ETAT DE FRIBOURG
STAAT FREIBURG

Conseil d'Etat CE
Staatsrat SR

Message 2019-CE-239 21 avril 2020

—

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

En bref

Le présent projet propose des modifications de la loi sur le guichet de cyberadministration (LGCyb) et de la loi sur la protection des données (LPrD).

Son objectif premier est de poser les bases légales permettant le ***passage en phase de production des projets pilotes menés par l'Etat en matière d'informatique en nuage*** (*cloud computing*), de manière à ce que certains des outils testés puissent être déployés ***dès l'automne 2020***. Ces bases légales sont nécessaires du point de vue de la protection des données personnelles. Sur ce plan, le projet prend donc de l'avance, pour des raisons de calendrier, sur les travaux de révision totale de la LPrD actuellement en cours et revêt un caractère urgent.

Toutefois, les réflexions menées dans ce contexte nous ont amené à envisager le projet sous un angle plus large.

Tout d'abord, au vu de l'importance qu'elle prend en pratique, ***l'externalisation de traitements de données*** a été examinée globalement, et pas seulement sous l'angle de la protection des données personnelles. Les dispositions y relatives sont dès lors réparties entre la LGCyb (principes généraux) et la LPrD (compléments relatifs à la protection des données personnelles).

Ensuite, le projet complète les dispositions de la LGCyb sur le ***Référentiel cantonal*** de personnes, organisations et nomenclatures. Il s'agit notamment de permettre l'utilisation systématique du numéro AVS (NAVS) dans ce référentiel, dans le but d'identifier de manière sûre et univoque les personnes recensées. Sur ce plan également, le projet anticipe sur les solutions à venir pour des raisons de calendrier. L'utilisation systématique du NAVS devrait en principe être facilitée prochainement par le droit fédéral; mais le projet du Conseil fédéral doit encore être discuté aux Chambres et son entrée en vigueur n'est pas pour tout de suite. Or les besoins pour le Référentiel cantonal existent déjà actuellement et, si l'on ne veut pas retarder les travaux, une base légale cantonale est indispensable à la poursuite de la mise en place du Référentiel.

Enfin, le projet propose des ***modifications et clarification complémentaires de la LGCyb*** sur divers points: portée de la loi pour les communes (art. 1a et art. 5); traitements de données personnelles dans le guichet virtuel (art. 3a et 9a); participation du canton à l'association iGovPortal.ch (art. 9b); et utilisation d'un moyen d'identification électronique par les administrations cantonales et communales (art. 20a). Prises globalement, les différentes modifications de la LGCyb justifient que celle-ci soit renommée (d'une loi sur le guichet de cyberadministration, on passe à une loi sur la cyberad-

ministration); en outre, afin d'améliorer la lisibilité du texte, il paraît opportun de transformer cette loi partiellement révisée en une loi entièrement renumérotée et nouvellement datée (cf. la première clause finale).

1. Contexte général

Il y a un peu plus de trois ans, le Grand Conseil adoptait la loi du 2 novembre 2016 sur le guichet de cyberadministration de l'Etat (LGCyb; RSF 17.4). L'objectif était de régler la création et la gestion d'un guichet virtuel unique, porte d'entrée vers les différents services de l'administration sur Internet, et de poser les prérequis techniques et les principes généraux de la cyberadministration cantonale.

Depuis, de nombreux travaux ont été menés dans le but de moderniser le canton, de rendre les opérations administratives plus aisées et plus économiques pour les administré-e-s et d'accroître l'efficience de l'administration. Fribourg s'est, par exemple, distingué sur la scène nationale en participant à des projets d'innovation dans le but de faciliter les démarches administratives en ligne[1]. Il est aussi le premier canton en Suisse à proposer la délivrance d'actes authentiques de l'état civil au format électronique[2].

La mise sur pied d'une véritable cyberadministration à l'échelon cantonal est cependant un vaste projet qui nécessite de repenser fondamentalement le fonctionnement et l'organisation de l'administration. Dans ce but, la LGCyb permet explicitement de travailler par l'entremise de projets pilotes décidés par le Conseil d'Etat afin d'avancer pas à pas et de ne préparer des bases légales formelles que lorsque les entités concernées ont pu tester et valider les enseignements de ces divers projets (cf. art. 20 LGCyb). Cette manière de travailler permet au canton de Fribourg d'avancer dans sa transformation numérique de manière aussi prudente et clairvoyante que possible.

Le présent projet se situe ainsi dans la ligne des deux ordonnances expérimentales que le Conseil d'Etat a adoptées depuis l'entrée en vigueur de la LGCyb:

> La première ordonnance expérimentale, qui recouvre quatre projets pilotes, avait pour objectif d'observer les possibilités techniques et les exigences sécuritaires indispensables à l'externalisation du traitement de données personnelles dans le *cloud*. Les enseignements tirés permettent au Conseil d'Etat de proposer des dispositions légales appropriées visant à exploiter plus largement cette technologie dans un environnement le plus adapté et le plus sûr possible Ces dispositions devaient à l'origine être introduites dans le contexte de la révision totale de la LPrD qui est en préparation depuis un certain temps. Néanmoins, cette révision totale est un projet de grande portée et sa mise au point prendra vraisemblablement encore beaucoup de temps, si l'on se réfère aux travaux de révision de la loi fédérale sur la protection des données. Or il est important de pouvoir passer rapidement de la phase pilote à la phase de production pour ces différents projets d'informatique en nuage; cela est même essentiel pour le projet «outils bureautiques collaboratifs Microsoft 365» qui devait être implémenté dans les écoles du canton *dès l'automne 2020* et dont la mise en œuvre a dû être avancée en raison de la crise du coronavirus et des besoins des élèves pour le travail à domicile. Par ailleurs, le besoin se faisait également sentir d'édicter des dispositions générales sur l'externalisation de traitements informatiques en dehors du domaine de la protection des données. Au vu de l'importance que prend l'externalisation de solutions informatiques dans l'organisation de l'administration, il se justifie de poser en la matière des règles générales à l'échelon de la loi. Le projet propose de régler de manière globale ce problème de l'externalisation dans la LGCyb et dans le texte actuel de la LPrD, sans attendre la révision totale de cette dernière.

> La deuxième ordonnance expérimentale porte sur la mise en œuvre du Référentiel cantonal de données de personnes, organisations et nomenclatures. Le projet est actuellement toujours en cours et devrait se poursuivre jusqu'à l'été 2021. Les travaux menés jusqu'à ce jour ont cependant révélé qu'il ne pourra pas atteindre ses objectifs si le NAVS ne peut pas être utilisé de manière systématique dans le Référentiel cantonal afin d'identifier les personnes de manière sûre et univoque. Or, en l'état actuel de la législation fédérale, une telle utilisation du NAVS requiert l'adoption par le canton d'une base légale formelle circonstanciée. Le projet complète dès lors dans ce sens les dispositions de la LGCyb relatives au Référentiel cantonal. Sur le plan fédéral, un projet de modification de la loi sur l'assurance-vieillesse et survivants permettant l'utilisation systématique du numéro AVS par les autorités est actuellement en discussion aux Chambres (Message 19.057 et projet du 30 octobre 2019, *FF 2019 6955* et 6993). Mais son adoption prendra encore du temps et, si l'on attend son entrée en vigueur, cela retarderait inutilement les travaux du Référentiel.

2. Contenu du projet

Le projet introduit dans la législation cantonale (LGCyb et LPrD) les bases légales nécessaires à l'externalisation du traitement de données auprès de tiers (§ 2.1) et complète les dispositions de la LGCyb relative au Référentiel en autorisant notamment l'utilisation systématique du NAVS à l'intérieur de celui-ci (§ 2.2). En outre, en vue d'accompagner les travaux en cours et futurs dans le domaine de la digitalisation de

[1] https://www.egovernment.ch/fr/umsetzung/innovationen/innovationen-20182019/.

[2] https://www.fr.ch/diaf/vie-quotidienne/demarches-et-documents/premiere-suisse-des-actes-detat-civil-authentiques-electroniques.

l'administration, il complète la LGCyb sur d'autres points et la convertit en une véritable loi sur la cyberadministration (§ 2.3).

2.1. Externalisation du traitement de données et d'outils informatiques

Le recours à l'externalisation et plus particulièrement au *cloud* constitue une réponse à des exigences nouvelles dans le fonctionnement et l'organisation de l'Etat, qui résultent du déploiement des technologies numériques dans la société: explosion des volumes de données produites et utilisées, exigences de haute disponibilité et de sécurité, volonté des organes de l'Etat de se concentrer sur le cœur de leur activité et de se désengager de certaines opérations qui ne correspondent pas à leur métier, besoins de nouveaux moyens d'accès aux services en situation de mobilité, en tout lieu, à tout moment et sur tout support.

Il est vrai cependant que l'utilisation de tels services requiert la prise de précautions adaptées aux circonstances et aux risques engendrés. C'est pourquoi, avant d'autoriser plus largement l'externalisation de données, le Conseil d'Etat a dans un premier temps adopté l'ordonnance 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) (RSF 17.42). A l'origine, cette ordonnance devait permettre de tester jusqu'à la fin de l'année 2020 quatre solutions «cloud» ciblées et d'explorer les possibilités techniques à mettre en place, en particulier dans le domaine de la sécurité. Néanmoins, déjà en automne de l'année passée, les résultats du projet portant spécifiquement sur la solution «outils bureautiques collaboratifs Microsoft 365» ont fait l'objet d'un rapport d'évaluation du Service de l'informatique et des télécommunications (ci-après: le SITel) qui a été transmis au Conseil d'Etat en novembre 2019. Ce rapport arrive notamment aux conclusions suivantes:

> «le déploiement des entités incluses dans le projet pilote est un succès et […] cette opération est maitrisée. Par ailleurs, les réponses aux préoccupations de l'ATPrD [*Autorité cantonale de la transparence et de la protection des données*] ont été apportées, voire même complétées par des mesures supplémentaires».
> «Les expériences acquises avec ce seul projet sont suffisamment concluantes pour que le Conseil d'Etat puisse proposer au Grand Conseil l'adoption des bases légales formelles nécessaires permettant l'externalisation du traitement de données personnelles, y compris sensibles, de manière générale (dans le «cloud»)».

Ainsi, sur la base des expériences acquises avec la solution Microsoft 365, le Conseil d'Etat considère qu'il dispose de suffisamment de retours probants pour proposer au Grand Conseil l'adoption de ces bases légales formelles. Tenant compte des expériences menées durant la phase pilote, le projet crée un cadre juridique à même de soutenir l'utilisation de ces nouveaux outils au sein des collectivités publiques dans un environnement le plus adapté et le plus sécurisé possible. L'entrée en vigueur rapide de ces dispositions est cependant essentielle car deux applications actuellement utilisées dans le domaine de l'enseignement ne seront plus disponibles à partir de la rentrée 2020. Or le moyen destiné à les remplacer est précisément le passage à la solution Microsoft 365. C'est pourquoi cette partie du projet est présentée séparément du reste de la révision totale de la LPrD.

Les différentes mesures de sécurité exigées par la loi reprennent notamment les recommandations de la Conférence des préposé-e-s suisses à la protection des données (PRIVATIM)[1]. Toutefois, le recours à des solutions de *cloud computing* pouvant concerner aussi bien des données personnelles que des données non personnelles ou encore des outils informatiques, ces mesures sont réparties entre la LGCyb et la LPrD: les dispositions introduites aux articles 17b à 17f LGCyb constituent le cadre minimal à respecter pour toutes les externalisations, y compris lorsqu'elles portent sur le traitement de données personnelles; en outre, dans ce dernier cas de figure, l'organe responsable devra veiller à respecter, en plus, les dispositions spéciales de la législation sur la protection des données (art. 12b LPrD).

Il est à noter encore que la mise au point d'un cadre légal adapté à l'utilisation de solutions de *cloud computing* correspond à l'un des objectifs du «Catalogue de mesures pour la stratégie d'informatique en nuages des autorités suisses 2012–2020» (Orientation O_2: Adaptation des bases légales)[2]. Le plan directeur de la digitalisation et des systèmes d'information qui décline et complète, pour la durée de la législature 2017–2021, les orientations stratégiques du programme gouvernemental dans le domaine de la digitalisation et des systèmes d'information prévoit la mise en place du *cloud* pour le fonctionnement de l'Etat. Avec les dispositions proposées, le canton de Fribourg réalise donc un des objectifs fixés par la Confédération et la Conférence des gouvernements cantonaux pour la période concernée.

2.2. Utilisation systématique du numéro AVS et des numéros IDE et REE par le Référentiel cantonal

Le 24 juin 2019, le Conseil d'Etat a adopté, en se fondant sur l'article 21 LGCyb, une ordonnance expérimentale concernant la mise en œuvre du Référentiel cantonal de données de personnes, organisations et nomenclatures (projets pilotes) (RSF 17.45). Cette ordonnance est destinée à mettre en œuvre

[1] PRIVATIM, *Aide-mémoire «Risques et mesures spécifiques à la technologie de Cloud computing»*, version 2.1 du 17 décembre 2019. Texte disponible à l'adresse: https://www.privatim.ch/wp-content/uploads/2019/12/privatim_Aide-memoire_Cloud_v2_1_20191217.pdf.

[2] Egovernement suisse, *Catalogue des mesures pour la stratégie d'informatique en nuages des autorités suisses 2012–2020,* 25 octobre 2012 (https://www.egovernment.ch/files/8814/5398/6362/Katalog-f.pdf.).

les articles 13 al. 1 let. b, 15 et 16 LGCyb qui prévoient la création d'une plate-forme informatique gérant un référentiel centralisé de données. Elle sera remplacée au terme de la phase pilote par une loi au sens formel.

Lorsqu'il a proposé le projet de LGCyb en 2016, le Conseil d'Etat avait renoncé à utiliser systématiquement le NAVS comme identificateur de personnes, préférant créer à la place un numéro d'identification cantonal. Les expériences menées à ce jour ont cependant révélé le besoin de pouvoir traiter le NAVS en plus du numéro d'identification cantonal. D'une part, le NAVS permet de régler convenablement la plupart des problèmes d'arbitrage liés à l'identification des personnes ou résultant d'informations manquantes ou incohérentes. D'autre part, il est aussi essentiel pour certains échanges de données avec d'autres autorités, notamment celles qui sont situées hors du canton de Fribourg.

En application de l'article 50e al. 3 de la loi du 20 décembre 1946 sur l'assurance-vieillesse et survivants (LAVS; RS 831.10), toute utilisation systématique du NAVS par des organes cantonaux en dehors du champ d'application des assurances sociales requiert aujourd'hui impérativement l'adoption d'une base légale circonstanciée par le Grand Conseil, indiquant l'organe autorisé à traiter systématiquement le NAVS et le but du traitement. Un projet de modification de cette réglementation est toutefois actuellement à l'étude au niveau fédéral dans le but d'autoriser les différents organes de la Confédérations, des cantons et des communes à utiliser systématiquement le NAVS de manière générale pour accomplir leurs tâches. Si ce projet de loi venait à être adopté, une base légale spécifique ne serait plus nécessaire mais des mesures de sécurité particulières devraient être mises en œuvre[1].

Avec la réglementation proposée, le projet satisfait aux règles actuellement en vigueur et anticipe l'adoption des futures bases légales en cours d'examen. Conformément aux articles 15 à 15b et 17b du projet, l'autorité en charge du Référentiel cantonal est autorisée à utiliser systématiquement le NAVS dans le but d'identifier de manière sûre et univoque les personnes recensées. Toute autre utilisation reste en revanche interdite. En particulier, il n'est pas permis d'utiliser le NAVS comme moyen d'apparier des données entre elles afin d'évaluer certaines caractéristiques personnelles des citoyens et citoyennes ou de mener des investigations dans le but, notamment, d'identifier des individus en situation d'irrégularité. Un pareil usage du NAVS et du Référentiel cantonal nécessiterait, en effet, obligatoirement l'adoption d'une loi spéciale par le Grand Conseil.

Sous l'angle sécuritaire, l'article 15b énonce que l'utilisation systématique du NAVS requiert la mise en place de mesures organisationnelles et techniques afin de prévenir toute utilisation abusive de ce dernier. Par rapport à l'avant-projet, le projet renonce à maintenir l'obligation de conserver le NAVS dans une base de données distincte des autres données. Des voix se sont, en effet, élevées dans le cadre de la consultation pour dénoncer le caractère inadapté, disproportionné et fastidieux de cette mesure. A la place, le projet s'aligne au moyen d'un renvoi sur les prescriptions en matière de sécurité prévues dans le projet du Conseil fédéral relatif à la modification de la LAVS précitée (cf. les articles 153d et 153e du projet du Conseil fédéral).

En plus du NAVS, le projet introduit aux articles 16 à 16b des dispositions similaires afin d'autoriser l'utilisation systématique des numéros IDE et REE, lesquels constituent le pendant du NAVS pour les personnes morales.

