

CHA/Avant-projet du 27.11.2019

Loi adaptant la législation cantonale à certains aspects de la digitalisation

du ...

Actes concernés (numéros RSF):

Nouveau: –

Modifié(s): **17.1** | 17.4

Abrogé(s): –

Le Grand Conseil du Canton de Fribourg

Vu le message du Conseil d'Etat du xx.xx.xxxx

Sur la proposition de cette autorité

Décrète

I.

L'acte RSF [17.1](#) (Loi sur la protection des données (LPrD), du 25.11.1994) est modifié comme il suit:

Art. 13b (*nouveau*)

Externalisation

¹ L'externalisation du traitement de données personnelles, y compris de données sensibles, auprès de personnes extérieures à l'administration doit respecter l'ensemble des obligations légales en matière de protection des données, en particulier l'article 18 sur le traitement de données sur mandat.

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 Les exigences en matière de sécurité doivent être mises en œuvre concrètement en fonction du type de données externalisées, des risques spécifiques ainsi que des systèmes ou technologies utilisés.

⁴ Le Conseil d'Etat précise les exigences à respecter, notamment concernant le choix et le contrôle des mandataires, la sécurité des données et la surveillance par l'Autorité cantonale de surveillance. Il publie une liste à jour des mandataires auprès desquels des données personnelles de l'Etat sont externalisées.

Art. 18 al. 1 (modifié), al. 2 (modifié), al. 3 (nouveau)

¹ L'organe public qui fait traiter des données personnelles par un tiers demeure responsable de la protection des données. En particulier il:

- a) *(nouveau)* prend toutes les précautions commandées par les circonstances quant au choix du ou de la mandataire, son instruction et sa surveillance;
- b) *(nouveau)* assure la protection des données par la conclusion systématique d'un contrat qui décrit au minimum l'objet, la nature, la finalité et la durée du traitement, le type de données personnelles et les catégories de personnes concernées, ainsi que les obligations et les droits du responsable du fichier et du ou de la mandataire;
- c) *(nouveau)* veille à ce que les données externalisées puissent être récupérées dans le but de changer de mandataire ou de procéder à leur ré-internalisation.

² Le traitement sur mandat de données faisant l'objet d'une obligation légale ou contractuelle de garder le secret n'est autorisé que si la confidentialité des données en cause est garantie, y compris à l'égard du ou de la mandataire.

³ Le ou la mandataire ne peut à son tour confier le traitement à un tiers qu'avec l'autorisation préalable du responsable du fichier.

II.

L'acte RSF [17.4](#) (Loi sur le guichet de cyberadministration de l'Etat (LGCyb), du 02.11.2016) est modifié comme il suit:

Titre de l'acte (modifié)

Loi sur la cyberadministration (LCyb)

Art. 2 al. 1

¹ Dans la présente loi, le terme ou l'expression:

- f) *(nouveau)* «cyberadministration» désigne l'utilisation des technologies de l'information et de la communication aussi bien dans le fonctionnement et l'organisation de l'Etat que dans ses relations avec les tiers;
- g) *(nouveau)* «externalisation» désigne une forme de sous-traitance qui implique au minimum de confier temporairement ou de façon prolongée l'hébergement de données à une personne extérieure à l'Etat.

Art. 3a *(nouveau)*

Traitements de données personnelles

¹ Les traitements de données nécessaires en vue de la délivrance de la prestation ou du service demandé requièrent le consentement libre et éclairé de la personne concernée. Le guichet virtuel conserve la preuve du consentement.

² Lorsque le consentement a été donné en vue d'une prestation périodique, la personne concernée a la possibilité de retirer son consentement en tout temps et sans motif.

³ Les données traitées par le guichet virtuel sont conservées pendant une durée limitée. Le Conseil d'Etat règle les détails.

Art. 4 al. 1 *(modifié)*

¹ L'utilisation du guichet virtuel est gratuite.

Art. 9a *(nouveau)*

Protection des données par défaut et consentement

¹ Le guichet de cyberadministration et les applications qu'il supporte sont pré-réglés pour assurer par défaut le niveau de protection des données le plus élevé.

² Si elle le souhaite, la personne concernée peut consentir à un traitement élargi de ses données afin de bénéficier de services et/ou de prestations supplémentaires.

Art. 9b *(nouveau)*

Participation à des organisations intercantionales

¹ Le Conseil d'Etat peut décider de participer à une organisation intercantonale dans le but de partager des compétences et de développer des solutions communes relatives au guichet virtuel. Il peut lui déléguer des tâches dans ce domaine.

Art. 15 al. 1

¹ L'enregistrement des personnes physiques dans le référentiel cantonal contient en particulier les données suivantes:

h1) (*nouveau*) identificateurs sectoriels utilisés par les métiers en lien avec leurs propres bases de données;

Art. 15a (*nouveau*)

Utilisation systématique du numéro AVS – Principes

¹ En application de l'article 50e al. 3 de la loi fédérale du 20 décembre 1946 sur l'assurance-vieillesse et survivants, le référentiel cantonal est autorisé à utiliser systématiquement le numéro AVS dans les buts suivants:

- a) identifier de manière sûre et univoque les personnes physiques recensées;
- b) assurer un taux d'exactitude des données traitées le plus élevé possible;
- c) actualiser automatiquement les données d'une personne en cas de changement.

