Message complémentaire 2019-CE-239 22 septembre 2020

—

du Conseil d'Etat au Grand Conseil accompagnant les propositions de modification du projet de loi adaptant la législation cantonale à certains aspects de la digitalisation

1. Raison d'être

Le projet de loi cité en titre a été l'objet d'une intervention de l'Autorité de la transparence et de la protection des données (ATPrD) qui a exprimé des divergences de vues avec le projet du Conseil d'Etat après son dépôt devant le Grand Conseil. Des discussions ont eu lieu avec l'ATPrD et ont abouti à un remaniement partiel du projet que le Conseil d'Etat vous propose ci-après.

2. Généralités

a) Le Conseil d'Etat a adopté le 21 avril 2020 un projet de loi adaptant la législation cantonale à certains aspects de la digitalisation. Ce projet propose des modifications de la loi sur le guichet de cyberadministration (LGCyb), qui en font une loi sur la cyberadministration (LCyb), complétées par des modifications de la loi sur la protection des données (LPrD). Dans le Message accompagnant ce projet (pt 6), le Conseil d'Etat a relevé l'avis émis par l'Autorité de la transparence et de la protection des données (ATPrD) durant les travaux préparatoires et lors de la consultation sur l'avant-projet: l'ATPrD était opposée à l'idée de faire entrer de manière anticipée les dispositions concernant l'externalisation de données personnelles, estimant inopportun de «saucissonner» les travaux de révision de la loi sur la protection des données en cours; elle relevait en outre qu'elle était également opposée à l'extension de l'utilisation du numéro AVS dans le cadre du référentiel cantonal.

b) Par la suite, l'ATPrD a informé le Conseil d'Etat, avec copie de son courrier au Grand Conseil, qu'elle n'avait été ni informée de l'adoption du projet définitif ni consultée sur la dernière version du projet qui, à ses yeux, avait été profondément modifié par rapport à la version mise en consultation. Elle communiquait dès lors son désaccord quant au projet. Dans un deuxième temps, l'ATPrD a demandé à être entendue par la Commission parlementaire chargée de l'examen du projet, qui l'a invitée à s'exprimer en séance. Suite à cette audition, la Commission parlementaire n'a pas souhaité trancher les divergences de vues entre le Conseil d'Etat et l'ATPrD et a de ce fait suspendu l'examen du projet pour que le Conseil d'Etat recherche une solution de compromis avec l'ATPrD.

c) Plusieurs discussions ont eu lieu avec l'ATPrD. Cette dernière est finalement revenue sur sa position concernant ce qu'elle a appelé le «saucissonnage de la LPrD»: la Chancellerie d'Etat souhaitant finaliser l'avant-projet définitif de la LPrD une fois la nouvelle loi fédérale sur la protection des données adoptée, l'ATPrD était consciente que la nouvelle mouture de la LPrD ne pourrait pas entrer en vigueur avant 2022 et qu'il était nécessaire de traiter l'externalisation et la sous-traitance préalablement. L'ATPrD a en revanche demandé une répartition différente des règles sur l'externalisation entre la loi sur la protection des données et la loi sur la cyberadministration, a maintenu son opposition de principe à l'utilisation du numéro AVS dans le référentiel cantonal et a demandé d'autres modifications du projet.

d) Donnant suite à la demande de la Commission parlementaire de chercher un compromis, le Conseil d'Etat utilise la possibilité qui lui est offerte par l'article 196 al. 3 de la loi sur le Grand Conseil et vous propose, par le biais du présent message complémentaire, des modifications de son projet initial. Il s'agit des propositions de modification discutées avec l'ATPrD auxquelles le Conseil d'Etat a pu se rallier.
Certaines divergences de vues persistent toutefois entre le Conseil d'Etat et l'ATPrD. Il est fait brièvement état des principales d'entre elles dans le commentaire des articles concernés. Toutefois, deux divergences paraissent particulièrement importantes et méritent une explication supplémentaire.

e) La première divergence importante concerne les articles 15 al. 1 let. h, 15a et 15b du projet de modification de la LGCyb. L'ATPrD reste opposée par principe à l'utilisation du numéro AVS dans le référentiel cantonal, même si elle est consciente du fait que, sur le plan fédéral, un projet de modification de la loi sur l'AVS est en discussion, avec pour but de généraliser l'utilisation systématique de ce numéro par toutes les administrations publiques. L'avis du Conseil d'Etat sur cette question est largement expliqué dans le Message initial (pt 2.2). A ses yeux, l'utilisation du numéro AVS telle que prévue par le projet est essentielle pour la concrétisation du projet Fribourg 4.0 et ne crée pas de problème sous l'angle de la protection de la vie privée. Elle est conforme à la loi fédérale actuelle qui veut que toute utilisation du NAVS repose sur une base légale formelle (art. 50e al. 3 LAVS). Il ne s'agit en effet pas dans le

cas présent d'utilisation générale par les administrations cantonale et communales telle que prévue par le projet de modification du droit fédéral. Il s'agit d'une utilisation strictement limitée au seul référentiel cantonal. Elle a pour but de faciliter la vie des citoyens et citoyennes. Cette utilisation est assortie d'un cadre clair en terme de gestion de la sécurité des données dans le but de prévenir les risques d'utilisation abusive des données personnelles détenues par les administrations.

f) La deuxième divergence de vues importante concerne l'article 12e du projet de modification de la LPrD (version du projet complémentaire). L'ATPrD souhaite que l'externalisation de données personnelles sensibles ou sous secret particulier puisse avoir lieu uniquement en Suisse. Cette position est nouvelle par rapport à l'avant-projet de loi sur la protection des données qui a été mis en consultation fin 2019 et qui a été élaboré sous l'égide de la Préposée à la protection des données, et elle n'est en l'état consacrée nulle part ailleurs en Suisse. Le Conseil d'Etat ne peut pas s'y rallier. Il s'agirait d'une contrainte démesurée qui paralyserait le développement de la cyberadministration et de l'utilisation du cloud dans notre canton, car elle exclurait du marché bon nombre de prestataires ne disposant pas d'infrastructures en Suisse. Le canton de Fribourg se trouverait dès lors fortement désavantagé et entravé tant sur le plan technique que financier par rapport à la Confédération et aux autres cantons dans le cadre de son processus de digitalisation: il n'aurait plus la possibilité de travailler avec des entreprises européennes leaders dans leur domaine et disposant d'infrastructures hautement spécialisées et sécurisées. Les strictes exigences qui devront être fixées par contrat (cf. art. 12c al. 1 let. c du projet de modification de la LPrD) ainsi que la cautèle fixée pour toutes les données personnelles à l'article 12b al. 2 du projet de modification de la LPrD constituent sur ce plan des garanties adéquates. On peut rappeler à cet égard que l'équivalence demandée par l'article 12b al. 2 LPrD est actuellement définie directement par le Préposé fédéral à la protection des données et à la transparence (art. 6 et 31 al. 1 let. d de la loi fédérale sur la protection des données) et, pour l'instant, elle concerne essentiellement les pays de l'Union européenne régis par le RGPD (Règlement général de l'Union européenne sur la protection des données, Règlement (UE) 2016/679 du 27 avril 2016).

3. Commentaire des modifications apportées au projet initial

3.1. Modifications de la LGCyb

Art. 3a, traitement de données personnelles

L'adjonction d'une deuxième phrase à l'alinéa 1 constitue un simple rappel et ne pose aucun problème.

Art. 15, 15a et 15b, utilisation du numéro AVS dans le référentiel

Comme cela a déjà été relevé, l'ATPrD maintient son opposition de principe à l'utilisation du numéro AVS dans le référentiel cantonal (cf. à ce sujet ci-dessus pt 1.e). Néanmoins, au vu des développements récents du droit fédéral et si le Grand Conseil accepte le principe de cette utilisation, l'ATPrD a souhaité que le projet prévoie expressément qu'elle soit consultée au préalable sur les mesures de sécurité. L'article 15b a dès lors été complété dans ce sens par un alinéa 2.

A noter par ailleurs que l'ATPrD a approuvé expressément la formulation de l'article 15b al. 1.

Art. 16, référentiel des personnes morales

Le projet complémentaire corrige sur ce point une coquille du projet initial: ce n'est pas la lettre e de l'article 16 al. 1 qui doit être remplacée par le texte proposé, mais bien la lettre f.

Art. 21, projets pilotes

Lors des discussions qui ont eu lieu avec l'ATPrD, celle-ci a demandé que le contenu de l'article 21 LGCyb soit déplacé dans la LPrD, car il traite spécifiquement de données personnelles. Ni l'avant-projet ni le projet ne proposaient de modifications à ce sujet, et l'ATPrD ne s'était pas exprimée sur ce point lors de la consultation. Néanmoins, ce déplacement est prévu dans l'avant-projet de révision totale de la LPrD. Il s'agit donc ici également d'une anticipation sur cette révision, à laquelle le Conseil d'Etat peut se rallier. Le contenu de cet article 21 LGCyb est dès lors remplacé par un simple renvoi et le traitement des projets pilotes sera désormais réglé dans la LPrD (cf. art. 12f LPrD).

