

**MESSAGE N° 56** 4 mars 2008  
**du Conseil d'Etat au Grand Conseil**  
**accompagnant le projet de loi modifiant**  
**la loi sur la protection des données**  
**(adaptation au droit international,**  
**en particulier aux accords Schengen/Dublin)**

Nous avons l'honneur de vous soumettre un projet de loi adaptant la loi sur la protection des données aux engagements internationaux (accords Schengen/Dublin et protocole additionnel à la convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel) pris par la Suisse dans le domaine de la protection des données.

Le présent message est structuré de la manière suivante:

1. Engagements internationaux de la Suisse
2. Déroulement des travaux
3. Nécessité de procéder à l'adaptation de la LPrD
4. Lignes directrices et champ d'application du projet
5. Commentaire des articles
6. Répartition des tâches Etat-communes
7. Constitutionnalité et conformité au droit fédéral et européen
8. Conséquences financières et en personnel

## **1. ENGAGEMENTS INTERNATIONAUX DE LA SUISSE**

L'Union européenne et le Conseil de l'Europe ont élaboré des instruments juridiques visant à harmoniser la protection des données au niveau international. Ces instruments définissent un standard minimal de protection qui doit être garanti dans tous les Etats membres. Les principaux sont:

- pour l'Union européenne, la *directive 95/46/CE* du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données;
- pour le Conseil de l'Europe, la convention, du 28 janvier 1981, pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (*convention 108*) et son *protocole additionnel*, du 8 novembre 2001, concernant les autorités de contrôle et les flux transfrontières de données.

La Suisse s'est engagée à appliquer le contenu de la directive 95/46/CE, dans l'accord entre la Confédération suisse, l'Union européenne et la Communauté européenne sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen (cf. FF 2004 p. 6090).

Par ailleurs, les Chambres fédérales ont adopté, le 24 mars 2006, l'arrêté fédéral sur l'adhésion de la Suisse au protocole additionnel à la convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (FF 2006 p. 3521). Ce protocole sera soumis au Conseil

fédéral pour ratification et devrait entrer en vigueur le 1<sup>er</sup> avril 2008.

En conséquence, les règles européennes énoncées dans ces deux actes doivent être transposées dans la législation suisse, y compris au niveau cantonal. Tel est précisément l'objet du projet de révision qui vous est soumis. A signaler que les adaptations de la loi fédérale sur la protection des données (LPD) ont été adoptées le 24 mars 2006, parallèlement à l'adoption du protocole additionnel. Les nouvelles dispositions fédérales sont entrées en vigueur le 1<sup>er</sup> janvier 2008.

## **2. DÉROULEMENT DES TRAVAUX**

### a. En général

Le 15 septembre 2006, la Direction de la sécurité et de la justice a institué un groupe de travail chargé d'élaborer un avant-projet de loi révisant la loi cantonale sur la protection des données accompagné d'un commentaire. La présidence de ce groupe a été confiée à M<sup>me</sup> Alexandra Rumo-Jungo, professeure à l'Université, présidente de la Commission cantonale de la protection des données; le groupe était par ailleurs composé de M. Christophe Maillard, conseiller juridique DIAF, de M<sup>me</sup> Dominique Nouveau Stoffel, préposée cantonale à la protection des données, de M. Guy Python, préposé à la protection des données de la ville de Fribourg, de M. Thierry Steiert, conseiller scientifique DSJ, de M. Luc Vollery, conseiller juridique SLeg (remplacé dès novembre 2006 par M<sup>me</sup> Josette Moullet Auberson, conseillère juridique SLeg) et de M<sup>me</sup> Marie-Thérèse Weber-Gobet, députée. Le secrétariat et la tenue du procès-verbal ont été assurés par M<sup>me</sup> Lydia Oberson, collaboratrice de l'autorité cantonale de surveillance de la protection des données.

A l'origine, la révision projetée visait un triple but:

- adaptation de la loi cantonale sur la protection des données (LPrD) à la directive 95/46/CE et au protocole additionnel précités;
- adaptation de cette même loi à la récente révision de la LPD;
- prise en compte des expériences faites avec la LPrD depuis son entrée en vigueur.

Il est toutefois rapidement apparu qu'il ne serait pas possible de réaliser les trois volets de cette révision dans les délais impartis par la Confédération pour l'adoption des adaptations des lois cantonales aux accords Schengen/Dublin. Le mandat du groupe de travail a par conséquent été limité au premier volet, à savoir l'adaptation de la LPrD aux exigences du droit international. Les deux autres volets d'adaptations seront réalisés ultérieurement.

### b. Soutien de la Conférence des gouvernements cantonaux (CdC) et de la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP)

La CdC et la CCDJP sont chargées de la mise en œuvre et du développement des accords Schengen/Dublin en ce qui concerne les cantons. Ces Conférences ont confié à M. Beat Rudin, spécialiste du domaine de la protection des données (ci-après le délégué de la CdC), le soin d'élaborer, à l'intention des cantons, un guide pratique pour la mise en œuvre des prescriptions en matière de protection des données reprises avec les accords Schengen/

Dublin. Ce guide consiste en une liste, complétée par des explications, des exigences générales que doivent remplir les législations cantonales en matière de protection des données dans le cadre de l'association aux accords Schengen/Dublin et de la mise en œuvre des dispositions du protocole additionnel. Ce guide a servi de base aux travaux du groupe chargé de la révision.

### c. Procédure de consultation

Du 31 mai au 31 août 2007, le Conseil d'Etat a mis en consultation auprès de ses Directions, des organismes intéressés et des partis politiques le projet du groupe de travail, après y avoir apporté de légères modifications.

Dans l'ensemble, le projet du Conseil d'Etat a été accueilli favorablement. Les réserves les plus nombreuses sont celles liées à la difficulté pour les communes de mettre en place des autorités de surveillance de la protection des données satisfaisant aux exigences imposées par les accords internationaux. Le renforcement des pouvoirs des autorités de surveillance de la protection des données a, pour sa part, donné lieu à deux avis critiques. Pour le surplus, le projet a suscité quelques remarques ponctuelles qui ont été prises en compte dans le projet définitif, lorsqu'elles étaient compatibles avec les exigences du droit international et entraient dans le cadre de la modification en cours, à savoir l'adaptation de la loi actuelle aux engagements internationaux de la Suisse.

## 3. NÉCESSITÉ DE PROCÉDER À L'ADAPTATION DE LA LPRD

### a. En général

L'examen de la LPrD à la lumière du guide pratique précité a montré que la loi actuelle correspond déjà en grande partie aux standards requis.

La forme juridique (loi au sens formel) et les dispositions fixant le champ d'application de la loi, les principes régissant le traitement des données personnelles ainsi que les droits des personnes concernées remplissent en particulier les exigences dictées par les engagements internationaux de la Suisse.

Certaines lacunes ont néanmoins été constatées; elles rendent nécessaires d'adapter la LPrD. Sont visés: l'indépendance de l'autorité de contrôle en matière de protection des données (b.), les pouvoirs de cette autorité (c.) et la réglementation des «flux transfrontières de données» (d.).

Par ailleurs, au cours des travaux, il est apparu qu'il n'est pas toujours aisé de déterminer si la législation actuelle remplit ou non les exigences du droit européen. Les «cas-limites» non retenus dans le projet sont présentés ci-dessous par souci de transparence (e.).

A noter que les exigences de la directive 95/46/CE ainsi que celles de la convention 108 et de son protocole additionnel s'appliquent à l'ensemble de la surveillance de la protection des données, y compris, le cas échéant, à celle assurée par les autorités communales de surveillance et par les autorités instituées par les corporations ecclésiastiques.

### b. Indépendance des autorités de contrôle

L'article 28 ch. 1 de la directive 95/46/CE et l'article 1 ch. 3 du protocole additionnel prescrivent que les auto-

rités de contrôle doivent exercer leurs tâches en toute indépendance.

Pratiquement, la garantie de la totale indépendance des autorités de contrôle en matière de protection des données comporte des aspects institutionnels et des aspects personnels (A. EPINEY, *Datenschutz und «Bilaterale II»*, *Zu den Auswirkungen der Schengen-Assoziierung auf das schweizerische Datenschutzrecht – ausgewählte Aspekte*, in RSJ 2006 121/126 sv.; A. EPINEY / S. THEUERKAUF, *Datenschutz in Europa – Ueberblick und Implikationen in der Bilateralen II*, in *Datenschutz in Europa und die Schweiz*, La protection des données en Europe et la Suisse, p. 71 ss; B. RUDIN / B. BAERISWYL, «Schengen» und der Datenschutz in den Kantonen: Anforderungen – Beurteilung – Handlungsbedarf, in *Datenschutz in Europa und die Schweiz*, La protection des données en Europe et la Suisse, p. 193 ss).

Sur le plan institutionnel, le mode d'élection de l'autorité de contrôle, son statut au sein de l'organisation cantonale, son autonomie budgétaire ainsi que la liberté dont elle dispose dans la planification et l'exécution de son activité, et la manière dont sont réglées les conditions d'engagement et de résiliation des rapports de travail de la personne qui la dirige sont des éléments-clés.

Les aspects personnels de l'indépendance, quant à eux, supposent que les personnes chargées de la surveillance de la protection des données disposent des qualités personnelles et des compétences requises pour l'exercice de leur tâche et qu'elles ne soient pas soumises à des conflits d'intérêts. Cette dernière condition implique que les personnes concernées soient tenues de faire connaître leurs liens d'intérêts publics ou privés et de se récuser lorsque l'autorité traite de dossiers qui les touchent plus particulièrement.

En pratique, le niveau d'indépendance des autorités de contrôle est fonction de la combinaison de ces divers éléments. Une élection par le parlement et un rattachement à cette autorité offrent naturellement une garantie optimale d'indépendance. Toutefois, le déficit qu'implique par exemple une nomination par l'Exécutif (qui équivaut à la nomination du contrôleur par le contrôlé) peut être compensé par d'autres garanties institutionnelles.

L'organisation actuelle de l'autorité cantonale de surveillance de la protection des données, qui est formée d'une Commission et d'un ou d'une préposé-e, offre déjà de bonnes garanties d'indépendance. En effet, la Commission est élue par le Grand Conseil, auquel doit être adressé le rapport annuel en matière de protection des données. Ce rôle important du parlement permet d'assurer le degré d'indépendance requis, alors que le ou la préposé-e est nommé-e par le Conseil d'Etat. A signaler encore que, sur le plan organisationnel, l'autorité cantonale de surveillance est seulement rattachée administrativement à une Direction du Conseil d'Etat et qu'il n'y a donc pas de lien de subordination entre cette autorité d'une part et l'Exécutif et l'administration d'autre part (cf. art. 61 LOCEA).

Cela étant, il apparaît raisonnable de conserver le système actuel en procédant à quelques adaptations dictées par la nécessité de renforcer, conformément aux exigences européennes, l'indépendance de l'autorité cantonale de surveillance de la protection des données. Les adaptations en question sont prévues aux articles 30 et 32 du projet (pour le surplus, cf. ci-dessous commentaires relatifs à ces dispositions).

### c. Pouvoirs des autorités de contrôle

L'article 28 ch. 3, 2<sup>e</sup> et 3<sup>e</sup> tirets de la directive 95/46/CE et l'article 1 ch. 2a du protocole additionnel prescrivent que les autorités de contrôle en matière de protection des données doivent être dotées de pouvoirs effectifs d'intervention et avoir le pouvoir d'ester en justice dans les cas de violation des dispositions légales sur la protection des données.

#### – *Pouvoirs effectifs d'intervention*

Selon l'article 28 ch. 3, 2<sup>e</sup> tiret de la directive 95/46/CE, qui explicite l'article 1 ch. 2a du protocole additionnel, les pouvoirs effectifs d'intervention comprennent notamment le pouvoir «de rendre des avis préalablement à la mise en œuvre des traitements, d'assurer une publication appropriée de ces avis ou celui d'ordonner le verrouillage, l'effacement ou la destruction de données, ou d'interdire temporairement ou définitivement un traitement, ou celui d'adresser un avertissement ou une admonestation au responsable du traitement, ou celui de saisir les parlements nationaux ou d'autres institutions politiques». Ces différentes mesures sont énoncées à titre d'exemples dans la directive. On peut en déduire que la liste n'a pas un caractère cumulatif.

Les législations nationales doivent mettre en place un système garantissant que les mesures requises par les autorités de contrôle en matière de protection des données seront effectivement mises en œuvre. A cet égard, il est précisé, dans les considérants de la directive 95/46/CE, que «en cas de non-respect des droits des personnes concernées par le responsable du traitement des données, un recours juridictionnel doit être prévu par la législation nationale» (cf. cons. 55). Le rapport explicatif sur le protocole additionnel précise pour sa part que les Etats parties «devraient accorder à l'autorité de contrôle le pouvoir, soit d'ester en justice, soit de porter à la connaissance de la justice toute violation aux principes de la protection des données. (...) L'obligation des Parties d'accorder à l'autorité ce pouvoir peut être remplie en lui donnant le pouvoir de prendre des décisions judiciaires» (cf. ch. 15).

