der **Bearbeitung durch Auftragsbearbeiter**, die zur Folge hat, dass das Bearbeiten von Daten oder die Verwaltung von Informatiktools auf die Infrastrukturen des Auftragsbearbeiters übertragen werden* (cf. art. 3 al. 1 let. g LCyb / 3 al. 1 let. e1).

Similitudes et différences avec quelques notions connues

> Avec l'hébergement de données

> Avec la communication de données (à l'étranger)

> Avec la sous-traitance «ordinaire»

2. Stratégie d'informatique en nuage des autorités suisses 2012-2020

Constat

Les lois, ordonnances et règlements existants ont le plus souvent été créés à une époque où l'informatique en nuage, ses possibilités et ses risques **étaient encore inconnus**. C'est pourquoi il existe des dispositions qui, à tort, gênent ou même empêchent son utilisation. D'un autre côté, les nouvelles possibilités et risques de l'informatique en nuage nécessitent des prescriptions complémentaires. La réglementation **doit être adaptée** en conséquence.

2. Stratégie d'informatique en nuage des autorités suisses 2012-2020

Objectif

Les bases légales soutiennent **l'utilisation responsable** de l'informatique en nuage par la Confédération, les cantons et les communes. Les conditions cadres de la protection des données et des informations **restent garanties**. Tout **obstacle légal injustifié** est éliminé et des **prescriptions spécifiques** à l'informatique en nuage sont ajoutées quand cela est nécessaire.

Mesures

> Identification d'obstacles légaux et de prescriptions à ajouter

En collaboration avec des associations et des organisations intéressées, les autorités identifient les adaptations requises et entreprennent les démarches subséquentes.

> Elimination des points faibles

Les autorités concernées procèdent aux adaptations légales nécessaires afin d'éliminer les points faibles identifiés.

3. Appréhension et mise en œuvre à l'échelon de la Confédération

> Message du Conseil fédéral concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données (septembre 2017)

*« Lorsque des données sont stockées «en nuage», il s'agit en principe **de sous-traitance**, qui doit satisfaire aux conditions y afférentes. Si des données sont transférées à cet effet **à l'étranger**, il faut en outre que les conditions prévues aux art. 13 et 14 soient remplies. »* (FF 2017 6565, p. 6652)

> Bericht zur Bedarfsabklärung für eine « Swiss Cloud » (décembre 2020)

*« Umgekehrt wünschen sich Vertreter aus **der Wirtschaft und kantonalen Verwaltungen**, dass die Bundesverwaltung eine Vorreiterrolle übernimmt: Sie solle deutlich auf Cloud-Leistungen setzen und dies auch aktiv kommunizieren. Abgesehen von nachvollziehbaren wirtschaftlichen Interessen der beteiligten Akteure, wird **dabei nicht klar, weshalb die Bundesverwaltung eine Vorreiterrolle** in der Cloud-Nutzung einnehmen sollte. »*

3. Appréhension et mise en œuvre à l'échelon de la Confédération

> Stratégie d'informatique en nuage de l'administration fédérale (décembre 2020)

*«Il appartient **au propriétaire des données d'évaluer** si leur traitement est admis dans un nuage public ainsi que les mesures nécessaires à cet effet. Pour ce faire, il doit tout d'abord effectuer une analyse des besoins de protection, l'un des critères examinés étant le degré de confidentialité (non classifié, INTERNE, CONFIDENTIEL, SECRET).* […] *Des moyens auxiliaires correspondants (guides, listes de contrôle, processus) **sont mis à disposition** (cf. chap. 5) pour faciliter l'acquisition et l'utilisation conformes au droit et peu risquées des services en nuage public par les unités administratives de la Confédération. »*

4. Appréhension et mise en œuvre à l'échelon du canton de Fribourg

2018 Projet pilote « Cloud »

- *Observer sur un périmètre limité les possibilités techniques et les exigences sécuritaires indispensables à l'utilisation du Cloud*