Art. 21a, droit transitoire

Le droit transitoire prévu dans le projet du Conseil d'Etat doit être adapté aux modifications figurant dans le projet complémentaire. Comme la LPrD ne renverra plus aux dispositions de la future LCyb sur l'externalisation, le contenu du droit transitoire doit être réparti entre celle-ci et la LPrD. La référence à l'article 12b LPrD est dès lors supprimée dans la future LCyb, et une disposition transitoire similaire est introduite dans la LPrD pour les externalisations de données personnelles (cf. art. 34a LPrD).

Ces modifications n'ont pas été discutées avec l'ATPrD mais ne font que prendre acte des décisions prises.

3.2. Modifications de la LPrD

Art. 12b à 12e, externalisation

Dans le projet initial du Conseil d'Etat, le thème de l'externalisation est traité de la manière suivante: le socle de base

des exigences qui doivent être respectées pour qu'une externalisation soit possible est fixé dans la future LCyb; en outre, lorsque l'externalisation concerne des données personnelles, elle doit satisfaire à des exigences supplémentaires qui sont fixées dans la LPrD. Cette répartition de la matière entre les deux lois ne convient pas à l'ATPrD. Celle-ci a demandé que toutes les règles relatives à l'externalisation de données personnelles figurent directement dans la LPrD. Cela signifie que le contenu des articles 17c à 17e de la future LCyb doit être intégralement repris dans la LPrD et figurera désormais dans les deux lois. Sur le plan légistique, cette répétition ne paraît pas indispensable; néanmoins, si elle est de nature à clarifier la situation aux yeux de l'ATPrD, le Conseil d'Etat peut s'y rallier.

Dès lors, dans le projet complémentaire, la future LCyb et la LPrD comprennent toutes deux un corps complet de règles sur l'externalisation. La future LCyb s'appliquera lorsque l'externalisation concernera des données qui ne sont pas des données personnelles; et la LPrD s'appliquera lorsque l'externalisation concernera des données personnelles. Dans la LPrD, les règles en question sont présentées de manière un peu différente que dans la future LCyb, car le contenu des règles de base est complété par les exigences supplémentaires prévues initialement dans la première version de l'article 12b LPrD. Mais sur le fond, il n'y a pas de changement.

Cela étant, lors des discussions qui ont eu lieu avec l'ATPrD, celle-ci a encore demandé certains changements de fond supplémentaires, auxquels le Conseil d'Etat ne peut pas se rallier. Il s'agit notamment des points suivants:

> A l'article 12c al. 1 let. b, l'ATPrD souhaite que le chiffre 2 soit complété avec les catégories de personnes concernées. Cela est superflu car soit les catégories de personnes découlent des catégories de données (p. ex.: données médicales = patients; données fiscales = contribuables), soit elles ne sont pas significatives.

> Toujours à l'article 12c al. 1 let. b, l'ATPrD demande que le chiffre 4 soit supprimé, parce qu'elle doit pouvoir effectuer les contrôles désirés selon ses besoins et ne doit pas être limitée par le contrat. Cette demande résulte d'une mauvaise compréhension de la règle: l'inscription de cet élément dans le contrat ne vise pas à limiter la possibilité pour l'ATPrD de faire des contrôles, mais a pour but de poser expressément cette exigence à l'égard du sous-traitant. Ce dernier ne sera généralement pas un organe soumis d'office à la LPrD; ce n'est donc qu'en passant par le contrat que l'on évitera toute ambiguïté sur le fait qu'il est soumis au contrôle de l'ATPrD.

> L'ATPrD demande par ailleurs la suppression de l'art. 12c al. 2. Il s'agit selon elle d'une répétition inutile puisque tant le responsable de traitement que les participants au traitement sont définis; de plus, ces informations sont précisées clairement dans le registre des fichiers. Il s'agit toutefois d'une disposition organisationnelle qui est importante pour les services de l'Etat et pour le sous-traitant, de manière à ce que celui-ci n'ait qu'un seul interlocuteur et non pas tous les services de l'Etat à la fois. Cet élément n'a par ailleurs aucun impact sur la protection des données et, du point de vue des citoyens, l'Etat assume de toute manière l'ensemble des responsabilités.

> Sur l'adjonction à l'article 12e al. 1 demandée par l'ATPrD (hébergement uniquement en Suisse des données sensibles), cf. ci-dessus pt 1.f.

Art. 12f, essais pilotes

Cf. à ce sujet le commentaire de la modification de l'article 21 LGCyb. Il s'agit ici d'un simple déplacement dans la LPrD d'une disposition qui figure actuellement dans la LGCyb. L'ATPrD a par ailleurs demandé quelques modifications du texte par rapport à la version de la LGCyb auxquelles le Conseil d'Etat s'est rallié.

Art. 34a, droit transitoire

Cf. à ce sujet le commentaire de l'article 21a de la future LCyb.

Ergänzende Botschaft 2019-CE-239 22. September 2020

—

des Staatsrats an den Grossen Rat zur Begleitung der Änderungsvorschläge des Gesetzesentwurfs zur Anpassung der kantonalen Gesetzgebung an gewisse Aspekte der Digitalisierung

1. Begründung

Der im Titel zitierte Gesetzesentwurf war Gegenstand einer Intervention der Kantonalen Behörde für Öffentlichkeit und Datenschutz (ÖDSB), die Meinungsverschiedenheiten zum Entwurf des Staatsrats zum Ausdruck brachte, nachdem dieser beim Grossen Rat eingereicht worden war. Es haben Gespräche mit der ÖDSB stattgefunden, die zu einer teilweisen Überarbeitung des Entwurfs, den der Staatsrat Ihnen nachstehend vorschlägt, geführt haben.

2. Allgemeines

a) Am 21. April 2020 verabschiedete der Staatsrat einen Gesetzesentwurf zur Anpassung der kantonalen Gesetzgebung an bestimmte Aspekte der Digitalisierung. Dieser Entwurf schlägt Änderungen des Gesetzes über den E-Government-Schalter des Staates (E-GovSchG), die es zu einem E-Government-Gesetz (E-GovG) machen, und Änderungen des Gesetzes über den Datenschutz (DSchG) vor. In der Botschaft zu diesem Entwurf (Punkt 6) hat der Staatsrat die Stellungnahme, die von der Behörde für Öffentlichkeit und Datenschutz (ÖDSB) während der Vorbereitungsarbeiten und während der Vernehmlassung des Vorentwurf abgegeben wurde, zur Kenntnis genommen: Die ÖDSB sprach sich gegen die Idee aus, die Bestimmungen über die Auslagerung von Personendaten im Voraus einzubringen, da sie es für unangemessen hielt, die laufenden Revisionsarbeiten am Datenschutzgesetz zu torpedieren; sie unterstrich zudem, dass sie sich auch gegen die Ausweitung der Verwendung der AHV-Nummer im Rahmen des kantonalen Bezugssystems ausspricht.

b) In der Folge teilte die ÖDSB dem Staatsrat mit einer Kopie ihres Schreibens an den Grossen Rat mit, dass sie weder über die Annahme des Schlussentwurfs informiert noch zur letzten Fassung des Entwurfs, die ihrer Ansicht nach gegenüber der in die Vernehmlassung gegebenen Fassung tiefgreifend geändert worden sei, angehört worden sei. Sie teilte daher mit, dass sie mit dem Entwurf nicht einverstanden ist. In einem zweiten Schritt beantragte die ÖDSB eine Anhörung vor der mit der Prüfung des Entwurfs beauftragten parlamentarischen Kommission, die sie dazu einlud, sich an ihrer Sitzung zu äussern. Nach dieser Anhörung wollte die parlamentarische Kommission nicht über die Meinungsverschiedenheiten zwischen dem Staatsrat und der ÖDSB entscheiden und setzte daher die Prüfung des Entwurfs aus, damit der Staatsrat mit der ÖDSB eine Kompromisslösung suchen konnte.

c) Es fanden mehrere Gespräche mit der ÖDSB statt, die schliesslich ihre Position zu dem, was sie als «Salamitaktik beim DSchG» bezeichnete, revidierte: Da die Staatskanzlei den Schlussentwurf des DSchG nach der Verabschiedung des neuen Bundesgesetzes über den Datenschutz fertig stellen wollte, war sich die ÖDSB bewusst, dass die neue Fassung des DSchG nicht vor 2022 in Kraft treten kann und dass es notwendig war, sich vorher mit der Auslagerung und der Auftragsbearbeitung zu befassen. Andererseits forderte die ÖDSB eine andere Aufteilung der Vorschriften zur Auslagerung zwischen dem Datenschutzgesetz und dem Gesetz über den E-Government-Schalter, hielt an ihrer grundsätzlichen Ablehnung der Verwendung der AHV-Nummer im kantonalen Bezugssystem fest und verlangte weitere Änderungen des Entwurfs.

d) Auf das Ersuchen der parlamentarischen Kommission, einen Kompromiss zu suchen, macht der Staatsrat von der ihm in Artikel 196 Abs. 3 des Grossratsgesetzes gebotenen Möglichkeit Gebrauch und schlägt Ihnen mit dieser ergänzenden Botschaft Änderungen an seinem ursprünglichen Entwurf vor. Es handelt sich um mit der ÖDSB diskutierte Änderungsvorschläge, denen der Staatsrat zustimmen konnte. Es bestehen jedoch weiterhin einige Meinungsverschiedenheiten zwischen dem Staatsrat und der ÖDSB, von denen die wichtigsten im Kommentar zu den betreffenden Artikeln kurz erwähnt werden. Zwei Meinungsverschiedenheiten scheinen jedoch besonders wichtig zu sein und bedürfen einer weiteren Erläuterung.

e) Die erste wichtige Meinungsverschiedenheit betrifft Art. 15 Abs. 1 Bst. h, 15a und 15b des Entwurfs zur Änderung des E-GovSchG. Die ÖDSB ist nach wie vor grundsätzlich gegen die Verwendung der AHV-Nummer im kantonalen Bezugssystem, auch wenn sie weiss, dass auf Bundesebene ein Entwurf zur Änderung des AHV-Gesetzes diskutiert wird, mit dem die systematische Verwendung dieser Nummer durch alle öffentlichen Verwaltungen ermöglicht werden soll.