2.3. Autres modifications

Le projet apporte également quelques adaptations ponctuelles dans la LGCyb qui tirent les enseignements de sa première mouture et tiennent compte de certains changements survenus depuis son adoption:

- il clarifie la question de l'application de la loi aux communes et, ce faisant, leur permet de recourir à l'externalisation aux mêmes conditions que les organes cantonaux (art. 1a);
- il introduit l'exigence du consentement libre et éclairé de la personne concernée afin que le guichet virtuel puisse collecter les données personnelles nécessaires à la délivrance de la prestation ou du service requis et les transmettre au service compétent pour traiter sa demande (art. 3a);
- il introduit également le principe de la protection des données par défaut (*privacy by default*) dans le fonctionnement du guichet virtuel, tout en réservant la possibilité pour les usagers et usagères de consentir à un traitement élargi de leurs données (art. 9a);
- il permet au Conseil d'Etat d'adhérer à des organisations intercantonales spécialisées dans le domaine de la cyberadministration en lien avec le guichet virtuel et formalise dans ce cadre la participation du canton Fribourg à l'association iGovPortal.ch (art. 9b);
- il règle la question du recours à l'utilisation de moyens d'identification électronique (ci-après: MIE) pour se connecter de façon sûre et sécurisée aux différentes plateformes électroniques utilisées par les collectivités publiques et y passer des transactions (art. 20a);
- il remodèle en partie la structure de la LGCyb pour lui permettre d'assumer à l'avenir son rôle de loi générale et transversale dans le domaine de la cyberadministration et procède à son renommage en loi sur la cyberadministration (LCyb). Ces travaux de restructuration seront néanmoins totalement achevés dans un deuxième temps par le service en charge des publications qui procèdera au toilettage complet du texte.

[1] Cf. FF 2019 6993 (projet de loi) et FF 2019 2019 6955 (Message).

3. Déroulement des travaux

Durant l'automne 2019, la Chancellerie d'Etat, avec l'appui de la Direction des finances (DFIN), a constitué un groupe de travail en vue d'adapter la législation cantonale à certains aspects de la digitalisation. Celui-ci était composé d'une représentante de la DFIN, de la préposée à la protection des données et de représentants du Service de législation.

Durant le mois de décembre 2019, le Conseil d'Etat a mis simultanément en consultation deux avant-projets étroitement liés l'un à l'autre: l'avant-projet de révision totale de la loi sur la protection des données et l'avant-projet de loi adaptant la législation cantonale à certains aspects de la digitalisation. Le temps de consultation du deuxième projet était cependant plus court car il nécessitait des modifications rapides de la législation en vigueur concernant l'externalisation et les travaux de mise en œuvre du Référentiel cantonal. Il a été mis en consultation du 3 décembre 2019 au 31 janvier 2020.

De manière générale, cet avant-projet a été bien accueilli. La quasi-totalité des participants à la consultation soutiennent les modifications proposées qu'ils jugent correspondre à un besoin réel. Néanmoins, plusieurs participants ont exprimé le souci que la sécurité des données soit garantie et/ou que les risques d'utilisation abusive du NAVS soient écartés. Ils ont dans ce sens parfois demandé l'ajout de règles supplémentaires destinées à rehausser le niveau de sécurité. Seule l'ATPrD a rejeté le projet dans sa globalité mais plus pour des raisons de forme que de fond (cf. § 6 ci-dessous).

Parmi les reproches formulés, certains ont critiqué l'obligation faite de conserver le NAVS dans une base de données séparée des autres données, qu'ils ont jugée inadéquate et disproportionnée. D'autres ont relevé un risque de confusion entre certains termes utilisés (notamment: «traitement», «hébergement», «externalisation») et ont demandé de recourir à une terminologie plus claire et uniformisée.

Les travaux de mise au point du texte ont tenu compte dans une large mesure des retours de la consultation. D'une part, les dispositions relatives à la sécurité et à la protection des données en cas d'externalisation ont été complétées et améliorées en même temps qu'elles ont été mieux systématisées à l'intérieur de la LGCyb et de la LPrD. D'autre part, le projet renonce à maintenir l'obligation de conserver le NAVS dans une base de données distincte des autres données conservées. Les mesures de sécurité à mettre en œuvre correspondront à ce que le projet du Conseil fédéral prévoit sans aller plus loin que celui-ci. Finalement des efforts ont été faits dans le but d'uniformiser et de mieux systématiser la terminologie employée. Les définitions introduites ont dans ce but été précisées et complétées par l'ajout de nouvelles définitions permettant de mieux comprendre les relations entre traitement, hébergement, externalisation, responsable du fichier et sous-traitant.

4. Conséquences du projet

4.1. Conséquences financières et en personnel

Les conséquences financières du projet découlent principalement du besoin d'utiliser un MIE sûr et sécurisé. Pour favoriser le développement de la cyberadministration à l'échelle du canton, le Conseil d'Etat entend faire en sorte que l'utilisation du guichet virtuel et des autres plateformes électroniques mises à disposition soit totalement gratuite. Cela implique que le canton prenne à sa charge les coûts liés aux moyens de se connecter à ces services et de passer des transactions au travers de ceux-ci.

Dans le but d'assurer un niveau de sécurité le plus élevé possible, le Conseil d'Etat juge essentiel de faire l'acquisition d'une solution du marché qui soit au bénéfice d'une certification au sens de la loi fédérale sur le dossier électronique du patient (LDEP; RS 816.1) comme de la future loi fédérale sur les services d'identification électronique (LSIE), si elle est acceptée. Sur la base d'une estimation des coûts, les dépenses liées à l'introduction d'un MIE à l'échelon cantonal s'élève à CHF 2,5 mio sur une période de cinq ans. Ce montant inclut les frais d'utilisation du MIE en tenant compte du nombre d'utilisateurs et d'utilisatrices et de transactions envisagés; il n'inclut en revanche pas la mise en place et le fonctionnement de l'enregistrement du MIE, qui seront confiés à des autorités déjà existantes.

Pour le reste, le projet se limite à préciser et à compléter certains éléments relatifs au guichet virtuel et au Référentiel cantonal ainsi qu'à fixer un cadre légal à l'externalisation de données et d'outils informatiques. Il n'entraîne de ce fait pas directement de nouvelles dépenses ni de besoins en personnel nouveaux. Les dépenses qui résulteront de l'externalisation de données ou d'applications informatiques dépendront des futurs projets qui seront décidés dans ce domaine par les organes compétents.

On peut malgré tout relever que, même indépendamment du présent projet, la nécessité pour la DFIN ou pour le SITel de disposer d'un ou d'une juriste spécialisé-e dans le droit des nouvelles technologies se fait de plus en plus sentir. Actuellement, l'Etat confie un certain nombre de mandats à des personnes externes dans ce domaine. Sur le plan financier, il n'en coûterait pas nécessairement plus de disposer d'une personne pour traiter ces questions en interne. Le problème sera toutefois rediscuté ultérieurement dans le cadre de l'attribution des nouveaux postes au sein de l'Etat.

4.2. Conséquences sur les rapports Etat–communes

Dans le cadre des travaux liés à la digitalisation des collectivités publiques, les conséquences sur les rapports entre l'Etat et les communes sont, par nature, difficiles à prédire. La digitalisation est une étape incontournable du développement des administrations tant cantonales que communales. Les modifications proposées permettent aux communes de recourir à l'externalisation à l'instar de ce qui est prévu pour les organes cantonaux. S'agissant des travaux liés à la mise en œuvre du Référentiel cantonal, tout est fait pour inclure les communes de manière progressive sur la base de conventions passées avec elles. Le projet octroie par ailleurs la possibilité pour l'Etat de collaborer avec les communes pour l'identification des détenteurs de MIE et devenir autorité d'enregistrement. Cela fera l'objet de discussions ultérieures. En fin de compte, les conséquences concrètes sur les rapports entre l'Etat et les communes se dessineront petit à petit, au fur et à mesure de l'avancée des projets qui seront menés et auxquels les communes voudront s'associer. Une chose est cependant certaine: une digitalisation efficace des prestations publiques dans le canton de Fribourg impliquera une collaboration accrue entre les communes et l'Etat. Les discussions ont démarré et vont encore devoir se concrétiser.

5. Conformité au droit supérieur

Le projet traite de questions d'ordre organisationnel et de protection des données qui relèvent principalement du droit cantonal. Dans ces domaines, il convient en particulier de prendre en considération l'article 12 al. 2 Cst./Fr qui garantit le droit à la protection des données personnelles et aussi l'article 54 Cst./Fr qui traite de la question de la délégation de tâches prévues par la loi à des tiers. Le projet prévoit toute une série de mesures visant à garantir le respect de ces deux dispositions.

Le projet traite aussi de la question de l'utilisation systématique du NAVS dans le cadre du Référentiel cantonal. Les conditions d'une telle utilisation par les cantons en dehors du domaine des assurances sociales sont fixées pour le moment à l'article 50e al. 3 LAVS. Les dispositions du projet sont conformes aux exigences du droit fédéral. Elles anticipent par ailleurs l'entrée en vigueur des nouvelles normes actuellement en discussion au plan fédéral dans ce domaine.

6. Avis de l'autorité de la transparence et de la protection des données (ATPrD)

Durant les travaux préparatoires, l'ATPrD a indiqué qu'elle s'opposait au fait de faire entrer de manière anticipée les dispositions concernant l'externalisation de données personnelles, sans toutefois y être opposée sur le fond. En effet, elle estime qu'il n'est pas opportun de «saucissonner» les travaux de révision de la LPrD, que le projet de révision totale de cette loi forme un tout et qu'il n'y a aucune raison de faire entrer de manière anticipée certaines des dispositions qu'il contient. Elle a réitéré ce point de vue lors de la phase de consultation.

S'agissant de l'utilisation systématique du NAVS dans le cadre du Référentiel cantonal, l'ATPrD n'a jamais caché son scepticisme face à ce thème, et ce même si les possibilités d'une telle utilisation venaient à être élargies lors d'une révision du droit fédéral. Durant la phase de consultation, l'ATPrD a maintenu sa position à ce sujet. Elle a cependant ajouté que si, contre son avis, l'utilisation systématique du NAVS était maintenue, alors elle considère qu'il est indispensable que le NAVS soit stocké dans une base de données distincte des autres données traitées.

Comme cela a déjà été mentionné plus haut, le Conseil fédéral a adopté, le 30 octobre 2019, un projet de modification de la LAVS concernant l'utilisation systématique du NAVS. Selon ce projet, les cantons et les communes pourront utiliser systématiquement le NAVS sans qu'il ne soit plus nécessaire pour cela d'adopter une base légale spécifique. Ainsi, même si les présentes dispositions n'étaient pas adoptées, il est probable que le Référentiel cantonal pourra de toute manière traiter le NAVS dans un délai d'une année à deux ans. Un tel délai ralentirait cependant considérablement les travaux de mise en œuvre du Référentiel cantonal, ce qui aurait un impact non négligeable sur le fonctionnement de l'administration ainsi qu'en termes de coûts.

7. Adaptations de la LGCyB – Commentaires

7.1. Dispositions générales

Art. 1a (nouveau) – Application aux communes

A la demande de l'Association des Communes Fribourgeoises, une disposition a été introduite dans le but de clarifier l'application des dispositions de la LGCyb aux communes. La disposition proposée n'apporte cependant pas véritablement de changement de fond. Hormis le cas de l'externalisation, elle ne fait que reprendre ce que prévoit déjà l'actuel article 5 al. 1 LGCyb. Le fait de déplacer cette disposition au début de l'acte devrait toutefois simplifier sa compréhension générale pour les communes.

Le projet conserve ainsi l'idée principale voulant que la participation des communes doit se faire le plus possible sur une base volontaire et collaborative. Cette manière de travailler doit permettre à ces dernières de s'associer aux travaux menés par l'administration cantonale selon un rythme adapté à leurs besoins et à leurs ressources. L'instrument principal de cette collaboration est de ce fait celui d'une convention passée entre l'Etat et chaque commune plutôt que l'adoption de règles fixes énoncées dans la loi.

Art. 2 let. f, g et h (nouvelles) – Terminologie

> «cyberadministration» (*let. f*): la définition correspond, sous une forme succincte, à celles qui sont retenues dans les stratégies suisse[1] et fribourgeoise[2] de cyberadministration. Elle sert à mettre en évidence le fait que la cyberadministration ne concerne pas uniquement la fourniture de prestations à la population sous forme électronique (*front office*) mais qu'elle englobe aussi les changements apportés concernant l'organisation et le fonctionnement interne de l'Etat (*back office*).

> «externalisation» (*let. g*): la définition vise à couvrir l'ensemble des modèles de services accessibles en ligne via un réseau informatique (*cloud* ou *cloud computing*). «Ces modèles vont du simple hébergement de données à l'utilisation de systèmes et de solutions informatiques en ligne (*Infrastructure-as-a-Service/IaaS, Platform-as-a-Service/PaaS, Software-as-a-Service/SaaS)*». Chacun de ces modèles a pour point commun que l'objet externalisé n'est plus traité localement chez l'organe responsable, mais chez un sous-traitant.

> «*sous-traitant*» (*let. h*): la définition inclut toute personne ou organisation qui traite des données ou gère des outils informatiques pour le compte d'une autorité, y compris, donc, mais pas exclusivement les fournisseurs de services *cloud*. A l'intérieur d'une même collectivité, le fait de confier le traitement de données ou la gestion d'outils informatiques à un service central, comme c'est le cas, par exemple, du SITel, n'est toutefois pas considéré comme un cas de sous-traitance.

7.2. Guichet virtuel

Art. 3a (nouveau) – Traitement de données personnelles

Alinéa 1 – Dans la mesure où les lois spéciales qui autorisent le traitement de données personnelles ne valent que pour les organes de l'Etat auxquels elles font référence, le guichet de cyberadministration ne peut pas s'en prévaloir pour traiter les données nécessaires à la délivrance de la prestation ou du service requis. C'est pourquoi il est demandé à la personne de donner son consentement pour que le guichet de cyberadministration puisse collecter auprès d'elle les données nécessaires au traitement de sa demande et les communiquer à l'organe compétent pour y donner suite.

La disposition indique les conditions de validité du consentement qui doit en particulier être libre et éclairé. Ces conditions incluent le caractère spécifique et univoque du consentement qui n'a pour cette raison pas besoin d'être mentionnés expressément dans la disposition légale.

Dans le contexte du guichet de cyberadministration, la condition du consentement libre signifie que la personne qui refuserait un certain traitement de données ne peut pas se voir imputer un désagrément autre que celui d'avoir à se rendre au guichet physique pour déposer sa demande ou de l'adresser par courrier écrit. On réservera toutefois les cas où la loi impose la tenue de certaines procédures au format électronique, comme c'est le cas par exemple aujourd'hui pour les demandes de permis de construire qui sont traitées au moyen de l'application FRIAC (cf. art. 135a de la loi du 2 décembre 2008 sur l'aménagement du territoire et les constructions [LATeC; RSF 710.1]).

Quant au caractère éclairé du consentement, il est en principe satisfait lorsque la personne est informée des organes de l'Etat et des éventuels prestataires tiers participant à la délivrance de la prestation ou du service requis, des données qui sont transmises dans ce cadre et des finalités des traitements effectués. A noter que le consentement ne peut pas porter sur n'importe quelles données. Conformément aux principes de proportionnalité et de finalité, les données collectées au moyen du consentement doivent nécessairement être limitées aux données strictement nécessaires à la délivrance de la prestation demandée.

Alinéa 2 – La disposition indique que le consentement est une décision réversible et que la personne concernée conserve ainsi le contrôle sur l'utilisation de ses données.

Alinéa 3 – Conformément aux exigences provenant du droit de la protection des données, l'organe qui traite des données sur la base du consentement de la personne doit être en mesure de démontrer que cette dernière a effectivement donné son consentement en cas de contrôle. Cette exigence implique la mise en place d'un module de gestion du consentement qui sera mis en place au sein de l'administration. L'article 21a al. 2 du projet prévoit que ce nouvel outil devra être opérationnel dans un délai de trois ans après l'adoption de la présente modification.

Alinéa 4 – Dans le cadre de la délivrance de prestations ou de services sous forme électronique, le guichet virtuel se limite à assurer le rôle de passerelle entre la population et les organes compétents de l'Etat. C'est pourquoi il n'a en principe pas de raison de conserver les données plus longtemps que le temps nécessaire au traitement de la demande. La question de la durée de conservation des données par le guichet virtuel est réglée actuellement à l'article 8 de l'ordonnance du 15 mai 2017 sur le guichet de cyberadministration de l'Etat (OGCyb; RSF 17.41). Le Conseil d'Etat pourra permettre également que des prestations répondant à un besoin transversal de l'administration et à des exigences de conservation plus étendues puissent être proposées.

---

[1] Stratégie suisse de cyberadministration du 1er mai 2017, p. 2 (document disponible à l'adresse Internet: https://www.egovernment.ch/files/6014/8361/7687/Stratgie-suisse-de-cyberadministration.pdf.

[2] Stratégie de cyberadministration de l'Etat de Fribourg du 2 décembre 2014, p. 4 (document disponible à l'adresse Internet: https://www.fr.ch/sites/default/files/contens/cha/_www/files/pdf70/fr_DIV_strategie_ cyberadministration_web.pdf.

Art. 4 al. 1 – Frais et émoluments

La modification introduite vise à affirmer le caractère gratuit de l'accès au guichet de cyberadministration, quel que soit le moyen utilisé pour ce faire. Cette gratuité inclut également l'utilisation du MIE choisi par l'Etat de Fribourg afin de se connecter aux différentes plateformes électroniques mises à disposition des usagers et des usagères (cf. art. 20a).

Art. 5 al. 1 et 2 – Communes

Le contenu de l'ancien alinéa 1er a été déplacé sans changement dans le nouvel article 1a, car il ne concerne pas le guichet virtuel. Le nouveau texte ne fait que reprendre le contenu de l'ancien alinéa 2 sans y apporter de changement de fond.

Art. 9a (nouveau) – Protection des données par défaut et consentement

Alinéa 1 – La disposition introduit le principe de la protection des données par défaut dans le fonctionnement du guichet de cyberadministration. Selon ce principe, qui constitue dorénavant l'un des piliers du droit de la protection des données, l'architecture technique du guichet de cyberadministration et les applications qu'il supporte doivent par défaut être configurées afin que seules les données personnelles nécessaires au regard de chaque finalité spécifique du traitement soient traitées.