Les pouvoirs d'intervention actuels de l'autorité cantonale de surveillance en matière de protection des données ne satisfont pas aux exigences décrites ci-dessus. L'article 30 al. 2 let. c LPrD donne en effet à la Commission cantonale de la protection des données seulement la compétence d'inviter les organes concernés à prendre les mesures nécessaires en cas de violation ou de risque de violation des prescriptions légales. Cette compétence d'adresser des recommandations ne garantit pas que ces violations, ou risques de violations, puissent être prévenus. Les mécanismes ordinaires de contrôle de l'activité administrative ne permettent en effet pas à l'autorité cantonale de surveillance d'imposer le respect des principes de la LPrD si cela va à l'encontre de la volonté des organes concernés, en particulier de celle du Conseil d'Etat. La haute surveillance exercée par le Grand Conseil (cf. art. 189 al. 1 LGC) ne garantit pas l'existence de pouvoirs effectifs d'intervention au sens du droit européen (A. EPINEY, *Datenschutz und «Bilaterale II»*, *Zu den Auswirkungen der Schengen-Assoziierung auf das schweizerische Datenschutzrecht – ausgewählte Aspekte*, in RSJ 2006 121/128; A. EPINEY / S. THEUERKAUF, *Datenschutz in Europa – Ueberblick und Implikationen in den Bilateralen II*, in *Datenschutz in Europa und die Schweiz*, *La protection des données en Europe et la Suisse*, p. 75; S. FÜ-

ZESSERY MINELLI / S. BRUNNER, *La protection des données et les Accords Schengen/Dublin*, in *Accords bilatéraux II Suisse-UE et autres accords récents*, éd. C. KADDOUS / M. JAMETTI GREINER, p. 438; B. RUDIN, *Kantonale Datenschutzgesetzgebung: Gesetzpflichtiger Inhalt*, expertise du 28 mars 2007 réalisée sur demande du canton de Saint-Gall, p. 47: «Es geht nicht darum, dem Kontrollorgan Entscheidungsbefugnisse einzuräumen, sondern nur darum, die Möglichkeit zu schaffen, dass es erreichen kann, dass die datenschutzrechtlichen Anliegen Eingang in ein förmliches rechtliches Verfahren finden».)

La LPrD doit être adaptée sur ce point (cf. ci-dessous commentaires relatifs à l'art. 22a ainsi qu'à l'art. 27 al. 2).

#### – *Pouvoir d'ester en justice*

Selon le droit européen, l'autorité de contrôle doit être habilitée à agir en justice en cas de violation des dispositions régissant la protection des données ou à pouvoir porter ces cas à la connaissance de l'autorité judiciaire (art. 28, ch. 3, 3<sup>e</sup> tiret de la directive 95/46/CE et art. 1 ch. 2a du protocole additionnel).

En dehors des infractions pénales poursuivies d'office, qui peuvent être dénoncées aux autorités de poursuite pénale conformément à l'article 146 al. 2 CPP, l'autorité cantonale de surveillance en matière de protection des données ne dispose pas de cette compétence. Il convient donc de compléter la LPrD dans le sens voulu par la directive européenne. Ce pouvoir d'ester en justice a été intégré dans le présent projet sous forme d'un droit de recours (cf. ci-dessous commentaires relatifs à l'art. 22a ainsi qu'à l'art. 27 al. 2).

### d. «Flux transfrontières de données»

Les articles 25 et 26 de la directive 95/46/CE et l'article 2 du protocole additionnel obligent les Etats parties à adopter une réglementation détaillée en matière de «flux transfrontières de données».

La LPrD ne contient pas de règles spécifiques en la matière et doit dès lors être complétée dans ce domaine (cf. ci-dessous commentaire relatif à l'article 12a).

### e. «Cas-limites»

Dans les quatre cas suivants, il apparaît préférable, pour les motifs indiqués ci-dessous, de renoncer à insérer de nouvelles dispositions dans la LPrD.

#### – *Devoir d'informer lors de décisions individuelles automatisées*

L'article 15 de la directive 95/46/CE prescrit que les Etats doivent adopter des règles spécifiques s'agissant du devoir d'informer lors de décisions individuelles automatisées. Ce devoir doit être compris comme un «devoir d'information particulier lorsqu'une décision produisant des effets juridiques ou affectant de manière significative la personne concernée est prise sur le seul fondement d'un traitement automatisé de données visant à évaluer certains aspects de sa personnalité». Il vise à éviter que des décisions soient prises sans appréciation humaine et sans que la personne concernée en soit informée (cf. FF 2003 p. 1945).

La réglementation des décisions de ce type vise toutefois principalement les entreprises privées. Les organes soumis à la LPrD ne sont pas directement concernés.



#### – Contrôle préalable

Selon l'article 20 de la directive 95/46/CE, les Etats membres doivent soumettre à un contrôle préalable les traitements de données susceptibles de présenter des risques particuliers. Il n'est cependant pas nécessaire, dans notre système, de prévoir une disposition sur le contrôle préalable. En effet, le contrôle préalable des actes législatifs, tel qu'il est prévu à l'article 30a al. 1 let. b du projet, qui reprend l'article 30 al. 2 let. b de la loi actuelle, offre une garantie suffisante: le contrôle des traitements effectués par les organes soumis à la LPrD est réalisé dans le cadre du processus législatif. En cas de doute, les organes publics ont naturellement la possibilité de s'adresser au ou à la préposé-e pour s'assurer de la licéité des traitements qu'ils prévoient d'entreprendre.

A signaler que le contrôle préalable n'a pas non plus été introduit dans la LPD.

#### – Sanctions

Selon l'article 24 de la directive 95/46/CE qui reprend l'article 10 de la convention 108, la loi devrait prévoir des sanctions applicables en cas de violation des dispositions sur la protection des données. Ces dispositions ne sont pas reprises dans le projet pour les raisons suivantes.

Les infractions qui constituent une violation du secret de fonction sont déjà sanctionnées en droit actuel (art. 320 CP).

Dans les cas où il n'y a pas violation du secret de fonction, par exemple lorsque des données personnelles sont traitées dans un but autre que celui pour lequel elles ont été collectées ou dans un but qui, selon les règles de la bonne foi, ne peut pas être considéré comme compatible avec celui-ci (cf. art. 5 al. 1 LPrD), le respect des dispositions internationales demanderait en revanche théoriquement que l'on prévienne des sanctions.

En pratique, ces situations pourront cependant à l'avenir être efficacement traitées par l'autorité cantonale de surveillance de la protection des données, grâce aux pouvoirs accrus qui lui sont accordés. Par ailleurs, l'instauration d'un système de sanctions reviendrait à réintroduire, par la petite porte, des éléments relevant du droit disciplinaire, qui a été abandonné en 2003 lors de l'entrée en vigueur de la loi sur le personnel de l'Etat.

Il ne se justifie pas non plus d'introduire un système de sanctions uniquement pour les personnes ou organes qui ne sont pas tenus au secret de fonction, par exemple dans les cas de traitements sur mandat (cf. art. 18 LPrD). En effet, ces personnes ou organes traitent des données sur une base contractuelle impliquant en particulier le respect d'un devoir de discrétion étendu. Le mandataire ne doit pas révéler à des tiers les informations qui lui sont confiées par le mandant; il doit également taire tout ce qu'il apprend ou devine en exerçant son mandat. Il doit également garantir que des tiers ne puissent pas accéder aux données qu'il détient. Par ailleurs, conformément à l'article 18 LPrD, il incombe à l'organe public qui confie des tâches à des tiers de prendre les mesures nécessaires pour écarter les risques de dysfonctionnement et, le cas échéant, y remédier.

#### – Extension du droit à l'information

Le législateur fédéral a introduit dans la LPD une nouvelle disposition régissant l'obligation d'informer lors de la collecte de données personnelles sensibles et de profils de la personnalité (art. 7a nLPD).

Le projet d'adaptation de la LPrD aux exigences du droit international ne contient pas de règle similaire, car, selon le guide pratique du délégué de la CdC, la réglementation de la LPrD actuelle répond déjà aux exigences minimales du droit européen en la matière. L'insertion d'une disposition cantonale étendant le droit à l'information, inspirée du nouvel article 7a LPD, pourra naturellement être étudiée à nouveau dans le prochain volet d'adaptation de la LPrD (cf. ci-dessus ch. 2.a).

## 4. LIGNES DIRECTRICES ET CHAMP D'APPLICATION DU PROJET

### a. Lignes directrices

Les lignes directrices qui ont prévalu lors de l'élaboration du projet sont les suivantes:

- les modifications doivent être limitées à ce qui est nécessaire au vu du droit européen;
- elles doivent transposer les prescriptions européennes de manière à ne pas retarder la mise en application des accords Schengen/Dublin («réussir l'évaluation qui sera réalisée par l'Union européenne»);
- elles doivent s'insérer au mieux dans l'ordre juridique cantonal;
- elles doivent, dans la mesure du possible, ne pas s'écarter des solutions retenues dans la loi fédérale sur la protection des données.

### b. Champ d'application

Le champ d'application de ces modifications s'étend à l'ensemble de la protection des données, telle qu'elle est régie par la LPrD. Une limitation de ce champ d'application aux domaines couverts par les accords Schengen/Dublin ne serait pas admissible, ni praticable du reste. En effet, les dispositions du protocole additionnel ont un champ d'application général et ne sont pas limitées au dossier Schengen/Dublin. Par ailleurs, dans le domaine du traitement des données, on ne peut pas «compartimenter» strictement les données dans des catégories étanches. Le standard minimal exigé par l'Union européenne ne peut être garanti que si les exigences de la directive 95/46/CE sont appliquées de manière générale. Finalement, sur le plan interne, il serait difficile de justifier une différence dans la protection accordée par l'Etat selon que les données traitées relèvent du domaine Schengen/Dublin ou non.

## 5. COMMENTAIRE DES ARTICLES

### *Remarque préalable*

La LPrD actuelle est formulée au masculin. Il est souhaitable de saisir l'occasion de la révision en cours pour adapter les dispositions de cette loi aux exigences de la formulation non sexiste, en application des recommandations applicables en la matière. Seules sont toutefois commentées ci-dessous les modifications ayant une portée matérielle.

## Article 12a

La LPrD actuelle ne règle pas expressément les flux transfrontières de données (communications de données à l'étranger).

Conformément à l'article 25 de la directive 95/46 et à l'article 2 du protocole additionnel, les transferts de données personnelles vers des Etats tiers ne doivent en principe être autorisés que si ces Etats offrent un niveau de protection adéquat. Si le niveau de protection requis n'est pas garanti, le transfert doit être interdit sauf dans des cas exceptionnels, à savoir lorsque le droit interne prévoit la possibilité du transfert pour des intérêts spécifiques de la personne concernée ou lorsque des intérêts légitimes prévalent, en particulier des intérêts publics importants, ou encore lorsque des garanties pouvant notamment résulter de clauses contractuelles sont fournies par la personne responsable du transfert et sont jugées suffisantes par les autorités compétentes.

Ces dispositions doivent être transposées en droit suisse. Au plan fédéral, un nouvel article 6 a été inséré à cet effet dans la LPD. L'article 12a du projet cantonal reprend matériellement cet article.

L'alinéa 1 énonce le principe selon lequel la communication de données personnelles à l'étranger n'est possible que dans les Etats offrant un niveau de protection adéquat. En principe, l'Etat destinataire offre un tel niveau de protection lorsque sa législation répond aux exigences de la convention 108. Il convient cependant de tenir compte également, dans la mesure du possible, de la manière dont est appliquée la loi étrangère.

L'alinéa 2 énumère les cas exceptionnels dans lesquels une communication est admise, bien que l'Etat destinataire n'offre pas de garanties suffisantes. La formulation des exceptions correspond à celle retenue dans la LPD. Il est ainsi clair que les exceptions prévues par le droit cantonal doivent être interprétées de la même manière que celles qui sont applicables au niveau fédéral. Toutefois, les lettres f) et g) de l'article 6 al. 2 LPD ne sont pas reprises dans le projet cantonal, car elles visent des cas qui n'entrent pas dans le champ d'application de la LPrD.

L'alinéa 3 précise que l'organe public doit informer le ou la préposée cantonal-e à la protection des données de l'existence des garanties prévues à l'alinéa 2 let. a) préalablement au transfert des données personnelles.

A noter que le préposé fédéral à la protection des données et à la transparence tiendra une liste des Etats dont la législation offre un niveau de protection adéquat.

## Article 22a

L'article 28 ch. 3 2<sup>e</sup> tiret de la directive 95/46/CE et l'article 1 ch. 2a du protocole additionnel prescrivent que les autorités de contrôle en matière de protection des données doivent être dotées de pouvoirs effectifs d'intervention (cf. ci-dessus ch. 3.c).

Le mécanisme retenu à l'article 22a du projet permet d'ancrer dans la législation cantonale les pouvoirs effectifs d'intervention de l'autorité de surveillance de la protection des données, en restant le plus proche possible de la situation actuelle, qui a fait ses preuves.

Ce mécanisme s'articule de la manière suivante:

Dans un *premier temps*, en cas de violation ou de risque de violation des dispositions sur la protection des don-

nées, l'autorité de surveillance de la protection des données formule, comme actuellement, des recommandations (art. 22a al. 1). Elle peut proposer que soient prises toutes les mesures nécessaires au rétablissement ou au maintien d'une situation juridiquement correcte en relation avec le traitement des données personnelles, tel que décrit à l'article 3 let. d LPrD. A titre d'exemples, on peut mentionner l'interdiction de la collecte, l'interdiction de la communication ou la destruction des données.

Le destinataire de la recommandation sera, suivant les cas, l'organe concerné (art. 22a al. 1) ou l'autorité hiérarchique à laquelle il est subordonné (art. 22a al. 2).

Lorsque les violations ou risques de violation sont le fait d'entités hiérarchiquement indépendantes (par exemple la direction d'un établissement ou un conseil communal), l'autorité de surveillance leur transmet directement ses recommandations.

En revanche, lorsque les problèmes sont le fait d'un organe ou d'une personne soumis à un lien de subordination hiérarchique, il convient, dans l'idée de responsabiliser tous les organes concernés, d'informer l'autorité hiérarchique supérieure. Cette autorité exerce en effet une surveillance complète sur ses subordonnés et est ainsi en mesure d'exiger d'eux qu'ils respectent les dispositions applicables en matière de protection des données.