Die Stellungnahme des Staatsrates zu dieser Frage wird zu Beginn der ursprünglichen Botschaft (Punkt 2.2) ausführlich erläutert. Seiner Ansicht nach ist die Verwendung der AHV-Nummer, wie sie im Entwurf vorgesehen ist, für die Realisierung des Projekts Freiburg 4.0 unerlässlich und stellt aus der Sicht des Schutzes von Personendaten kein Problem dar. Sie ist konform mit der geltenden Gesetzgebung des Bundes zur AHV-Nummer, die verlangt, dass jede Verwendung der AHV-Nr. auf einer formellen gesetzlichen Grundlage beruht (Art. 50e Abs. 3 AHVG). Es handelt sich im vorliegenden Fall also nicht um eine allgemeine Nutzung durch die kantonalen und kommunalen Verwaltungen, wie sie im Entwurf zur Änderung des Bundesrechts vorgesehen ist. Diese Verwendung ist strikt auf das kantonale Bezugssystem beschränkt. Dessen Zweck ist es, Bürgerinnen und Bürgern das Leben zu erleichtern. Diese Verwendung geht einher mit einem klaren Rahmen für das Management der Datensicherheit, um die Risiken der missbräuchlichen Verwendung von Personendaten, die sich im Besitz von Verwaltungen befinden, zu verhindern.

f) Die zweite grosse Meinungsverschiedenheit betrifft Artikel 12e des Änderungsentwurfs zum DSchG (Version des ergänzenden Entwurfs). Die ÖDSB möchte, dass besonders schützenswerte Personendaten oder Daten, die einer besonderen Geheimhaltung unterworfen sind, nur in die Schweiz ausgelagert werden dürfen. Diese Einstellung ist neu im Vergleich zum Ende 2019 in die Vernehmlassung gegebenen Vorentwurf des Datenschutzgesetzes, der unter der Federführung der Datenschutzbeauftragten ausgearbeitet wurde, und sie ist nirgendwo sonst in der Schweiz verankert. Der Staatsrat kann dem nicht zustimmen. Dies wäre ein unverhältnismässiger Zwang, der die Entwicklung des E-Governments und die Nutzung der Cloud in unserem Kanton lähmen würde, da er viele Anbieterinnen und Anbieter, die in der Schweiz über keine Infrastruktur verfügen, vom Markt ausschliessen würde. Der Kanton Freiburg wäre somit gegenüber dem Bund und den anderen Kantonen in seinem Digitalisierungsprozess technisch und finanziell erheblich benachteiligt und behindert: Er wäre nicht mehr in der Lage, mit europäischen Unternehmen zusammenzuarbeiten, die auf ihrem Gebiet führend sind und über hoch spezialisierte und sichere Infrastrukturen verfügen. Die strengen Anforderungen, die in einem Vertrag festgelegt werden müssen (vgl. Art. 12c Abs. 1 Bst. c des Entwurfs zur Änderung des DSchG), sowie die in Art. 12b Abs. 2 des Entwurfs zur Änderung des DSchG für alle Personendaten festgelegte Kautel stellen in dieser Hinsicht angemessene Garantien dar. Es sei in diesem Zusammenhang daran erinnert, dass die nach Artikel 12b Absatz 2 DSchG geforderte Gleichwertigkeit derzeit direkt vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten festgelegt wird (Artikel 6 und 31 Abs. 1 Bst. d des Bundesgesetzes über den Datenschutz) und vorerst hauptsächlich die von der DSVGO betroffenen Länder der Europäischen Union betrifft (Verordnung des Europäischen Parlaments und des Rats vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)).

3. Kommentar zu den Änderungen im Vergleich zum ursprünglichen Entwurf

3.1. Änderungen am Gesetz über den E-Government-Schalter

Art. 3a, Bearbeitung von Personendaten

Die Hinzufügung eines zweiten Satzes in Absatz 1 ist ein einfacher Hinweis und stellt kein Problem dar.

Art. 15, 15a und 15b, Verwendung der AHV-Nummer im kantonalen Bezugssystem

Wie bereits erwähnt, hält die ÖDSB an ihrer grundsätzlichen Ablehnung der Verwendung der AHV-Nummer im kantonalen Bezugssystem fest (siehe Punkt 1.e weiter oben). Dennoch wollte die ÖDSB angesichts der jüngsten Entwicklungen im Bundesrecht und sofern der Grosse Rat den Grundsatz einer solchen Verwendung akzeptiert, dass im Entwurf ausdrücklich vorgesehen wird, dass sie zu den Sicherheitsmassnahmen angehört wird. Artikel 15b ist daher zu diesem Zweck durch einen Absatz 2 ergänzt worden.

Zu beachten ist auch, dass die ÖDSB dem Wortlaut des Artikels 15b Abs. 1 ausdrücklich zugestimmt hat.

Art. 16, Kantonales Bezugssystem für juristische Personen

Der ergänzende Entwurf korrigiert einen Tippfehler im ursprünglichen Entwurf in diesem Punkt: es ist nicht Buchstabe e des Artikels 16 Abs. 1, der durch den vorgeschlagenen Text ersetzt werden soll, sondern Buchstabe f.

Art. 21, Pilotprojekte

In den Diskussionen, die mit der ÖDSB stattfanden, beantragte diese, den Inhalt von Artikel 21 E-GovSchG ins DSchG zu übertragen, weil er im Speziellen Personendaten behandelt. Weder im Vorentwurf noch im Entwurf wurden diesbezüglich Änderungen vorgeschlagen, und die ÖDSB hatte sich während der Vernehmlassung zu diesem Punkt nicht geäussert. Dennoch ist dieser Schritt im Vorentwurf der Totalrevision des DSchG vorgesehen, so dass es auch hier darum geht, dieser Revision vorzugreifen, welcher der Staatsrat zustimmen kann. Der Inhalt dieses Artikels 21 E-GovSchG wird daher durch einen einfachen Querverweis ersetzt und die Behandlung von Pilotprojekten wird fortan im DSchG geregelt (vgl. Art. 12f DSchG).

Art. 21a Übergangsrecht

Das im Entwurf des Staatsrats vorgesehene Übergangsrecht muss an die im ergänzenden Entwurf enthaltenen Änderungen angepasst werden. Da das DSchG nicht mehr auf die Bestimmungen des künftigen E-GovG über die Auslagerung verweist, muss der Inhalt des Übergangsrechts zwischen ersterem und dem DSchG aufgeteilt werden. Der Verweis auf Artikel 12b DSchG wird daher im zukünftigen E-GovG gestrichen, und im DSchG wird eine ähnliche Übergangsbestimmung für die Auslagerung von Personendaten eingeführt (vgl. Art. 34a DSchG).

Diese Änderungen wurden mit der ÖDSB nicht diskutiert, sondern es wurden lediglich die getroffenen Entscheide anerkannt.

3.2. Änderungen am DSchG

Art. 12b–12e, Auslagerung

Im ersten Entwurf des Staatsrates wird das Thema Auslagerung wie folgt behandelt: Die Basis der Anforderungen, die erfüllt sein müssen, damit eine Auslagerung möglich wird, ist im künftigen E-GovG festgelegt; darüber hinaus muss die Auslagerung von Personendaten zusätzliche Anforderungen erfüllen, die im DSchG festgelegt sind. Diese Aufteilung des Sachverhalts zwischen den beiden Gesetzen ist für die ÖDSB nicht angemessen. Die ÖDSB hat gefordert, dass alle Vorschriften über die Auslagerung von Personendaten direkt ins DSchG aufgenommen werden. Dies bedeutet, dass der Inhalt der Artikel 17c–17e des künftigen E-GovG vollständig ins DSchG aufgenommen werden muss und nun in beiden Gesetzen erscheinen wird. Gesetzgebungsmethodisch gesehen scheint diese Wiederholung nicht unerlässlich zu sein; wenn sie jedoch geeignet ist, die Situation in den Augen der ÖDSB zu klären, kann der Staatsrat ihr zustimmen.

