Ordonnance

Entrée en vigueur :
01.12.2018

du 4 décembre 2018

autorisant le Service de l'informatique et des télécommunications à externaliser le traitement de certaines données dans le « Cloud » (projets pilotes)

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,

Arrête :

Art. 1

Le Service de l'informatique et des télécommunications (ci-après : le SITel) est autorisé à externaliser dans le « Cloud » le traitement de certaines données de l'Etat de Fribourg dans le cadre des projets pilotes suivants :

a) « Outils bureautiques collaboratifs » Microsoft 365 de Microsoft ;

b) « Services de communication unifiée » CiscoWebex Teams de Cisco ;

c) « Documentation Front End » SAP Enable Now de SAP ;

d) « Gestion des achats et des contrats » SAP Ariba de SAP.

Art. 2

[1] Chaque projet pilote est circonscrit à des populations d'utilisateurs et d'utilisatrices de test (« test users ») et est limité dans le temps.

[2] Les conditions spécifiques applicables à chaque projet sont énoncées dans les annexes 1 à 4, qui font partie intégrante de la présente ordonnance.

Art. 3

[1] En cas de fuite de données ou de panne de l'application, le SITel en informe sans délai le Conseil d'Etat ainsi que l'Autorité cantonale de la transparence et de la protection des données.

[2] Le SITel transmet le rapport d'évaluation prévu à l'article 21 al. 3 LGCyb au Conseil d'Etat ainsi qu'à l'Autorité cantonale de la transparence et de la protection des données.

Art. 4

[1] La présente ordonnance entre en vigueur avec effet rétroactif au 1er décembre 2018 et porte effet jusqu'au 31 décembre 2020.

[2] Si le Conseil d'Etat décide sur la base du rapport d'évaluation de poursuivre un ou plusieurs traitements énoncés à l'article 1, les dispositions pertinentes de la présente ordonnance restent valables jusqu'au 31 décembre 2022 ou jusqu'au moment de l'entrée en vigueur des bases légales formelles nécessaires.

Le Président : La Chancelière :

G. GODEL D. GAGNAUX-MOREL

A1 – ANNEXE 1

« Outils bureautiques collaboratifs » Microsoft 365

A1-1 But

Le projet pilote poursuit les objectifs suivants :

a) permettre, en vue de l'élaboration des bases légales nécessaires, l'exploration des caractéristiques techniques des services « Cloud » ;

b) clarifier les exigences de sécurité à prendre en compte lors de l'élaboration desdites bases légales ;

c) gagner la confiance numérique en mettant les solutions collaboratives « Cloud » à la disposition des entités participant au projet pilote ;

d) tester le niveau d'acceptation desdites entités et récolter auprès d'elles les retours d'expérience afin de permettre un déploiement rapide par la suite.

A1-2 Périmètre

Le projet pilote est mis en application auprès des personnes et dans les entités suivantes :

a) certaines écoles sélectionnées par la Commission informatique dans le domaine de l'enseignement, soit la Haute Ecole pédagogique Fribourg, le Collège de Gambach, l'Ecole professionnelle artisanale et commerciale Bulle et l'Ecole professionnelle et commerciale Fribourg ;

b) les membres du Grand Conseil et son Secrétariat ;

c) les membres du Conseil d'Etat ;

d) la Chancellerie d'Etat ;

e) les secrétariats généraux des Directions du Conseil d'Etat ;

f) le Service de l'informatique et des télécommunications (SITel) ;

g) l'Etablissement cantonal d'assurance des bâtiments (ECAB).

A1-3 Catégories de données

L'externalisation dans le « Cloud » concerne les données traitées au moyen des outils bureautiques collaboratifs (messagerie, calendriers personnels et partagés, notes).

A1-4 Droits d'accès aux données

Les droits d'accès aux données sont gérés par les administrateurs et administratrices internes du SITel, selon les principes applicables en cas d'exploitation en interne.

A1-5 Sécurité des données

Afin que la protection et la sécurité des données soient garanties, les exigences suivantes sont prévues :

a) le traitement des données est externalisé dans un Etat européen disposant d'un niveau de protection des données équivalant au niveau suisse ;

b) les données sont cryptées, et la clé de cryptage est détenue par le SITel ;

c) le SITel informe de manière adéquate les utilisateurs et utilisatrices des risques liés à l'utilisation de l'application et des mesures à prendre pour garantir la confidentialité du traitement des données.

A1-6 Responsabilité

Le projet pilote est placé sous la responsabilité du SITel, sous la supervision de la Commission informatique de l'Etat, qui adopte toutes les mesures propres à garantir la protection et la sécurité des données.

A1-7 Modalités contractuelles

Les contrats relatifs au projet pilote sont soumis au droit suisse et contiennent une clause de confidentialité ainsi qu'une clause d'élection de for en Suisse.

A2 – ANNEXE 2

« Services de communication unifiée » Cisco Webex Teams

A2-1 But

Le projet pilote poursuit les objectifs suivants :

a) permettre, en vue de l'élaboration des bases légales nécessaires, l'exploration des caractéristiques techniques des services de communication unifiée ;

b) clarifier les exigences de sécurité à prendre en compte lors de l'élaboration desdites bases légales ;

c) tester le niveau d'acceptation des services de communication unifiée auprès des entités participant au projet pilote ;

d) récolter les retours d'expérience afin de définir le profil des utilisateurs et utilisatrices à retenir à l'avenir pour le périmètre de déploiement.