Alinéa 2 – Conformément à son droit à l'autodétermination informationnelle, la personne concernée doit conserver le plus possible la maîtrise des données la concernant et être en mesure de décider des usages possibles de celles-ci. Cela inclut en particulier le droit pour elle de consentir à un traitement élargi de ses données si elle y voit un intérêt particulier. Elle peut dans ce sens accepter l'utilisation de *cookies* informatiques en vue d'améliorer les performances et le fonctionnement du guichet virtuel, participer à un sondage en ligne ou encore s'inscrire à une *newsletter* dans le but de recevoir périodiquement des informations sur un thème qui l'intéresse. La présente disposition confère une assise juridique à ce type de traitements de données qui ne reposent pas sur l'existence d'une base légale spécifique.

En outre, l'avancement de la cyberadministration et des projets liés permettra progressivement d'accroître les domaines pour lesquels les citoyens et citoyennes pourront facultativement et de manière éclairée donner leur consentement par le biais d'interfaces spécialement créées en vue de la délivrance des prestations mises à leur disposition depuis le guichet virtuel ou d'autres services spécialement proposés. On peut ainsi penser que l'exercice des différents droits reconnus aux personnes concernées par la législation sur la protection des données pourront à l'avenir être exercés directement depuis le guichet virtuel.

Art. 9b (nouveau) – Participation à des organisations intercantonales

Contrairement aux administrations d'autres pays qui fonctionnent de manière centralisée, la Suisse est un Etat fédéral qui compte 27 administrations (la Confédération et les 26 cantons). Cela implique souvent qu'une même solution est développée en interne 27 fois et que les coûts de production sont par conséquent multipliés par autant à l'échelle de la Suisse.

Pour réduire les coûts de production et aussi partager et profiter des expériences des autres cantons, le canton de Fribourg a développé des partenariats dans le domaine de la cyberadministration. Il a en particulier créé en 2017 l'association intercantonale iGovPortal.ch avec la République et canton du Jura. Cette association qu'a rejoint le canton de Soleure et à laquelle se joindra celui de Saint-Gall dès l'été 2020 met à la disposition de ses membres le code source, le code objet ainsi que la documentation technique pour la création complète d'un guichet virtuel de cyberadministration doté d'un large catalogue de prestations. En contrepartie, chaque membre est invité à partager les améliorations et les nouvelles applications qu'il développe lui-même à partir de la solution de base et qui présentent un intérêt pour les autres membres. L'association IGovPortal.ch permet de la sorte de mutualiser les efforts et les coûts de développement supportés par chaque canton dans le domaine de la cyberadministration.

La disposition confère une assise juridique à la participation du canton à l'association iGovPortal.ch et permet au Conseil d'Etat de rejoindre d'autres types d'organisations actives dans le développement de solutions relatives à la fourniture de prestations sous forme électronique. La participation des cantons à des organisations intercantonales est expressément encouragée à l'article 48 de la Constitution fédérale.

7.3. Référentiel cantonal

Art. 15 al. 1 let. h1 (nouvelle) – Référentiel des personnes physiques

Pour pouvoir fonctionner, le Référentiel cantonal doit être en mesure de traiter les identifiants sectoriels de différents domaines d'activité de l'Etat, mais aussi des communes et, dans la mesure où le droit fédéral l'autorise, de la Confédération. Cela permet de faire le lien avec les autres systèmes d'information qui lui communiquent des données et ainsi d'identifier de manière sûre et univoque les personnes recensées. La modification proposée confère l'assise juridique nécessaire à cette fin.

Art. 15a (nouveau) – Utilisation systématique du numéro AVS – Principe

L'utilisation du NAVS par les cantons en dehors du champ d'application des assurances sociales est réglée à l'article 50e al. 3 LAVS. Selon cette disposition, l'utilisation du NAVS requiert l'adoption d'une base légale circonstanciée, dans une loi adoptée par le Grand Conseil, indiquant le but de l'utilisation et les organes légitimés à traiter le NAVS. Conformément à la disposition proposée, l'organe en charge du Référentiel cantonal (cf. art. 17a) est habilité à traiter systématiquement le NAVS dans le but d'identifier de manière sûre et univoque les personnes recensées, de corriger les divergences et les incohérences constatées sur les données conservées (mauvaise orthographe, données inexactes ou données devenues obsolètes, etc.) et de procéder automatiquement aux changements qui sont annoncés auprès d'une collectivité publique (notamment, changement d'adresse ou changement d'état civil). Cet objectif vise par ailleurs de satisfaire au principe d'exactitude des données ancré à l'article 7 LPrD.

Art. 15b (nouveau) – Utilisation systématique du numéro AVS – Mesures de sécurité

Le Référentiel cantonal est hébergé sur les infrastructures informatiques de l'Etat. Il n'est pas concerné par une externalisation dans le *cloud*. Nécessaire au bon fonctionnement de l'Etat, l'utilisation systématique du NAVS comme identificateur de personnes n'en constitue pas moins un traitement de données personnelles qui doit offrir toutes les garanties de sécurité aux administré-e-s. C'est pourquoi des mesures techniques et organisationnelles sont indispensables afin d'encadrer son utilisation.

Selon l'avant-projet, il était prévu que le NAVS soit conservé dans une base de données séparée des autres données personnelles. Ainsi, la connaissance du NAVS n'aurait pas permis de faire directement le lien avec un individu déterminé. La mise en place de cette mesure de sécurité a néanmoins rencontré de fortes oppositions dans le cadre de la procédure de consultation. Il lui était reproché d'être inutilement compliquée à mettre en œuvre et de ne pas apporter un gain significatif en terme de sécurité puisque le fait d'avoir des bases de données séparées ne représente pas à lui seul une garantie de sécurité, mais que cette dernière doit faire l'objet d'une approche globale. La réalisation de cette séparation représenterait ainsi une source de coûts supplémentaires sans garantie de sécurité supplémentaire.

La solution finalement retenue consiste à calquer strictement le droit cantonal sur le droit fédéral par le biais d'un renvoi. Ainsi en cas d'adoption par le Parlement fédéral de la modification de la LAVS concernant l'utilisation systématique du NAVS, les mesures techniques et organisationnelles prévues aux 153d et 153e du projet de révision de la LAVS précité s'appliqueront automatiquement.

Art. 16 let. e, 16a et 16b (nouveaux) – Utilisation systématique du numéro IDE et REE

L'équivalent du NAVS en Suisse comme identificateur de personnes pour les personnes morales sont le numéro d'identification des entreprises (IDE) et le numéro d'enregistrement non significatif (REE).

L'utilisation de ces identifiants est réglée à l'article 10 al. 3 de la loi fédérale du 9 octobre 1992 sur la statistique fédérale (LSF; RS 431.01)[1] et dans la loi fédérale du 18 juin 2010 sur le numéro d'identification des entreprises (LIDE; RS 431.03). Leur but est en particulier d'«identifier les entreprises de manière univoque, afin de simplifier et de sécuriser les échanges d'informations dans les processus administratifs et les travaux statistiques» (art. 1 LIDE).

Les articles 16 let. e, 16a et 16b du projet prévoient une réglementation analogue à celle qui concerne l'utilisation systématique du NAVS. Les mesures de sécurité concrètes à mettre en place pourront cependant être allégées par rapport à celles prévalant pour le NAVS compte tenu du risque moins important d'atteinte aux droits et aux libertés des personnes concernées pouvant résulter de l'utilisation de ces informations.

Art. 17a (nouveau) – Organe responsable du Référentiel cantonal

L'organe responsable du Référentiel cantonal est désigné par le Conseil d'Etat. En l'état il s'agit de la Commission de gouvernance des données référentielles, qui dépend de la Chancellerie d'Etat (cf. art. A1–1 de l'ordonnance concernant la mise en œuvre du Référentiel cantonal de données de personnes, organisations et nomenclatures [projet pilote]; RSF 17.45).

En tant qu'organe responsable du Référentiel cantonal, la Commission assume la fonction de responsable du fichier au sens de la LPrD. Elle est aussi autorisée à utiliser systématiquement le NAVS.

7.4. Externalisation

Art. 17b (nouveau) – Principes en matière d'externalisation

Alinéa 1er – La disposition constitue la base légale permettant aux collectivités publiques de procéder à l'externalisation du traitement de leurs données et de la gestion d'outils informatiques. Elle est assortie de nombreuses exigences décrites dans les articles suivants dans le but d'assurer un niveau de sécurité le plus élevé possible et de permettre à l'Etat et aux communes de conserver autant que faire se peut la maîtrise de leur patrimoine informationnel.

[1] La disposition est complétée par l'ordonnance du 30 juin 1993 sur le Registre des entreprises et des établissements (OREE; RS 431.903).

Alinéa 2 – La disposition introduit deux réserves aux possibilités de recourir à l'externalisation:

> Lorsque l'externalisation concerne le traitement de données personnelles, elle doit satisfaire aux exigences supplémentaires que prévoit la LPrD; cela concerne non seulement les dispositions prévues à l'articles 12b LPrD dont il est question ci-dessous mais l'ensemble de la législation en matière de protection des données (let. *a*);
> Lorsque l'externalisation envisagée implique que l'organe public délègue entièrement l'accomplissement d'une tâche que la loi lui attribue, la délégation devra dans ce cas impérativement être prévue dans une loi spécifique adoptée par le Grand Conseil comme l'exige l'article 54 Cst./Fr (let. *b*).

Art. 17c (nouveau) – Respect des secrets particuliers

Selon l'aide-mémoire de la Conférence des préposé-e-s à la protection des données (PRIVATIM), en cas d'externalisation de données soumises au secret professionnel ou à un autre secret particulier, des mesures supplémentaires de sécurité doivent être mises en place[1]:

> Les données doivent être cryptées et les clés de décryptage doivent en principe être mise exclusivement à la disposition de l'organe public. Les clés doivent être protégées en cas de perte, soustraction tout comme utilisation et prise de connaissance abusive;
> Si cela n'est pas possible, le fournisseur du service du Cloud peut conserver les clés s'il s'engage par contrat à ne les utiliser qu'avec le consentement exprès de l'organe public. Il faut tenir un procès-verbal des accès. De plus, le fournisseur du service du Cloud doit protéger les clés en cas de perte, soustraction tout comme utilisation et prise de connaissance abusives. Il doit aussi garantir que les données ne peuvent pas être compromises lors du processus de cryptage.

La disposition prévue retranscrit ces exigences au niveau de la loi dans un langage qui est neutre sur le plan de la technologie.

Art. 17d (nouveau) – Mesures de sécurité

Alinéa 1er – L'organe public qui procède à une externalisation doit s'assurer que le sous-traitant prenne des mesures techniques et organisationnelles dans le but d'assurer la conservation et l'exploitation de son patrimoine informationnel. Les mesures à prendre concrètement dépendent à chaque fois du type de données ou d'outils informatiques externalisés, de leur finalité et de leur degré de confidentialité. Les mesures mises en place doivent suivre l'état de la technique.

Alinéa 2 – Lorsque l'externalisation porte sur des données indispensables au fonctionnement d'une collectivité, l'organe public doit mettre en place en dispositif permettant d'assurer la continuité de l'activité externalisée en cas d'incident. A titre d'exemple, les recueils de la législation fribourgeoise qui sont gérés à l'aide d'une application de la maison Sitrox et sont conservés sur les infrastructures de celle-ci font régulièrement l'objet d'une copie sur des supports appartenant à l'Etat et permettant leur réutilisation. Le but de cette mesure est de se prémunir contre le risque de perte ou de corruption de ces données. L'article 17d al. 2 n'impose néanmoins pas spécifiquement l'obligation de procéder systématiquement à des copies des données externalisées mais laisse aux autorités compétentes le choix des mesures les mieux adaptées à chaque cas d'espèce.

Art. 17e (nouveau) – Responsabilités

Alinéa 1er – La règle de base en matière d'externalisation est que l'organe qui externalise le traitement de ses données ou la gestion de ses outils informatiques sur les infrastructures d'un sous-traitant reste pleinement responsable de leur pérennité, de leur conservation et de leur exploitation. La disposition énonce un certain nombre de points importants à prendre en considération sous l'angle des responsabilités au moment de procéder à une externalisation. En particulier, l'organe qui confie à un sous-traitant des éléments de son patrimoine informationnel doit choisir ce dernier avec soin, l'instruire sur les tâches à accomplir au moyen d'un contrat suffisamment précis et surveiller qu'il respecte les éléments du contrat. Il doit aussi s'assurer de pouvoir récupérer en tout temps les données et les outils informatiques qui ont été externalisées. Le cas échéant, les contrats existants qui ne respectent pas entièrement ces exigences devront être adaptés dans un délai maximal de cinq ans (cf. art. 21a al. 1 LGCyb).

On peut donner ici, à titre d'exemple, une *check-list* des différents éléments qu'un contrat d'externalisation devrait, selon les circonstances, inclure:

a) l'objet, la nature et la finalité du traitement;
b) les catégories des données traitées et leur degré de confidentialité;
c) l'emplacement des serveurs assurant l'hébergement des données ou des applications;
d) les mesures mises en place afin de garantir la sécurité et la confidentialité des données;
e) les personnes ou les catégories de personnes ayant accès aux données ou aux applications concernées;
f) les droits et les possibilités de contrôle de l'autorité qui procède à l'externalisation, notamment la possibilité d'effectuer des audits sur le site du sous-traitant;

[1] Cf. www.privatim.ch > publications > Mémentos et guides (https://www.privatim.ch/wp-content/uploads/2019/12/privatim_Aide-memoire_Cloud_v2_1_20191217.pdf).

g) l'interdiction faite au sous-traitant de sous-traiter à son tour le traitement de données sans l'accord préalable de l'autorité responsable et la signature d'un contrat d'externalisation posant les mêmes exigences que celui passé entre l'autorité responsable et le sous-traitant;
h) les devoirs d'annonce du sous-traitant en cas d'incident, de perte ou de vol de données;
i) les possibilités de récupérer les données et les applications concernées en cours de contrat;
j) les processus à respecter en cas de résiliation du contrat, en particulier la restitution des données et des applications ainsi que leur destruction ou désinstallation chez le sous-traitant;
k) dans la mesure du possible, l'applicabilité du droit suisse et la désignation d'un for en Suisse en cas de litige.

Ces éléments pourront toutefois évoluer avec le temps et en fonction des types d'externalisation.

Alinéa 2 – Certaines solutions de *cloud computing* ne sont pas limitées à un seul organe d'une collectivité publique mais peuvent s'étendre à plusieurs d'entre eux, voire à tous. Il est évident alors que chaque organe public concerné ne peut pas personnellement s'assurer que le sous-traitant respecte ses engagements. Dans ce cas, le Conseil d'Etat désignera un organe principalement responsable qui fera également office d'interlocuteur principal du sous-traitant.

Alinéa 3 – Au sein de l'administration cantonale, les démarches en matière d'externalisation sont centralisées auprès du SITel qui travaille en étroite collaboration avec les organes concernés. Cette manière de procéder permet de développer une pratique cohérente et autant que possible uniforme. En cas d'externalisation, le SITel veillera donc conjointement avec l'organe public à ce que la réglementation en matière d'externalisation soit respectée, notamment que le contrat d'externalisation contienne les clauses nécessaires dans le domaine de la sécurité. La disposition réserve toutefois le cas des organes publics qui gèrent leur informatique de façon autonome, à l'instar, par exemple, de l'Université, de l'Office de la circulation et de la navigation ou encore de l'Hôpital fribourgeois. Ces organes sont seuls responsables de l'externalisation de leurs données et de leurs outils informatiques.

7.5. Moyen d'identification électronique

Art. 20a (nouveau) – Moyen d'identification électronique (MIE)

Un MIE est un moyen d'identification personnel qui permet à un individu de s'authentifier lorsqu'il veut faire usage d'un service en ligne. Un MIE est constitué d'éléments matériels et/ou immatériels et offre des niveaux de sécurité différents selon sa forme: un identifiant personnel (nom de la personne) et un mot de passe; il peut être complété, le cas échéant, par un SMS, un identifiant biométrique ou une clé USB.

Alinéa 1er – L'accès aux prestations en ligne fournies par une collectivité publique est en principe toujours subordonné à l'utilisation d'un MIE. Des exceptions sont permises dans le but d'offrir certaines prestations ne nécessitant pas une identification garantissant l'identité réelle de la personne.

Alinéa 2 – Tous les MIE ne permettent pas de garantir le même niveau d'identification. Or la délivrance de certaines prestations exige de s'assurer préalablement que le demandeur ou la demanderesse est bien la personne qu'il ou elle prétend être. Pour cela, le MIE utilisé doit passer par un processus d'identification fort impliquant généralement que la personne concernée se présente la première fois physiquement (ou par vidéo-conférence) à une personne certifiée qui va procéder à son identification formelle. Ce type de MIE est actuellement fourni par des prestataires privés qui sont au bénéfice d'une certification par une entreprise accréditée par la Confédération. La disposition permet au Conseil d'Etat d'imposer l'utilisation d'un MIE certifié dans les cas où cela est nécessaire. Le MIE certifié qui sera utilisé à l'échelon du canton sera choisi au terme d'une procédure d'appel d'offre public. Pour que l'accès aux prestations de cyberadministration soit gratuit, les frais d'utilisation du MIE (*login* et conclusion de transactions) seront pris en charge par l'Etat pour les administré-e-s qui utiliseront le MIE choisi par l'Etat de Fribourg.

Alinéa 3 – Les utilisateurs et les utilisatrices d'un MIE certifié doivent se faire identifier formellement afin de garantir de façon la plus sûre possible la preuve de leur identité. Le projet prévoit que l'Etat peut dans ce but instaurer ses propres autorités d'enregistrement et/ou travailler de concert avec les communes dans ce but. Concrètement, il s'agira de former le personnel de certains services cantonaux et des communes partenaires à procéder à l'identification des utilisateurs et des utilisatrices. Cette procédure sera à chaque fois gratuite pour le bénéficiaire. La mise en place des formations destinées à instruire le personnel sera assurée par le canton.