Daher enthalten sowohl das künftige E-GovG als auch das DSchG im ergänzenden Entwurf einen vollständigen Satz von -Vorschriften zur Auslagerung. Das künftige E-GovG ist anwendbar, wenn die Auslagerung Daten betrifft, die keine Personendaten sind, und das DSchG ist anwendbar, wenn die Auslagerung Personendaten betrifft. Im DSchG werden die fraglichen Vorschriften etwas anders dargestellt als im künftigen E-GovG, weil die Grundregeln inhaltlich durch die zusätzlichen Anforderungen ergänzt werden, die ursprünglich in der ersten Fassung von Artikel 12b DSchG vorgesehen waren. In der Sache gibt es aber keine Änderung.

Während der Gespräche mit der ÖDSB forderte diese jedoch weiterhin bestimmte zusätzliche sachliche Änderungen, denen der Staatsrat nicht zustimmen kann. Es handelt sich namentlich um folgende Punkte:

> In Art. 12c Abs. 1 Bst. b wünscht die ÖDSB, dass Ziffer 2 mit den betroffenen Personengruppen ergänzt wird. Dies ist unnötig, da entweder die Personenkategorien aus den Datenkategorien abgeleitet werden können (z.B.: medizinische Daten = Patientinnen und Patienten; Steuerdaten = Steuerzahlerinnen und Steuerzahler) oder nicht von Bedeutung sind.

> Die ÖDSB beantragt in Art. 12c Abs. 1 Bst. b weiterhin die Streichung von Zif. 4, weil sie die gewünschten Prüfungen nach ihren Bedürfnissen durchführen können muss und nicht durch den Vertrag eingeschränkt werden darf. Dieser Antrag ist das Ergebnis eines Missverständnisses der Bestimmung: Durch die Aufnahme dieses Elements in den Vertrag soll die Möglichkeit der ÖDSB, Kontrollen durchführen zu können, nicht eingeschränkt werden, sondern diese Anforderung soll ausdrücklich gegenüber dem Auftragsbearbeiter festgelegt werden. Letzterer wird als Organ im Allgemeinen nicht von Amtes wegen dem DSchG unterliegen; nur wenn diese über den Vertrag geregelt wird, kann daher jede Unklarheit darüber vermieden werden, dass er der Kontrolle der ÖDSB unterliegt.

> Die ÖDSB fordert auch die Streichung von Art. 12c Abs. 2. Ihrer Ansicht nach ist dies eine unnötige Wiederholung, da sowohl der Verantwortliche für die Bearbeitung als auch die an der Bearbeitung Beteiligten definiert sind; darüber hinaus sind diese Informationen im Register der Datensammlungen eindeutig angegeben. Dabei handelt es sich jedoch um eine organisatorische Regelung, die für die staatlichen Ämter und den Auftragsbearbeiter wichtig ist, so dass der Auftragsbearbeiter nur einen Gesprächspartner hat und nicht alle staatlichen Ämter gleichzeitig. Zudem hat dieser Sachverhalt keine Auswirkungen auf den Datenschutz, und aus der Sicht der Bürger übernimmt der Staat ohnehin alle Verantwortung.

> Zur von der ÖDSB beantragten Ergänzung von Art. 12e Abs. 1 (Hosting von besonders schützenswerten personenbezogenen Daten nur in der Schweiz) vgl. oben Ziff. 2.f.

Art. 12f, Pilotversuche

Siehe hierzu den Kommentar zur Änderung von Artikel 21 E-GovSchG. Es handelt sich dabei um eine einfache Versetzung einer Bestimmung, die derzeit im E-GovSchG steht, in das DSchG. Die ÖDSB forderte auch einige Änderungen am Text im Vergleich zur Fassung des E-GovSchG, denen der Staatsrat zugestimmt hat.

Art. 34 Übergangsrecht

Vgl. den Kommentar zu Artikel 21a des zukünftigen E-GovG.

Les propositions de modification du projet de loi du 21 avril 2020 sont marquées en grisé.

—

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 2019-CE-239 du Conseil d'Etat du 21 avril 2020;
Sur la proposition de cette autorité,

Décrète:

I.

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)

Die Änderungsvorschläge des Gesetzesentwurfs vom 21. April 2020 sind grau markiert.

—

Gesetz zur Anpassung der kantonalen Gesetzgebung an bestimmte Aspekte der Digitalisierung

vom…

Betroffene Erlasse (SGF Nummern):

Neu: –
Geändert: 17.1 | **17.4**
Aufgehoben: –

Der Grosse Rat des Kantons Freiburg

nach Einsicht in die Botschaft 2019-CE-239 des Staatsrats vom 21. April 2020;
auf Antrag dieser Behörde,

beschliesst:

I.

Der Erlass SGF 17.4 (Gesetz über den E-Government-Schalter des Staates (E-GovSchG), vom 02.11.2016) wird wie folgt geändert:

Erlasstitel *(geändert)*

E-Government-Gesetz (E-GovG)

Préambule *(modifié)*

Le Grand Conseil du canton de Fribourg

Vu les messages 2016-CE-41 et 2019-CE-239 du Conseil d'Etat des 30 août 2016 et 21 avril 2020;

Sur la proposition de cette autorité,

Décrète:

Art. 1a *(nouveau)*

Application aux communes

[1] Les communes (y compris les établissements communaux et les associations de communes) participent aux solutions informatiques de la cyberadministration conformément aux dispositions de l'article 20.

[2] Leur sont en outre applicables les dispositions de la section 3a sur l'externalisation ainsi que, dans la mesure fixée par l'article 5, les dispositions de la section 1a sur le guichet virtuel.

[3] L'implication de certaines communes dans la phase pilote de mise en œuvre et d'exploitation du référentiel cantonal est définie par le Conseil d'Etat.

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 des collectivités publiques que dans leurs relations avec les tiers;

g) *(nouveau)* «externalisation» désigne une forme de sous-traitance impliquant la délocalisation du traitement de données ou de la gestion d'outils informatiques sur les infrastructures du sous-traitant;

h) *(nouveau)* «sous-traitant» désigne une personne privée ou un organe public relevant d'une autre collectivité qui traite des données ou gère des outils informatiques pour le compte d'une autorité administrative.

Ingress *(geändert)*

Der Grosse Rat des Kantons Freiburg

nach Einsicht in die Botschaften 2016-CE-41 und 2019-CE-239 des Staatsrates vom 30. August 2016 und vom 21. April 2020;

auf Antrag dieser Behörde,

beschliesst:

Art. 1a *(neu)*

Gültigkeit für die Gemeinden

[1] Die Gemeinden (einschliesslich der Gemeindeanstalten und der Gemeindeverbände) beteiligen sich an den Informatiklösungen des E-Governments gemäss den Bestimmungen von Artikel 20.

[2] Für sie gelten ausserdem die Bestimmungen des Abschnitts 3a über die Auslagerung und, soweit in Artikel 5 festgehalten wird, die Bestimmungen von Abschnitt 1a über den virtuellen Schalter.

[3] Die Mitwirkung einiger Gemeinden bei der Pilotphase der Schaffung und des Betriebs des kantonalen Bezugssystems wird vom Staatsrat festgelegt.

Art. 2 Abs. 1

[1] In diesem Gesetz bezeichnet der Begriff oder der Ausdruck:

f) *(neu)* «E-Government» die Nutzung von Informations- und Kommunikationstechnologien sowohl beim Betrieb und bei der Organisation der Gemeinwesen als auch in ihren Beziehungen zu Dritten;

g) *(neu)* «Auslagerung» eine 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;

h) *(neu)* «Auftragsbearbeiter» eine Privatperson oder ein zu einem anderen Gemeinwesen gehörendes öffentliches Organ, die oder das für eine Verwaltungsbehörde Daten bearbeitet oder Informatiktools verwaltet.

Intitulé de section après Art. 2 *(nouveau)*

1a Guichet virtuel

Art. 3a *(nouveau)*

Traitements de données personnelles

[1] Les traitements de données personnelles nécessaires en vue de la délivrance de la prestation ou du service demandé requièrent le consentement libre et éclairé de la personne concernée. Ils sont soumis à la législation sur la protection des données.

[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] La preuve du consentement donné est conservée et doit pouvoir être démontrée en tout temps.

[4] 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. 5 al. 1 *(modifié)*, ***al. 2*** *(modifié)*

[1] Sur la base de conventions de droit administratif passées avec l'Etat, les communes (y compris les établissements communaux et les associations de communes) peuvent offrir leurs propres prestations par le biais du guichet virtuel.

[2] Les conventions définissent en particulier la participation des communes aux frais d'investissement et de fonctionnement du guichet virtuel.

Art. 9a *(nouveau)*

Protection des données par défaut et consentement

[1] Le guichet de cyberadministration et les applications qu'il supporte sont préréglés pour assurer par défaut que seules les données personnelles nécessaires au regard de chaque finalité spécifique du traitement sont traitées.

Abschnittsüberschrift nach Art. 2 *(neu)*

1a Virtueller Schalter

Art. 3a *(neu)*

Bearbeiten von Personendaten

[1] Das für die Ausführung der Leistung oder der gewünschten Dienstleistung nötige Bearbeiten der Personendaten erfordert die freie und aufgeklärte Einwilligung der betroffenen Person. Es unterliegt der Gesetzgebung über den Datenschutz.

[2] Wenn das Einverständnis für eine wiederkehrende Leistung gegeben wurde, kann die betroffene Person ihr Einverständnis jederzeit ohne Angabe von Gründen widerrufen.