Lorsqu'un organe public fait traiter des données personnelles par un tiers, la situation est similaire à celle qui est réalisée lorsqu'il existe un lien hiérarchique (cf. art. 18). L'organe public dispose, sous l'angle qui intéresse la concrétisation des pouvoirs effectifs d'intervention, de pouvoirs analogues à ceux d'une autorité hiérarchique supérieure. C'est donc à lui que doivent être adressées les recommandations de l'autorité de surveillance.

Dans un *second temps*, le destinataire de la recommandation doit se prononcer, dans le délai imparti par l'autorité de surveillance, sur la suite qu'il entend donner à cette recommandation. Il le fait par voie de décision (art. 22a al. 3).

Cette décision est particulière. En effet, elle ne correspond pas exactement à la notion de décision telle qu'elle est définie à l'article 4 du code de procédure et de juridiction administrative (CPJA): alors que, selon le CPJA, la décision est, pour l'essentiel, une mesure adoptée dans un cas d'espèce en vue de créer, de modifier, d'annuler ou de constater des droits ou des obligations, l'article 22a al. 3 ss du projet vise des «décisions» par lesquelles les destinataires des recommandations expriment simplement leur volonté de suivre, de suivre partiellement ou de ne pas suivre lesdites recommandations.

Les exigences du droit international imposent cependant que l'on introduise dans notre législation ces décisions d'un type particulier (concrétisation des pouvoirs effectifs d'intervention; cf. ci-dessus ch. 3, c, 1<sup>er</sup> tiret). Les dispositions du CPJA régissant les décisions au sens de l'article 4 de ce code sont applicables par analogie aux décisions prévues à l'article 22a al. 3 du projet.

Dans un *troisième temps*, l'autorité de surveillance de la protection des données a la possibilité d'exiger le respect de sa recommandation en s'adressant à l'autorité ordinaire de recours désignée par le CPJA (al. 4). A défaut d'autorité compétente au sens du CPJA, par exemple lorsque la décision émane d'une Eglise reconnue, le recours doit être adressé au Tribunal cantonal unifié (al. 5).

La procédure spéciale instituée à l'article 22a du projet n'est ouverte qu'aux autorités de surveillance de la protection des données (al. 4 *in fine*). Le projet ne va pas au-delà des exigences du droit international et les particuliers qui pourraient éventuellement être concernés par la violation des règles sur la protection des données doivent, comme c'est le cas actuellement, agir par le biais de l'article 27 LPrD.

Ainsi conçu, ce nouveau mécanisme complète le droit de recours prévu à l'article 27 al. 2 du projet et permet à l'autorité de surveillance de la protection des données d'intervenir efficacement également dans les cas de violations de la loi qui ne lèsent pas directement des personnes concernées au sens des articles 23 à 26 LPrD.

#### **Article 27 al. 2**

Cette disposition renforce les pouvoirs de l'autorité de surveillance de la protection des données conformément à l'article 28 ch. 3, 3<sup>e</sup> tiret de la directive 95/46/CE et à l'article 1 ch. 2a du protocole additionnel, qui exigent que les autorités de contrôles disposent du «pouvoir d'ester en justice» en cas de violation des dispositions applicables en matière de protection des données.

En droit actuel, en dehors des cas d'infractions pénales poursuivies d'office qui peuvent être dénoncées aux autorités de poursuite pénale conformément à l'article 146 al. 2 CPP, seules les personnes dont les droits ou obligations pourraient être atteints par les décisions relatives au traitement de données personnelles ont qualité pour recourir (cf. art. 76 CPJA).

Il convient donc de compléter l'article 27 de la LPrD de manière à étendre la qualité pour recourir à l'autorité de surveillance de la protection des données. Les autorités de recours sont définies aux articles 114 ss CPJA, conformément au renvoi de l'article 27 al. 1 LPrD.

Compte tenu de la volonté de mettre en place un système de contrôle efficace au sens du droit européen, il est nécessaire que l'autorité de surveillance de la protection des données ait connaissance de toutes les décisions susceptibles de recours. A défaut, son contrôle ne pourrait être qu'aléatoire. Le projet prévoit donc que les organes publics communiquent à l'autorité de surveillance de la protection des données les décisions qu'ils prennent en application des articles 23 à 26 LPrD.

Pour le surplus, cf. ci-dessus chiffre 3.c.

#### **Article 29 al. 2 et 3**

Ces dispositions fixent les conditions minimales que doivent remplir les autorités communales de surveillance de la protection des données.

On ne saurait se satisfaire d'un niveau de protection inférieur pour la seule raison que les traitements des données personnelles sont surveillés par un organe communal. Dès lors, comme les engagements internationaux pris par la Suisse imposent des exigences strictes en matière d'autorité de contrôle, les autorités communales compétentes doivent remplir ces exigences. Si tel n'est pas le cas, il appartient à l'autorité cantonale de surveillance de veiller au respect de la protection des données par les communes concernées.

Par rapport à la situation actuelle, l'article 29 al. 2 du projet renforce les pouvoirs des autorités communales de surveillance de la protection des données. Elles devront

en particulier avoir la qualité pour recourir lorsque les droits d'une personne concernée par un traitement de données sont lésés (cpr art. 27 al. 2 et 30a al. 1 let. d du projet) et être dotées de pouvoirs effectifs d'intervention (cpr art. 22a et 30a al. 1 let. c du projet; cf. également ci-dessus chiffre 3.c).

Par ailleurs, en vertu de l'alinéa 3, les communes devront garantir l'indépendance de leur autorité de surveillance. Cette indépendance comporte un aspect institutionnel, dans le sens où il faut éviter que le surveillant soit soumis d'une manière ou d'une autre à l'influence des personnes et organes qu'il doit contrôler, par exemple en raison de son mode d'élection, de la réglementation de ses rapports de travail, etc. Elle a également une composante financière, dans le sens où l'autorité de surveillance doit être dotée des moyens, financiers et en personnel, nécessaires à l'accomplissement de ses tâches et être libre de disposer comme elle le juge utile du budget qui lui est alloué, à l'instar de l'autorité cantonale de surveillance de la protection des données (sur la notion de l'indépendance, cf. également ci-dessus chiffre 3.b).

A noter que l'article 29 al. 2 de la LPrD actuelle donne déjà la possibilité aux communes d'instituer leur propre autorité de surveillance. Les communes de Bulle, Fribourg, Marly et Villars-sur-Glâne se sont dotées d'une telle autorité. Il incombe à ces communes de veiller à ce que l'organe de surveillance qu'elles ont institué réponde aux exigences du droit européen. Il existe des solutions permettant de réduire les inconvénients du nouveau système. Une piste envisageable pourrait par exemple être celle des regroupements de communes.

#### **Articles 30 à 32**

Les dispositions de la LPrD actuelle régissant l'autorité cantonale de surveillance en matière de protection des données ne satisfont pas entièrement aux exigences minimales requises par la directive 95/46/CE et par le protocole additionnel (cf. ci-dessus ch. 3.b et 3.c).

Techniquement, l'insertion des modifications requises dans la LPrD appelle une restructuration formelle des articles 30 à 32. Seules les modifications matérielles sont commentées ci-dessous. Elles concernent les articles 30, 30a al. 1 let. c et d, 31a al. 1 let. f et g, et 32 al. 3 à 6.

##### **a. Article 30**

L'article 28 ch. 1 de la directive 95/46/CE et l'article 1 ch. 3 du protocole additionnel prescrivent que les autorités de contrôle doivent exercer leurs tâches en toute indépendance (cf. également ci-dessus ch. 3.b).

L'indépendance institutionnelle de la Commission cantonale de la protection des données est déjà garantie par les règles actuelles de la LPrD (cf. en particulier l'art. 30 al. 1). Le projet reprend par conséquent textuellement cette disposition, en précisant cependant que la durée du mandat du président ou de la présidente et des membres de la Commission est de quatre ans, conformément aux dispositions de la loi réglant la durée des fonctions publiques accessoires. Cette durée correspond à la durée actuelle des mandats.

Toutefois, en pratique, la Commission cantonale de la protection des données ne peut exercer ses tâches de manière vraiment indépendante que si elle dispose des connaissances spécifiques indispensables à une surveillance efficace. A cet égard, le domaine de la santé et



celui de l'informatique sont particulièrement sensibles. Il est par conséquent nécessaire que la Commission bénéficie directement de connaissances particulières dans ces deux domaines. Pour le surplus, elle doit être composée de représentants et de représentantes des domaines les plus concernés par la protection des données. Le choix doit être guidé par les besoins de la Commission et par la disponibilité des personnes disposant des compétences requises pour siéger en son sein (al. 2).

Comme il n'est matériellement pas possible de rassembler toutes les connaissances nécessaires au sein de la Commission, le projet rappelle formellement qu'elle peut s'adjoindre le soutien d'experts ou d'expertes ou faire appel à des tiers (al. 3).

Sur la question de l'indépendance budgétaire, cf. le nouvel article 32 al. 3.

b. Article 30a al. 1 let. c

L'article 30a al. 1 let. c renvoie simplement au nouvel article 22a (cf. ci-dessus ch. 3.c et commentaire relatif à l'art. 22a).

c. Article 30a al. 1 let. d

L'article 30a al. 1 let. d renvoie simplement au nouvel article 27 al. 2 (cf. ci-dessus ch. 3.c et commentaire relatif à l'art. 27 al. 2).

d. Article 31 al. 1 let. f et g

Il convient de compléter la liste des attributions du ou de la préposée par deux nouvelles tâches liées au renforcement de la surveillance de la protection des données sur le plan international.

A la lettre f), la collaboration entre les divers organes de contrôle doit être comprise comme un échange d'informations utiles. A signaler que la collaboration est prévue à l'article 28 ch. 6 de la directive 95/46/CE et à l'article 1 ch. 5 du protocole additionnel.

La lettre g) découle quant à elle du nouvel article 12a sur les «flux transfrontières de données».

e. Article 32 al. 3 à 6

L'indépendance totale voulue par le droit européen exige que le statut financier de l'autorité cantonale de surveillance en matière de protection des données soit réaménagé. Cette autorité doit être dotée d'un budget propre, dont elle puisse disposer librement en fonction des besoins liés à l'accomplissement de ses tâches. Cf. références citées ci-dessus ch. 3 b.

En application de ces exigences, l'alinéa 3 de l'article 32 prescrit que l'autorité cantonale de surveillance dispose d'une enveloppe budgétaire.

Les alinéas 4 à 6 correspondent aux exigences posées par le droit européen en matière d'indépendance personnelle des membres des autorités de contrôle pour renforcer la confiance des autorités et de la population à l'égard de ces autorités.

L'alinéa 4 reprend l'alinéa 3 de la LPrD actuelle en le complétant par une adjonction concernant l'obligation de discrétion. Il est ainsi clair que les membres de l'autorité cantonale de surveillance sont soumis à cette obligation, au même titre que les membres des autres commissions de l'Etat (cf. art. 26 du règlement sur l'organisation et le fonctionnement des commissions de l'Etat).

L'alinéa 5 est une nouveauté dans le canton. L'obligation de signaler les liens d'intérêts est cependant déjà connue en droit fédéral et dans d'autres législations cantonales. Les intérêts visés sont par exemple les activités professionnelles, les fonctions assumées au sein de commissions ou au sein d'organes de direction, de surveillance ou de conseil de personnes morales, les fonctions politiques, etc.

L'alinéa 6 est introduit dans le projet pour des motifs de transparence; il explicite simplement un principe déjà applicable en droit actuel.

## **6. RÉPARTITION DES TÂCHES ETAT-COMMUNES**

Théoriquement, le projet n'a pas d'incidence sur la répartition des tâches entre l'Etat et les communes. En pratique, il est toutefois possible qu'il exerce un effet dissuasif sur les communes, en raison des nouvelles exigences à remplir par les autorités de surveillance. Si les communes renonçaient à instituer leurs propres autorités de surveillance, il en résulterait un transfert des tâches correspondantes à l'Etat.

## **7. CONSTITUTIONNALITÉ ET CONFORMITÉ AU DROIT FÉDÉRAL ET EUROPÉEN**

Le projet est conforme à la Constitution cantonale (cf. art. 12 Cst.) et au droit fédéral. Par ailleurs son objectif étant l'adaptation de la législation cantonale aux deux instruments juridiques européens principaux en matière de protection des données (directive 95/46/CE et convention 108, y compris son protocole additionnel), il est également conforme au droit européen.

## **8. CONSÉQUENCES FINANCIÈRES ET EN PERSONNEL**

Le projet de révision, en particulier la mise en œuvre des pouvoirs effectifs d'intervention qui visent à garantir un contrôle efficace au sens de la réglementation européenne, impliquent de nouvelles tâches pour l'autorité cantonale de surveillance:

Conformément à l'article 27 al. 2, cette dernière devra à l'avenir examiner les décisions qui sont communiquées au ou à la préposé-e et déposer les éventuels recours nécessaires à l'encontre de ces décisions.

Elle devra également procéder aux contrôles nécessaires à la mise en œuvre de l'article 22a, ou mandater des tiers à cet effet. A cet égard, elle devra disposer de moyens financiers et en personnel lui permettant d'intervenir activement auprès des organes concernés par la LPrD. Des interventions réactives, faisant suite à des requêtes qui lui seraient adressées, ne sauraient être considérées comme suffisantes au regard des exigences européennes.

Par ailleurs, si elle constate des dysfonctionnements, l'autorité cantonale de surveillance aura, selon le projet, des tâches complémentaires par rapport à la situation actuelle. Elle ne se bornera pas à édicter des recommandations sur les mesures à prendre pour remédier aux problèmes, comme c'est le cas aujourd'hui. Au contraire, si ses recommandations ne sont pas suivies d'effet, elle aura pour tâche de recourir auprès de l'autorité judiciaire

compétente, afin de garantir le respect des dispositions sur la protection des données.

Ces tâches supplémentaires requièrent le renforcement des effectifs en personnel dont dispose le ou la préposé-e à la protection des données. L'augmentation se monte à 0,5 ÉPT. De plus, les montants alloués pour les travaux de la Commission et pour les contrôles externes devront être augmentés de manière appropriée.