7.6. Dispositions finales

Art. 21a (nouveau) – Droit transitoire

La présente modification apporte des changements qui sont loin d'être anodins dans l'organisation et le fonctionnement de l'Etat. Ces changements sont justifiés par le souci d'avancer dans le domaine de la digitalisation dans un environnement sûr permettant au canton de Fribourg de tirer le meilleur profit des technologies de l'information et de la communication tout en garantissant un niveau de sécurité le plus élevé possible tant du point de vue de l'Etat que des citoyens et citoyennes. L'importance des changements proposés rend néanmoins nécessaire l'introduction d'un délai transitoire pour que les organes concernés puissent s'adapter aux nouvelles exigences qui leur sont fixées et développer les nouveaux outils qui doivent l'être.

Clause finale

Les modifications apportées par la présente révision ne sont pas uniquement importantes sous l'angle matériel; elles le sont aussi sous l'angle formel. Malgré les efforts qui ont été consentis dans le but de conférer à la loi une structure la plus compréhensible possible, l'ampleur des modifications apportées en rend malgré tout la lecture malaisée. Or seule une révision totale de l'acte permettrait de redonner à la loi une nouvelle structure complète. Une telle révision dépasserait néanmoins le cadre et l'objectif de la présente modification. A la place, la clause finale charge les organes responsables des publications officielles de convertir l'ancienne LGCyb en une nouvelle loi entièrement révisée une fois qu'elle aura été adoptée par le Grand Conseil.

8. Adaptations de la LPrD – Commentaires

Art. 3 al. 1 let. d, et e1 et i (nouvelles) – Définitions

> «traitement» (let. d): la définition d'un traitement de données est complétée pour intégrer, en plus des autres formes de traitement mentionnées à titre indicatif, la notion d'hébergement.
> «externalisation» (let. e[1]): la définition reprend celle données dans la LGCyb, qu'elle adapte au contexte particulier de la protection des données personnelles.
> «sous-traitant» (let. i): la définition reprend celle données dans la LGCyb, qu'elle adapte au contexte particulier de la protection des données personnelles.

Art. 12b (nouveau) – Externalisation

La disposition fixe les règles particulières à respecter concernant l'externalisation de données personnelles auprès d'un sous-traitant.

Alinéa 1er – La disposition débute par deux renvois. Le premier renvoi porte sur les règles générales de la LGCyb en matière d'externalisation. L'externalisation de données personnelles constitue une forme qualifiée d'externalisation. Elle doit donc commencer par satisfaire aux exigences générales prévues aux articles 17b à 17e LGCyb, qui s'appliquent à toutes les formes d'externalisation quelles que soient leur nature et leur contenu. Le deuxième renvoi porte sur les règles en matière de sous-traitance (cf. art. 18 LPrD), dont l'externalisation constitue une catégorie particulière.

Alinéa 2: La disposition ajoute un certain nombre d'exigences spécifiques qui sont propres au droit de la protection des données:

> Toute externalisation de données personnelles doit être précédée d'une analyse préalable visant à définir les mesures de sécurité appropriées à mettre en œuvre compte tenu des risques que l'externalisation présente pour la personnalité et les droits fondamentaux des personnes concernées (*let. a*).
> Lorsque l'externalisation porte sur des données sensibles au sens de l'article 3 al. 1 let. c LPrD et qu'elle engendre un risque concret d'atteinte aux des personnes concernées, les mesures de sécurité à mettre en œuvre doivent être égales à celles prévues en cas d'externalisation de secrets (*let. b*). La notion de données sensibles est une notion figée qui ne tient pas compte de l'existence d'un risque réel. Ainsi, par exemple, le simple fait d'être porteur de lunettes entre déjà dans la catégorie des données sensibles liées à la santé. Ce type d'information ne nécessite toutefois pas un besoin de protection accru. Le projet prévoit par conséquent de lier l'externalisation de données sensibles à l'existence d'un risque concret d'atteinte. Ça n'est que lorsque ces deux conditions sont réunies que les mesures de sécurité les plus élevées devront être mises en œuvre. Pour savoir si on est face à un risque concret d'atteinte, on tiendra compte de différents critères tels que le nombre de données sensibles concernées, la finalité du traitement ou encore le contexte dans lequel l'externalisation intervient.
> La localisation des lieux de traitement est un point important en matière d'externalisation car il détermine le droit applicable au traitement des données et, par conséquent, l'ensemble des règles que le sous-traitant est tenu de respecter de par la loi. Le projet prévoit dans ce sens que les lieux de traitement doivent toujours être situés sur le territoire suisse ou sur le territoire d'un Etat dont la législation garantit un niveau de protection équivalent (*let. c*). Pour savoir si un Etat garantit un niveau de protection des données équivalent, le responsable du fichier ira consulter la liste que le PFPDT tient conformément à l'article 6 al. 1 de la loi fédérale sur la protection des données[1].
> En cas d'externalisation de données personnelles, le sous-traitant est soumis au devoir d'informer immédiatement le responsable du fichier pour le cas où il se trouverait confronté à l'obligation de transmettre certaines données à une autorité étrangère. Ce peut être le cas en raison d'une décision de justice mais aussi en application d'une législation étrangère. En particulier, le *Cloud Act* (*Clarifying Lawful Overseas Use of Data Act*) adopté par les Etats-Unis en 2018 permet aux forces de l'ordre américaines de contraindre les fournisseurs de services américains, par mandat ou assignation, à fournir les données demandées stockées sur leurs serveurs, qu'ils soient situés aux États-Unis ou dans des pays étrangers, y com-

[1] Cette liste est consultable à l'adresse Internet suivante: www.edoeb.admin.ch > Protection des données > Commerce et économie > Transmission à l'étranger > Liste des Etats (https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/handel-und-wirtschaft/uebermittlung-ins-ausland.html). A noter qu'avec l'entrée en vigueur de la nouvelle loi fédérale sur la protection des données, la liste des Etats dont la législation assure un niveau de protection équivalent à la Suisse sera tenue directement par le Conseil fédéral (cf. art. 13 al. 1 LPD tel qu'introduit par le projet de loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales [cf. FF 2017 6803]).

pris la Suisse. L'introduction du devoir d'information doit permettre aux responsables de fichier de prendre les mesures nécessaires dans pareille situation, notamment, le cas échéant, de s'adresser à la justice pour empêcher la communication de données par voie de mesures (super-) provisionnelles.

> Le sous-traitant ne peut pas sous-traiter à son tour le traitement qui lui a été confié sans en informer préalablement le responsable du fichier et avoir obtenu son accord. Comme le responsable du fichier conserve la responsabilité de toute la chaîne de sous-traitance, il doit être en mesure d'évaluer les risques en relation avec chaque partenaire concerné.

Alinéa 3 – A l'instar de l'article 17b al. 2 let. b LGCyb, la disposition réserve les cas où l'externalisation équivaut à une délégation de tâche au sens de l'article 54 Cst./Fr. En pareil cas, l'externalisation envisagée devra être prévue au moyen d'une base légale adoptée par le Grand Conseil.

Art. 18 – Sous-traitance

Le changement opéré est d'ordre terminologique. La notion de «traitement sur mandat» est remplacée par celle de «sous-traitance». Des modifications plus substantielles de cette disposition, dont la portée va plus loin que la seule externalisation, pourront être introduites ultérieurement dans le cadre des travaux de révision totale de la LPrD.

Botschaft 2019-CE-239 21. April 2020

—

des Staatsrats an den Grossen Rat zum Gesetzesentwurf zur Anpassung der kantonalen Gesetzgebung an bestimmte Aspekte der Digitalisierung

In Kürze

In diesem Entwurf werden Änderungen des Gesetzes über den E-Government-Schalter des Staates (E-GovSchG) und des Gesetzes über den Datenschutz (DSchG) beantragt.

Das Hauptziel besteht darin, dass gesetzliche Grundlagen geschaffen werden, damit ***Pilotprojekte, die vom Staat im Bereich des Cloud-Computing durchgeführt werden, in die Produktionsphase übergehen können,*** so dass gewisse getestete Tools ***ab Herbst 2020*** implementiert werden können. Diese gesetzlichen Grundlagen sind unter dem Gesichtspunkt des Schutzes von Personendaten notwendig. Auf dieser Ebene hat der Entwurf aus Gründen des Zeitplans einen Vorsprung auf die Arbeiten zur Totalrevision des DSchG, die derzeit im Gang ist, und ist dringend.

Alle Überlegungen, die vor diesem Hintergrund angestellt wurden, führten uns aber dazu, den Entwurf unter einem breiteren Gesichtspunkt zu planen.

Zunächst wurde ***die Auslagerung des Bearbeitens von Daten*** angesichts der Bedeutung, die sie in der Praxis hat, umfassend und nicht nur unter dem Gesichtspunkt des Schutzes der Personendaten geprüft. Die entsprechenden Bestimmungen werden deshalb auf das E-GovSchG (allgemeine Grundsätze) und das DSchG (Ergänzungen zum Schutz der Personendaten) aufgeteilt.

Ausserdem vervollständigt der Entwurf die Bestimmungen des E-GovSchG über das ***kantonale Bezugssystem*** von Daten von Personen, von Organisationen und von Verzeichnissen. Es geht namentlich darum, die systematische Verwendung der AHV-Nummer (AHV-Nr.) in diesem Bezugssystem zu bewilligen, damit die verzeichneten Personen sicher und eindeutig identifiziert werden können. Auch auf dieser Ebene nimmt der Entwurf aus Gründen des Zeitplans künftige Lösungen vorweg. Die systematische Verwendung der AHV-Nr. sollte grundsätzlich demnächst im Bundesrecht erleichtert werden; aber der Entwurf des Bundesrats muss noch in den eidgenössischen Kammern diskutiert werden und wird nicht sofort in Kraft treten. Der Bedarf für das kantonale Bezugssystem ist aber schon jetzt vorhanden, und wenn die Arbeiten nicht verzögert werden sollen, braucht es unbedingt eine kantonale gesetzliche Grundlage, damit die Schaffung des Bezugssystems fortgesetzt werden kann.

Schliesslich werden im Entwurf ***zusätzliche Änderungen und Klärungen des E-GovSchG*** zu verschiedenen Punkten beantragt: Wirkung des Gesetzes für die Gemeinden (Art. 1a und Art. 5); Bearbeiten von Personendaten im vir-

tuellen Schalter (Art. 3a und 9a); Mitwirkung des Kantons beim Verein iGovPortal.ch (Art. 9b); und Verwendung eines Mittels zur elektronischen Identifikation durch die Kantonsverwaltung und die Gemeindeverwaltungen (Art. 20a). Zusammengenommen rechtfertigen alle Änderungen des E-GovSchG dessen Umbenennung (von einem Gesetz über den E-Government-Schalter wird übergegangen zu einem E-Government-Gesetz); ausserdem scheint es angebracht, dieses teilrevidierte Gesetz in ein völlig neu nummeriertes und neu datiertes Gesetz umzuwandeln, damit der Text besser lesbar wird (s. erste Schlussklausel).

1. Allgemeines Umfeld

Vor gut drei Jahren verabschiedete der Grosse Rat das Gesetz vom 2. November 2016 über den E-Government-Schalter des Staates (E-GovSchG; SGF 17.4). Das Ziel bestand darin, die Schaffung und Verwaltung eines virtuellen Schalters als einzigen Zugang zu den verschiedenen Ämtern der Verwaltung auf dem Internet zu regeln und die technischen Voraussetzungen und die allgemeinen Grundsätze des kantonalen E-Government festzulegen.

Seither wurden zahlreiche Arbeiten ausgeführt mit dem Ziel, den Kanton zu modernisieren, die Verwaltungshandlungen für die Bürgerinnen und Bürger einfacher und wirtschaftlicher zu machen und die Effizienz der Verwaltung zu erhöhen. Freiburg hat sich beispielsweise auf nationaler Ebene dadurch ausgezeichnet, dass der Kanton an Innovationsprojekten, mit denen das Ziel verfolgt wird, die Verwaltungsvorgänge online zu erleichtern, mitgewirkt hat[1]. Er ist auch der erste Kanton der Schweiz, der die Ausstellung öffentlicher Zivilstandsurkunden im elektronischen Format anbietet[2].

Die Schaffung eines wirklichen E-Government auf Kantonsebene ist aber ein umfangreiches Projekt, für das der Betrieb und die Organisation der Verwaltung grundsätzlich überdacht werden müssen. Dazu ermöglicht das E-GovSchG ausdrücklich ein Arbeiten mit Pilotprojekten, die vom Staatsrat beschlossen werden, damit schrittweise vorwärtsgegangen werden kann und die formalen gesetzlichen Grundlagen erst dann vorbereitet werden, wenn die betreffenden Einheiten die Lehren aus diesen verschiedenen Projekten gezogen haben, und die entsprechenden Lösungen testen und bestätigen konnten (s. Art. 20 E-GovSchG). Mit dieser Arbeitsweise kann der Kanton Freiburg mit der elektronischen Umgestaltung so vorsichtig und weitblickend wie möglich weiterfahren.

Dieser Entwurf liegt also in der Linie von zwei experimentellen Verordnungen, die der Staatsrat seit dem Inkrafttreten des E-GovschG erlassen hat:

> Mit der ersten experimentellen Verordnung, die vier Pilotprojekte umfasst, wurde das Ziel verfolgt, zu beobachten, welche technische Möglichkeiten und Sicherheitsanforderungen es beim Auslagern des Bearbeitens von Personendaten in die *Cloud* unbedingt braucht. Die daraus gezogenen Lehren ermöglichen dem Staatsrat, die geeigneten gesetzlichen Bestimmungen zu beantragen, um diese Technologie in einem möglichst angemessenen und sicheren Umfeld in grösserem Umfang zu nutzen. Diese Bestimmungen sollten ursprünglich vor dem Hintergrund der Totalrevision des DSchG, die seit einiger Zeit vorbereitet wird, eingeführt werden. Diese Totalrevision ist jedoch ein Projekt von grosser Tragweite, und seine Ausarbeitung nimmt wahrscheinlich noch viel Zeit in Anspruch, wenn die Arbeiten zur Revision des Bundesgesetzes über den Datenschutz zum Vergleich herangezogen werden. Es ist aber wichtig, dass bei diesen verschiedenen Projekten des Cloud-Computing schnell von der Pilotphase zur Produktionsphase übergegangen werden kann; es ist sogar wesentlich für das Projekt «Kollaborative Office-Tools Microsoft 365», das *ab Herbst 2020* in allen Schulen des Kantons hätte implementiert werden sollen und dessen Umsetzung nun aufgrund der Coronaviruskrise und des Bedarfs der Schülerinnen und Schüler für die Arbeit zuhause vorgezogen werden musste. Ausserdem machte sich auch das Bedürfnis, allgemeine Bestimmungen über die Auslagerung von elektronischen Bearbeitungen ausserhalb des Datenschutzbereichs zu erlassen, bemerkbar. Angesichts der Bedeutung, welche die Auslagerung von Informatiklösungen in der Organisation der Verwaltung erlangt, ist es gerechtfertigt, die allgemeinen Vorschriften auf diesem Gebiet auf Gesetzesstufe zu verankern. Im Entwurf wird beantragt, dieses Problem der Auslagerung im E-GovSchG und im derzeitigen Text des DSchG zu lösen, ohne auf die Totalrevision dieses Gesetzes zu warten.
> In der zweiten experimentellen Verordnung wird die Schaffung des kantonalen Bezugssystems von Daten von Personen, von Organisationen und von Verzeichnissen geregelt. Das Projekt läuft derzeit immer noch und dürfte bis in den Sommer 2021 fortgesetzt werden. Die bis jetzt ausgeführten Arbeiten haben hingegen gezeigt, dass es seine Ziele nicht erreichen kann, wenn im kantonalen Bezugssystem nicht systematisch die AHV-Nr. verwendet werden darf, um Personen sicher und eindeutig zu identifizieren. Beim jetzigen Stand der Bundesgesetzgebung muss der Kanton für eine solche Nutzung der AHV-Nr. eine entsprechende formale gesetzliche Grundlage erlassen. Im Entwurf werden deshalb die Bestimmungen des E-GovSchG über das kantonale Bezugssystem in diesem Sinn ergänzt. Auf Bundesebene wird derzeit ein Entwurf

[1] https://www.egovernment.ch/de/umsetzung/innovationen/innovationen-20182019/.

[2] https://www.fr.ch/de/ilfd/alltag/vorgehen-und-dokumente/schweizer-premiere-elektronische-oeffentliche-zivilstandsurkunden.

zur Änderung des Bundesgesetzes über die Alters- und Hinterlassenenversicherung, mit der die systematische Verwendung der AHV-Nr. durch die Behörden erlaubt werden soll, in den Kammern diskutiert (Botschaft 19.057 und Entwurf vom 30. Oktober 2019, *BBl 2019 7359* und 7397). Aber für die Verabschiedung braucht es noch Zeit, und wenn man wartet, bis die Änderung in Kraft tritt, werden die Arbeiten am Bezugssystem unnötig verzögert.

2. Inhalt des Entwurfs

Mit dem Entwurf werden in der kantonalen Gesetzgebung (E-GovSchG und DSchG) die nötigen gesetzlichen Grundlagen für die Auslagerung des Bearbeitens von Daten an Dritte geschaffen (§ 2.1) und die Bestimmungen des E-GovSchG über das Bezugssystem ergänzt, indem namentlich die systematische Verwendung der AHV-Nr. darin gestattet wird (§ 2.2). Ausserdem wird das E-GovSchG in weiteren Punkten ergänzt und in ein wirkliches Gesetz über das E-Government umgewandelt, um die laufenden und die künftigen Arbeiten im Bereich der Digitalisierung der Verwaltung zu begleiten (§ 2.3).