[3] Der Beweis für das Einverständnis wird aufbewahrt und muss jederzeit vorgewiesen werden können.

[4] Die vom virtuellen Schalter behandelten Daten werden während eines begrenzten Zeitraums aufbewahrt. Der Staatsrat regelt die Einzelheiten.

Art. 4 Abs. 1 *(geändert)*

[1] Die Nutzung des virtuellen Schalters ist gratis.

Art. 5 Abs. 1 *(geändert)*, ***Abs. 2*** *(geändert)*

[1] Auf der Grundlage von verwaltungsrechtlichen Verträgen mit dem Staat können die Gemeinden (einschliesslich der Gemeindeanstalten und der Gemeindeverbände) ihre eigenen Leistungen über den virtuellen Schalter anbieten.

[2] In den Verträgen werden insbesondere die Beteiligung der Gemeinden an den Investitions- und Betriebskosten des virtuellen Schalters festgehalten.

Art. 9a *(neu)*

Datenschutz durch datenschutzfreundliche Voreinstellungen und Zustimmung

[1] Der E-Government-Schalter und die Anwendungen, die er unterstützt, sind so voreingestellt, dass standardmässig sichergestellt wird, dass nur die Personendaten, die für die jeweiligen Bearbeitungszwecke nötig sind, bearbeitet werden.

[2] 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 intercantonales

[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.

Intitulé de section après Art. 9b

2 *(abrogé)*

Intitulé de section après Art. 12 *(modifié)*

3 Référentiel cantonal

Intitulé de section après section 3

3.1 *(abrogé)*

Art. 15 al. 1

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

h) *(modifié)* numéro AVS;

h1) *(nouveau)* identificateurs sectoriels utilisés par les métiers;

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, l'utilisation systématique du numéro AVS dans le référentiel cantonal est autorisée dans les buts suivants:

[2] Wenn die betroffene Person es wünscht, kann sie einem erweiterten Bearbeiten ihrer Daten zustimmen, um Zugang zu zusätzlichen Dienstleistungen und Leistungen zu erhalten.

Art. 9b *(neu)*

Mitwirken in interkantonalen Organisationen

[1] Der Staatsrat kann beschliessen, an einer interkantonalen Organisation mitzuwirken, um Kompetenzen zu teilen und gemeinsam Lösungen für den virtuellen Schalter zu entwickeln. Er kann ihr Aufgaben in diesem Bereich delegieren.

Abschnittsüberschrift nach Art. 9b

2 *(aufgehoben)*

Abschnittsüberschrift nach Art. 12 *(geändert)*

3 Kantonales Bezugssystem

Abschnittsüberschrift nach Abschnitt 3

3.1 *(aufgehoben)*

Art. 15 Abs. 1

[1] Der Eintrag der natürlichen Personen im kantonalen Bezugssystem enthält insbesondere folgende Daten:

h) *(geändert)* AHV-Nummer;

h1) *(neu)* sektorielle Identifikatoren, die von den Fachbereichen verwendet werden;

Art. 15a *(neu)*

Systematische Verwendung der AHV-Nummer – Grundsätze

[1] In Anwendung von Artikel 50e Abs. 3 des Bundesgesetzes vom 20. Dezember 1946 über die Alters- und Hinterlassenenversicherung wird die systematische Verwendung der AHV-Nummer im kantonalen Bezugssystem zu folgenden Zwecken bewilligt:

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 qui sont 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 autorise d'autres organes publics ou des tiers à traiter cette donnée, le numéro AVS peut leur être communiqué par voie d'appel.

Art. 15b *(nouveau)*

Utilisation systématique du numéro AVS – Mesures de sécurité

[1] Le numéro AVS est protégé contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées, adaptées à l'évolution des technologies disponibles et conformes aux exigences du droit fédéral.

[2] L'Autorité cantonale de la transparence et de la protection des données est consultée sur le choix des mesures à mettre en place.

Art. 16 al. 1

[1] L'enregistrement d'une personne morale dans le référentiel cantonal comprend en particulier les données suivantes:

f) *(modifié)* numéro unique d'identification des entreprises (ci-après: numéro IDE) au sens de la loi fédérale du 18 juin 2010 sur le numéro d'identification des entreprises (LIDE) et numéro d'enregistrement non significatif (ci-après: numéro REE) au sens de l'article 10 de la loi fédérale du 9 octobre 1992 sur la statistique;

a) sichere und eindeutige Identifizierung der verzeichneten natürlichen Personen;

b) Gewährleistung einer höchstmöglichen Genauigkeit der bearbeiteten Daten;

c) automatische Nachführung der Daten einer Person bei Änderungen.

[2] Die Verwendung der AHV-Nummer zu anderen Zwecken als denjenigen gemäss Absatz 1 ist verboten. Insbesondere ist es verboten, die AHV-Nummer als Mittel zur Verknüpfung der Daten unter sich zu Profiling- oder Untersuchungszwecken zu verwenden. Die Spezialgesetze bleiben vorbehalten.

[3] Sofern ein Bundesgesetz oder ein kantonales Gesetz andere öffentliche Organe oder Dritte ermächtigt, diese Angabe zu bearbeiten, darf die AHV-Nummer ihnen über ein Abrufverfahren bekanntgegeben werden.

Art. 15b *(neu)*

Systematische Verwendung der AHV-Nummer – Sicherheitsmassnahmen

[1] Die AHV-Nummer wird mit geeigneten organisatorischen und technischen Massnahmen, die der Entwicklung der verfügbaren Technologien angepasst sind und den Anforderungen des Bundesrechts entsprechen, gegen jegliches unbewilligte Bearbeiten geschützt.

[2] Die Kantonale Behörde für Öffentlichkeit und Datenschutz wird bei der Wahl der zu treffenden Massnahmen konsultiert.

Art. 16 Abs. 1

[1] Der Eintrag einer juristischen Person im kantonalen Bezugssystem umfasst insbesondere folgende Daten:

f) *(geändert)* Unternehmens-Identifikationsnummer (UID-Nummer) im Sinn des Bundesgesetzes vom 18. Juni 2010 über die Unternehmens-Identifikationsnummer (UIDG) und nicht sprechende Identifikationsnummer (BUR-Nummer) im Sinne von Artikel 10 des Bundesstatistikgesetzes vom 9. Oktober 1992;

Art. 16a *(nouveau)*

Utilisation systématique des numéros IDE et REE – Principes

[1] Le numéro IDE et le numéro REE peuvent être utilisés systématiquement dans le référentiel cantonal 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 des numéros IDE et REE à d'autres fins que celles qui sont décrites à l'alinéa 1 est prohibée. En particulier, il est interdit de faire usage des numéros IDE et REE comme moyen d'apparier des données entre elles à des fins de profilage ou d'investigation. Les lois spéciales sont réservées.

[3] Les numéros IDE et REE peuvent être communiqués par voie d'appel à d'autres organes publics ou à des tiers dans la mesure où le droit fédéral le permet et conformément aux conditions posées par celui-ci.

Art. 16b *(nouveau)*

Utilisation systématique des numéros IDE et REE – Mesures de sécurité

[1] Les numéros IDE et REE sont protégés contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées, adaptées à l'évolution des technologies disponibles et conformes aux exigences du droit fédéral.

Art. 17a *(nouveau)*

Organe responsable du référentiel cantonal

[1] Le Conseil d'Etat désigne l'organe responsable du référentiel cantonal, qui a qualité de responsable du fichier au sens de la législation sur la protection des données.

[2] L'organe responsable est autorisé à utiliser de manière systématique les numéros AVS, IDE et REE conformément à la présente loi.

Art. 16a *(neu)*

Systematische Verwendung der UID- und der BUR-Nummer – Grundsätze

[1] Die UID- und die BUR-Nummer dürfen systematisch zu folgenden Zwecken im kantonalen Bezugssystem verwendet werden:

a) sichere und eindeutige Identifizierung der verzeichneten juristischen Personen;

b) Gewährleistung einer höchstmöglichen Genauigkeit der bearbeiteten Daten;

c) automatische Nachführung der Daten einer Person bei Änderungen.

[2] Die Verwendung der UID- und der BUR-Nummer zu anderen Zwecken als denjenigen gemäss Absatz 1 ist verboten. Insbesondere ist es verboten, die UID- und die BUR-Nummer als Mittel zur Verknüpfung der Daten untereinander zu Profiling- oder Ermittlungszwecken zu verwenden. Die Spezialgesetze bleiben vorbehalten.

[3] Die UID- und die BUR-Nummer dürfen weiteren öffentlichen Organen und Dritten mit Abrufverfahren bekanntgegeben werden, soweit es das Bundesrecht erlaubt, dabei gelten die Bedingungen gemäss diesem Recht.

Art. 16b *(neu)*

Systematische Verwendung der UID- und der BUR-Nummer – Sicherheitsmassnahmen

[1] Die UID- und die BUR-Nummer werden mit geeigneten organisatorischen und technischen Massnahmen, die der Entwicklung der verfügbaren Technologien angepasst sind und den Anforderungen des Bundesrechts entsprechen, gegen jegliches unbewilligte Bearbeiten geschützt.