Compte tenu de ces divers éléments, l'enveloppe budgétaire destinée à l'autorité cantonale de surveillance de la protection des données devrait, à l'avenir, se monter à 250 000 francs par année (ce qui correspond à une augmentation de 50 000 francs par rapport à la situation actuelle).

---

**BOTSCHAFT Nr. 56** 4. März 2008  
**zum Entwurf des Gesetzes zur Änderung des Gesetzes über den Datenschutz (Anpassung an das internationale Recht, insbesondere an die Abkommen von Schengen und Dublin)**

Wir unterbreiten Ihnen einen Gesetzesentwurf zur Anpassung des Gesetzes über den Datenschutz an die einschlägigen internationalen Verpflichtungen der Schweiz (Abkommen von Schengen/Dublin und Zusatzprotokoll zum Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten).

Diese Botschaft ist wie folgt gegliedert:

1. Internationale Verpflichtungen der Schweiz
2. Ablauf der Arbeiten
3. Notwendigkeit einer Anpassung des DSchG
4. Leitlinien und Geltungsbereich des Gesetzesentwurfs
5. Kommentar zu den einzelnen Artikeln
6. Aufgabenteilung Staat–Gemeinden
7. Verfassungsmässigkeit, Bundesrechtskonformität und Europaverträglichkeit
8. Finanzielle und personelle Auswirkungen

## **1. INTERNATIONALE VERPFLICHTUNGEN DER SCHWEIZ**

Die Europäische Union und der Europarat haben Rechtsinstrumente zur internationalen Harmonisierung des Datenschutzes ausgearbeitet. Diese legen einen Mindestschutz fest, der in allen Mitgliedstaaten gewährleistet sein muss. Die wichtigsten Rechtsinstrumente sind:

- Europäische Union: *Richtlinie 95/46/EG* des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr;
- Europarat: Übereinkommen vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (*Übereinkommen 108*) und sein *Zusatzprotokoll* vom 8. November 2001 be-

züglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung.

Die Schweiz hat sich mit dem Abkommen zwischen der Schweizerischen Eidgenossenschaft, der Europäischen Union und der Europäischen Gemeinschaft über die Assoziierung dieses Staates bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands verpflichtet, den Inhalt der Richtlinie 95/46/EG anzuwenden (vgl. BBl 2004 S. 6467).

Zudem haben die eidgenössischen Räte am 24. März 2006 den Bundesbeschluss betreffend den Beitritt der Schweiz zum Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten verabschiedet (BBl 2006 S. 3649). Dieses Protokoll wird dem Bundesrat zur Ratifikation unterbreitet und wird voraussichtlich am 1. April 2008 in Kraft treten.

Infolgedessen müssen die Bestimmungen dieser beiden europäischen Rechtsakte in das schweizerische und das kantonale Recht überführt werden. Dies ist der Zweck der vorliegenden Gesetzesvorlage. Es gilt zu beachten, dass die Revision des Bundesgesetzes über den Datenschutz (DSG) am gleichen Tag angenommen wurde wie das Zusatzprotokoll, d.h. am 24. März 2006. Die neuen Bundesbestimmungen sind am 1. Januar 2008 in Kraft getreten.

## **2. ABLAUF DER ARBEITEN**

### **a. Allgemeines**

Am 15. September 2006 setzte die Sicherheits- und Justizdirektion eine Arbeitsgruppe ein, die den Auftrag hatte, einen Gesetzesvorentwurf zur Änderung des kantonalen Datenschutzgesetzes und einen Kommentar dazu auszuarbeiten. Die Arbeitsgruppe wurde von Alexandra Rumo-Jungo, Professorin an der Universität Freiburg und Präsidentin der kantonalen Datenschutzkommission, geleitet und setzte sich wie folgt zusammen: Christophe Maillard, Rechtsberater ILFD, Dominique Nouveau Stoffel, kantonale Datenschutzbeauftragte, Guy Python, Datenschutzbeauftragter der Stadt Freiburg, Thierry Steiert, wissenschaftlicher Berater SJD, Luc Vollery, Rechtsberater GeGA (im November 2006 abgelöst von Josette Moullet Auberson, Rechtsberaterin GeGA), und Grossrätin Marie-Thérèse Weber-Gobet. Das Sekretariat und das Protokoll führte Lydia Oberson, Mitarbeiterin der kantonalen Aufsichtsbehörde für Datenschutz.

Die geplante Revision hatte ursprünglich drei Ziele:

- Anpassung des kantonalen Datenschutzgesetzes (DSchG) an die Richtlinie 95/46 EG und an das oben erwähnte Zusatzprotokoll;
- Anpassung des DSchG an die kürzlich erfolgte Revision des DSG;
- Anpassung des DSchG aufgrund der seit seinem Inkrafttreten gemachten Erfahrungen.

Es zeigte sich jedoch rasch, dass es nicht möglich war, alle drei Ziele innerhalb der Frist zu verwirklichen, die der Bund zur Anpassung der kantonalen Gesetze an die Abkommen von Schengen und Dublin gesetzt hatte. Daher wurde der Auftrag der Arbeitsgruppe auf den ersten Punkt beschränkt, d.h. die Anpassung des DSchG an das internationale Recht. Die beiden anderen Aspekte werden im Rahmen einer späteren Revision behandelt werden.



b. Unterstützung der Konferenz der Kantonsregierungen (KdK) und der Konferenz der kantonalen Justiz- und Polizeidirektoren (KKJPD)

Die KdK und die KKJPD sind mit der Umsetzung und Entwicklung der Abkommen von Schengen und Dublin in Bezug auf die Kantone betraut. Sie beauftragten den Datenschutzspezialisten Beat Rudin (nachfolgend: Beauftragter der KdK), für die Umsetzung der mit den Abkommen von Schengen und Dublin übernommenen Datenschutzvorschriften eine Wegleitung zuhanden der Kantone auszuarbeiten. Die Wegleitung besteht aus einer mit Erläuterungen versehenen Liste mit den allgemeinen Bedingungen, die die Gesetzgebung der Kantone im Rahmen der Assoziierung an Schengen/Dublin und der Umsetzung des Zusatzprotokolls in Bezug auf den Datenschutz erfüllen muss. Sie diene der mit der Revision beauftragten Arbeitsgruppe als Arbeitsgrundlage.

c. Vernehmlassungsverfahren

Der Staatsrat hat den von der Arbeitsgruppe ausgearbeiteten Vorentwurf mit einigen kleineren Änderungen vom 31. Mai bis zum 31. August 2007 einem breiten Vernehmlassungsverfahren unterzogen.

Im Allgemeinen wurde der Entwurf des Staatsrates gut aufgenommen. Zahlreiche Vorbehalte wurden seitens der Gemeinden geäussert, da die Schaffung von kommunalen Datenschutzbehörden, die den Anforderungen des internationalen Rechts genügen, mit Schwierigkeiten verbunden wäre. Die Erweiterung der Kompetenzen der Datenschutzbehörden wurde von zwei Vernehmlassungsteilnehmern kritisiert. Des Weiteren wurden einzelne Bemerkungen angebracht, welche in der Schlussfassung des Entwurfs berücksichtigt wurden, sofern sie mit dem internationalen Recht übereinstimmen und im Zusammenhang mit der vorliegenden Revision stehen, d.h. mit der Anpassung des geltenden Gesetzes an die internationalen Verpflichtungen der Schweiz.

### 3. NOTWENDIGKEIT EINER ANPASSUNG DES DSCHG

a. Allgemeines

Die Überprüfung des DSchG anhand der Wegleitung hat gezeigt, dass das geltende Gesetz dem geforderten Standard bereits weitgehend entspricht.

Insbesondere in Bezug auf die Rechtsform (Gesetz im formellen Sinn) und die Bestimmungen über den Geltungsbereich des Gesetzes, die Grundsätze für die Bearbeitung von Personendaten und die Rechte der betroffenen Personen genügt das Gesetz den Anforderungen, die sich durch die internationalen Verpflichtungen der Schweiz ergeben.

Trotzdem wurden einige Mängel festgestellt, die eine Anpassung des DSchG notwendig machen. Dies betrifft die Unabhängigkeit der Aufsichtsbehörde für Datenschutz (b.), ihre Befugnisse (c.) und die Regelung der «grenzüberschreitenden Datenübermittlung» (d.).

Im Laufe der Arbeiten zeigte sich im Übrigen, dass es nicht immer leicht ist festzustellen, ob die geltende Gesetzgebung den Anforderungen des Europarechts entspricht oder nicht. Die nicht in den Entwurf aufgenommenen «Grenzfälle» werden im Folgenden aus Transparenzgründen ebenfalls aufgeführt (e.).

Die Bestimmungen der Richtlinie 95/46/EG sowie des Übereinkommens 108 und seines Zusatzprotokolls gelten übrigens für die gesamte Datenschutzaufsicht, einschliesslich der allfälligen Aufsicht durch kommunale Aufsichtsbehörden und Behörden der kirchlichen Körperschaften.

b. Unabhängigkeit der Aufsichtsbehörden

Gemäss Artikel 28 Abs. 1 der Richtlinie 95/46/EG und Artikel 1 Ziff. 3 des Zusatzprotokolls müssen die Aufsichtsbehörden die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit ausüben.

Die Garantie der völligen Unabhängigkeit der Aufsichtsbehörden für den Datenschutz umfasst in der Praxis institutionelle und personelle Aspekte (A. EPINEY, Datenschutz und «Bilaterale II», Zu den Auswirkungen der Schengen-Assoziierung auf das schweizerische Datenschutzrecht – ausgewählte Aspekte, *in* SJZ 2006 121/126 ff.; A. EPINEY / S. THEUERKAUF, Datenschutz in Europa – Ueberblick und Implikationen in den Bilateralen II, *in* Datenschutz in Europa und die Schweiz, La protection des données en Europe et la Suisse, S. 71 ff; B. BUDIN. / B. BAERISWYL, «Schengen» und der Datenschutz in den Kantonen: Anforderungen – Beurteilung – Handlungsbedarf, *in* Datenschutz in Europa und die Schweiz, La protection des données en Europe et la Suisse, S. 193 ff.).

Zu den Kernelementen auf institutioneller Ebene gehören der Wahlmodus der Aufsichtsbehörde, ihre Stellung innerhalb der Organisation des Kantons, ihre Budgetautonomie und ihre Unabhängigkeit bei der Planung und Ausführung ihrer Tätigkeit sowie das Anstellungsverhältnis ihrer Leiterin oder ihres Leiters und dessen Auflösung.

Zu den personellen Aspekten gehört dagegen, dass die mit der Datenschutzaufsicht beauftragten Personen über die persönlichen und fachlichen Qualifikationen verfügen, die für die Ausübung ihrer Aufgaben erforderlich sind, und dass sie keinen Interessenkonflikten ausgesetzt sind. Diese letzte Bedingung bedeutet, dass die Betroffenen verpflichtet sind, ihre öffentlichen und privaten Interessenbindungen offen zu legen und in den Ausstand zu treten, wenn die Behörde Dossiers behandelt, die sie besonders betreffen.

In der Praxis ist der Unabhängigkeitsgrad der Aufsichtsbehörden von der Kombination dieser verschiedenen Elemente abhängig. Eine Wahl durch das Parlament und eine Angliederung an das Parlament bieten natürlich eine optimale Garantie für die Unabhängigkeit der Aufsichtsbehörde. Ein Defizit wie z.B. eine Ernennung durch die Exekutive (was einer Ernennung des Kontrolleurs durch den Kontrollierten gleichkommt) kann jedoch durch andere institutionelle Garantien wettgemacht werden.

Mit der jetzigen Organisation der kantonalen Aufsichtsbehörde für Datenschutz, die sich aus einer Kommission und einer oder einem Datenschutzbeauftragten zusammensetzt, ist deren Unabhängigkeit bereits weitgehend gesichert. Die Kommission wird vom Grossen Rat gewählt, dem sie jedes Jahr einen Datenschutzbericht vorlegen muss. Aufgrund dieser wichtigen Rolle des Parlaments verfügt die Aufsichtsbehörde über eine ausreichende Unabhängigkeit, während die oder der Datenschutzbeauftragte vom Staatsrat ernannt wird. Auf organisatorischer Ebene ist weiter zu beachten, dass die Aufsichtsbehörde für Datenschutz lediglich administrativ einer Direktion des Staatsrats zugewiesen ist und dass

zwischen dieser Behörde einerseits und der Exekutive und der Verwaltung andererseits folglich kein Subordinationsverhältnis besteht (vgl. Art. 61 SVOG).

Aus diesem Grund ist es sinnvoll, das bisherige System beizubehalten und lediglich einige Anpassungen vorzunehmen, um die Unabhängigkeit der kantonalen Aufsichtsbehörde für Datenschutz zu stärken, wie dies die europäischen Bestimmungen vorschreiben. Diese Anpassungen betreffen Artikel 30 und 32 des Gesetzesentwurfs (vgl. im Übrigen den Kommentar zu diesen Bestimmungen).

### c. Befugnisse der Aufsichtsbehörden

Nach Artikel 28 Abs. 3 erster und zweiter Spiegelstrich der Richtlinie 95/46/EG sowie Artikel 1 Ziff. 2a des Zusatzprotokolls müssen die Aufsichtsbehörden über «wirksame Einwirkungsbefugnisse» und ein «Klagerecht» bei Verstössen gegen die Gesetzesvorschriften im Bereich des Datenschutzes verfügen.