2.1. Auslagerung des Bearbeitens von Daten und von Informatiktools

Die Inanspruchnahme der Auslagerung und insbesondere in die *Cloud* bildet eine Antwort auf die neuen Anforderungen beim Betrieb und bei der Organisation des Staates, die Folgen der Einführung der digitalen Technologien in der Gesellschaft sind: explosionsartige Zunahme der Menge an produzierten und verwendeten Daten, hohe Anforderungen an Verfügbarkeit und Sicherheit, Absicht der Organe des Staates, sich auf den Kern ihrer Tätigkeit zu konzentrieren und gewisse Handlungen, die nicht unter ihren Fachbereich fallen, nicht mehr auszuführen, Bedarf an neuen Mitteln für den mobilen Zugriff auf die Dienstleistungen, überall, jederzeit und von jedem Endgerät aus.

Es ist jedoch wahr, dass für die Nutzung solcher Dienstleistungen Vorsichtsmassnahmen, die den Umständen und den damit verbundenen Risiken angemessen sind, getroffen werden müssen. Deswegen hat der Staatsrat, bevor er die Auslagerung von Daten in grossem Stil bewilligt, zunächst die Verordnung vom 4. Dezember 2018 über die Bewilligung für das Amt für Informatik und Telekommunikation zur Auslagerung der Bearbeitung gewisser Daten in die «Cloud» (Pilotprojekte) (SGF 17.42) erlassen. Ursprünglich sollten mit dieser Verordnung bis Ende 2020 vier gezielte Cloud-Lösungen getestet werden, ferner sollte erforscht werden, welche technischen Möglichkeiten, namentlich im Bereich der Sicherheit, geschaffen werden müssen. Schon im Herbst des vergangenen Jahres waren die Ergebnisse des Projekts, die besonders die Lösung «Kollaborative Office-Tools Microsoft 365» betrafen, Gegenstand eines Evaluationsberichts des Amts für Informatik und Telekommunikation (ITA), der im November 2019 dem Staatsrat unterbreitet wurde. Dieser Bericht gelangt namentlich zu folgenden Schlussfolgerungen:

> «das Deployment in den Einheiten, die im Pilotprojekt eingeschlossen wurden, ist ein Erfolg, und […] diese Operation ist geschafft. Ausserdem wurden Antworten auf die Sorgen der ÖDSB [*Behörde für Öffentlichkeit und Datenschutz*] gegeben und sogar mit zusätzlichen Massnahmen ergänzt».
> «Die Erfahrungen, die allein mit diesem Projekt gemacht wurden, sind überzeugend genug, damit der Staatsrat dem Grossen Rat den Erlass der nötigen formalen gesetzlichen Grundlagen für die allgemeine Auslagerung des Bearbeitens von Personendaten, auch von besonders schützenswerten, (in die «Cloud») beantragen kann».

So ist der Staatsrat der Meinung, dass er aufgrund der mit Microsoft 365 gemachten Erfahrungen über genügend überzeugende Rückmeldungen verfügt, um dem Grossen Rat zu beantragen, die formalen gesetzlichen Grundlagen zu verabschieden. Indem die Erfahrungen, die während der Pilotphase durchgeführt wurden, berücksichtigt werden, wird mit dem Entwurf ein rechtlicher Rahmen geschaffen, mit dem man in der Lage ist, die Nutzung der neuen Tools bei Gemeinwesen in einer möglichst geeigneten und gesicherten Umgebung zu unterstützen. Es ist aber wesentlich, dass diese Bestimmungen schnell in Kraft treten, denn zwei Anwendungen, die derzeit im Unterrichtsbereich verwendet werden, stehen nach Schuljahresbeginn 2020 nicht mehr zur Verfügung. Sie sollen eben mit dem Übergang auf die Lösung Microsoft 365 ersetzt werden. Deshalb wird dieser Teil des Projekts getrennt vom Rest der Totalrevision des DSchG unterbreitet.

Die verschiedenen Sicherheitsmassnahmen, die im Gesetz gefordert werden, nehmen insbesondere die Empfehlungen der Konferenz der schweizerischen Datenschutzbeauftragen (PRIVATIM) auf[1]. Da aber sowohl Personendaten als auch nicht personenbezogene Daten oder Informatiktools betroffen sein können, wenn zu *Cloud*-Lösungen gegriffen wird, werden die Massnahmen zwischen dem E-GovSchG und dem DSchG aufgeteilt: Die Bestimmungen, die in den Artikeln 17b–17f E-GovSchG eingeführt werden, bilden den Mindestrahmen, der bei allen Auslagerungen, sogar, wenn sie das Bearbeiten von Personendaten betreffen, eingehalten werden muss; in letzterem Fall muss das verantwortliche Organ ausserdem dafür sorgen, dass zudem die Spezialbestimmungen der Gesetzgebung über den Datenschutz eingehalten werden (Art. 12b DSchG).

[1] PRIVATIM, *Merkblatt «Cloud-spezifische Risiken und Massnahmen»,* Version 2.1 vom 17. Dezember 2019. Der Text kann unter folgender Adresse heruntergeladen werden: https://www.privatim.ch/wp-content/uploads/2019/12/privatim-Cloud-Papier_v2_1_20191217.pdf.

Es sei noch darauf hingewiesen, dass die Schaffung eines geeigneten gesetzlichen Rahmens für die Nutzung von *Cloud*-Lösungen einem Ziel des «Massnahmenkatalogs zur Cloud Computing Strategie der Schweizer Behörden 2012–2020» (Stossrichtung S2: Anpassung der rechtlichen Grundlagen) entspricht[1]. Im Richtplan der Digitalisierung und der Informationssysteme für die Legislaturperiode 2017–2021, der die strategischen Ausrichtungen des Regierungsprogramms im Bereich der Digitalisierung und der Informationssysteme angibt und vervollständigt, wird die Schaffung der Cloud für den Betrieb des Staates vorgesehen. Mit den beantragten Bestimmungen verwirklicht der Kanton Freiburg also ein Ziel, das vom Bund und von der Konferenz der Kantonsregierungen für den betreffenden Zeitraum festgelegt wurde.

2.2. Systematische Verwendung der AHV-Nummer sowie der UID- und der BUR-Nummer im kantonalen Bezugssystem

Am 24. Juni 2019 erliess der Staatsrat gestützt auf Artikel 21 E-GovSchG eine Experimentalverordnung über das kantonale Bezugssystem von Daten von Personen, von Organisationen und von Verzeichnissen (Pilotprojekte) (SGF 17.45). Mit dieser Verordnung sollen die Artikel 13 Abs. 1 Bst. b, 15 und 16 E-GovSchG umgesetzt werden; in diesen Artikeln wird die Schaffung einer Informatikplattform, mit der ein zentrales Datenbezugssystem verwaltet wird, vorgesehen. Sie wird nach der Pilotphase durch ein Gesetz im formellen Sinn ersetzt.

Als der Staatsrat 2016 den Entwurf des E-GovSchG beantragte, hat er darauf verzichtet, systematisch die AHV-Nr. als persönliche User-ID zu verwenden und zog es stattdessen vor, eine kantonale Identifikationsnummer zu schaffen. Die bis jetzt durchgeführten Experimente zeigten jedoch den Bedarf, neben der kantonalen Identifikationsnummer die AHV-Nr. bearbeiten zu können. Einerseits kann mit der AHV-Nr. namentlich die Mehrheit der Schlichtungsprobleme im Zusammenhang mit der Identifizierung der Personen oder infolge von fehlenden oder uneinheitlichen Informationen gelöst werden. Andererseits ist sie auch wesentlich für gewisse Formen des Datenaustauschs mit anderen Behörden, namentlich, wenn sie sich ausserhalb des Kantons Freiburg befinden.

In Anwendung von Artikel 50e Abs. 3 des Gesetzes vom 20. Dezember 1946 über die Alters- und Hinterlassenenversicherung (AHVG; SR 831.10), dürfen kantonale Organe ausserhalb der Sozialversicherung nur dann systematisch die AHV-Nr. verwenden, wenn vom Grossen Rat eine entsprechende gesetzliche Grundlage verabschiedet wird; darin werden das Organ, das ermächtigt wird, systematisch die AHV-Nr. zu bearbeiten, und der Zweck des Bearbeitens angegeben. Ein Entwurf zur Änderung dieser Regelung wird aber derzeit auf Bundesebene geprüft; das Ziel besteht darin, dass die verschiedenen Organe des Bundes, der Kantone und der Gemeinden allgemein ermächtigt werden, systematisch die AHV-Nr. zu verwenden, um ihre Aufgaben zu erfüllen. Wenn dieser Gesetzesentwurf angenommen würde, wäre eine spezifische gesetzliche Grundlage nicht mehr nötig, aber besondere Sicherheitsmassnahmen müssten getroffen werden[2].

Mit der beantragten Regelung entspricht der Entwurf den derzeit geltenden Bestimmungen und nimmt den Erlass künftiger gesetzlicher Grundlagen, die zurzeit geprüft werden, vorweg. Gemäss den Artikeln 15–15b und 17b des Entwurfs ist die Behörde, die mit dem kantonalen Bezugssystem beauftragt ist, ermächtigt, systematisch die AHV-Nr. zu verwenden, um die verzeichneten Personen sicher und eindeutig zu identifizieren. Jegliche andere Verwendung bleibt hingegen untersagt. Es ist insbesondere nicht erlaubt, sie als Mittel zur Zuordnung von Daten, mit der gewisse persönliche Eigenschaften der Bürgerinnen und Bürger beurteilt oder Nachforschungen namentlich zur Identifizierung von Personen in regelwidriger Situation angestellt werden können, zu verwenden. Für eine solche Verwendung der AHV-Nr. und des kantonalen Bezugssystems müsste der Grosse Rat obligatorisch ein Spezialgesetz erlassen.

Unter dem Sicherheitsaspekt wird in Artikel 15b gesagt, dass für die systematische Verwendung der AHV-Nr. organisatorische und technische Massnahmen getroffen werden müssen, damit jeglichem Missbrauch vorgebeugt wird. Anders als im Vorentwurf wird im Entwurf darauf verzichtet, die Pflicht, die AHV-Nr. in einer anderen Datenbank als den Datenbanken der übrigen Daten aufzubewahren, festzuhalten. In der Vernehmlassung wurden Stimmen laut, die sich beklagten, dass diese Massnahme unangemessen, unverhältnismässig und mühsam sei. Stattdessen richtet sich der Entwurf mit einem Verweis nach den geplanten Sicherheitsvorschriften im Entwurf des Bundesrates zur Änderung des AHVG (s. die Artikel 153d und 153e des Entwurfs des Bundesrats).

Neben den Bestimmungen zur AHV-Nr. werden in den Artikeln 16–16b des Entwurfs ähnliche Vorschriften eingeführt, um die systematische Verwendung der UID- und der BUR-Nummer, die bei den juristischen Personen das Gegenstück zur AHV-Nr. bilden, zu bewilligen.

2.3. Übrige Änderungen

Im Entwurf wird das E-GovSchG auch in einigen Punkten angepasst, wobei die Lehren aus der ersten Fassung gezogen und einige Änderungen, die seit seinem Erlass eingetreten sind, berücksichtigt werden.

[1] Egovernement Schweiz, *Massnahmenkatalog zur Cloud Computing Strategie der Schweizer Behörden* 2012–2020, 25. Oktober 2012 (https://www.egovernment.ch/de/umsetzung/e-government-schweiz-2008–2015/cloud-computing-schweiz/).

[2] S. BBl 2019 7397 (Gesetzesentwurf) und BBl 2019 7359 (Botschaft).

- Die Frage der Anwendung des Gesetzes auf die Gemeinden wird geklärt, dadurch können diese unter den gleichen Voraussetzungen wie die kantonalen Organe die Auslagerung zuhilfenehmen (Art. 1a).
- Die Anforderung der freien und aufgeklärten Einwilligung der betroffenen Person, damit der virtuelle Schalter die nötigen Personendaten für das Erbringen der Leistung oder der gewünschten Dienstleistung beschaffen und der Dienststelle, die zuständig ist, das Gesuch zu behandeln, übermitteln darf, wird eingeführt (Art. 3a).
- Auch der Grundsatz des standardmässigen Datenschutzes (*privacy by default*) beim Betrieb des virtuellen Schalters wird eingeführt, wobei die Möglichkeit für die Benützerinnen und Benützer, einem erweiterten Bearbeiten ihrer Daten zuzustimmen, vorbehalten bleibt (Art. 9a).
- Der Staatsrat darf interkantonalen Fachorganisationen im Bereich des E-Government, die eine Verbindung zum virtuellen Schalter haben, beitreten; damit wird die Mitwirkung des Kantons Freiburg beim Verein iGovPortal.ch formalisiert (Art. 9b).
- Die Frage der Verwendung eines elektronischen Identifizierungsmittels (EIM), um sicher und gesichert auf die verschiedenen Plattformen, die von den Gemeinwesen verwendet werden, zuzugreifen und dort Geschäfte abzuschliessen, wird geregelt (Art. 20a).
- Die Struktur des E-GovSchG wird teilweise neugestaltet, damit es künftig seine Rolle als allgemeines und Querschnittsgesetz im Bereich des E-Government spielen kann; es heisst neu E-Government-Gesetz (E-GovG). Diese Umstrukturierungsarbeiten werden aber in einem zweiten Schritt vollständig abgeschlossen, wenn das Amt, das für die Veröffentlichungen zuständig ist, den Text ganz überarbeitet hat.

3. Ablauf der Arbeiten

Im Herbst 2019 bildete die Staatskanzlei mit Unterstützung der Finanzdirektion (FIND) eine Arbeitsgruppe zur Anpassung der kantonalen Gesetzgebung an bestimmte Aspekte der Digitalisierung. Ihr gehörten eine Vertreterin der FIND, die Datenschutzbeauftragte und Vertreter des Amtes für Gesetzgebung an.

Im Dezember 2019 schickte der Staatsrat gleichzeitig zwei Vorentwürfe, die eng miteinander verbunden waren, in die Vernehmlassung: den Vorentwurf der Totalrevision des Gesetzes über den Datenschutz und den Vorentwurf zur Anpassung der kantonalen Gesetzgebung an gewisse Aspekte der Digitalisierung. Die Zeit der Vernehmlassung für den zweiten Entwurf war hingegen kürzer, denn es brauchte schnell Änderungen der geltenden Gesetzgebung über die Auslagerung und die Arbeiten zur Schaffung des kantonalen Bezugssystems. Er war vom 3. Dezember 2019 bis 31. Januar 2020 in der Vernehmlassung.

Der Vorentwurf wurde im Allgemeinen gut aufgenommen. Fast alle Vernehmlassungsteilnehmer unterstützen die beantragten Änderungen und sind der Meinung, dass sie einem wirklichen Bedürfnis entsprechen. Dennoch haben einige Teilnehmer ihre Sorgen darüber geäussert, dass die Datensicherheit auch wirklich gewährleistet ist und keine Gefahr besteht, dass die AHV-Nr. missbräuchlich verwendet wird. Sie haben in diesem Sinn manchmal gefordert, dass zusätzliche Vorschriften angefügt werden, um das Sicherheitsniveau zu erhöhen. Nur die ÖDSB lehnt den Entwurf insgesamt ab, aber eher aus formalen als aus materiellen Gründen (s. § 6 unten).

Unter den geäusserten Vorwürfen befanden sich einige Stimmen, welche die Aufbewahrung der AHV-Nr. in einer separaten, von den anderen Daten getrennten Datenbank kritisierten; sie fanden dieses Vorgehen unangemessen und unverhältnismässig. Andere haben auf eine Verwechslungsgefahr zwischen einigen verwendeten Begriffen (namentlich: «Bearbeiten», «Hosting», «Auslagerung») hingewiesen und die Verwendung einer klareren und einheitlicheren Terminologie verlangt.

Bei den Schlussarbeiten am Text wurden die Rückmeldungen aus der Vernehmlassung weitgehend berücksichtigt. Einerseits wurden die Bestimmungen über die Datensicherheit und den Datenschutz bei einer Auslagerung ergänzt und verbessert und gleichzeitig systematischer ins E-GovSchG und ins DSchG eingefügt. Andererseits wird im Entwurf darauf verzichtet, vorzuschreiben, dass die AHV-Nr. in einer von den anderen Daten getrennten Datenbank aufbewahrt werden muss. Die Sicherheitsmassnahmen, die getroffen werden müssen, entsprechen denjenigen, die im Entwurf des Bundesrats vorgesehen sind, ohne dass sie darüber hinaus gehen. Schliesslich wurden Anstrengungen unternommen, um die verwendete Terminologie zu vereinheitlichen und systematischer zu gestalten. Die eingeführten Definitionen wurden zu diesem Zweck genauer formuliert und mit dem Hinzufügen neuer Definitionen ergänzt, so dass das Verhältnis zwischen Bearbeiten, Hosting, Auslagerung, Verantwortlicher der Datensammlung und Auftragsbearbeiter besser verstanden werden kann.

4. Folgen des Entwurfs

4.1. Finanzielle und personelle Folgen

Die finanziellen Folgen des Entwurfs rühren hauptsächlich vom Bedürfnis her, ein sicheres und gesichertes Elektronisches Identifizierungsmittel (EIM) zu verwenden. Um die Entwicklung des E-Government auf Kantonsebene zu fördern, will der Staatsrat, dass die Benutzung des virtuellen Schalters und weiterer Plattformen, die angeboten werden, vollkommen gratis ist. Das hat zur Folge, dass der Kanton die Kosten im Zusammenhang mit den Mitteln für den

Zugriff auf diese Dienstleistungen und für den Abschluss von Geschäften über diese Dienstleistungen übernimmt.