Art. 17a *(neu)*

Für das kantonale Bezugssystem verantwortliches Organ

[1] Der Staatsrat bezeichnet das für das kantonale Bezugssystem verantwortliche Organ, das die Eigenschaft eines Verantwortlichen der Datensammlung im Sinne der Gesetzgebung über den Datenschutz hat.

[2] Das verantwortliche Organ wird ermächtigt, systematisch die AHV-, die UID- und die BUR-Nummer gemäss diesem Gesetz zu verwenden.

Intitulé de section après Art. 17a *(nouveau)*

3a Externalisation

Art. 17b *(nouveau)*

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. 17c *(nouveau)*

Respect des secrets particuliers

[1] Le traitement de données qui font l'objet d'une obligation légale ou contractuelle de garder le secret ne peut être externalisé que si la confidentialité à l'égard du sous-traitant est assurée de manière que ce dernier ne puisse avoir accès à leur contenu.

[2] Lorsque le sous-traitant doit impérativement avoir accès aux données pour des raisons techniques, le contrat d'externalisation fixe les exigences particulières nécessaires, en particulier l'engagement du sous-traitant de n'accéder au contenu des données qu'avec le consentement exprès de l'autorité administrative qui procède à l'externalisation et l'obligation de tenir un journal des accès.

Art. 17d *(nouveau)*

Mesures de sécurité

[1] L'intégrité, l'authenticité, la disponibilité et la confidentialité du patrimoine informationnel concerné par une externalisation ainsi que la pérennité de sa conservation et de son exploitation doivent être garanties par des mesures organisationnelles et techniques appropriées et adaptées à l'évolution des technologies disponibles.

Abschnittsüberschrift nach Art. 17a *(neu)*

3a Auslagerung

Art. 17b *(neu)*

Grundsätze

[1] Das elektronische Bearbeiten von Daten und das Verwalten von Informatiktools dürfen zu den Bedingungen gemäss diesem Abschnitt ausgelagert werden.

[2] Vorbehalten bleiben aber:

a) die Anforderungen gemäss der Gesetzgebung über den Datenschutz, wenn die Auslagerung das Bearbeiten von Personendaten betrifft;

b) die besonderen Anforderungen gemäss Artikel 54 der Kantonsverfassung vom 16. Mai 2004, wenn die Auslagerung eine Delegation von Aufgaben an Dritte im Sinne dieser Bestimmung zur Folge hat.

Art. 17c *(neu)*

Wahren besonderer Geheimnisse

[1] Das Bearbeiten von Daten, für die eine gesetzliche oder vertragliche Geheimhaltungspflicht gilt, darf nur ausgelagert werden, wenn die Vertraulichkeit gegenüber dem Auftragsbearbeiter sichergestellt wird, so dass dieser keinen Zugriff auf ihren Inhalt hat.

[2] Wenn der Auftragsbearbeiter aus technischen Gründen unbedingt Zugriff auf die Daten haben muss, werden im Auslagerungsvertrag die nötigen besonderen Anforderungen festgelegt, insbesondere die Verpflichtung des Auftragsbearbeiters, nur mit ausdrücklichem Einverständnis der Verwaltungsbehörde, welche die Daten auslagert, auf den Inhalt der Daten zuzugreifen, und die Pflicht, ein Zugriffsjournal zu führen.

Art. 17d *(neu)*

Sicherheitsmassnahmen

[1] Die Integrität, die Authentizität, die Verfügbarkeit und die Vertraulichkeit des Informationserbes, die von einer Auslagerung betroffen sind, sowie deren ständige Aufbewahrung und Verwendung müssen mit geeigneten organisatorischen und technischen Massnahmen, die der Entwicklung der verfügbaren Technologien angepasst sind, sichergestellt werden.

[2] Lorsque l'externalisation concerne des données indispensables au fonctionnement de l'administration, la continuité des activités externalisées doit, en cas d'incident, être garantie par un dispositif adéquat.

Art. 17e *(nouveau)*

Responsabilités

[1] L'autorité administrative qui procède à une externalisation demeure responsable de la pérennité de la conservation et de l'exploitation de son patrimoine informationnel. En particulier:

a) elle prend les précautions commandées par les circonstances quant au choix du sous-traitant, à son instruction et à sa surveillance;

b) elle assure la sécurité des données et de ses propres systèmes d'information par la conclusion d'un contrat qui décrit au minimum l'objet, la nature, la finalité et la durée de l'externalisation, les catégories de données concernées ainsi que les obligations et les droits de chaque partie;

c) elle ne confie pas au sous-traitant des traitements qu'elle ne serait pas en droit d'effectuer elle-même;

d) elle veille à ce que les données et les outils informatiques concernés par une externalisation puissent être récupérés en tout temps, notamment dans le but de changer de sous-traitant, de procéder à leur réinternalisation ou de les verser aux archives historiques.

[2] Lorsque l'externalisation concerne plusieurs autorités différentes au sein d'une même collectivité publique, une autorité principalement responsable est désignée.

[3] Au sein de l'administration cantonale, la responsabilité de la mise en œuvre et du suivi des règles de la présente section est assumée conjointement par l'autorité administrative et par le service en charge de l'informatique [1)]. Sont réservés les cas dans lesquels l'autorité administrative gère de manière autonome ses systèmes informatiques.

[1)] Actuellement: Service de l'informatique et des télécommunications.

[2] Wenn die Auslagerung Daten betrifft, die für den Betrieb der Verwaltung unentbehrlich sind, muss die Fortführung der ausgelagerten Tätigkeiten bei einem Zwischenfall mit einem angemessenen Dispositiv sichergestellt werden.

Art. 17e *(neu)*

Verantwortung

[1] Die Verwaltungsbehörde, die Daten auslagert, bleibt verantwortlich für die ständige Aufbewahrung und den ständigen Betrieb ihres Informationserbes. Insbesondere:

a) ergreift sie die Vorsichtsmassnahmen, die bei der Wahl des Auftragsbearbeiters, den Weisungen an ihn und der Aufsicht über ihn aufgrund der Umstände geboten sind;

b) gewährleistet sie die Datensicherheit und die Sicherheit ihrer eigenen Informationssysteme mit dem Abschluss eines Vertrags, in dem mindestens der Gegenstand, die Art, der Zweck und die Dauer der Auslagerung, die betroffenen Kategorien von Daten sowie die Pflichten und Rechte jeder Partei festgehalten werden;

c) überträgt sie dem Auftragsbearbeiter kein Bearbeiten, das sie nicht selber ausführen darf;

d) sorgt sie dafür, dass sie die von einer Auslagerung betroffenen Daten und In-formatiktools jederzeit zurückbekommen kann, namentlich damit sie den Auftragsbearbeiter wechseln, die Daten wieder bei sich bearbeiten oder sie dem historischen Archiv abliefern kann.

[2] Wenn die Auslagerung mehrere verschiedene Behörden desselben Gemeinwesens betrifft, wird eine hauptverantwortliche Behörde bezeichnet.

[3] Bei der Kantonsverwaltung übernehmen die Verwaltungsbehörde und das Amt, das für die Informatik zuständig ist [1)], gemeinsam die Verantwortung für die Umsetzung und die Kontrolle der Vorschriften dieses Abschnitts. Fälle, in denen die Verwaltungsbehörde ihre Informatiksysteme autonom verwaltet, bleiben vorbehalten.

[1)] Derzeit: Amt für Informatik und Telekommunikation.

Intitulé de section après Art. 17e *(nouveau)*

3b Développement de la cyberadministration

Intitulé de section après section 3b

3.2 *(abrogé)*

Art. 20a *(nouveau)*

Moyen d'identification électronique

[1] L'accès aux prestations électroniques fournies par l'Etat et les communes est en principe subordonné à l'utilisation par les usagers et usagères d'un moyen d'identification électronique.

[2] Pour certaines prestations, l'Etat peut imposer l'utilisation d'un moyen d'identification électronique déterminé qui doit répondre au niveau d'exigences prévu pour les prestations concernées; les frais d'utilisation sont alors pris en charge par l'Etat.

[3] L'Etat peut mettre en place des autorités d'enregistrement qui procèdent gratuitement à la vérification de l'identité des personnes détentrices du ou des moyens d'identification électronique choisis. D'entente avec l'Etat, les communes peuvent également offrir ce service.

[4] Le Conseil d'Etat règle les modalités par voie d'ordonnance.

Art. 21 al. 1 *(modifié)*, ***al. 2*** *(abrogé)*, ***al. 3*** *(abrogé)*, ***al. 4*** *(abrogé)*

[1] Le traitement automatisé de données personnelles sensibles dans des projets pilotes ou pendant la phase d'adoption ou d'adaptation des bases légales est régi par la loi sur la protection des données.

[2] Abrogé

[3] Abrogé

[4] Abrogé

Abschnittsüberschrift nach Art. 17e *(neu)*

3b Entwicklung des E-Government

Abschnittsüberschrift nach Abschnitt 3b

3.2 *(aufgehoben)*

Art. 20a *(neu)*

Elektronische Identifizierungsmittel

[1] Der Zugang zu den elektronischen Leistungen, die vom Staat und von den Gemeinden erbracht werden, kann grundsätzlich davon abhängig gemacht werden, dass die Nutzerinnen und Nutzer ein elektronisches Identifizierungsmittel verwenden.