#### – Wirksame Einwirkungsbefugnisse

Die wirksamen Einwirkungsbefugnisse umfassen laut Artikel 28 Abs. 3 zweiter Spiegelstrich der Richtlinie 95/46/EG, der Artikel 1 Ziff. 2a des Zusatzprotokolls konkretisiert, vor allem die Befugnis, «vor der Durchführung der Verarbeitungen Stellungnahmen abzugeben und für eine geeignete Veröffentlichung der Stellungnahmen zu sorgen, oder die Befugnis, die Sperrung, Löschung oder Vernichtung von Daten oder das vorläufige oder endgültige Verbot einer Verarbeitung anzuordnen, oder die Befugnis, eine Verwarnung oder eine Ermahnung an den für die Verarbeitung Verantwortlichen zu richten oder die Parlamente oder andere politische Institutionen zu befassen». Diese verschiedenen Massnahmen werden in der Richtlinie als Beispiele aufgeführt. Daraus lässt sich schliessen, dass die Aufzählung keinen kumulativen Charakter hat.

Die einzelstaatlichen Gesetzgebungen müssen ein System einführen, das die tatsächliche Einhaltung der Datenschutzvorschriften gewährleistet. In den Erwägungen zur Richtlinie 95/46 EG wird denn auch festgehalten, dass das nationale Recht einen Rechtsbehelf vorsehen muss für den Fall, dass die Rechte betroffener Personen durch die für die Datenverarbeitung zuständige Person missachtet werden. Laut Bericht zum Zusatzprotokoll müssen die Mitgliedstaaten dem Kontrollorgan die Befugnis zuweisen, Behörden zu kontrollieren, bzw. Klage zu erheben oder jegliche Verletzung von Datenschutzgrundsätzen der Justiz zu unterbreiten. Dieser Pflicht können die Mitgliedstaaten dadurch nachkommen, dass sie der Behörde die Befugnis zum Erlass von bindenden Verfügungen übertragen (vgl. Ziff. 15).

Die heutigen Eingriffsbefugnisse der kantonalen Aufsichtsbehörde für Datenschutz vermögen den oben erwähnten Anforderungen nicht zu genügen. Nach Artikel 30 Abs. 2 Bst. c DSchG ist die kantonale Datenschutzkommission lediglich befugt, die zuständigen Behörden aufzufordern, die notwendigen Massnahmen zu ergreifen, wenn gesetzliche Vorschriften verletzt werden oder verletzt werden könnten. Mit diesem Empfehlungsrecht ist nicht gewährleistet, dass solche Verstösse bzw. die Gefahr solcher Verstösse verhindert werden. Die ordentlichen Mechanismen zur Kontrolle der Verwaltungstätigkeit erlauben es der kantonalen Aufsichtsbehörde also nicht, die Grundsätze des DSchG gegen den Willen der Behörden, insbesondere des Staatsrats, durchzusetzen.

Die Oberaufsicht durch den Grossen Rat (vgl. Art. 189 Abs. 1 GRG) garantiert keine wirksamen Einwirkungsbefugnisse im Sinne des Europarechts (A. EPINEY, Datenschutz und «Bilaterale II», Zu den Auswirkungen der Schengen-Assoziierung auf das schweizerische Datenschutzrecht – ausgewählte Aspekte, in RSJ 2006 121/128; A. EPINEY / S. THEUERKAUF, Datenschutz in Europa – Ueberblick und Implikationen in den Bilateralen II, in Datenschutz in Europa und die Schweiz, La protection des données en Europe et la Suisse, S. 75; S. FÜZZESSERY MINELLI / S. BRUNNER, La protection des données et les Accords Schengen/Dublin, in Accords bilatéraux II Suisse-UE et autres accords récents, éd. C. KADDOUS / M. JAMETTI GREINER, S. 438; B. RUDIN, Kantonale Datenschutzgesetzgebung: Gesetzpflichtiger Inhalt, Gutachten vom 28. März 2007, erstellt auf Antrag des Kantons St. Gallen, S. 47: «Es geht nicht darum, dem Kontrollorgan Entscheidungsbefugnisse einzuräumen, sondern nur darum, die Möglichkeit zu schaffen, dass es erreichen kann, dass die datenschutzrechtlichen Anliegen Eingang in ein förmliches rechtliches Verfahren finden».).

Daher muss das DSchG in diesem Punkt geändert werden (vgl. Kommentar zu Artikel 22a sowie Art. 27 Abs. 2).

#### – Klagerecht

Gemäss europäischem Recht muss die Aufsichtsbehörde bei Verstössen gegen Datenschutzvorschriften über ein «Klagerecht» verfügen bzw. über das Recht, solche Fälle der Gerichtsbehörde zur Kenntnis zu bringen (Art. 28 Abs. 3 dritter Spiegelstrich der Richtlinie 95/46/EG und Art. 1 Ziff. 2a des Zusatzprotokolls).

Mit Ausnahme der Offizialdelikte, die gemäss Artikel 146 Abs. 2 StGB den Strafverfolgungsbehörden angezeigt werden können, verfügt die kantonale Aufsichtsbehörde für Datenschutz über kein Klagerecht. Deshalb muss das DSchG an die europäische Richtlinie angepasst werden. Dieses Klagerecht wird in Form eines Beschwerderechts in diesen Entwurf aufgenommen (vgl. Kommentar zu Art. 22 a sowie zu Art. 27 Abs. 2).

### d. «Grenzüberschreitende Datenübermittlung»

Die Artikel 25 und 26 der Richtlinie 95/46/EG sowie Artikel 2 des Zusatzprotokolls verpflichten die Vertragsstaaten, die «grenzüberschreitende Datenübermittlung» detailliert zu regeln.

Das DSchG enthält keine spezifischen Bestimmungen zum grenzüberschreitenden Datenverkehr und muss deshalb ergänzt werden (vgl. Kommentar zu Artikel 12a).

### e. «Grenzfälle»

In den folgenden vier Fällen wurde aus den nachstehend geschilderten Gründen darauf verzichtet, neue Bestimmungen in das DSchG aufzunehmen.

#### – Informationspflicht bei automatisierten Einzelentscheidungen

Artikel 15 der Richtlinie 95/46/EG schreibt vor, dass die Staaten spezielle Regeln in Bezug auf die Informationspflicht bei automatisierten Einzelentscheidungen erlassen müssen. Diese Pflicht ist als besondere Informationspflicht zu verstehen, die dann besteht, «wenn ein Entscheid, der für die betroffene Person rechtliche Folgen hat oder sie sonst wesentlich betrifft, ausschliesslich auf einer automatisierten Datenbearbeitung beruht, welche die Bewertung einzelner Aspekte ihrer Persönlichkeit bezweckt». Damit soll verhindert werden, dass Entschei-

de getroffen werden, ohne dass eine Beurteilung durch Menschen vorgenommen und die betroffene Person darüber informiert wird (vgl. BBl 2003 S. 2134).

Die Regelung solcher Entscheide betrifft jedoch in erster Linie die Privatunternehmen. Die dem DSchG unterstellten Organe sind nicht direkt betroffen.

#### – Vorabkontrolle

Gemäss Artikel 20 der Richtlinie 95/46/EG müssen die Mitgliedstaaten Datenbearbeitungen, die spezifische Risiken beinhalten können, vorgängig prüfen. In unserem System braucht es jedoch keine Bestimmung über eine Vorabkontrolle. Die vorgängige Kontrolle der Gesetzeserlasse, wie sie in Artikel 30a Abs. 1 Bst. b des Entwurfs vorgesehen ist, der Artikel 30 Abs. 2 Bst. b des geltenden Gesetzes übernimmt, umfasst bereits eine ausreichende Garantie: Die Kontrolle der Bearbeitung von Daten durch die dem DSchG unterstellten Organe ist im Rahmen des Gesetzgebungsverfahrens gewährleistet. Im Zweifelsfall können die öffentlichen Organe natürlich die oder den Datenschutzbeauftragten fragen, ob die von ihnen geplanten Bearbeitungen zulässig sind.

Die Vorabkontrolle wurde übrigens auch nicht in das DSG aufgenommen.

#### – Sanktionen

Nach Massgabe von Artikel 24 der Richtlinie 95/46/EG, der Artikel 10 des Übereinkommens 108 übernimmt, sollte das Gesetz die Sanktionen festlegen, die bei Verstössen gegen die Datenschutzvorschriften anzuwenden sind. Darauf wurde aus den folgenden Gründen verzichtet.

Verstösse, die eine Verletzung des Amtsgeheimnisses darstellen, werden bereits durch das geltende Recht sanktioniert (Art. 320 StGB).

Für die Fälle, in denen keine Verletzung des Amtsgeheimnisses vorliegt, beispielsweise wenn Personendaten nicht zu dem Zweck bearbeitet werden, für den sie beschafft wurden, oder zu einem Zweck, der mit diesem nicht nach Treu und Glauben vereinbar ist (vgl. Art. 5 Abs. 1 DSchG), müssten jedoch aufgrund der internationalen Bestimmungen theoretisch Sanktionen vorgesehen werden.

In der Praxis kann die kantonale Aufsichtsbehörde für Datenschutz solche Fälle künftig aber sehr wirksam behandeln, da sie zusätzliche Befugnisse erhält. Ausserdem würden mit der Einführung eines Sanktionssystems Elemente des Disziplinarrechts, das mit dem Inkrafttreten des Gesetzes über das Staatspersonal im Jahr 2003 abgeschafft wurde, gleichsam durch die Hintertür wieder eingeführt.

Es ist auch nicht nötig, ein Sanktionssystem nur für die Personen oder Organe vorzusehen, die nicht an das Amtsgeheimnis gebunden sind, zum Beispiel im Falle einer Bearbeitung von Daten im Auftrag (vgl. Art. 18 DSchG). Diese Personen oder Organe bearbeiten die Daten ja auf der Grundlage eines Vertrags, der insbesondere eine umfassende Schweigepflicht vorsieht. Der Auftragnehmer darf Informationen, die ihm der Auftraggeber anvertraut, nicht Dritten mitteilen; er muss auch über alles schweigen, was er in Ausübung seines Auftrags erfährt oder errät. Des Weiteren muss er sicherstellen, dass Dritte keinen Zugriff auf die von ihm bearbeiteten Daten haben. Gemäss Artikel 18 DSchG obliegt es im Übrigen dem öffentlichen Organ, das Aufgaben Dritten überträgt, die

erforderlichen Massnahmen zu ergreifen, um Missstände zu verhindern oder zu beheben.

#### – Erweiterung des Informationsanspruchs

Der Bundesgesetzgeber hat eine neue Bestimmung in das DSG aufgenommen, die die Informationspflicht beim Beschaffen von besonders schützenswerten Personendaten und Persönlichkeitsprofilen regelt (Art. 7a nDSG).

Der Entwurf zur Anpassung des DSchG an das internationale Recht enthält keine vergleichbare Regel, da das geltende Gesetz gemäss Wegleitung des Delegierten der KdK bereits den Mindestanforderungen des europäischen Rechts entspricht. Eine an den neuen Artikel 7a DSG angelehnte kantonale Norm zur Erweiterung des Informationsanspruchs könnte im Rahmen der nächsten Anpassung des DschG aufgenommen werden (vgl. oben Ziff. 2.a).

## 4. LEITLINIEN UND GELTUNGSBEREICH DES GESETZESENTWURFS

### a. Leitlinien

Die Arbeitsgruppe orientierte sich bei der Ausarbeitung des Entwurfs an folgenden Leitlinien:

- Die Änderungen sind auf die Anpassungen zu beschränken, die infolge des europäischen Rechts erforderlich sind.
- Die europäischen Vorschriften sind so in das kantonale Recht zu überführen, dass die Umsetzung der Abkommen von Schengen und Dublin nicht verzögert wird («Evaluation durch die Europäische Union bestehen»).
- Die Bestimmungen müssen sich möglichst gut in die kantonale Rechtsordnung einfügen.
- Sie sollten möglichst nicht von den Bestimmungen des Bundesgesetzes über den Datenschutz abweichen.

### b. Geltungsbereich

Der Geltungsbereich der Änderungen erstreckt sich auf den gesamten Datenschutz, wie er durch das DSchG geregelt ist. Eine Beschränkung des Geltungsbereichs auf den durch die Abkommen von Schengen und Dublin abgedeckten Bereich wäre weder zulässig noch praktikabel. Die Bestimmungen des von der Schweiz bereits angenommenen Zusatzprotokolls sind allgemein anwendbar und nicht auf Schengen/Dublin beschränkt. Ausserdem lassen sich Daten beim Bearbeiten nicht in streng voneinander getrennte Kategorien unterteilen. Der von der Europäischen Union geforderte Mindeststandard kann nur gewährleistet werden, wenn die Bestimmungen der Richtlinie 95/46/EG allgemein angewendet werden. Schliesslich wäre ein unterschiedlicher Schutz des Staates, je nach dem, ob die bearbeiteten Daten unter Schengen/Dublin fallen oder nicht, intern schwierig zu rechtfertigen.

## 5. KOMMENTAR ZU DEN EINZELNEN ARTIKELN

### Vorbemerkung

Das heutige DschG ist nicht geschlechtsneutral formuliert. Deshalb soll die vorliegende Revision zum Anlass



genommen werden, um dieses Gesetz gestützt auf die einschlägigen Richtlinien den Anforderungen an eine geschlechtsneutrale Formulierung anzupassen. Nachstehend werden lediglich Bestimmungen mit einer materiellen Tragweite kommentiert.

### Artikel 12a

Das geltende DSchG regelt die grenzüberschreitende Datenübermittlung (Mitteilungen ins Ausland) nicht ausdrücklich.

Gemäss Artikel 25 der Richtlinie 95/46/EG und Artikel 2 des Zusatzprotokolls darf die Übermittlung personenbezogener Daten in Drittstaaten grundsätzlich nur bewilligt werden, wenn diese Staaten ein angemessenes Schutzniveau gewährleisten. Ist der erforderliche Schutz nicht garantiert, so ist die Übermittlung zu untersagen; ausgenommen sind Sonderfälle, d.h., wenn das innerstaatliche Recht die Möglichkeit einer Übermittlung vorsieht, um bestimmten Interessen der betroffenen Person oder legitimen überwiegenden Interessen, insbesondere wichtigen öffentlichen Interessen, Rechnung zu tragen, oder wenn die für die Übermittlung verantwortliche Person Sicherheitsvorkehrungen trifft, die sich insbesondere aus vertraglichen Klauseln ergeben und diese nach Auffassung der zuständigen Behörden angemessen sind.