Um das höchstmögliche Sicherheitsniveau sicherstellen zu können, erachtet es der Staatsrat als wesentlich, dass eine Lösung, die sich auf dem Markt befindet und über eine Zertifizierung im Sinne des Bundesgesetzes über das elektronische Patientendossier (EPDG; SR 816.1) und, wenn es angenommen wird, des künftigen Bundesgesetzes über elektronische Identifizierungsdienste (BGEID) verfügt, angeschafft wird. Aufgrund einer Kostenschätzung belaufen sich die Ausgaben im Zusammenhang mit der Einführung eines EIM auf Kantonsebene auf 2,5 Mio. Franken über einen Zeitraum von fünf Jahren. In diesem Betrag sind die Kosten für die Verwendung des EIM eingeschlossen, und die Zahl der Benützerinnen und Benützer und der geplanten Geschäfte werden berücksichtigt; hingegen schliesst dieser Betrag die Einrichtung und den Betrieb der Registrierung des EIM, mit denen bereits bestehende Behörden beauftragt werden, nicht ein.

Im Übrigen beschränkt sich der Entwurf darauf, gewisse Elemente zum virtuellen Schalter und zum kantonalen Bezugssystem zu präzisieren und zu ergänzen und einen gesetzlichen Rahmen für die Auslagerung von Daten und Informatiktools festzulegen. Daher hat er keine direkten neuen Ausgaben und keinen neuen Personalbedarf zur Folge. Die Ausgaben, welche die Folge der Auslagerung von Daten oder von Informatikanwendungen sind, hängen von den künftigen Projekten ab, die in diesem Bereich von den zuständigen Organen beschlossen werden.

Trotz allem kann darauf hingewiesen werden, dass sich unabhängig von diesem Entwurf ein Bedarf der FIND oder des ITA an einer spezialisierten Juristin oder einem spezialisierten Juristen im Recht der neuen Technologien immer mehr bemerkbar macht. Zurzeit überträgt der Staat einige Aufträge in diesem Bereich an externe Personen. Auf finanzieller Ebene würde es nicht unbedingt mehr kosten, wenn man eine Person hätte, welche diese Fragen intern behandelt. Das Problem wird später im Rahmen der Zuteilung der neuen Stellen beim Staat ohnehin erneut diskutiert.

4.2. Folgen für das Verhältnis zwischen Staat und Gemeinden

Im Rahmen der Arbeiten im Zusammenhang mit der Digitalisierung der Gemeinwesen sind die Folgen für das Verhältnis zwischen Staat und Gemeinden naturgemäss schwer vorherzusagen. Die Digitalisierung ist eine unumgängliche Etappe in der Entwicklung sowohl der Staatsverwaltung als auch der Gemeindeverwaltungen. Mit den beantragten Änderungen können die Gemeinden im selben Mass Auslagerungen machen, wie das auch für die kantonalen Organe geplant ist. Bei den Arbeiten zur Schaffung des kantonalen Bezugssystems wird alles unternommen, um die Gemeinden nach und nach und auf der Grundlage von Vereinbarungen mit ihnen miteinzubeziehen. Im Entwurf wird dem Staat ausserdem die Möglichkeit gegeben, bei der Identifizierung der Inhaberinnen und Inhaber von EIM mit den Gemeinden zusammenzuarbeiten und Registrierungsbehörde zu werden. Das wird Gegenstand späterer Diskussionen sein. Schliesslich werden sich die konkreten Folgen für das Verhältnis zwischen Staat und Gemeinden je nach Fortschritt der Projekte, die durchgeführt werden und an denen die Gemeinden mitmachen wollen, langsam abzeichnen. Etwas ist aber sicher: Eine wirksame Digitalisierung der öffentlichen Leistungen im Kanton Freiburg setzt eine verstärkte Zusammenarbeit von Gemeinden und Staat voraus. Die Diskussionen haben begonnen und müssen noch konkreter werden.

5. Übereinstimmung mit dem übergeordneten Recht

Im Entwurf werden Fragen der Organisation und des Datenschutzes behandelt, für die grundsätzlich kantonales Recht gilt. In diesen Bereichen müssen insbesondere Artikel 12 Abs. 2 KV, in dem das Recht auf den Schutz der Personendaten garantiert wird, und auch Artikel 54 KV, in dem die Frage der gesetzlich vorgesehenen Delegation öffentlicher Aufgaben an Dritte behandelt wird, berücksichtigt werden. Im Entwurf wird eine Reihe von Massnahmen vorgesehen, mit denen sichergestellt werden soll, dass die beiden Bestimmungen eingehalten werden.

Im Entwurf wird auch die Frage der systematischen Verwendung der AHV-Nummer im Rahmen des kantonalen Bezugssystems behandelt. Die Voraussetzungen für eine solche Verwendung ausserhalb des Sozialversicherungsbereichs durch die Kantone werden bis jetzt in Artikel 50e Abs. 3 AHVG festgehalten. Die Bestimmungen des Entwurfs entsprechen den Anforderungen des Bundesrechts. Sie nehmen ausserdem das Inkrafttreten der neuen Bestimmungen in diesem Bereich, die derzeit auf Bundesebene diskutiert werden, vorweg.

6. Stellungnahme der Kantonalen Behörde für Öffentlichkeit und Datenschutz (ÖDSB)

Während der Vorbereitungsarbeiten gab die ÖDSB an, dass sie dagegen sei, dass die Bestimmungen über die Auslagerung von Personendaten vorzeitig in Kraft gesetzt werden, ohne dass sie deren Inhalt ablehnte. Sie ist der Meinung, dass es nicht angebracht sei, das DSchG «tranchenweise» zu revidieren, denn der Entwurf der Totalrevision bilde eine Einheit und deshalb gebe es keinen Grund, bestimmte in ihm enthaltene Bestimmungen vorzeitig in Kraft treten zu lassen. Sie hat diesen Standpunkt in der Vernehmlassung wiederholt.

Bei der systematischen Verwendung der AHV-Nr. im Rahmen des kantonalen Bezugssystems hat die ÖDSB nie einen Hehl daraus gemacht, dass sie dieser Verwendung gegenüber

skeptisch gegenüber stehe, auch wenn die Möglichkeiten einer solchen Verwendung bei einer Revision des Bundesrechts ausgeweitet würden. In der Vernehmlassung hat die ÖDSB ihren Standpunkt zu diesem Thema beibehalten. Sie hat aber angefügt, dass sie der Meinung sei, dass die AHV-Nr. unbedingt in einer von den anderen bearbeiteten Daten getrennten Datenbank gespeichert werden sollte, wenn die systematische Verwendung der AHV-Nr. entgegen ihrer Auffassung beibehalten werde.

Wie bereits erwähnt hat der Bundesrat am 30. Oktober 2019 einen Entwurf zur Änderung des AHVG im Sinne der systematischen Verwendung der AHV-Nr. verabschiedet. Laut diesem Entwurf können die Kantone und die Gemeinden die AHV-Nummer systematisch verwenden, ohne dass sie dazu eine besondere gesetzliche Grundlage erlassen müssen. Selbst wenn diese Bestimmungen nicht erlassen werden sollten, könnte das kantonale Bezugssystem wahrscheinlich ohnehin in einem bis zwei Jahren die AHV-Nr. systematisch bearbeiten. Mit einer solchen Frist würden die Arbeiten zur Schaffung des kantonalen Bezugssystems aber beträchtlich verzögert, was eine nicht vernachlässigbare Auswirkung auf den Betrieb der Verwaltung und auf die Kosten hätte.

7. Anpassungen des E-GovSchG – Kommentare

7.1. Allgemeine Bestimmungen

Art. 1a (neu) – Gültigkeit für die Gemeinden

Auf Verlangen des Freiburger Gemeindeverbands wurde eine Bestimmung eingeführt, um die Gültigkeit der Bestimmungen des E-GovSchG für die Gemeinden zu klären. In der beantragten Bestimmung gibt es aber nicht unbedingt eine materielle Änderung. Ausser dem Fall der Auslagerung wird nur übernommen, was bereits im derzeitigen Artikel 5 Abs. 1 E-GovSchG vorgesehen ist. Dass diese Bestimmung an den Anfang des Erlasses verschoben wurde, dürfte aber das allgemeine Verständnis für die Gemeinden vereinfachen.

Im Entwurf wird somit die Grundidee, gemäss der die Mitwirkung der Gemeinden möglichst auf freiwilliger und kollaborativer Basis stattfinden sollte, beibehalten. Dank dieser Arbeitsweise können diese sich den Arbeiten der Kantonsverwaltung nach einem Rhythmus, der ihren Bedürfnissen und ihren Ressourcen angemessen ist, anschliessen. Das Hauptinstrument dieser Mitarbeit ist deshalb viel mehr eine Vereinbarung zwischen dem Staat und jeder Gemeinde als der Erlass von festen Vorschriften im Gesetz.

Art. 2 Bst. f, g und h (neu) – Terminologie

> «E-Government» (*Bst. f*): Die Definition des «E-Government» entspricht in kurzer Form denjenigen in der schweizerischen[1] und in der freiburgischen[2] E-Government-Strategie. Sie dient dazu hervorzuheben, dass das E-Government nicht nur die Lieferung von Leistungen für die Bevölkerung in elektronischer Form betrifft (*Front Office*), sondern auch die Veränderungen bei der Organisation und beim internen Betrieb des Staates umfasst (*Back Office*).
> «Auslagerung» (*Bst. g*): Mit der Definition sollen alle Dienstleistungsmodelle, die online über ein Computernetzwerk (*Cloud oder Cloud-Computing)* zugänglich sind, abgedeckt werden. «Diese Modelle gehen vom einfachen Hosting bis zur Nutzung von Systemen und Informatiklösungen online (*Infrastructure-as-a-Service/IaaS, Platform-as-a-Service/PaaS, Software-as-a-Service/SaaS)*». All diesen Modellen ist gemeinsam, dass der ausgelagerte Gegenstand nicht mehr lokal beim verantwortlichen Organ, sondern bei einem Auftragsbearbeiter bearbeitet wird.
> «*Auftragsbearbeiter*» (*Bst. h*): Die Definition schliesst alle Personen und Organisationen, die für eine Behörde Daten bearbeiten und Informatiktools verwalten, ein; dazu gehören auch, aber nicht nur, die *Cloud*-Dienstleister. Innerhalb desselben Gemeinwesens wird die Übertragung des Bearbeitens von Daten und der Verwaltung von Informatiktools an eine zentrale Dienststelle, wie das beispielsweise für das ITA gilt, aber nicht als Auftragsbearbeitung betrachtet.

7.2. Virtueller Schalter

Art. 3a (neu) – Bearbeiten von Personendaten

Absatz 1 – Insofern als die Spezialgesetze, in denen das Bearbeiten von Personendaten bewilligt wird, nur für die Organe des Staates, auf die sie verweisen, gelten, kann sich der E-Government-Schalter nicht darauf berufen, um die nötigen Daten zur Erbringung der Leistung oder der gewünschten Dienstleistung zu bearbeiten. Deshalb wird die Person ersucht, ihre Einwilligung zu geben, damit der E-Government-Schalter bei ihr die nötigen Daten für das Bearbeiten ihres Gesuchs beschaffen und sie dem dafür zuständigen Organ bekanntgeben kann.

In der Bestimmung werden die Voraussetzungen für die Gültigkeit der Einwilligung, die insbesondere frei und aufgeklärt erfolgen muss, angegeben. In diesen Voraussetzungen

[1] E-Government Strategie Schweiz vom 1. Mai 2017, S. 2 (das Dokument kann unter dem folgenden Link heruntergeladen werden: https://www.egovernment.ch/de/umsetzung/e-government-strategie/).

[2] E-Governement-Strategie des Staates Freiburg vom 2. Dezember 2014, S. 4 (das Dokument kann unter dem folgenden Link heruntergeladen werden: https://www.fr.ch/sites/default/files/contens/cha/_www/files/pdf70/de_DIV_strategie_cyberadministration_web.pdf),

ist die spezifische und eindeutige Natur der Zustimmung, die deswegen in der Gesetzesbestimmung nicht ausdrücklich erwähnt werden muss, eingeschlossen.

Beim E-Government-Schalter bedeutet die Voraussetzung der freien Einwilligung, dass der Person, die ein gewisses Bearbeiten von Daten ablehnt, kein anderer Nachteil entstehen darf, als dass sie zum physischen Schalter gehen oder ihr Gesuch per Post einreichen muss. Dennoch bleiben die Fälle, in denen die Durchführung gewisser Verfahren in elektronischer Form gesetzlich vorgeschrieben wird, vorbehalten; das gilt heute beispielsweise für die Baubewilligungsgesuche, die mit der Anwendung FRIAC behandelt werden (s. Art. 135a des Raumplanungs- und Baugesetzes vom 2. Dezember 2008 [RPBG; SGF 710.1]).

Die aufgeklärte Einwilligung ist grundsätzlich gegeben, wenn die Person über die Organe des Staates und allfällige dritte Dienstanbieter, die an der Erbringung der Leistung oder der gewünschten Dienstleistung mitwirken, die Daten, die in diesem Rahmen bekanntgegeben werden, und den Zweck des Bearbeitens informiert wurde. Es sei darauf hingewiesen, dass die Einwilligung nicht für irgendwelche Daten gelten kann. Gemäss dem Verhältnismässigkeitsprinzip und dem Grundsatz der Zweckbindung müssen die Daten, die dank der Einwilligung beschafft werden, notwendigerweise auf die unbedingt nötigen Daten für das Erbringen der gewünschten Leistung beschränkt werden.

Absatz 2 – In der Bestimmung wird angegeben, dass die Einwilligung widerrufen werden kann und die Person so die Kontrolle über die Verwendung ihrer Daten behält.

Absatz 3 – Gemäss den Anforderungen des Datenschutzrechts muss das Organ, das aufgrund der Einwilligung der Person Daten bearbeitet, bei einer Kontrolle in der Lage sein, zu beweisen, dass diese tatsächlich ihre Einwilligung gegeben hat. Diese Anforderung hat zur Folge, dass bei der Verwaltung ein Modul zum Management der Einwilligung geschaffen werden muss. In Artikel 21a Abs. 2 des Entwurfs wird vorgesehen, dass dieses neue Tool in einer Frist von 3 Jahren nach dem Erlass dieser Änderung betriebsbereit sein muss.

Absatz 4 – Im Rahmen des Erbringens der Dienstleistung in elektronischer Form beschränkt sich der virtuelle Schalter darauf, die Rolle der Verbindung zwischen Bevölkerung und zuständigen Organen des Staates sicherzustellen. Deshalb besteht im Prinzip kein Grund dafür, die Daten länger aufzubewahren, als es für die Behandlung des Gesuchs nötig ist. Die Frage, wie lange die Daten vom virtuellen Schalter aufbewahrt werden müssen, wird derzeit in Artikel 8 der Verordnung vom 15. Mai 2017 über den E-Government-Schalter des Staates (E-GovSchV; SGF 17.41) geregelt. Der Staatsrat kann auch ermöglichen, dass Leistungen, die quer über verschiedene Verwaltungseinheiten hinweg erbracht werden und an die höhere Aufbewahrungsanforderungen gestellt werden, angeboten werden können.

Art. 4 Abs. 1 – Kosten und Gebühren

Mit der Änderung soll bestätigt werden, dass der Zugriff zum E-Government-Schalter unabhängig vom dabei gewählten Zugangskanal gratis ist. Diese Kostenlosigkeit schliesst auch die Benützung des EIM ein, das vom Staat Freiburg gewählt wurde, damit sich Benützerinnen und Benützer auf den elektronischen Plattformen einloggen können (s. Art. 20a).

Art. 5 Abs. 1 und 2 – Gemeinden

Der Inhalt des ehemaligen Absatzes 1 wurde ohne Änderung in den neuen Artikel 1a versetzt, denn er betrifft den virtuellen Schalter nicht. Der neue Text übernimmt lediglich den Inhalt des ehemaligen Absatzes 2, ohne ihn materiell zu ändern.

Art. 9a (neu) – Datenschutz durch datenschutzfreundliche Voreinstellungen und Zustimmung

Absatz 1 – In dieser Bestimmung wird der Grundsatz des Datenschutzes durch datenschutzfreundliche Voreinstellungen beim Betrieb des E-Government-Schalters eingeführt. Gemäss diesem Grundsatz, der künftig ein Stützpfeiler des Datenschutzrechts wird, muss die technische Architektur des E-Government-Schalters und der Anwendungen, die er unterstützt, so voreingestellt werden, dass nur die Personendaten, die es für jeden besonderen Zweck braucht, bearbeitet werden.

Absatz 2 – Gemäss dem Recht auf informationelle Selbstbestimmung muss die betroffene Person die Kontrolle über die sie betreffenden Daten möglichst behalten und imstande sein, über die möglichen Verwendungen dieser Daten zu entscheiden. Das schliesst insbesondere das Recht für sie ein, dass sie einem erweiterten Bearbeiten ihrer Daten zustimmen kann, wenn sie darin einen besonderen Vorteil sieht. Sie kann in diesem Sinne der Verwendung von *Cookies* zur Verbesserung der Leistungen und des Betriebs des virtuellen Schalters zustimmen, an einer Online-Umfrage teilnehmen oder sich für einen *Newsletter* anmelden, um regelmässig Informationen zu einem Thema, das sie interessiert, zu erhalten. Mit dieser Bestimmung wird dieser Art des Bearbeitens von Daten, die nicht auf einer besonderen gesetzlichen Grundlage beruht, eine rechtliche Grundlage gegeben.