[2] Für gewisse Leistungen kann der Staat die Verwendung eines bestimmten elektronischen Identifizierungsmittels vorschreiben, das dem vorgesehenen Anforderungsniveau für die betreffenden Leistungen entsprechen muss; die Kosten für die Verwendung werden dann vom Staat übernommen.

[3] Der Staat kann Registrierungsbehörden schaffen, die kostenlos Personen, die im Besitz des oder der gewählten Mittel zur elektronischen Identifizierung sind, prüfen. Im Einvernehmen mit dem Staat können die Gemeinden diese Dienstleistung ebenfalls anbieten.

[4] Der Staatsrat regelt die Einzelheiten in einer Verordnung.

Art. 21 Abs. 1 *(geändert)*, ***Abs. 2*** *(aufgehoben)*, ***Abs. 3*** *(aufgehoben)*, ***Abs. 4*** *(aufgehoben)*

[1] Die automatisierte Verarbeitung besonders schützenswerter Personendaten in Pilotprojekten oder während der Phase der Verabschiedung oder Anpassung von Rechtsgrundlagen wird im Gesetz über den Datenschutz geregelt.

[2] Aufgehoben

[3] Aufgehoben

[4] Aufgehoben

Art. 21a *(nouveau)*

Droit transitoire relatif à la modification du …

[1] Pour autant que besoin, les contrats d'externalisation conclus avant l'entrée en vigueur de la modification du … de la présente loi sont adaptés aux exigences de la section relative à l'externalisation lors de leur renouvellement, mais au plus tard dans un délai de cinq ans.

[2] Les modalités de la gestion du consentement prévu à l'article 3a et de l'utilisation des moyens d'identification électronique mentionnés à l'article 20a sont mises en œuvre progressivement, mais au plus tard dans un délai de trois ans.

II.

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

Art. 3 al. 1

[1] On entend par:

d) *(modifié)* traitement, toute opération relative à des données personnelles – quels que soient les moyens et procédés utilisés –, notamment la collecte, la conservation, l'hébergement, l'exploitation, la modification, la communication, l'archivage ou la destruction de données;

e1) *(nouveau)* externalisation du traitement, une forme de sous-traitance impliquant la délocalisation du traitement sur les infrastructures du sous-traitant;

i) *(nouveau)* sous-traitant, la personne privée ou l'organe public relevant d'une autre collectivité qui traite des données personnelles pour le compte d'un ou plusieurs responsables du fichier.

Art. 12b *(nouveau)*

Externalisation

[1] Le traitement de données personnelles, y compris de données sensibles, peut être externalisé aux conditions posées par les présentes dispositions.

Art. 21a *(neu)*

Übergangsrecht zur Änderung vom

[1] Falls nötig werden die Auslagerungsverträge, die vor dem Inkrafttreten der Änderung vom … dieses Gesetzes abgeschlossen wurden, bei ihrer Erneuerung, aber spätestens innert 5 Jahren an die Anforderungen des Abschnitts über die Auslagerung angepasst.

[2] Die Einzelheiten zur Verwaltung der Zustimmung gemäss Artikel 3a und zur Verwendung der Mittel zur elektronischen Identifikation gemäss Artikel 20a werden nach und nach, aber spätestens innert 3 Jahren umgesetzt.

II.

Der Erlass SGF 17.1 (Gesetz über den Datenschutz (DSchG), vom 25.11.1994) wird wie folgt geändert:

Art. 3 Abs. 1

[1] Die folgenden Ausdrücke bedeuten:

d) *(geändert)* Bearbeiten, jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Hosten, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten;

e1) *(neu)* Auslagerung des Bearbeitens, Form der Bearbeitung durch Auftragsbearbeiter, das zur Folge hat, dass das Bearbeiten auf die Infrastrukturen des Auftragsbearbeiters übertragen wird;

i) *(neu)* Auftragsbearbeiter, Privatperson oder öffentliches Organ eines anderen Gemeinwesens, das Personendaten für einen oder mehrere Verantwortliche der Datensammlung bearbeitet.

Art. 12b *(neu)*

Auslagerung

[1] Die Bearbeitung personenbezogener Daten, einschliesslich besonders schützenswerter Daten, kann unter den in diesen Bestimmungen festgelegten Bedingungen ausgelagert werden.

[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.

Art. 12c *(nouveau)*

Externalisation – Responsabilités

[1] L'organe public qui procède à une externalisation demeure responsable de la protection des données personnelles, en particulier de leur confidentialité ainsi que de la pérennité de leur conservation et de leur exploitation. En particulier:

a) il prend les précautions commandées par les circonstances quant au choix du sous-traitant, à son instruction et à sa surveillance;

b) il assure la protection et la sécurité des données et de ses propres systèmes d'information par la conclusion d'un contrat qui décrit au minimum:

   1. l'objet, la nature, la finalité et la durée de l'externalisation;
   2. les catégories de données concernées;
   3. les obligations et les droits de chaque partie;
   4. les droits et possibilités de contrôle de l'autorité de surveillance en matière de protection des données;
   5. l'interdiction faite au sous-traitant de sous-traiter à son tour un traitement sans l'autorisation préalable du responsable du fichier;
   6. le devoir du sous-traitant d'informer immédiatement le responsable du fichier lorsque, en vertu d'une loi étrangère ou d'une décision de justice, il est tenu de communiquer des données à une autorité étrangère ou risque de devoir le faire;

c) il ne confie pas au sous-traitant des traitements qu'il ne serait pas en droit d'effectuer lui-même;

[2] Die Daten müssen jederzeit auf dem Gebiet der Schweiz oder auf dem Gebiet eines Staates, der einen gleichwertigen Datenschutz gewährleistet, bearbeitet werden.

[3] Wenn die Auslagerung eine Delegation von Aufgaben an Dritte im Sinne von Artikel 54 der Kantonsverfassung vom 16. Mai 2004 zur Folge hat, gelten die besonderen Anforderungen gemäss dieser Bestimmung.

Art. 12c *(neu)*

Auslagerung – Verantwortung

[1] Das öffentliche Organ, das Daten auslagert, bleibt für den Schutz der Personendaten, insbesondere für die Vertraulichkeit und die Kontinuität ihrer Aufbewahrung und Nutzung, verantwortlich. Insbesondere:

a) ergreift es die Vorsichtsmassnahmen, die bei der Wahl des Auftragsbearbeiters, den Weisungen an diesen und der Aufsicht über diesen aufgrund der Umstände geboten sind;

b) gewährleistet es den Schutz und die Sicherheit der Daten und deren eigenen Informationssysteme, indem sie einen Vertrag abschliesst, der mindestens Folgendes beschreibt:

   1. den Gegenstand, die Art, den Zweck und die Dauer der Auslagerung;
   2. die betroffenen Datenkategorien;
   3. die Pflichten und Rechte jeder Partei;
   4. die Rechte und die Kontrollmöglichkeiten der Aufsichtsbehörde im Bereich des Datenschutzes;
   5. das an den Auftragsbearbeiter gerichtete Verbot, ohne vorherige Genehmigung des für die Datensammlung Verantwortlichen seinerseits einen weiteren Auftragsbearbeiter für die Bearbeitung zu beauftragen;
   6. die Pflicht des Auftragsbearbeiters, den Verantwortlichen der Datensammlung unverzüglich zu informieren, wenn er aufgrund eines ausländischen Gesetzes oder eines richterlichen Entscheids die Daten einer ausländischen Behörde bekanntgeben muss oder Gefahr läuft, dass er es tun muss.

c) überträgt es dem Auftragsbearbeiter kein Bearbeiten, das es nicht selber ausführen darf.

d) il veille à ce que les données et les outils informatiques concernés par une externalisation puissent être récupérés en tout temps, notamment dans le but de changer de sous-traitant, de procéder à leur réinternalisation ou de les verser aux archives historiques.

[2] Lorsque l'externalisation concerne plusieurs organes différents au sein d'une même collectivité publique, un organe principalement responsable est désigné.

[3] Au sein de l'administration cantonale, la responsabilité de la mise en œvre et du suivi des règles de la présente section est assumée conjointement par l'organe compétent à raison de la matière et par le service en charge de l'informatique. Sont réservés les cas dans lesquels l'organe compétent à raison de la matière gère de manière autonome ses systèmes informatiques.

Art. 12d *(nouveau)*

Externalisation – Mesures de sécurité

[1] L'intégrité, l'authenticité, la disponibilité et la confidentialité des données personnelles externalisées ainsi que la pérennité de leur conservation et de leur exploitation doivent être garanties par des mesures organisationnelles et techniques appropriées et adaptées à l'évolution des technologies disponibles.

[2] La définition des mesures de sécurité tient compte des risques que le traitement des données en question présente pour la personnalité et les droits fondamentaux des personnes concernées.

[3] Lorsque l'externalisation concerne des données indispensables au fonctionnement de l'administration, la continuité des activités externalisées doit, en cas d'incident, être garantie par un dispositif adéquat.

