Règlement

du 29 juin 1999

sur la sécurité des données personnelles (RSD)

Le Conseil d'Etat du canton de Fribourg

Vu l'article 22 de la loi du 25 novembre 1994 sur la protection des données (LPrD) ;

Vu les avis de la Commission cantonale de la protection des données et de la Commission informatique de l'Etat ;

Sur la proposition de la Direction de la justice, de la police et des affaires militaires,

Arrête :

CHAPITRE PREMIER
Dispositions générales

Art. 1 Objet et champ d'application

[1] Le présent règlement fixe les principes généraux et les exigences minimales en matière de sécurité des données personnelles.

[2] Il s'applique à tout traitement de données personnelles soumis à la loi sur la protection des données (LPrD).

[3] Les dispositions spéciales fédérales ou cantonales relatives à la sécurité de certaines applications sont réservées.

Art. 2 Définitions

[1] Au sens du présent règlement, on entend par :

a) *sécurité informatique* le domaine de l'informatique visant à assurer la protection physique des sites de traitement de l'information et des infrastructures de télécommunications, l'intégrité des logiciels de base et des logiciels d'application, ainsi que l'intégrité, la disponibilité et la confidentialité des informations, que celles-ci soient stockées ou qu'elles soient en transit sur les réseaux ;

b) *journalisation* l'enregistrement, à des fins de contrôle ou de reconstitution, de tout ou partie des activités effectuées sur un système ou sur une application informatiques ;

c) *procédure d'appel* le mode de communication automatisé des données par lequel les destinataires, en vertu d'une autorisation du responsable du fichier, décident de leur propre chef, sans contrôle préalable, du moment et de l'étendue de la communication.

2 Pour le reste, les définitions figurant à l'article 3 LPrD s'appliquent.

CHAPITRE 2

Règles applicables à toute forme de traitement des données

Art. 3 Principes généraux

1 Les données personnelles doivent être protégées contre toute atteinte à leur confidentialité et contre tout traitement non autorisé.

2 La protection doit être assurée lors de chaque phase du traitement des données, de la collecte à la destruction ; elle doit être assurée à l'égard de toute personne, à l'intérieur comme à l'extérieur de l'administration.

3 La protection doit être harmonisée avec les mesures visant à assurer la sécurité des documents de l'administration en général, ainsi qu'avec les mesures prises à titre de sécurité informatique.

Art. 4 Responsabilité
a) De l'organe public

1 L'organe public qui traite des données personnelles est responsable de leur sécurité.

2 Après avoir procédé à une évaluation des risques encourus par les données traitées dans l'accomplissement de ses tâches (art. 8 et 9), il prescrit les mesures propres à assurer leur sécurité (art. 10 et 11).

3 Il vérifie régulièrement l'application, par les utilisateurs et utilisatrices, des mesures prescrites.

Art. 5 b) Des utilisateurs et utilisatrices

1 Les collaborateurs et collaboratrices qui traitent des données personnelles sont responsables de l'application des mesures prescrites par l'organe dont ils relèvent.

2 Lorsque les utilisateurs et utilisatrices sont des mandataires non soumis aux dispositions du présent règlement, leurs responsabilités en matière de sécurité sont définies dans le contrat mentionné à l'article 18 al. 2 LPrD.

Art. 6 c) En cas de traitement conjoint

Lorsque plusieurs organes publics traitent conjointement des données, la répartition des responsabilités en matière de sécurité entre le responsable du fichier et les participants au fichier doit figurer dans la déclaration du fichier (art. 19 al. 2 let. e LPrD).

Art. 7 d) Réserve

Les responsabilités particulières en matière de sécurité informatique du Service de l'informatique et des télécommunications (ci-après : le SITel) ou du service informatique compétent sont réservées.

Art. 8 Evaluation des risques
a) En général

[1] L'organe public évalue, pour chaque fichier, les risques d'atteinte à la confidentialité des données et les risques de traitement non autorisé ; suivant les besoins, il évalue également les risques d'atteinte à l'intégrité et à la disponibilité des données.

[2] Constituent notamment de tels risques :

a) les risques de falsification, de vol ou d'utilisation illicite ;

b) les risques de modification, de copie ou d'accès non autorisés ;

c) les risques de perte accidentelle et d'erreurs techniques.

Art. 9 b) Attribution d'un degré de confidentialité

[1] L'organe public attribue à chaque fichier un degré de confidentialité, selon l'échelle suivante :

a) *1er degré* : accessible au public ;

b) *2e degré* : à usage interne ;

c) *3e degré* : confidentiel ou secret.