Ausserdem können dank dem Voranschreiten des E-Government und der damit verbundenen Projekte die Bürgerin und der Bürger in immer mehr Bereichen freiwillig und aufgeklärt über Schnittstellen, die extra für das Erbringen von Leistungen am virtuellen Schalter und für weitere, besonders angebotene Dienstleistungen geschaffen wurden, ihre Einwilligung geben. So ist es vorstellbar, dass die verschiedenen

anerkannten Rechte der Personen, die von der Gesetzgebung über den Datenschutz betroffen sind, künftig direkt vom virtuellen Schalter aus ausgeübt werden können.

Art. 9b (neu) – Mitwirken in interkantonalen Organisationen

Anders als die Verwaltungen in den Ländern, die zentralistisch funktionieren, ist die Schweiz ein Bundesstaat, der 27 Verwaltungen kennt (der Bund und die 26 Kantone). Das bedeutet oft, dass ein und dieselbe Lösung intern 27 Mal entwickelt wird und die Produktionskosten schweizweit deshalb mit demselben Faktor multipliziert werden.

Um die Produktionskosten von Lösungen zu vermindern und auch die Erfahrungen der anderen Kantone zu teilen und von ihnen zu profitieren, hat der Kanton Freiburg Partnerschaften im Bereich des E-Government entwickelt. Er hat 2017 mit dem Kanton Jura insbesondere den interkantonalen Verein iGovPortal.ch gegründet. Dieser Verein, dem sich der Kanton Solothurn angeschlossen hat und zu dem im Sommer 2020 der Kanton St. Gallen stossen wird, stellt seinen Mitgliedern den Quellcode, den Objektcode und die technische Dokumentation zur vollständigen Schaffung eines E-Government-Schalters mit einem umfangreichen Leistungskatalog zur Verfügung. Als Gegenleistung wird jedes Mitglied eingeladen, die Verbesserungen und neuen Anwendungen, die es von der Grundlösung aus selber entwickelt, und die für die übrigen Mitglieder von Interesse sind, zu teilen. Dank dem Verein iGovPortal.ch können so der Aufwand und die Entwicklungskosten, die jeder Kanton im Bereich des E-Government trägt, geteilt werden.

In dieser Bestimmung wird die rechtliche Grundlage für das Mitwirken des Kantons beim Verein iGovPortal.ch geschaffen und der Staatsrat ermächtigt, anderen Arten von Organisationen, die in der Entwicklung von Lösungen für das Erbringen von Leistungen in elektronischer Form tätig sind, beizutreten. Die Mitwirkung der Kantone in interkantonalen Organisationen wird in Artikel 48 der Bundesverfassung ausdrücklich begrüsst.

7.3. Kantonales Bezugssystem

Art. 15 Abs. 1 Bst. h1 (neu) – Bezugssystem der natürlichen Personen

Damit das kantonale Bezugssystem funktionieren kann, muss es in der Lage sein, die fachspezifischen Identifikatoren der verschiedenen Tätigkeitsbereiche des Staates, aber auch der Gemeinden und, soweit das Bundesrecht es bewilligt, des Bundes zu bearbeiten. Damit kann es den Link zu den übrigen Informationssystemen, die ihm Daten bekanntgeben, herstellen und so die aufgeführten Personen sicher und eindeutig identifizieren. Mit der beantragten Änderung wird die dafür notwendige rechtliche Grundlage geschaffen.

Art. 15a (neu) – Systematische Verwendung der AHV-Nummer – Grundsätze

Die Verwendung der AHV-Nr. ausserhalb des Geltungsbereichs der Sozialversicherungen durch die Kantone wird in Artikel 50e Abs. 3 AHVG geregelt. Gemäss dieser Bestimmung braucht es für die Verwendung der AHV-Nr. eine angemessene Grundlage in einem Gesetz, das vom Grossen Rat erlassen wird und in dem der Zweck der Verwendung und die zum Bearbeiten der AHV-Nr. ermächtigten Organe angegeben werden. Laut der beantragten Bestimmung ist das Organ, das für das kantonale Bezugssystem zuständig ist (s. Art. 17a) ermächtigt, systematisch die AHV-Nr. zu bearbeiten, um die aufgeführten Personen sicher und eindeutig zu identifizieren, Abweichungen und Ungereimtheiten, die bei den aufbewahrten Daten festgestellt wurden, zu korrigieren (falsche Rechtschreibung, ungenaue und veraltete Daten usw.) und automatisch die Änderungen, die bei einem Gemeinwesen gemeldet werden, auszuführen (namentlich Adress- oder Zivilstandsänderungen). Mit diesem Ziel soll ausserdem dem Grundsatz der Richtigkeit der Daten nach Artikel 7 DSchG entsprochen werden.

Art. 15b (neu) – Systematische Verwendung der AHV-Nummer – Sicherheitsmassnahmen

Das kantonale Bezugssystem wird auf den Informatikinfrastrukturen des Staats gehostet. Es wird nicht in die *Cloud* ausgelagert. Die systematische Verwendung der AHV-Nr. als persönliche User-ID ist nötig für den guten Betrieb des Staates, bildet aber dennoch ein Bearbeiten von Personendaten, bei dem den Bürgerinnen und Bürgern volle Sicherheit garantiert werden muss. Deshalb braucht es unbedingt technische und organisatorische Massnahmen, um die Verwendung zu kontrollieren.

Gemäss dem Vorentwurf war vorgesehen, dass die AHV-Nr. getrennt von den übrigen Personendaten in einer Datenbank aufbewahrt wird. So wäre es nicht möglich gewesen, direkt den Link zu einer bestimmten Person zu machen, wenn die AHV-Nr. bekannt ist. Die Schaffung dieser Sicherheitsmassnahme stiess aber im Vernehmlassungsverfahren auf starken Widerspruch. Der Vorwurf wurde geäussert, dass ihre Schaffung unnötig kompliziert sei und sie bei der Sicherheit keinen bedeutenden Gewinn bringe, denn allein die Tatsache, zwei getrennte Datenbanken zu haben, bildet für sich allein noch keine Sicherheitsgarantie, die Sicherheit muss vielmehr mit einem umfassenden Ansatz gewährleistet werden. Die Realisierung dieser Trennung stelle daher eine Quelle von zusätzlichen Kosten ohne zusätzliche Sicherheitsgarantie dar.

Die schliesslich gewählte Lösung besteht darin, mit einem Verweis im kantonalen Recht streng das Bundesrecht zu übernehmen. Falls das Bundesparlament die Änderung des AHVG zur systematischen Verwendung der AHV-Nr. annimmt, gelten die technischen und organisatorischen

Massnahmen gemäss den Artikeln 153d und 153e des Entwurfs zur genannten Änderung des AHVG automatisch.

Art. 16 Bst. e, 16a und 16b (neu) – Systematische Verwendung der UID- und der BUR-Nummer

Das Gegenstück zur AHV-Nr. in der Schweiz als persönliche User-ID für die juristischen Personen bilden die Unternehmens-Identifikationsnummer (UID) und die nichtsprechende Identifikationsnummer (BUR).

Die Verwendung dieser Identifikatoren wird in Artikel 10 Abs. 3 des Bundesstatistikgesetzes vom 9. Oktober 1992 (BStatG; SR 431.01)[1] und im Bundesgesetz vom 18. Juni 2010 über die Unternehmens-Identifikationsnummer (UIDG; SR 431.03) geregelt. Ihr Zweck besteht insbesondere darin, dass «Unternehmen eindeutig identifiziert werden sollen, damit Informationen in administrativen und statistischen Prozessen einfach und sicher ausgetauscht werden können» (Art. 1 UIDG).

In den Artikeln 16 Bst. e, 16a und 16b des Entwurfs wird eine Regelung, die sinngemäss derjenigen über die systematische Verwendung der AHV-Nr. entspricht, vorgesehen. Die konkreten Sicherheitsmassnahmen, die getroffen werden müssen, können aber gegenüber denjenigen, die für die AHV-Nr. gelten, vereinfacht werden, weil die Gefahr einer Beeinträchtigung der Rechte und Freiheiten der betroffenen Personen, die sich aus der Nutzung dieser Informationen ergeben könnte, geringer ist.

Art. 17a (neu) – Für das kantonale Bezugssystem verantwortliches Organ

Der Staatsrat bezeichnet das für das kantonale Bezugssystem verantwortliche Organ. Im Moment ist dies die Kommission für die Governance der Referenzdaten, die administrativ der Staatskanzlei zugewiesen ist (s. Art. A1–1 der Verordnung über das kantonale Bezugssystem von Daten von Personen, von Organisationen und von Verzeichnissen [Pilotprojekt]; SGF 17.45).

Als verantwortliches Organ für das kantonale Bezugssystem nimmt die Kommission die Funktion des Verantwortlichen der Datensammlung im Sinne des DSchG wahr. Sie ist auch ermächtigt, systematisch die AHV-Nr. zu verwenden.

7.4. Auslagerung

Art. 17b (neu) – Grundsätze bei der Auslagerung

Absatz 1 – Die Bestimmung bildet die gesetzliche Grundlage, dank der die Gemeinwesen das Bearbeiten ihrer Daten und die Verwaltung ihrer Informatiktools auslagern können. Dazu gehören zahlreiche Anforderungen, die in den folgenden Artikeln beschrieben werden, damit ein höchstmögliches Sicherheitsniveau gewährleistet werden kann und um es dem Staat und den Gemeinden zu ermöglichen, so viel Kontrolle wie möglich über ihre Informationssysteme zu behalten.

Absatz 2 – In der Bestimmung werden zwei Vorbehalte zu den Möglichkeiten der Auslagerung eingeführt:

> Wenn das Bearbeiten von Personendaten ausgelagert wird, so muss die Auslagerung den zusätzlichen Anforderungen gemäss DSchG genügen; das betrifft nicht nur die Bestimmungen von Artikel 12b DSchG, von denen weiter unten die Rede ist, sondern die ganze Datenschutzgesetzgebung (Bst. *a*).
> Wenn die geplante Auslagerung zur Folge hat, dass das öffentliche Organ die Erfüllung einer Aufgabe, für die es laut Gesetz zuständig ist, delegiert, muss die Delegation unbedingt in einem Gesetz, das vom Grossen Rat verabschiedet wurde, vorgesehen sein, wie das in Artikel 54 KV vorgeschrieben wird (Bst. *b*).

Art. 17c (neu) – Wahren besonderer Geheimnisse

Laut dem Merkblatt der Konferenz der schweizerischen Datenschutzbeauftragten (PRIVATIM) müssen zusätzliche Sicherheitsmassnahmen geschaffen werden, wenn Daten, die dem Berufsgeheimnis oder einem besonderen Geheimnis unterstehen, ausgelagert werden[2]:

> Die Daten müssen verschlüsselt werden und die Schlüssel zur Entschlüsselung müssen grundsätzlich ausschliesslich dem öffentlichen Organ zur Verfügung gestellt werden. Die Schlüssel müssen gegen Verlust, Diebstahl und missbräuchliche Verwendung und Kenntnisnahme geschützt werden.
> Wenn das nicht möglich ist, darf der Erbringer der Cloud-Dienstleistung die Schlüssel aufbewahren, wenn er sich vertraglich verpflichtet, sie nur mit dem ausdrücklichen Einverständnis des öffentlichen Organs zu verwenden. Es muss ein Zugriffsprotokoll geführt werden. Ausserdem muss der Erbringer der Cloud-Dienstleistung die Schlüssel vor Verlust, Diebstahl und missbräuchlicher Verwendung und Kenntnisnahme schützen. Er muss auch sicherstellen, dass die Daten während des Verschlüsselungsverfahrens nicht gefährdet sind.

In der geplanten Bestimmung werden diese Anforderungen auf Gesetzesebene in einer Sprache, die auf technologischer Ebene neutral ist, festgehalten.

[1] Die Bestimmung wird mit der Verordnung vom 30. Juni 1993 über das Betriebs- und Unternehmensregister (BURV; SR 431.903) ergänzt.

[2] s. www.privatim.ch > Publikationen > Leitfäden und Merkblätter (https://www.privatim.ch/wp-content/uploads/2019/12/privatim-Cloud-Papier_v2_1_20191217.pdf).

Art. 17d (neu) – Sicherheitsmassnahmen

Absatz 1 – Das öffentliche Organ, das eine Auslagerung macht, muss sich vergewissern, dass der Auftragsbearbeiter technische und organisatorische Massnahmen ergreift, damit die Aufbewahrung und das Bearbeiten seines Informationserbes sichergestellt werden. Welche Massnahmen konkret ergriffen werden müssen, hängt jedes Mal von der Art der ausgelagerten Daten oder Informatiktools, des Zwecks und der Vertraulichkeitsstufe ab. Die getroffenen Massnahmen müssen dem Stand der Technik entsprechen.

Absatz 2 – Wenn die Auslagerung Daten betrifft, die für den Betrieb eines Gemeinwesens unbedingt notwendig sind, muss das öffentliche Organ ein Dispositiv schaffen, mit dem die Fortführung der ausgelagerten Tätigkeiten bei einem Zwischenfall sichergestellt werden kann. Die Sammlungen der Freiburger Gesetzgebung beispielsweise, die mit einer Anwendung der Firma Sitrox verwaltet und auf deren Infrastruktur aufbewahrt werden, werden regelmässig auf Datenträger, die dem Staat gehören und mit denen sie wiederverwendet werden können, kopiert. Das Ziel dieser Massnahme besteht darin, sich vor der Gefahr eines Verlusts oder einer Verfälschung dieser Daten zu schützen. In Artikel 17d Abs. 2 wird aber nicht besonders vorgeschrieben, dass die ausgelagerten Daten systematisch kopiert werden müssen, sondern den zuständigen Behörden die Wahl der am ehesten angemessenen Massnahmen für jeden Einzelfall gelassen.

Art. 17e (neu) – Verantwortung

Absatz 1 – Die Grundregel bei der Auslagerung lautet, dass das Organ, welches das Bearbeiten seiner Daten auf Infrastrukturen eines Auftragsbearbeiters auslagert, voll verantwortlich für den Fortbestand, das Aufbewahren und das Bearbeiten der Daten bleibt. In der Bestimmung wird eine gewisse Zahl konkreter Punkte erwähnt, die unter dem Gesichtspunkt der Verantwortung berücksichtigt werden müssen, wenn Daten ausgelagert werden. Insbesondere muss ein Organ, das einem Auftragsbearbeiter Teile seiner Daten übergibt, diesen sorgfältig auswählen, ihm mit einem möglichst genauen Vertrag Anweisungen zu den Aufgaben, die er erfüllen muss, geben und überwachen, ob er die Elemente des Vertrags einhält. Es muss sich auch vergewissern, dass es die Daten und die Informatiktools, die es ausgelagert hat, jederzeit zurückholen kann. Verträge, bei denen diese Anforderungen allenfalls nicht vollständig eingehalten werden, müssen in einer Frist von höchstens 5 Jahren angepasst werden (s. Art. 21a Abs. 1 E-GovSchG).

Es sei hier als Beispiel eine *Checkliste* der verschiedenen Elemente, die ein Auslagerungsvertrag je nach Umständen enthalten sollte, angeführt:

a) Gegenstand, Art und Zweck des Bearbeitens;
b) Kategorie der bearbeiteten Daten und ihre Vertraulichkeitsstufe,
c) Standort der Server, auf denen das Hosting der Daten und Anwendungen erfolgt;
d) Massnahmen, die ergriffen werden, um die Sicherheit und die Vertraulichkeit der Daten zu gewährleisten;
e) Personen oder Personenkategorien, die Zugriff auf die betroffenen Daten und Anwendungen haben;
f) Kontrollrechte und -möglichkeiten der Behörde, die Daten und Anwendungen auslagert, namentlich die Möglichkeit, am Standort des Auftragsbearbeiters Audits durchzuführen;
g) Verbot für den Auftragsbearbeiter, seinerseits das Bearbeiten von Daten weiter zu vergeben, ohne dass er die vorherige Zustimmung der verantwortlichen Behörde einholt und einen Auslagerungsvertrag, in dem dieselben Anforderungen wie diejenigen, die zwischen der verantwortlichen Behörde und dem Auftragsbearbeiter vereinbart wurden, festgehalten werden, unterzeichnet;
h) Meldepflicht des Auftragsbearbeiters bei einem Zwischenfall sowie bei Verlust oder Diebstahl der Daten;
i) Möglichkeiten, die betroffenen Daten und Anwendungen während der Laufzeit des Vertrags zurückzuerhalten;
j) Verfahren, die im Fall der Vertragsauflösung eingehalten werden müssen; insbesondere die Rückgabe der Daten und Anwendungen sowie deren Vernichtung oder Deinstallation beim Auftragsbearbeiter;
k) soweit möglich, Anwendbarkeit des Schweizer Rechts und Bezeichnung eines Gerichtsstands in der Schweiz im Streitfall.

Diese Elemente können sich aber mit der Zeit je nach Arten der Auslagerung weiter entwickeln.

Absatz 2 – Gewisse *Cloud*-Lösungen sind nicht auf ein Organ eines Gemeinwesens beschränkt, sondern können sich auf mehrere oder auf alle von ihnen erstrecken. Es ist dann offensichtlich, dass nicht jedes einzelne betroffene öffentliche Organ persönlich sicherstellen kann, dass der Auftragsbearbeiter seine Verpflichtungen einhält. In diesem Fall bezeichnet der Staatsrat ein hauptverantwortliches Organ, das auch Hauptansprechpartner des Auftragsbearbeiters ist.