A2-2 Périmètre

Le projet pilote est mis en application dans les entités suivantes :

a) le SITel ;

b) le Service de la mobilité ;

c) le Service cantonal des contributions.

A2-3 Catégories de données

Les données traitées sont les données échangées par les utilisateurs et utilisatrices grâce à la messagerie instantanée, au partage de fichiers, aux réunions vidéo, aux appels et aux autres outils de communication intégrés.

A2-4 Droits d'accès aux données

Les droits d'utilisation de la solution sont gérés par le SITel. L'échange des documents est en revanche effectué par les utilisateurs et utilisatrices.

A2-5 Sécurité des données

Afin que la protection et la sécurité des données soient garanties, les exigences suivantes sont prévues :

a) le traitement des données est externalisé dans un Etat européen disposant d'un niveau de protection des données équivalant au niveau suisse ;

b) les données sont cryptées, et la clé de cryptage est détenue par le SITel ;

c) le SITel informe de manière adéquate les utilisateurs et utilisatrices des risques liés à l'utilisation de l'application et des mesures à prendre pour garantir la confidentialité du traitement des données.

A2-6 Responsabilité

Le projet pilote est placé sous la responsabilité du SITel, sous la supervision de la Commission informatique de l'Etat, qui adopte toutes les mesures propres à garantir la protection et la sécurité des données.

A2-7 Modalités contractuelles

Les contrats relatifs au projet pilote sont soumis au droit suisse et contiennent une clause d'élection de for en Suisse.

A3 – ANNEXE 3

« Documentation Front End » SAP Enable Now

A3-1 But

Le projet pilote poursuit les objectifs suivants :

a) permettre, en vue de l'élaboration des bases légales nécessaires, l'exploration des caractéristiques techniques des services « Cloud » ;

b) clarifier les exigences de sécurité à prendre en compte lors de l'élaboration desdites bases légales ;

c) gagner la confiance numérique en mettant les solutions collaboratives « Cloud » à la disposition des entités participant au projet pilote ;

d) tester le niveau d'acceptation desdites entités et récolter auprès d'elles les retours d'expérience afin de permettre un déploiement rapide par la suite.

A3-2 Périmètre

Le projet pilote est mis en application au sein du SITel.

A3-3 Catégories de données

Les données traitées sont des données en rapport avec un contenu documentaire métier (guides d'utilisation, modes d'emploi, marches à suivre, descriptions de processus).

A3-4 Droits d'accès aux données

Les droits d'accès aux données sont gérés par les administrateurs et administratrices internes du SITel, selon les principes applicables en cas d'exploitation en interne.

A3-5 Sécurité des données

Afin que la protection et la sécurité des données soient garanties, les exigences suivantes sont prévues :

a) le traitement des données est externalisé dans un Etat européen disposant d'un niveau de protection des données équivalant au niveau suisse ;

b) le SITel informe de manière adéquate les utilisateurs et utilisatrices des risques liés à l'utilisation de l'application et des mesures à prendre pour garantir la confidentialité du traitement des données.

A3-6 Responsabilité

Le projet pilote est placé sous la responsabilité du SITel, sous la supervision de la Commission informatique de l'Etat, qui adopte toutes les mesures propres à garantir la protection et la sécurité des données.

A4 – ANNEXE 4

« Gestion des achats et des contrats » SAP Ariba

A4-1 But

Le projet pilote poursuit les objectifs suivants :

a) permettre, en vue de l'élaboration des bases légales nécessaires, l'exploration des caractéristiques techniques des services « Cloud » ;

b) clarifier les exigences de sécurité à prendre en compte lors de l'élaboration desdites bases légales ;

c) gagner la confiance numérique en mettant les solutions collaboratives « Cloud » à la disposition des entités participant au projet pilote ;

d) tester le niveau d'acceptation desdites entités et récolter auprès d'elles les retours d'expérience afin de permettre un déploiement rapide par la suite.

A4-2 Périmètre

Le projet pilote est mis en application au sein du SITel.

A4-3 Catégories de données

Les données traitées sont des données en rapport avec les achats et les contrats de prestations (contrats, fournisseurs, prix, dates, etc.).

A4-4 Droits d'accès aux données

Les droits d'accès aux données sont gérés par les administrateurs et administratrices internes du SITel, selon les principes applicables en cas d'exploitation en interne.

A4-5 Sécurité des données

Afin que la protection et la sécurité des données soient garanties, les exigences suivantes sont prévues :

a) le traitement des données est externalisé dans un Etat européen disposant d'un niveau de protection des données équivalant au niveau suisse ;

b) les données sont cryptées ;

c) le SITel informe de manière adéquate les utilisateurs et utilisatrices des risques liés à l'utilisation de l'application et des mesures à prendre pour garantir la confidentialité du traitement des données.

A4-6 Responsabilité

Le projet pilote est placé sous la responsabilité du SITel, sous la supervision de la Commission informatique de l'Etat, qui adopte toutes les mesures propres à garantir la protection et la sécurité des données.