² L'utilisation du numéro AVS à d'autres fins que celles décrites à l'alinéa 1 est prohibée. En particulier, il est interdit de faire usage du numéro AVS comme moyen d'apparier des données entre elles à des fins de profilage ou d'investigation. Les lois spéciales sont réservées.

³ Dans la mesure où une loi fédérale ou cantonale les autorise à traiter cette donnée, le référentiel cantonal peut communiquer le numéro AVS à d'autres organes publics ou à des tiers.

Art. 15b (*nouveau*)

Utilisation systématique du numéro AVS – Mesures de sécurité

¹ Le numéro AVS n'est pas conservé dans la même base de données que les autres données personnelles. Une table de concordance avec des identifiants sectoriels permet de faire la jonction entre le numéro AVS et les autres données relatives aux personnes concernées.

² Le numéro AVS est protégé contre tout traitement non autorisé par des mesures organisationnelles appropriées et des mesures techniques adaptées à l'évolution des technologies disponibles.

Art. 16a (nouveau)

Utilisation systématique des numéros IDE et REE – Principes

¹ Le référentiel cantonal utilise systématiquement le numéro unique d'identification des entreprises (IDE) au sens de la loi fédérale du 18 juin 2010 sur le numéro d'identification des entreprises (LIDE) et/ou le numéro d'enregistrement non significatif (REE) au sens de l'article 10 de la loi fédérale sur la statistique dans les buts suivants:

- a) identifier de manière sûre et univoque les personnes morales recensées;
- b) assurer un taux d'exactitude des données traitées le plus élevé possible;
- c) actualiser automatiquement les données d'une personne en cas de changement.

² L'utilisation du numéro IDE à d'autres fins que celles décrites à l'alinéa 1 est prohibée. En particulier, il est interdit de faire usage du numéro IDE comme moyen d'apparier des données entre elles à des fins d'investigation. Les lois spéciales sont réservées.

³ Le référentiel cantonal peut communiquer le numéro IDE à d'autres organes publics ou à des tiers conformément aux dispositions du droit fédéral.

Art. 16b (nouveau)

Utilisation systématique du numéro IDE – Mesures de sécurité

¹ Le numéro IDE est protégé contre tout traitement non autorisé par des mesures organisationnelles appropriées et des mesures techniques adaptées à l'évolution des technologies disponibles.

Intitulé de section après Art. 21 (nouveau)

3.3 Externalisation du traitement de données et d'applications informatiques

Art. 21a (nouveau)

Principes

¹ Dans le but d'accélérer la création et la mise à disposition de services et de contenus numériques et d'optimiser l'utilisation des systèmes d'information de l'Etat, les organes publics peuvent aux conditions fixées dans la présente section externaliser le traitement de leurs données et l'hébergement d'applications informatiques.

² Sont réservées les exigences de la loi sur la protection des données concernant l'externalisation de données personnelles et celles relatives à la délégation de tâches étatiques à des tiers au sens de l'article 54 de la Constitution cantonale.

Art. 21b (nouveau)

Mesures de sécurité

¹ L'intégrité, l'authenticité et la disponibilité du patrimoine informationnel de l'Etat ainsi que la pérennité de sa conservation et de son exploitation doivent être garanties par des mesures organisationnelles appropriées et des techniques adaptées à l'évolution des technologies disponibles. Les mesures nécessaires doivent en outre être prises pour que l'Etat conserve la maîtrise de ses données.

² Les données indispensables au fonctionnement de l'Etat sont copiées à intervalles réguliers sur des supports de données appartenant à l'Etat et permettant leur réutilisation.

Art. 21c (nouveau)

Responsabilité

¹ En cas d'externalisation, l'Etat demeure responsable de la sécurité de son patrimoine informationnel et applicatif. En particulier, il:

- a) prend toutes les précautions commandées par les circonstances quant au choix du fournisseur ou de la fournisseuse de service, son instruction et sa surveillance;
- b) assure la sécurité des données et de ses propres systèmes d'information par la conclusion systématique d'un contrat qui décrit au minimum l'objet, la nature, la finalité et la durée de l'externalisation, le type de données concernées, ainsi que les obligations et les droits de chaque partie;
- c) veille à ce que les données et les applications externalisées dont il est propriétaire puissent être récupérées dans le but de changer de fournisseur ou de fournisseuse de service, ou de procéder à leur ré-internalisation.

² L'externalisation de données faisant l'objet d'une obligation légale ou contractuelle de garder le secret n'est autorisée que si la confidentialité des données en cause est garantie, y compris à l'égard du fournisseur ou de la fournisseuse de service. Le droit applicable au lieu d'hébergement des données doit à cette fin assurer le même niveau de sécurité que si les données étaient stockées en interne.

³ Le fournisseur ou la fournisseuse de service n'est pas autorisé-e à sous-traiter certains aspects de l'externalisation auprès de tiers sans l'autorisation préalable de l'organe responsable.

III.

Aucune abrogation d'actes dans cette partie.

IV.

La présente loi est soumise au referendum législatif. Elle n'est pas soumise au referendum financier.

Le Conseil d'Etat fixe la date d'entrée en vigueur de la présente loi.

[Signatures]