Absatz 3 – Bei der Kantonsverwaltung werden die Schritte zur Auslagerung zentral beim ITA, das eng mit den betroffenen Organen zusammenarbeitet, zusammengefasst. Mit dieser Vorgehensweise kann eine zusammenhängende und möglichst einheitliche Praxis entwickelt werden. Bei einer Auslagerung sorgt das ITA zusammen mit dem öffentlichen

Organ dafür, dass die Regelung zur Auslagerung eingehalten wird, namentlich, dass der Auslagerungsvertrag die nötigen Klauseln zur Sicherheit enthält. In der Bestimmung wird aber der Fall der öffentlichen Organe, die ihre Informatik autonom verwalten, wie beispielsweise die Universität, das Amt für Strassenverkehr und Schifffahrt und das freiburger spital, vorbehalten. Diese Organe sind allein verantwortlich für die Auslagerung ihrer Daten und ihrer Informatiktools.

7.5. Elektronische Identifizierungsmittel

Art. 20a (neu) – Elektronische Identifizierungsmittel (EIM)

Ein EIM ist ein persönliches Identifizierungsmittel, mit dem eine Person sich authentifizieren kann, wenn sie einen Online-Dienst in Anspruch nehmen will. Ein EIM besteht aus materiellen und/oder immateriellen Elementen und bietet je nach seiner Form verschiedene Sicherheitsniveaus: eine persönliche User-ID (Name der Person) und ein Passwort, die allenfalls mit einem SMS, einer biometrischen User-ID oder einem USB-Stick ergänzt werden können.

Absatz 1 – Für den Zugriff auf Online-Leistungen, die von einem Gemeinwesen erbracht werden, muss grundsätzlich immer ein EIM benützt werden. Ausnahmen sind gestattet, damit gewisse Leistungen, bei denen keine Identifikation zur Sicherstellung der wirklichen Identität der Person erforderlich ist, angeboten werden können.

Absatz 2 – Nicht alle EIM können dasselbe Identifikationsniveau sicherstellen. Das Erbringen gewisser Leistungen setzt voraus, dass davor sichergestellt wird, dass die Gesuchstellerin oder der Gesuchsteller wirklich die Person ist, die sie oder er zu sein behauptet. Deswegen muss das benützte EIM über ein starkes Identifikationsverfahren erfolgen, bei dem die betroffene Person sich zunächst physisch (oder über Videokonferenz) einer zertifizierten Person, die sie formal identifiziert, vorstellt. Diese Art EIM wird derzeit von privaten Leistungserbringern, die von einem vom Bund akkreditierten Unternehmen zertifiziert wurden, erbracht. Mit der Bestimmung kann der Staatsrat in den Fällen, in denen es nötig ist, die Benützung eines zertifizierten EIM vorschreiben. Das zertifizierte EIM, das auf Kantonsebene benützt wird, wird nach einem Ausschreibungsverfahren ausgewählt. Damit der Zugriff auf die E-Government-Leistungen kostenlos ist, werden die Kosten für die Benützung des EIM (*Login* und Abschluss von Geschäften) für die Bürgerinnen und Bürger, die das vom Staat gewählte EIM benützen, vom Staat übernommen.

Absatz 3 – Die Nutzerinnen und Nutzer eines zertifizierten EIM müssen sich formal identifizieren lassen, damit der Beweis ihrer Identität so sicher wie möglich erbracht werden kann. Im Projekt wird vorgesehen, dass der Staat dazu seine eigenen Registrierungsbehörden schaffen und/oder mit den Gemeinden zusammenarbeiten kann. Konkret geht es darum, das Personal von gewissen Dienststellen des Kantons und der Partnergemeinden auszubilden, damit es die Nutzerinnen und Nutzer identifizieren kann. Dieses Verfahren ist für die Benützerin oder den Benützer jedes Mal gratis. Die Schaffung der Ausbildungen, um das Personal anzuleiten, wird vom Kanton sichergestellt.

7.6. Schlussbestimmungen

Art. 21a (neu) – Übergangsrecht

Diese Änderung bringt Veränderungen mit sich, die für die Organisation und die Arbeitsweise des Staats keineswegs bedeutungslos sind. Diese Veränderungen sind gerechtfertigt, weil sie vom Streben nach Fortschritt bei der Digitalisierung in einem sicheren Umfeld geleitet werden. Damit kann der Kanton Freiburg am meisten von den Informations- und Kommunikationstechnologien profitieren und gleichzeitig das höchstmögliche Sicherheitsniveau vom Gesichtspunkt sowohl des Staats als auch der Bürgerinnen und Bürger sicherstellen. Aufgrund der Bedeutung der beantragten Veränderungen braucht es aber eine Übergangsfrist, damit die betroffenen Organe sich an die neuen Anforderungen, die an sie gestellt werden, anpassen und die nötigen neuen Instrumente entwickeln können.

Schlussklausel

Die Änderungen, die mit dieser Revision angebracht werden, sind nicht nur unter dem materiellen, sondern auch unter dem formalen Gesichtspunkt bedeutend. Trotz den Anstrengungen, die mit dem Ziel gemacht wurden, dem Gesetz eine möglichst verständliche Struktur zu verleihen, ist es aufgrund des Umfangs der angebrachten Änderungen manchmal schwer lesbar. Nur mit einer Totalrevision des Erlasses kann dem Gesetz eine neue Gesamtstruktur gegeben werden. Eine solche Revision ginge jedoch über den Rahmen und das Ziel dieser Änderung hinaus. Stattdessen werden die Organe, die für die amtlichen Veröffentlichungen zuständig sind, in der Schlussklausel beauftragt, das alte E-GovSchG in ein neues totalrevidiertes Gesetz umzuwandeln, sobald es vom Grossen Rat angenommen wurde.

8. Anpassungen des DSchG – Kommentare

Art. 3 Abs. 1 Bst. d, e1 und i (neu) – Begriffe

> «Bearbeiten» (Bst. d): Die Definition des Bearbeitens von Daten wird ergänzt, um neben den anderen Formen des Bearbeitens, die zur Information erwähnt werden, den Begriff Hosting darin zu integrieren.
> «Auslagerung» (Bst. e[1]): Die Definition wird vom E-GovSchG übernommen; sie wird an den besonderen Kontext des Schutzes der Personendaten angepasst.

> «Auftragsbearbeiter» (Bst. i): Die Definition wird vom E-GovSchG übernommen; sie wird an den besonderen Kontext des Schutzes der Personendaten angepasst.

Art. 12b (neu) – Auslagerung

In der Bestimmung wird festgelegt, welche besonderen Vorschriften bei der Auslagerung von Personendaten an einen Auftragsbearbeiter eingehalten werden müssen.

Absatz 1 – Am Anfang der Bestimmung stehen zwei Verweise. Zuerst wird auf die allgemeinen Vorschriften des E-GovSchG über die Auslagerung verwiesen. Die Auslagerung von Personendaten ist eine qualifizierte Form der Auslagerung. Sie muss deshalb zunächst die allgemeinen Anforderungen nach den Artikeln 17b–17e E-GovSchG erfüllen, die unabhängig von Art und Inhalt für alle Formen der Auslagerung gelten. Dann wird auf die Vorschriften über die Auftragsbearbeitung (s. Art. 18 DSchG) verwiesen; die Auslagerung bildet eine besondere Kategorie der Auftragsbearbeitung.

Absatz 2: In der Bestimmung wird eine gewisse Zahl von besonderen Anforderungen, die typisch für das Datenschutzrecht sind, angefügt:

> Vor jeder Auslagerung von Daten muss eine Untersuchung gemacht werden, um festzulegen, welche geeigneten Sicherheitsmassnahmen angesichts der Risiken, die das Bearbeiten der fraglichen Daten für die Persönlichkeit und die Grundrechte der betroffenen Personen mit sich bringt, getroffen werden müssen (*Bst. a*).

> Wenn die Auslagerung besonders schützenswerte Personendaten im Sinn von Artikel 3 Abs. 1 Bst. c DSchG betrifft und sie eine konkrete Gefahr, dass die Rechte der betroffenen Personen verletzt werden, verursacht, müssen Sicherheitsmassnahmen getroffen werden, die denjenigen, die bei Auslagerung von Geheimnissen ergriffen werden müssen, entsprechen (*Bst. b*). Der Begriff der besonders schützenswerten Personendaten ist ein fester Begriff, der nicht berücksichtigt, ob ein wirkliches Risiko besteht. So fällt zum Beispiel die einfache Tatsache, dass jemand eine Brille trägt, schon in die Kategorie der besonders schützenswerten Personendaten im Zusammenhang mit der Gesundheit. Für diese Art von Information braucht es aber keinen erhöhten Schutz. Im Entwurf wird deshalb vorgesehen, die Auslagerung von besonders schützenswerten Personendaten mit dem Vorhandensein eines konkreten Risikos, dass die Rechte der betroffenen Person verletzt werden, zu verknüpfen. Erst wenn beide Voraussetzungen erfüllt sind, müssen die strengsten Sicherheitsmassnahmen ergriffen werden. Damit man weiss, ob man es mit einem konkreten Verletzungsrisiko zu tun hat, werden verschiedene Kriterien, wie die Zahl der betroffenen besonders schützenswerten Personendaten, der Zweck des Bearbeitens oder der Hintergrund, vor dem die Auslagerung geschieht, berücksichtigt.

> Wo sich die Orte des Bearbeitens befinden, ist ein wesentlicher Aspekt der Auslagerung, denn er bestimmt das Recht, das für das Bearbeiten der Daten gilt, und infolgedessen alle gesetzlichen Vorschriften, die der Auftragsbearbeiter einhalten muss. Im Entwurf wird in diesem Sinn vorgesehen, dass sich die Orte des Bearbeitens jederzeit auf Schweizer Gebiet oder auf dem Gebiet eines Staates, dessen Gesetzgebung ein gleichwertiges Datenschutzniveau garantiert, befinden müssen (*Bst. c*). Damit der Verantwortliche der Datensammlung weiss, ob ein Staat ein gleichwertiges Datenschutzniveau garantiert, sieht er in der Liste, die der EDÖB gemäss Artikel 6 Abs 1 des Bundesgesetzes über den Datenschutz führt, nach[1].

> Bei einer Auslagerung von Personendaten ist der Auftragsbearbeiter der Pflicht, den Verantwortlichen der Datensammlung unverzüglich zu informieren, wenn er aufgrund eines ausländischen Gesetzes oder eines richterlichen Entscheids die Daten einer ausländischen Behörde bekanntgeben muss, unterworfen. Dieser Fall kann aufgrund eines Entscheids der Justiz, aber auch in Anwendung einer ausländischen Gesetzgebung eintreten. Insbesondere der *Cloud Act* (*Clarifying Lawful Overseas Use of Data Act*), der 2018 von den Vereinigten Staaten erlassen wurde, ermöglicht den amerikanischen Ordnungskräften, amerikanische Dienstleistungserbringer mit Befehl oder Vorladung, Daten, die auf ihren Servern gelagert werden, herauszugeben, ungeachtet dessen, ob diese sich in den Vereinigten Staaten oder in anderen Ländern, einschliesslich der Schweiz, befinden. Mit der Einführung der Informationspflicht können die Verantwortlichen der Datensammlungen in einer solchen Situation die nötigen Massnahmen ergreifen, namentlich sich allenfalls an die Justiz wenden, um die Bekanntgabe von Daten mit (super) provisorischen Massnahmen zu verhindern.

> Der Auftragsbearbeiter darf seinerseits das Bearbeiten, mit dem er beauftragt wurde, nicht weitervergeben, ohne vorher den Verantwortlichen der Datensammlung zu informieren und dessen Einverständnis eingeholt zu haben. Da der Verantwortliche der Datensammlung die Verantwortung für die ganze Kette von Subunternehmen behält, muss er in der Lage sein, die Risiken im Zusammenhang mit jedem betroffenen Partner zu beurteilen.

[1] Diese Liste kann auf der folgenden Internet-Adresse eingesehen werden: www.edoeb.admin.ch > Datenschutz > Handel und Wirtschaft > Übermittlung ins Ausland > Staatenliste (https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland.html). Es sei darauf hingewiesen, dass die Liste der Staaten, deren Gesetzgebung ein Schutzniveau, das demjenigen der Schweiz ebenbürtig ist, anbietet, mit dem Inkrafttreten des neuen Bundesgesetzes über den Datenschutz direkt vom Bundesrat geführt wird (s. Art. 13 Abs. 1 DSG, der im Entwurf des Bundesgesetzes über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz eingeführt wird [s. BBl 2017 7193]).

Absatz 3 – Wie in Artikel 17b Abs. 2 Bst. b E-GovSchG behält diese Bestimmung den Fall, in dem die Auslagerung einer Delegation von Aufgaben an Dritte im Sinne von Artikel 54 KV gleichkommt, vor. In einem solchen Fall muss die geplante Auslagerung eine gesetzliche Grundlage, die vom Grossen Rat verabschiedet wurde, haben.

Art. 18 – Auftragsbearbeitung

Die Änderung ist terminologischer Natur. Der Begriff «Bearbeiten im Auftrag» wird durch «Auftragsbearbeitung» ersetzt. Substantiellere Änderungen dieser Bestimmung, deren Wirkung über die alleinige Auslagerung hinausgeht, können später im Rahmen der Arbeiten zur Totalrevision des DSchG eingeführt werden.

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)

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,

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)

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,

Décrète:

Art. 1a *(nouveau)*

Application aux communes

[1] Les communes (y compris les établissements communaux, les associations de communes et les agglomérations) 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.

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

[1a] Guichet virtuel

beschliesst:

Art. 1a *(neu)*

Gültigkeit für die Gemeinden

[1] Die Gemeinden (einschliesslich der Gemeindeanstalten, der Gemeindeverbände und der Agglomerationen) 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.

Abschnittsüberschrift nach Art. 2 *(neu)*

[1a] Virtueller Schalter

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.

[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, les associations de communes et les agglomérations) 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.

[2] La personne concernée peut consentir à un traitement élargi de ses données afin de bénéficier de services et/ou de prestations supplémentaires.

Art. 3a *(neu)*

Bearbeiten von Personendaten

[1] Das für die Ausführung der Leistung oder der gewünschten Dienstleistung nötige Bearbeiten der Daten erfordert die freie und aufgeklärte Einwilligung der betroffenen Person.

[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, der Gemeindeverbände und der Agglomerationen) 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] 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 *(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;

h[1]) *(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:

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.

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

h[1]) *(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 Alters- und Hinterlassenenversicherung wird die systematische Verwendung der AHV-Nummer im kantonalen Bezugssystem zu folgenden Zwecken bewilligt:

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] 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.

Art. 16 al. 1

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

e) *(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;

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] 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.

Art. 16 Abs. 1

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

e) *(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 *(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) Gewährleistungen einer höchstmöglichen Genauigkeit der bearbeiteten Daten;

c) automatische Nachführung der Daten einer Person bei Änderungen.

[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.

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] 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.

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] 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.

[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.

[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] 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 *(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.

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

3b Développement de la cyberadministration

Intitulé de section après section 3b

3.2 *(abrogé)*

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

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 Informatiktools 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.

Abschnittsüberschrift nach Art. 17e *(neu)*

3b Entwicklung des E-Government

Abschnittsüberschrift nach Abschnitt 3b

3.2 *(aufgehoben)*

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

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. 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 ainsi qu'aux exigences particulières de l'article 12b de la loi du 25 novembre 1994 sur la protection des données 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.

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. 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 und an die besonderen Anforderungen von Artikel 12b des Gesetzes vom 25. November 1994 über den Datenschutz 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.

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 à condition de respecter les exigences de la loi du … sur la cyberadministration (LCyb) en matière d'externalisation et les règles de l'article 18 sur la responsabilité en cas de sous-traitance.

[2] En outre:

a) 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;

b) l'externalisation de données sensibles est soumise aux règles de l'article 17c LCyb lorsqu'elle engendre un risque concret d'atteinte aux droits des personnes concernées;

c) le contrat d'externalisation définit les droits et possibilités de contrôle de l'autorité de surveillance en matière de protection des données;

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] Das Bearbeiten von Personendaten, einschliesslich von besonders schützenswerten Personendaten, darf unter der Voraussetzung, dass die Anforderungen des E-Government-Gesetzes vom … (E-GovG) über die Auslagerung und die Vorschriften von Artikel 18 über die Verantwortung bei einem Outsourcing eingehalten werden, ausgelagert werden.

[2] Ausserdem:

a) berücksichtigt die Definition der Sicherheitsmassnahmen die Gefahren, die das Bearbeiten der fraglichen Daten für die Persönlichkeit und die Grundrechte der betroffenen Personen mit sich bringt;

b) gelten für die Auslagerung von besonders schützenswerten Personendaten die Vorschriften von Artikel 17c E-GovG, wenn sie eine konkrete Gefahr, dass die Rechte der betroffenen Personen verletzt werden, verursachen;

c) werden im Auslagerungsvertrag die Rechte und die Kontrollmöglichkeiten der Datenschutzbehörde festgehalten;

d) 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;

e) le contrat d'externalisation prévoit 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;

f) le sous-traitant ne peut pas lui-même sous-traiter un traitement à un tiers sans l'autorisation préalable du responsable du fichier.

[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. 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.

III.

Aucune abrogation d'actes dans cette partie.

d) muss sich der Datenbearbeitungsort jederzeit auf Schweizer Gebiet oder auf dem Gebiet eines Staates, der ein gleichwertiges Datenschutzniveau garantiert, befinden;

e) wird im Auslagerungsvertrag die Pflicht des Auftragsbearbeiters festgehalten, 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;

f) der Auftragsbearbeiter darf nicht ohne vorgängige Genehmigung des Verantwortlichen der Datensammlung das Bearbeiten einem Dritten übertragen.

[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. 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.

III.

Keine Aufhebung von Erlassen in diesem Abschnitt.

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.

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.

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.

Schlussbestimmungen

—

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

Der Staatsrat legt das Inkrafttreten dieses Gesetzes fest.