Diese Bestimmungen müssen in das Schweizer Recht überführt werden. Auf Bundesebene wurde deshalb ein neuer Artikel 6 in das DSG aufgenommen. Artikel 12a des Entwurfs übernimmt diese Bestimmung inhaltlich.

Absatz 1 enthält den Grundsatz, wonach die grenzüberschreitende Bekanntgabe von Personendaten nur gestattet ist, wenn der Empfängerstaat einen angemessenen Schutz gewährleistet. Ein angemessener Schutz ist grundsätzlich dann gegeben, wenn die Gesetzgebung des Empfängerstaats den Anforderungen des Übereinkommens 108 entspricht. Darüber hinaus ist aber möglichst auch zu berücksichtigen, wie die ausländische Gesetzgebung in der Praxis umgesetzt wird.

Absatz 2 führt die Ausnahmefälle auf, in denen eine Bekanntgabe gestattet ist, obwohl der Empfängerstaat keine hinreichenden Garantien bietet. Die Ausnahmen entsprechen denjenigen des DSG. Die im kantonalen Recht vorgesehenen Ausnahmen müssen natürlich gleich ausgelegt werden wie die Ausnahmen nach Bundesrecht. Buchstabe f und g von Artikel 6 Abs. 2 DSG wurden jedoch nicht in den kantonalen Gesetzesentwurf aufgenommen, da sie Fälle betreffen, die nicht in den Geltungsbereich des DSchG fallen.

Absatz 3 präzisiert, dass das öffentliche Organ die bzw. den Datenschutzbeauftragten vor der Weitergabe der Personendaten über die in Absatz 2 Bst. a vorgesehenen Garantien informieren muss.

Es gilt zu beachten, dass der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte eine Liste der Staaten führt, deren Gesetzgebung einen angemessenen Schutz gewährleistet.

### Artikel 22a

Nach Artikel 28 Abs. 3 zweiter Spiegelstrich der Richtlinie 95/46/EG und Artikel 1 Ziff. 2a des Zusatzprotokolls müssen die Datenschutzaufsichtsbehörden über wirksame Einwirkungsbefugnisse verfügen (vgl. oben Ziff. 3.c).

Mit dem in Artikel 22a vorgeschlagenen System werden die wirksamen Eingriffsbefugnisse der Aufsichtsbehörde im kantonalen Recht verankert, wobei die bisherige Struktur, die sich bewährt hat, so weit als möglich beibehalten wird.

Dieses neue System präsentiert sich wie folgt:

In einer *ersten Phase* gibt die Aufsichtsbehörde im Falle einer Verletzung oder einer drohenden Verletzung der Datenschutzvorschriften zunächst eine Empfehlung ab, wie dies bereits heute der Fall ist (Art. 22a Abs. 1). Sie kann dabei die Betroffenen einladen, alle Massnahmen zu treffen, die zur Wiederherstellung oder Erhaltung einer rechtlich konformen Situation nach Artikel 3 Bst. d DSchG notwendig sind. Zu erwähnen wäre hier beispielsweise das Verbot des Beschaffens, das Verbot der Bekanntgabe oder die Vernichtung von Daten.

Die Empfehlung richtet sich je nachdem an das betroffene Organ (Art. 22a Abs. 1) oder an das hierarchisch übergeordnete Organ (Art. 22a Abs. 2).

Ist die Verletzung oder die drohende Verletzung von Datenschutzvorschriften einer hierarchisch unabhängigen Instanz (z.B. einer Anstaltsleitung oder einem Gemeinderat) zuzuordnen, so stellt die Aufsichtsbehörde ihre Empfehlungen unmittelbar diesem Organ zu.

Ist die Verletzung oder die drohende Verletzung hingegen einem Organ oder einer Person in einem hierarchischen Unterordnungsverhältnis zuzuordnen, so sollte die hierarchisch übergeordnete Stelle informiert werden. Auf diese Weise können alle beteiligten Instanzen in die Verantwortung genommen werden. Die übergeordnete Stelle übt nämlich eine umfassende Aufsicht über die ihr unterstellten Organe und Personen aus und kann diese somit auffordern, die einschlägigen Datenschutzbestimmungen einzuhalten.

Wenn Dritte Personendaten im Auftrag eines öffentlichen Organs bearbeiten, besteht eine ähnliche Situation, wie wenn ein hierarchisches Verhältnis vorliegt (vgl. Art. 18). Das öffentliche Organ verfügt unter dem Gesichtspunkt der Konkretisierung der wirksamen Einwirkungsbefugnisse über ähnliche Kompetenzen wie eine vorgesetzte Behörde. Daher sind die Empfehlungen der Kommission an das öffentliche Organ zu richten.

In einer *zweiten Phase* muss der Empfänger der Empfehlung innert einer von der Aufsichtsbehörde festgelegten Frist mitteilen, ob und gegebenenfalls wie er die Empfehlung befolgen will. Diese Mitteilung ergeht in Form einer Verfügung (Art. 22a Abs. 3).

Es handelt sich hier um ein aussergewöhnliches Verfahren, da dieser Entscheid nicht in allen Punkten mit der Definition der Verfügung gemäss Artikel 4 des Gesetzes über die Verwaltungsrechtspflege (VRG) übereinstimmt. Gemäss dieser Definition sind Verfügungen verbindliche Anordnungen, die im Einzelfall Rechte oder Pflichten begründen, ändern oder aufheben oder deren Bestehen oder Nichtbestehen feststellen, während Artikel 22a Abs. 3 ff. des Entwurfs sich auf «Entscheide» bezieht, mit welchen der Empfänger einer Empfehlung lediglich bekannt gibt, ob er dieser Empfehlung vollumfänglich oder teilweise Folge leisten will oder überhaupt nicht.

Das internationale Recht verlangt jedoch, dass solche besondere Entscheide in unserer Gesetzgebung vorgesehen werden (es handelt sich um eine Konkretisierung der wirksamen Eingriffsmöglichkeiten, vgl. oben Ziff. 3, 1. Spiegelstrich). Die Bestimmungen betreffend die Ver-

fügungen im Sinne von Artikel 4 VRG sind demnach sinngemäss auf die in Artikel 22a Abs. 3 des Entwurfs vorgesehenen Entscheide anwendbar.

In einer *dritten Phase* kann die Aufsichtsbehörde die Einhaltung ihrer Empfehlung erzwingen, indem sie bei der ordentlichen Beschwerdebehörde gemäss VRG Beschwerde erhebt. (Abs. 4). Ist keine Beschwerdebehörde im Sinne des VRG vorhanden, z.B. wenn der Entscheid von einer anerkannten Kirche erlassen wurde, so ist die Beschwerde an das vereinte Kantonsgericht zu richten (Abs. 5).

Das spezielle Verfahren gemäss Artikel 22a des Entwurfs steht ausschliesslich den Datenschutz-Aufsichtsbehörden zur Verfügung (Abs. 4 *in fine*). Der Entwurf geht insofern nicht über die Anforderungen des internationalen Rechts hinaus. Privatpersonen, die sich wegen einer Verletzung von Datenschutzvorschriften beschweren wollen, müssen wie bisher gemäss Artikel 27 DschG vorgehen.

Dieser neue Mechanismus ergänzt den in Artikel 27 Abs. 2 des Entwurfs vorgesehenen Beschwerdeweg und gibt der Aufsichtsbehörde eine wirksame Eingriffsmöglichkeit bei Gesetzesverletzungen, die nicht direkt Personen im Sinne von Artikel 23 bis 26 DschG betreffen.

#### **Artikel 27 Abs. 2**

Mit dieser Bestimmung werden die Befugnisse der Aufsichtsbehörde für Datenschutz gemäss Artikel 28 Abs. 3 dritter Spiegelstrich der Richtlinie 95/46/EG und Artikel 1 Ziff. 2a des Zusatzprotokolls ausgebaut, wonach die Aufsichtsbehörden über ein Klagerecht bei Verstössen gegen die Datenschutzvorschriften verfügen müssen.

Nach dem geltenden Recht sind lediglich Personen beschwerdeberechtigt, deren Rechte oder Pflichten von einem Entscheid über die Bearbeitung von Personendaten berührt sein könnten (vgl. Art. 76 VRG). Vorbehalten bleiben Straftaten, die von Amtes wegen verfolgt werden und die gemäss Art. 146 Abs. 2 StPO den Strafverfolgungsbehörden gemeldet werden können.

Artikel 27 DSchG ist also dahingehend zu ergänzen, dass die Beschwerdelegitimation auf die Aufsichtsbehörde für Datenschutz ausgedehnt wird. Die Beschwerdebehörden werden gemäss dem Verweis von Artikel 27 Abs. 1 DSchG in Artikel 114 ff. VRG definiert.

Gemäss den Vorschriften des europäischen Rechts soll ein wirksames Kontrollsystem geschaffen werden. Aus diesem Grund muss die Aufsichtsbehörde Kenntnis von allen Entscheiden erhalten, die Gegenstand einer Beschwerde bilden könnten. Andernfalls wäre die Kontrolle bloss aleatorisch. Der Entwurf sieht deshalb vor, dass die öffentlichen Organe der Aufsichtsbehörde für Datenschutz alle Entscheide mitteilt, die sie in Anwendung der Artikel 23 bis 26 DschG treffen.

Im Übrigen wird auf Ziffer 3.c. verwiesen.

#### **Artikel 29 Abs. 2 und 3**

Diese Bestimmungen umfassen die Mindestbedingungen, die die kommunalen Aufsichtsbehörden für Datenschutz erfüllen müssen.

Man kann nicht geringere Anforderungen an das Schutzniveau stellen, nur weil die Datenbearbeitung von einem Gemeindeorgan überwacht wird. Da die internationalen Verpflichtungen der Schweiz strikte Vorschriften für die

Aufsichtsbehörde enthalten, müssen die zuständigen Gemeindebehörden diese erfüllen. Ist dies nicht der Fall, so muss die kantonale Aufsichtsbehörde dafür sorgen, dass die betreffenden Gemeinden den Datenschutz gewährleisten.

Mit Artikel 29 Abs. 2 des Entwurfs werden die Befugnisse der kommunalen Aufsichtsbehörden erweitert. Diese müssen insbesondere beschwerdeberechtigt sein, wenn die Rechte einer von einer Datenbearbeitung betroffenen Person verletzt werden (vgl. Art. 27 Abs. 2 und 30a Abs. 1 Bst. d des Entwurfs), und über wirksame Einwirkungsbefugnisse verfügen (vgl. Art. 22a und 30a Abs. 1 Bst. c des Entwurfs; siehe auch oben Ziff. 3.c).

Aufgrund von Absatz 3 müssen die Gemeinden zudem die Unabhängigkeit ihrer Aufsichtsbehörde sicherstellen. Diese Unabhängigkeit umfasst einen institutionellen Aspekt, indem verhindert werden muss, dass die beaufsichtigende Behörde in irgendeiner Art und Weise von den von ihr beaufsichtigten Personen und Organen beeinflusst wird, beispielsweise aufgrund des Wahlmodus, der Regelung der Arbeitsverhältnisse usw. Sie hat auch eine finanzielle Komponente, d.h., die Aufsichtsbehörde muss die finanziellen und personellen Mittel haben, die zur Erfüllung ihrer Aufgaben erforderlich sind, und frei über ihr Budget verfügen können, wie dies bei der kantonalen Aufsichtsbehörde für Datenschutz der Fall ist (zur Unabhängigkeit vgl. auch oben Ziff. 3.b).

Es gilt zu beachten, dass die Gemeinden aufgrund von Artikel 29 Abs. 2 des geltenden DSchG bereits heute ihre eigene Aufsichtsbehörde bestellen können. Die Gemeinden Bulle, Freiburg, Marly und Villars-sur-Glâne verfügen über eine eigene Aufsichtsbehörde. Die Gemeinden müssen selbst dafür sorgen, dass ihre Aufsichtsbehörde den Anforderungen des Europarechts entspricht. Es gibt verschiedene Lösungen, um die Nachteile des neuen Systems zu verringern. Eine Möglichkeit wären beispielsweise Gemeindefusionen.

#### **Artikel 30 bis 32**

Die Bestimmungen des geltenden DSchG über die kantonale Aufsichtsbehörde für Datenschutz genügen den Mindestanforderungen der Richtlinie 95/46/EG und des Zusatzprotokolls nicht ganz (vgl. oben Ziff. 3.b und 3.c).

Die notwendigen Änderungen erfordern eine formelle Neugliederung der Artikel 30 bis 32. Im Folgenden werden lediglich die materiellen Änderungen erläutert. Sie betreffen die Artikel 30, 30a Abs. 1 Bst. c und d, 31a Abs. 1 Bst. f und g sowie 32 Abs. 3 bis 6.

##### **a. Artikel 30**

Artikel 28 Abs. 1 der Richtlinie 95/46/EG und Artikel 1 Ziff. 3 des Zusatzprotokolls schreiben vor, dass die Aufsichtsbehörden ihre Aufgaben in völliger Unabhängigkeit wahrnehmen (vgl. auch Ziff. 3.b).

Die institutionelle Unabhängigkeit der kantonalen Datenschutzkommission wird bereits durch die jetzigen Bestimmungen des DSchG gewährleistet (vgl. insbesondere Art. 30 Abs. 1). Der Entwurf übernimmt diese Bestimmung daher wörtlich, präzisiert aber, dass die Amtszeit der Präsidentin oder des Präsidenten und der Mitglieder der Kommission vier Jahre beträgt. Dies entspricht auch den Bestimmungen des Gesetzes betreffend die Dauer der öffentlichen Nebenämter, wonach die Amtsdauer 4 Jahre beträgt.