Art. 12e *(nouveau)*

Externalisation – Mesures relatives aux données sensibles

[1] Le traitement de données personnelles sensibles qui présente un risque concret d'atteinte aux droits des personnes concernées et le traitement de données qui font l'objet d'une obligation légale ou contractuelle de garder le secret peuvent être externalisés si la confidentialité à l'égard du sous-traitant est assurée de manière que ce dernier ne puisse avoir accès à leur contenu.

d) sorgt es dafür, dass es die von einer Auslagerung betroffenen Daten und Informatikwerkzeuge jederzeit zurückbekommen kann, namentlich damit es den Auftragsbearbeiter wechseln, die Daten wieder bei sich bearbeiten oder sie dem Historischen Archiv abliefern kann.

[2] Wenn die Auslagerung mehrere verschiedene Organe desselben Gemeinwesens betrifft, wird eine hauptverantwortliches Organ bezeichnet.

[3] Bei der Kantonsverwaltung übernehmen das sachlich zuständige Organ und das Amt, das für die Informatik zuständig ist, gemeinsam die Verantwortung für die Umsetzung und die Kontrolle der Vorschriften dieses Abschnitts. Fälle, in denen das sachlich zuständige Organ seine Informatiksysteme autonom verwaltet, bleiben vorbehalten.

Art. 12d *(neu)*

Auslagerung – Sicherheitsmassnahmen

[1] Die Unversehrtheit, die Authentizität, die Verfügbarkeit und die Vertraulichkeit der Personendaten, die von einer Auslagerung betroffen sind, sowie deren ständige Aufbewahrung und Verwendung müssen mit geeigneten organisatorischen und technischen Massnahmen, die der Entwicklung der verfügbaren Technologien angepasst sind, sichergestellt werden.

[2] Die Definition der Sicherheitsmassnahmen berücksichtigt die Gefahren, die das Bearbeiten der fraglichen Daten für die Persönlichkeit und die Grundrechte der betroffenen Personen mit sich bringt.

[3] Wenn die Auslagerung Daten betrifft, die für den Betrieb der Verwaltung unbedingt nötig sind, muss die Fortführung der ausgelagerten Tätigkeiten bei einem Zwischenfall mit einem angemessenen Dispositiv sichergestellt werden.

Art. 12e *(neu)*

Auslagerung – Massnahmen für besonders schützenswerte Personendaten

[1] Das Bearbeiten von besonders schützenswerten Personendaten bei dem ein konkretes Risiko besteht, dass gegen das Recht der betroffenen Personen verstossen wird, und das Bearbeiten von Daten die einer gesetzlichen oder vertraglichen Geheimhaltungspflicht unterliegen, darf dann ausgelagert werden, wenn die Vertraulichkeit gegenüber dem Auftragsbearbeiter sichergestellt ist, so dass dieser auf deren Inhalt keinen Zugriff hat.

[2] Lorsque le sous-traitant doit impérativement avoir accès aux données pour des raisons techniques, le contrat d'externalisation fixe les exigences particulières nécessaires, en particulier l'engagement du sous-traitant de n'accéder au contenu des données qu'avec le consentement exprès de l'organe public qui procède à l'externalisation et l'obligation de tenir un journal des accès.

Art. 12f *(nouveau)*

Essais pilotes

[1] Sur la base d'un dossier dûment établi et après consultation de l'Autorité cantonale de la transparence et de la protection des données, le Conseil d'Etat peut autoriser par voie d'ordonnance le traitement automatisé de données sensibles si cela paraît indispensable pour réaliser un essai pilote ou préparer une application pendant la procédure d'adoption ou d'adaptation de sa base légale.

[2] Une phase d'essai peut être considérée comme indispensable pour traiter les données:

a) si l'accomplissement des tâches nécessite l'introduction d'innovations techniques dont les effets doivent être évalués;

b) si l'accomplissement des tâches nécessite la prise de mesures organisationnelles ou techniques importantes dont l'efficacité doit être examinée, notamment dans le cadre d'une collaboration entre les organes fédéraux et les cantons.

[3] L'organe responsable transmet, au plus tard deux ans après la mise en œvre de la phase d'essai, un rapport d'évaluation au Conseil d'Etat et à l'Autorité de surveillance. Dans ce rapport, il lui propose la poursuite ou l'interruption du traitement.

[4] Si le Conseil d'Etat autorise la poursuite du traitement, il engage immédiatement la procédure législative pour donner une base légale formelle au traitement de ces données.

[2] Wenn der Auftragsbearbeiter aus technischen Gründen unbedingt Zugriff auf die Daten haben muss, werden im Auslagerungsvertrag die nötigen besonderen Anforderungen festgelegt, insbesondere die Verpflichtung des Auftragsbearbeiters, nur mit ausdrücklichem Einverständnis des öffentlichen Organs, welches die Daten auslagert, auf den Inhalt der Daten zuzugreifen, und die Pflicht, ein Zugriffsjournal zu führen.

Art. 12f *(neu)*

Pilotversuche

[1] Auf der Basis eines ordnungsgemäss erstellten Dossiers und nach Anhörung der kantonalen Behörde für Öffentlichkeit und Datenschutz darf der Staatsrat mit Verordnung das automatisierte Bearbeiten von heiklen Daten bewilligen, wenn das unbedingt nötig ist, um einen Pilotversuch durchzuführen oder eine Anwendung während des Genehmigungs- und Anpassungsverfahrens für die gesetzliche Grundlage vorzubereiten.

[2] Eine Versuchsphase kann als unbedingt nötig für das Bearbeiten von Daten betrachtet werden, wenn:

a) für die Erfüllung der Aufgaben technische Innovationen, deren Auswirkungen beurteilt werden müssen, eingeführt werden müssen;

b) für die Erfüllung der Aufgaben organisatorische oder technische Massnahmen, deren Wirksamkeit geprüft werden muss, ergriffen werden müssen, namentlich im Rahmen einer Zusammenarbeit zwischen den Organen des Bundes und den Kantonen.

[3] Das verantwortliche Organ übermittelt dem Staatsrat und der Aufsichtsbehörde spätestens zwei Jahre nach der Umsetzung der Versuchsphase einen Beurteilungsbericht. In diesem Bericht beantragt es ihm, dass das Bearbeiten fortgesetzt oder abgebrochen wird.

[4] Wenn der Staatsrat die Fortsetzung des Bearbeitens bewilligt, leitet er unverzüglich ein Gesetzgebungsverfahren ein, um dem Bearbeiten dieser Daten eine formale gesetzliche Grundlage zu geben.

Art. 18 al. 1 *(modifié)*

Responsabilité – Sous-traitance *(titre médian modifié)*

[1] L'organe public qui fait traiter des données personnelles par un sous-traitant demeure responsable de la protection des données. Il doit notamment donner au sous-traitant les instructions nécessaires et veiller à ce que ce dernier n'utilise les données ou ne les communique que pour l'exécution du mandat.

Art. 34a *(nouveau)*

Droit transitoire – Contrats d'externalisation

[1] Pour autant que besoin, les contrats d'externalisation conclus avant l'entrée en vigueur de la modification du … de la présente loi sont adaptés aux exigences des articles 12b et suivants lors de leur renouvellement, mais au plus tard dans un délai de cinq ans.

III.

Aucune abrogation d'actes dans cette partie.

IV.

Conversion de la LGCyb modifiée en une nouvelle loi

—

Les organes chargés des publications officielles convertissent la loi du 2 novembre 2016 sur le guichet de cyberadministration telle que modifiée par la présente loi en une loi entièrement révisée (renumérotation des éléments de structure, adaptation des renvois et références internes, suppression des dispositions caduques). Ils lui attribuent la date d'adoption de la présente loi.

Art. 18 Abs. 1 *(geändert)*

Verantwortung – Auftragsbearbeitung *(Artikelüberschrift geändert)*

[1] Das öffentliche Organ, das Personendaten von einem Auftragsbearbeiter bearbeiten lässt, bleibt für den Datenschutz verantwortlich. Es muss namentlich dem Auftragsbearbeiter die nötigen Weisungen geben und dafür sorgen, dass er die Daten nur für die Ausführung des Auftrags verwendet oder bekanntgibt.

Art. 34a *(neu)*

Übergangsrecht – Auslagerungsverträge

[1] Falls nötig werden die Auslagerungsverträge, die vor dem Inkrafttreten der Änderung vom … des vorliegenden Gesetzes abgeschlossen wurden, bei ihrer Erneuerung, aber spätestens innert 5 Jahren an die Anforderungen von Artikel 12b ff. angepasst.

III.

Keine Aufhebung von Erlassen in diesem Abschnitt.

IV.

Umwandlung des geänderten E-GovSchG in ein neues Gesetz

—

Die für die amtlichen Veröffentlichungen zuständigen Organe wandeln das Gesetz vom 2. November 2016 über das E-Government-Schalter in der durch dieses Gesetz geänderten Fassung in ein vollständig überarbeitetes Gesetz um (Umnummerierung der Strukturelemente, Anpassung der Querverseise und der internen Verweise, Streichung überholter Bestimmungen). Sie weisen ihm das Datum der Verabschiedung dieses Gesetzes zu.

Dispositions finales

—

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.

Schlussbestimmungen

—

Dieses Gesetz untersteht dem Gesetzesreferendum. Es untersteht nicht dem Finanzreferendum.

Der Staatsrat legt das Inkrafttreten dieses Gesetzes fest.