2020 Loi adaptant la législation cantonale à certains aspects de la digitalisation

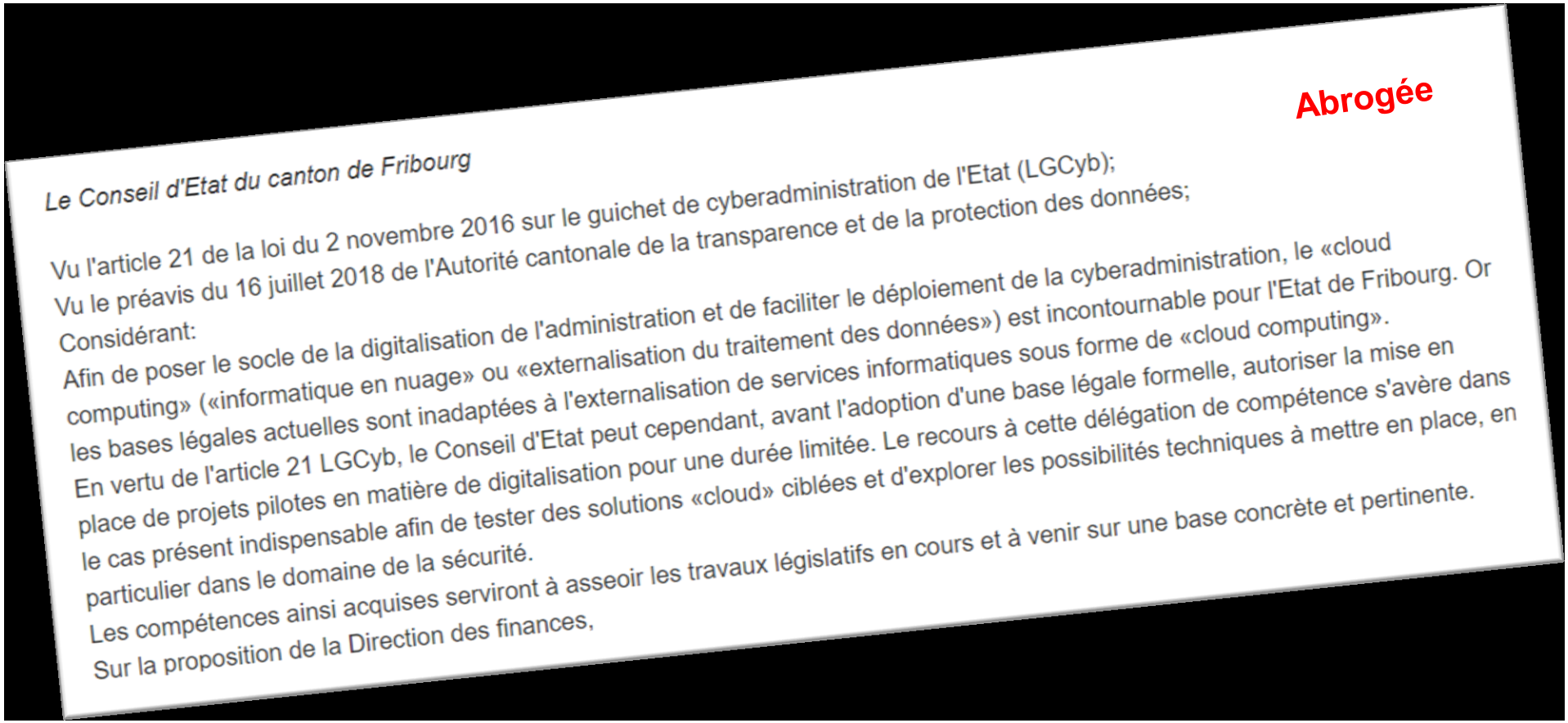
- ***Acte modificateur***
- *Projet Cloud*
- *Projet Référentiel cantonal*
- *Collaboration avec les communes*
- *Autres*

Loi sur la cyberadministration (Lcyb) et modification de la loi sur la protection des données (LPrD)

Adoption des bases légales sur l'externalisation du traitement de données et de la gestion d'outils informatiques

4. Appréhension et mise en œuvre à l'échelon du canton de Fribourg

Ordonnance autorisant le Service de l'informatique et des télécommunications à externaliser le traitement de certaines données



Abrogée

Le Conseil d'Etat du canton de Fribourg

Vu l'article 21 de la loi du 2 novembre 2016 sur le guichet de cyberadministration de l'Etat (LGCyb);
Vu le préavis du 16 juillet 2018 de l'Autorité cantonale de la transparence et de la protection des données;
Considérant:
Afin de poser le socle de la digitalisation de l'administration et de faciliter le déploiement de la cyberadministration, le «cloud computing» («informatique en nuage» ou «externalisation du traitement des données») est incontournable pour l'Etat de Fribourg. Or les bases légales actuelles sont inadaptées à l'externalisation de services informatiques sous forme de «cloud computing».
En vertu de l'article 21 LGCyb, le Conseil d'Etat peut cependant, avant l'adoption d'une base légale formelle, autoriser la mise en place de projets pilotes en matière de digitalisation pour une durée limitée. Le recours à cette délégation de compétence s'avère dans le cas présent indispensable afin de tester des solutions «cloud» ciblées et d'explorer les possibilités techniques à mettre en place, en particulier dans le domaine de la sécurité.
Les compétences ainsi acquises serviront à asseoir les travaux législatifs en cours et à venir sur une base concrète et pertinente.
Sur la proposition de la Direction des finances,