In der Praxis kann die kantonale Datenschutzkommission ihre Aufgabe indes nur dann völlig unabhängig ausüben, wenn sie über die für eine wirksame Aufsicht notwendigen Fachkenntnisse verfügt. Gesundheit und Informatik sind in dieser Hinsicht besonders heikle Bereiche. Die Kommission muss deshalb direkt über spezifische Kenntnisse auf diesem Gebiet verfügen. Zudem muss sie sich aus Vertreterinnen und Vertretern aus Bereichen zusammensetzen, die am meisten von der Datenschutzproblematik betroffen sind. Dabei ist von den Bedürfnissen der Kommission und der Verfügbarkeit der entsprechenden Fachleute auszugehen (Abs. 2).

Da unmöglich alle Fachgebiete in der Kommission vertreten sein können, sieht der Entwurf ausdrücklich vor, dass die Kommission Sachverständige oder Dritte beiziehen kann (Abs. 3).

In Bezug auf die Budgetautonomie wird auf den neuen Artikel 32 Abs. 3 verwiesen.

b. Artikel 30a Abs. 1 Bst. c

Der Artikel 30a Abs. 1 Bst. c verweist lediglich auf den neuen Artikel 22a (vgl. Ziff. 3.c oben sowie Kommentar ad Art. 22a).

c. Artikel 30a Abs. 1 Bst. d

Der Artikel 30a Abs. 1 Bst. d verweist lediglich auf den neuen Artikel 27 Abs. 2 (vgl. Ziff. 3.c oben sowie Kommentar ad Art. 27 Abs. 2).

d. Artikel 31 Abs. 1 Bst. f und g

Aufgrund der Verstärkung der Datenschutzaufsicht auf internationaler Ebene werden der oder dem Datenschutzbeauftragten zwei neue Befugnisse zugewiesen.

Die in Buchstabe f aufgeführte Zusammenarbeit zwischen den verschiedenen Aufsichtsorganen ist als Austausch zweckdienlicher Informationen zu verstehen. Die Zusammenarbeit ist übrigens in Artikel 28 Abs. 6 der Richtlinie 95/46/EG und in Artikel 1 Ziff. 5 des Zusatzprotokolls vorgesehen.

Buchstabe g ergibt sich aus dem neuen Artikel 12a über die grenzüberschreitende Datenübermittlung.

e. Artikel 32 Abs. 3 bis 6

Die vom europäischen Recht geforderte vollständige Unabhängigkeit der kantonalen Aufsichtsbehörde für Datenschutz macht gewisse Anpassungen in deren finanzhaushaltsrechtlichen Status notwendig. Sie muss ein eigenes Budget haben, über das sie entsprechend ihren Bedürfnissen in Zusammenhang mit der Erfüllung ihrer Aufgaben frei verfügen kann. Vgl. die oben erwähnten Referenzen, Ziff. 3. b.

Aufgrund dieser Anforderungen soll die kantonale Aufsichtsbehörde gemäss Artikel 32 Abs. 3 über ein Globalbudget verfügen.

Die Absätze 4 bis 6 entsprechen den Anforderungen des Europarechts hinsichtlich der persönlichen Unabhängigkeit der Mitglieder der Aufsichtsbehörden. Damit soll ebenfalls das Vertrauen der Behörden und der Bevölkerung gegenüber diesen Behörden gestärkt werden.

Absatz 4 entspricht dem Absatz 3 des bisherigen Gesetzes, mit einem Zusatz bezüglich der Schweigepflicht. So wird klargestellt, dass die Mitglieder der kantonalen Aufsichtsbehörde, wie die Mitglieder der anderen staatlichen

Kommissionen, dieser Schweigepflicht unterstehen (vgl. Art. 26 des Reglements über die Organisation und die Arbeitsweise der Kommissionen des Staates).

Der 5. Absatz enthält eine Neuheit, die in unserem kantonalen Recht bisher nicht vorkam. Das Bundesrecht sowie die Rechtsordnungen anderer Kantone kennen hingegen bereits die Pflicht, Interessenbindungen offen zu legen. Man denkt hier etwa an Erwerbstätigkeiten, an Tätigkeiten, die im Rahmen von Kommissionen, von Führungs- oder Aufsichtsorganen oder von Organen juristischer Personen ausgeübt werden, sowie an politische Tätigkeiten usw.

Absatz 6 dient der Transparenz und führt einen Grundsatz aus, der bereits im heutigen Recht Anwendung findet.

## 6. AUFGABENTEILUNG STAAT–GEMEINDEN

Der Entwurf hat theoretisch keine Auswirkungen auf die Aufgabenteilung zwischen Kanton und Gemeinden. Wegen der neuen Anforderungen an die Aufsichtsbehörden könnte er jedoch in der Praxis eine dissuasive Wirkung auf die Gemeinden haben. Wenn die Gemeinden auf eine eigene Aufsichtsbehörde verzichten, würde dies dazu führen, dass die entsprechenden Aufgaben dem Staat übertragen werden.

## 7. VERFASSUNGSMÄSSIGKEIT, BUNDESRECHTSKONFORMITÄT UND EUROPAVERTRÄGLICHKEIT

Der Entwurf ist mit der Kantonsverfassung (vgl. Art. 12 KV) und mit dem Bundesrecht vereinbar. Er bezweckt zudem die Anpassung der kantonalen Gesetzgebung an die beiden wichtigsten europäischen Rechtsinstrumente im Bereich des Datenschutzes (Richtlinie 95/46/EG und Übereinkommen 108, einschliesslich seines Zusatzprotokolls) und ist daher auch mit dem Europarecht vereinbar.

## 8. FINANZIELLE UND PERSONELLE AUSWIRKUNGEN

Die vorgesehene Revision, insbesondere die Umsetzung der wirksamen Einwirkungsbefugnisse, mit der eine effektive Kontrolle im Sinne des europäischen Rechts sichergestellt werden soll, zieht neue Aufgaben für die kantonale Aufsichtsbehörde nach sich:

Diese muss laut Artikel 27 Abs. 2 künftig die Entscheide prüfen, die der oder dem Datenschutzbeauftragten eröffnet werden, und allenfalls Beschwerde dagegen einlegen.

Des Weiteren muss sie die Kontrollen vornehmen, die zur Umsetzung von Artikel 22a notwendig sind, oder Dritte damit beauftragen. Dazu sollte sie über die finanziellen und personellen Mittel verfügen, die es ihr erlauben, bei den vom DSchG betroffenen Organen aktiv zu intervenieren. Könnte sie nur reaktiv tätig werden, wenn ein Anliegen an sie herangetragen wird, so wäre dies aufgrund der europäischen Bestimmungen nicht ausreichend.

Schliesslich wird die kantonale Aufsichtsbehörde bei allfälligen Missständen gegenüber der heutigen Situation über zusätzliche Kompetenzen verfügen. Sie wird sich



nicht darauf beschränken, Empfehlungen in Bezug auf die zu ergreifenden Massnahmen abzugeben. Bei Nichteinhaltung der Empfehlungen wird sie vielmehr bei der zuständigen Gerichtsbehörde Beschwerde einreichen, um die Einhaltung der Datenschutzvorschriften zu gewährleisten.

Diese zusätzlichen Aufgaben erfordern eine Erhöhung des Personalbestandes der Datenschutzbeauftragten um 0,5 VZE. Des Weiteren müssen die Kredite für die Kom-

missionsarbeiten und für externe Kontrollen angemessen erhöht werden.

Aus diesen Gründen müsste das Globalbudget der kantonalen Aufsichtsbehörde für Datenschutz neu 250 000 Franken pro Jahr betragen (dies entspricht einer Erhöhung um 50 000 Franken im Vergleich zur heutigen Situation).

\_\_\_\_\_

## Loi

*du*

**modifiant la loi sur la protection des données  
(adaptation au droit international,  
en particulier aux accords Schengen/Dublin)**

---

### *Le Grand Conseil du canton de Fribourg*

Vu la modification du 24 mars 2006 de la loi fédérale sur la protection des données;

Vu l'arrêté fédéral du 17 décembre 2004 portant approbation et mise en œuvre des accords bilatéraux d'association à l'Espace Schengen et à l'Espace Dublin;

Vu l'arrêté fédéral du 24 mars 2006 sur l'adhésion de la Suisse au Protocole additionnel du 8 novembre 2001 à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données;

Vu le message du Conseil d'Etat du 4 mars 2008;

Sur la proposition de cette autorité,

*Décrète:*

#### **Art. 1**

La loi du 25 novembre 1994 sur la protection des données (LPrD) (RSF 17.1) est modifiée comme il suit:

##### **Art. 10 titre médian et al. 2**

Communication ordinaire

a) Conditions

<sup>2</sup> *Remplacer* «un destinataire» *par* «un ou une destinataire».

## Gesetz

*vom*

**zur Änderung des Gesetzes über den Datenschutz  
(Anpassung an das internationale Recht,  
insbesondere an die Abkommen von Schengen und Dublin)**

---

### *Der Grosse Rat des Kantons Freiburg*

gestützt auf die Änderung vom 24. März 2006 des Bundesgesetzes über den Datenschutz;

gestützt auf den Bundesbeschluss vom 17. Dezember 2004 über die Genehmigung und die Umsetzung der bilateralen Abkommen zwischen der Schweiz und der EU über die Assoziierung an Schengen und an Dublin;

gestützt auf den Bundesbeschluss vom 24. März 2006 betreffend den Beitritt der Schweiz zum Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung;

nach Einsicht in die Botschaft des Staatsrates vom 4. März 2008;

auf Antrag dieser Behörde,

*beschliesst:*

#### **Art. 1**

Das Gesetz vom 25. November 1994 über den Datenschutz (DSchG) (SGF 17.1) wird wie folgt geändert:

##### **Art. 10 Artikelüberschrift und Abs. 2**

Ordentliche Datenbekanntgabe

a) Bedingungen

<sup>2</sup> *Den Ausdruck* «einem Empfänger» *durch* «einer Empfängerin oder einem Empfänger» *ersetzen*.

**Art. 12a (nouveau)** Communication transfrontière

<sup>1</sup> Des données personnelles ne peuvent être communiquées à l'étranger que dans les Etats qui garantissent un niveau de protection adéquat.

<sup>2</sup> Des données personnelles peuvent toutefois être communiquées dans les Etats n'offrant pas une telle garantie, lorsque l'une des conditions suivantes est réalisée:

- a) des garanties suffisantes, notamment contractuelles, permettent d'assurer un niveau de protection adéquat à l'étranger;
- b) la personne concernée a, en l'espèce, donné son consentement explicite;
- c) le traitement est en relation directe avec la conclusion ou l'exécution d'un contrat, et les données traitées concernent le cocontractant ou la cocontractante;
- d) la communication est, en l'espèce, indispensable soit à la sauvegarde d'un intérêt public prépondérant, soit à la constatation, l'exercice ou la défense d'un droit en justice;
- e) la communication est, en l'espèce, nécessaire à la protection de la vie ou de l'intégrité corporelle de la personne concernée.

<sup>3</sup> L'organe public informe le ou la préposé-e cantonal-e à la protection des données des garanties prises en vertu de l'alinéa 2 let. a avant la communication des données à l'étranger.

**Art. 18 al. 1 et 2**

<sup>1</sup> Remplacer «au mandataire» par «au ou à la mandataire» et «celui-ci» par «celui-ci ou celle-ci».

<sup>2</sup> Remplacer «le mandataire n'est pas soumis» par «le ou la mandataire n'est pas soumis-e».

**Art. 22a (nouveau)** Procédure en cas de non-respect des prescriptions

<sup>1</sup> En cas de violation ou de risque de violation des prescriptions sur la protection des données, l'autorité de surveillance invite l'organe public concerné à prendre, dans un délai déterminé, les mesures nécessaires pour remédier à la situation.

<sup>2</sup> Toutefois, lorsque l'organe concerné est une unité subordonnée, l'invitation est directement adressée à l'organe hiérarchiquement supérieur.

**Art. 12a (neu)** Bekanntgabe ins Ausland

<sup>1</sup> Personendaten dürfen nur in Staaten bekannt gegeben werden, die einen angemessenen Schutz gewährleisten.

<sup>2</sup> In Staaten, die keinen angemessenen Schutz gewährleisten, dürfen Personendaten jedoch bekannt gegeben werden, wenn eine der folgenden Bedingungen erfüllt ist:

- a) Hinreichende Garantien, insbesondere vertragliche Garantien, gewährleisten einen angemessenen Schutz im Ausland;
- b) Die betroffene Person hat im Einzelfall ausdrücklich eingewilligt;
- c) Die Bearbeitung steht in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags und es handelt sich um Personendaten des Vertragspartners;
- d) Die Bekanntgabe ist im Einzelfall entweder für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich;
- e) Die Bekanntgabe ist im Einzelfall erforderlich, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen.

<sup>3</sup> Vor der Bekanntgabe der Daten ins Ausland informiert das öffentliche Organ die kantonale Datenschutzbeauftragte oder den kantonalen Datenschutzbeauftragten über die Garantien nach Absatz 2 Bst. a.

**Art. 18 Abs. 1 und 2**

<sup>1</sup> Die Ausdrücke «einen Dritten» durch «eine Drittperson», «dem beauftragten Dritten» durch «der beauftragten Drittperson» und «er» durch «sie» ersetzen.

<sup>2</sup> Den Ausdruck «den beauftragten Dritten» durch «die beauftragte Drittperson» ersetzen.

**Art. 22a (neu)** Verfahren bei Nichteinhaltung der Vorschriften

<sup>1</sup> Bei einer Verletzung oder einer möglichen Verletzung der Datenschutzvorschriften fordert die Aufsichtsbehörde das betroffene öffentliche Organ auf, innert einer bestimmten Frist die nötigen Abhilfemassnahmen zu treffen.

<sup>2</sup> Handelt es sich um eine unterstellte Einheit, so ergeht die Aufforderung direkt an das hierarchisch übergeordnete Organ.



<sup>3</sup> Le ou la destinataire de la recommandation adopte, dans le délai imparti par l'autorité de surveillance, une décision sur la suite qu'il ou elle entend donner à la recommandation. La décision est communiquée à l'autorité de surveillance. L'absence de décision est considérée comme une décision de rejet.

<sup>4</sup> La décision de rejet, total ou partiel, de la recommandation est sujette à recours. Les dispositions du code de procédure et de juridiction administrative sont applicables par analogie. Toutefois, seule l'autorité de surveillance a qualité pour recourir.

<sup>5</sup> Lorsque la décision émane d'un organe pour lequel le code de procédure et de juridiction administrative ne prévoit pas de voie de droit, le recours est adressé au Tribunal cantonal.

**Art. 23 al. 2** (*ne concerne que le texte français*)

Remplacer «au requérant toutes les données le concernant» par «au requérant ou à la requérante toutes les données le ou la concernant».

**Art. 24 al. 3**

Remplacer «un médecin désigné» par «un ou une médecin désigné-e».

**Art. 27 al. 2 (nouveau)**

<sup>2</sup> En outre, les dispositions suivantes sont applicables:

- a) les organes publics communiquent également les décisions précitées à l'autorité de surveillance;
- b) l'autorité de surveillance a qualité pour recourir contre ces décisions.

**Art. 28 al. 2**

Remplacer «le juge» par «le ou la juge».

**Art. 29 al. 1, 2 et 3 (nouveau)**

<sup>1</sup> Remplacer «d'un préposé» par «d'un ou d'une préposé-e».

<sup>2</sup> Les communes peuvent instituer leur propre autorité de surveillance qui assume, sur le plan communal, les mêmes tâches que l'autorité cantonale.

<sup>3</sup> Der Empfehlungsempfänger erlässt innert der von der Aufsichtsbehörde gesetzten Frist eine Verfügung, worin er festhält, ob und gegebenenfalls wie er der Empfehlung Folge leisten will. Er informiert die Aufsichtsbehörde über den Erlass der Verfügung. Erlässt er keine solche Verfügung, so gilt dies als formelle Weigerung, der Empfehlung Folge zu leisten.

<sup>4</sup> Weigert sich der Empfänger, der Empfehlung vollständig oder teilweise Folge zu leisten, so kann gegen die entsprechende Verfügung Beschwerde erhoben werden. Die Bestimmungen des Gesetzes über die Verwaltungsrechtspflege sind sinngemäss anwendbar. Zur Beschwerde ist indes einzig die Aufsichtsbehörde befugt.

<sup>5</sup> Wird die Verfügung von einem Organ erlassen, für das das Gesetz über die Verwaltungsrechtspflege kein Rechtsmittel vorsieht, so wird die Beschwerde dem Kantonsgericht unterbreitet.

**Art. 23 Abs. 2**

*Betrifft nur den französischen Text.*

**Art. 24 Abs. 3**

*Den Ausdruck «einen von ihr gewählten Arzt» durch «eine von ihr gewählte Ärztin oder einen von ihr gewählten Arzt» ersetzen.*

**Art. 27 Abs. 2 (neu)**

<sup>2</sup> Im Übrigen sind folgende Bestimmungen anwendbar:

- a) Die öffentlichen Organe teilen die oben erwähnten Entscheide ebenfalls der Aufsichtsbehörde mit.
- b) Die Aufsichtsbehörde kann gegen diese Entscheide Beschwerde erheben.

**Art. 28 Abs. 2**

*Den Ausdruck «vom Richter» durch «von der Richterin oder vom Richter» ersetzen.*

**Art. 29 Abs. 1, 2 und 3 (neu)**

<sup>1</sup> *Den Ausdruck «einem Beauftragten» durch «einer oder einem Beauftragten» ersetzen.*

<sup>2</sup> Die Gemeinden können eine eigene Aufsichtsbehörde bestellen, die auf Gemeindeebene dieselben Aufgaben hat wie die kantonale Behörde.

<sup>3</sup> L'autorité communale est indépendante dans l'exercice de ses attributions et dispose des moyens nécessaires à l'accomplissement de ses tâches. A défaut, la surveillance est exercée par l'autorité cantonale.

**Art. 30** Commission cantonale

a) Composition, organisation et fonctionnement

<sup>1</sup> La Commission cantonale de la protection des données est formée d'un président ou d'une présidente et de quatre membres, élus pour une durée de quatre ans par le Grand Conseil à la suite d'une proposition du Conseil d'Etat. Son secrétariat est assuré par le ou la préposé-e.

<sup>2</sup> Le président ou la présidente et les membres doivent posséder, dans leur ensemble, les connaissances nécessaires à l'accomplissement des tâches de la Commission; celle-ci comprend en particulier un ou une professionnel-le de la santé et un ou une spécialiste en informatique.

<sup>3</sup> En cas de besoin, la Commission peut consulter des experts ou des expertes et inviter des tierces personnes à assister à tout ou partie de ses séances et, le cas échéant, à s'y exprimer avec voix consultative.

<sup>4</sup> Pour le surplus, la Commission règle son organisation et son fonctionnement.

**Art. 30a (nouveau)** b) Attributions

<sup>1</sup> La Commission exerce une surveillance générale dans le domaine de la protection des données. Elle a notamment pour tâches:

- a) de diriger l'activité du ou de la préposé-e;
- b) de donner son avis sur les projets d'actes législatifs touchant à la protection des données ainsi que dans les cas prévus par la loi;
- c) de mettre en œuvre la procédure prévue à l'article 22a en cas de violation ou de risque de violation des prescriptions sur la protection des données;
- d) d'interjeter les recours prévus à l'article 27 al. 2;
- e) d'exercer la haute surveillance sur les autorités communales de surveillance, dont elle reçoit le rapport d'activité.

<sup>2</sup> La Commission adresse chaque année au Grand Conseil, par l'intermédiaire du Conseil d'Etat, un rapport sur son activité et celle du ou de la préposé-e. Elle peut, dans la mesure où l'intérêt général le justifie, informer le public de ses constatations.

<sup>3</sup> Die Aufsichtsbehörde der Gemeinde ist in der Ausübung ihrer Zuständigkeiten unabhängig und verfügt über die nötigen Mittel zur Erfüllung ihrer Aufgaben. Sind diese Bedingungen nicht erfüllt, so wird die Aufsicht von der kantonalen Behörde wahrgenommen.

**Art. 30** Kantonale Kommission

a) Zusammensetzung, Organisation und Arbeitsweise

<sup>1</sup> Die kantonale Datenschutzkommission setzt sich aus der Präsidentin oder dem Präsidenten und vier Mitgliedern zusammen, die vom Grossen Rat auf Vorschlag des Staatsrates für vier Jahre gewählt werden. Ihr Sekretariat wird von der bzw. vom Datenschutzbeauftragten geführt.

<sup>2</sup> Die Präsidentin oder der Präsident und die Mitglieder müssen in ihrer Gesamtheit über die Kenntnisse verfügen, die zur Erfüllung der Aufgaben der Kommission erforderlich sind; diese umfasst insbesondere eine Fachperson aus dem Gesundheitswesen und eine Informatikspezialistin oder einen Informatikspezialisten.

<sup>3</sup> Wenn nötig kann die Kommission Sachverständige beiziehen oder Drittpersonen zu einer Sitzung oder einem Teil einer Sitzung einladen und ihnen gegebenenfalls beratende Stimme geben.

<sup>4</sup> Im Übrigen regelt die Kommission ihre Organisation und ihre Arbeitsweise.

**Art. 30a (neu)** b) Befugnisse

<sup>1</sup> Die Kommission übt die allgemeine Aufsicht auf dem Gebiet des Datenschutzes aus. Sie hat namentlich folgende Aufgaben:

- a) Sie leitet die Tätigkeit der oder des Datenschutzbeauftragten.
- b) Sie nimmt Stellung zu Entwürfen von Erlassen, die den Datenschutz betreffen, sowie in den vom Gesetz vorgesehenen Fällen.
- c) Bei einer Verletzung oder einer möglichen Verletzung von Datenschutzvorschriften führt sie das Verfahren nach Artikel 22a durch.
- d) Sie legt Beschwerde nach Artikel 27 Abs. 2 ein.
- e) Sie übt die Oberaufsicht über die kommunalen Aufsichtsbehörden aus und erhält deren Tätigkeitsbericht.

<sup>2</sup> Die Kommission erstattet dem Staatsrat zuhanden des Grossen Rates alljährlich einen Bericht über ihre Tätigkeit sowie über die Tätigkeit der oder des Datenschutzbeauftragten. Sie kann, sofern dies durch das öffentliche Interesse gerechtfertigt ist, die Öffentlichkeit über ihre Feststellungen informieren.

### **Art. 31** Préposé-e

<sup>1</sup> Le ou la préposé-e cantonal-e à la protection des données est nommé-e par le Conseil d'Etat, sur le préavis de la Commission.

<sup>2</sup> Il ou elle a pour tâches:

- a) de contrôler l'application de la législation relative à la protection des données, notamment en procédant systématiquement à des vérifications auprès des organes concernés;
- b) de conseiller les organes concernés, notamment lors de l'étude de projets de traitement;
- c) de renseigner les personnes concernées sur leurs droits;
- d) d'exécuter les travaux qui lui sont confiés par la Commission;
- e) de faire rapport à la Commission sur son activité et ses constatations;
- f) de collaborer avec le préposé fédéral à la protection des données et à la transparence ainsi qu'avec les autorités de surveillance de la protection des données des autres cantons et avec celles de l'étranger;
- g) d'examiner l'adéquation du niveau de protection assuré à l'étranger, au sens de l'article 12a al. 3.

<sup>3</sup> Le ou la préposé-e recueille les informations nécessaires à l'accomplissement de ses tâches. Il ou elle peut notamment demander des renseignements, exiger la production de documents, procéder à des inspections et se faire présenter des traitements. Le secret de fonction ne peut lui être opposé.

### **Art. 32 titre médian, al. 3 et al. 4 à 6 (nouveaux)**

Dispositions communes

<sup>3</sup> Elle [l'autorité cantonale de surveillance] dispose d'une enveloppe budgétaire dont le montant est déterminé chaque année à l'occasion de l'adoption du budget de l'Etat.

<sup>4</sup> Les membres de l'autorité cantonale de surveillance sont soumis au secret de fonction et à l'obligation de discrétion.

<sup>5</sup> Ils signalent, au moment de leur entrée en fonction et lors de chaque modification, les liens particuliers qui les rattachent à des intérêts privés ou publics.

<sup>6</sup> Les articles 21 à 25 du code de procédure et de juridiction administrative sont applicables à la récusation des membres de l'autorité cantonale de surveillance.

### **Art. 31** Die oder der Datenschutzbeauftragte

<sup>1</sup> Die oder der kantonale Datenschutzbeauftragte wird vom Staatsrat ernannt. Dieser holt vorgängig die Stellungnahme der Kommission ein.

<sup>2</sup> Die oder der Datenschutzbeauftragte:

- a) überwacht die Anwendung der Gesetzgebung über den Datenschutz, namentlich durch systematische Überprüfungen bei den betreffenden Organen;
- b) berät die betreffenden Organe, namentlich bei der Planung von Datenbearbeitungsvorhaben;
- c) informiert die betroffenen Personen über ihre Rechte;
- d) führt die Arbeiten aus, die ihr oder ihm von der Kommission zugewiesen werden;
- e) berichtet der Kommission über ihre oder seine Tätigkeit und teilt ihr ihre oder seine Feststellungen mit;
- f) arbeitet mit der oder dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten sowie mit den Datenschutzaufsichtsbehörden der anderen Kantone und des Auslandes zusammen;
- g) prüft, ob ein angemessener Schutz im Ausland im Sinne von Artikel 12a Abs. 3 gewährleistet wird.

<sup>3</sup> Die oder der Datenschutzbeauftragte holt die zur Erfüllung der Aufgaben benötigten Informationen ein. Sie oder er kann namentlich Auskünfte einholen, Akten herausverlangen, Inspektionen durchführen und sich Datenbearbeitungen vorführen lassen. Die angegangenen Stellen können sich ihr oder ihm gegenüber nicht auf das Amtsgeheimnis berufen.

### **Art. 32 Artikelüberschrift, Abs. 3 und Abs. 4–6 (neu)**

Gemeinsame Bestimmungen

<sup>3</sup> Sie [die kantonale Aufsichtsbehörde] verfügt über ein Globalbudget, dessen Betrag alljährlich bei der Verabschiedung des Staatsbudgets festgelegt wird.

<sup>4</sup> Die Mitglieder der kantonalen Aufsichtsbehörde unterstehen dem Amtsgeheimnis und der Schweigepflicht.

<sup>5</sup> Bei ihrem Amtsantritt und bei jeder späteren Änderung teilen sie ihre besonderen, privaten und öffentlichen Interessenbindungen mit.

<sup>6</sup> Die Artikel 21–25 des Gesetzes über die Verwaltungsrechtspflege sind für den Ausstand von Mitgliedern der kantonalen Aufsichtsbehörde anwendbar.

**Art. 2**

<sup>1</sup> Le Conseil d'Etat fixe la date d'entrée en vigueur de la présente loi.

<sup>2</sup> La présente loi est soumise au referendum législatif. Elle n'est pas soumise au referendum financier.

**Art. 2**

<sup>1</sup> Der Staatsrat bestimmt das Inkrafttreten dieses Gesetzes.

<sup>2</sup> Dieses Gesetz untersteht dem Gesetzesreferendum. Es untersteht nicht dem Finanzreferendum.