4. Appréhension et mise en œuvre à l'échelon du canton de Fribourg

Loi du 18.12.2020 adaptant la législation cantonale à certains aspects de la digitalisation (ROF 2020_195) (acte modificateur)

Loi sur la cyberadministration (RSF 184.1)	Loi sur la protection des données (RS 17.1)
Art. 27 Externalisation – Principes 1 Le traitement électronique de données et la gestion d'outils informatiques **peuvent être externalisés** aux conditions de la présente section. 2 Sont toutefois réservées: a) les exigences prévues par la **législation sur la protection des données**, lorsque l'externalisation porte sur le traitement de données personnelles; b) les exigences particulières de l'article 54 de la Constitution du canton de Fribourg du 16 mai 2004, lorsque l'externalisation implique **une délégation de tâches** à des tiers au sens de cette disposition.	**Art. 12b Externalisation – Principes** 1 Le traitement **de données personnelles**, y compris de données sensibles, **peut être externalisé** aux conditions posées par les présentes dispositions. 2 Les lieux de traitement doivent être situés en tout temps sur le territoire suisse ou sur le territoire d'un Etat garantissant un niveau de protection des données **équivalent**. 3 Lorsque l'externalisation implique une **délégation de tâches** à des tiers au sens de l'article 54 de la Constitution du canton de Fribourg du 16 mai 2004, les exigences particulières prévues par cette disposition sont applicables. 4 Le Conseil d'Etat présente tous les deux ans à la Commission des finances et de gestion **un rapport** sur l'externalisation.

4. Appréhension et mise en œuvre à l'échelon du canton de Fribourg

Questions choisies

Responsabilités
(Art. 30 LCyb / 12c LPrD)

> le ou les responsable(s) du traitement conserve(nt) la responsabilité des traitements de données qu'il confie à un tiers (**Cura in eligendo, in instruendo, in custodio**)

> Conclusion d'un **contrat** (contenu minimal : objet, nature, finalité et durée de l'externalisation, catégories de données concernées ainsi que obligations et droits de chaque partie)

> Application du principe ***Nemo plus iuris transferre potest quam ipse habet***

> **Récupération** des données externalisées

> Exigences spéciales pour l'externalisation **de données personnelles** (sous-sous-traitance, droits et possibilités de contrôle de l'autorité de surveillance, devoir d'annonce)

> **Responsabilité partagée** concernant le respect et la mise en œuvre des dispositions en matière d'externalisation entre l'organe métier et le service en charge de l'informatique et des télécommunications

> Si externalisation concerne **plusieurs organes différents**, désignation d'un organe principalement responsable

4. Appréhension et mise en œuvre à l'échelon du canton de Fribourg

Questions choisies

Mesures de sécurité
(Art. 29 LCyb / 12d LPrD)

> Mention des **objectifs de sécurité** à prendre en considération (intégrité, authenticité, disponibilité, pérennité, confidentialité)

> Mesures de sécurité à définir **au cas par cas** dans le contrat d'externalisation en fonction des **besoins spécifiques propres** à chaque type de traitement

> **Garantie de continuité** pour les activités indispensables au fonctionnement de l'administration

> Pour l'externalisation de **données personnelles**, rappel que les mesures à mettre en place servent également à servir les droits fondamentaux des citoyens et des citoyennes

4. Appréhension et mise en œuvre à l'échelon du canton de Fribourg

Questions choisies

Externalisation de secrets et de données sensibles (art. 28 LCyb / 12e LPrD)

> Reprise des exigences de **PRIVATIM** dans un langage technologiquement neutre (cf. § 3.3 de l'aide-mémoire sur les risques et les mesures spécifiques à la technologie du Cloud **[Version du 17.12.2019]**)

> En cas d'externalisation de données soumises à un secret, les données doivent être cryptées et les clés de décryptage doivent en principe être mises exclusivement à la disposition de l'organe public

> Si pas possible pour des raisons techniques, tout accès aux données requiert le consentement du responsable du traitement et doit faire l'objet d'une journalisation

> Exigences semblables pour l'externalisation de données sensibles lorsqu'il existe un risque concret d'atteinte

> Dans ces limites, la révélation à un fournisseur de services cloud d'information protégées par un secret n'est pas punissable (cf. art. 14 CP).

4. Appréhension et mise en œuvre à l'échelon du canton de Fribourg

Questions choisies

Divergences avec l'Autorité cantonale de la transparence et de la protection des données

> Notion de données personnelles
> Répartition des normes (LCyb – LPrD) et hiérarchie des normes
> Externalisation hors de Suisse
> For juridique

5. Discussion

CONTACT

Dr Michael Montavon, Service de législation de l'État de Fribourg
michael.montavon@fr.ch