[2] Il se fonde sur la nature des données personnelles traitées, sur le but, l'étendue et les formes du traitement, ainsi que sur les préjudices qu'un usage abusif des données peut causer aux personnes concernées.

[3] Au besoin, l'attribution d'un degré de confidentialité peut également porter sur des données ou des catégories de données spécifiques.

Art. 10 Définition des mesures
a) Autorisations d'accès

[1] L'organe public détermine, en fonction des tâches qu'elles sont appelées à exécuter, les personnes autorisées à accéder aux fichiers ainsi que l'étendue de leurs accès.

[2] L'autorisation d'accès peut également, notamment lors d'un traitement informatisé des données, porter sur des données ou des catégories de données spécifiques.

Art. 11 b) Mesures organisationnelles et techniques

[1] L'organe public définit, en fonction de l'étendue des risques et du degré de confidentialité des données, les mesures organisationnelles et techniques appropriées ; ces mesures peuvent porter aussi bien sur les personnes et les locaux que sur le matériel et la sécurité informatique.

[2] Les mesures doivent être proportionnées aux circonstances, techniquement adaptées, économiquement supportables et applicables en pratique.

Art. 12 Réévaluation périodique

L'organe public réévalue périodiquement les risques et le choix des mesures, notamment en fonction des possibilités techniques nouvelles.

Art. 13 Préarchivage et destruction

[1] La sécurité des données personnelles figurant dans les dossiers de préarchives doit être assurée.

[2] Les documents et autres supports de données personnelles qui ne sont pas destinés à être versés aux archives sont détruits de façon appropriée. Toute possibilité de reconstitution des données classées confidentielles ou secrètes doit être écartée.

CHAPITRE 3

Règles particulières relatives au traitement informatisé de données

Art. 14 Respect de la sécurité informatique

[1] Les systèmes, applications et réseaux informatiques servant au traitement de données personnelles doivent répondre aux exigences standard de la sécurité informatique.

[2] Ces exigences sont fixées dans la politique de sécurité des systèmes d'information prévue par les dispositions sur la gestion de l'informatique de l'Etat.

[3] La politique de sécurité des systèmes d'information est mise à la disposition des communes. Elle a force obligatoire pour tous les systèmes communaux qui sont reliés au réseau de l'administration cantonale.

Art. 15 Assistance et conseil

[1] Lors d'un traitement informatisé de données, le SITel conseille et assiste les services et établissements de l'administration cantonale pour toute question relative à la sécurité des données personnelles. Les compétences particulières de l'Université et des hautes écoles appartenant à la Haute Ecole spécialisée de Suisse occidentale en matière informatique sont réservées.

[2] Pour tout ce qui concerne la mise en œuvre de la politique de sécurité des systèmes d'information, les communes peuvent également bénéficier des conseils et de l'assistance du SITel. Celui-ci peut facturer les frais y relatifs.

[3] Le SITel, l'Université et les hautes écoles appartenant à la Haute Ecole spécialisée de Suisse occidentale collaborent dans ce domaine avec l'Autorité cantonale de la transparence et de la protection des données.

Art. 16 Applications et fichiers
a) Conception

[1] Les exigences liées à la sécurité des données personnelles doivent être prises en considération dès la conception des applications et des fichiers.

[2] Les coûts y relatifs doivent être intégrés dans la planification financière des applications.

Art. 17 b) Authentification et contrôle des accès

[1] L'accès aux systèmes informatiques permettant le traitement de données personnelles doit être protégé par un dispositif comprenant :

a) une procédure d'authentification comprenant au moins l'identification des utilisateurs et utilisatrices et l'introduction d'un mot de passe ;

b) un système de contrôle des accès, fondé sur une définition d'autorisations individuelles d'accès.

[2] L'accès aux applications et/ou aux fichiers doit également être protégé par un tel dispositif :

a) lorsque des données classées confidentielles ou secrètes sont traitées ;

b) ou que l'autorité cantonale ou communale de surveillance en matière de protection des données le demande.

[3] Les responsables du système, de l'application ou des fichiers définissent les autorisations individuelles d'accès en fonction des tâches que les utilisateurs et utilisatrices sont appelés à exécuter. Ils désignent un organe chargé de l'administration des accès, qui gère les autorisations d'accès et

règle les modalités de la procédure d'authentification sous leur responsabilité.

Art. 18 c) Journalisation

Lorsque les mesures préventives ne suffisent pas à garantir la sécurité des données personnelles, le traitement des données doit faire l'objet d'une procédure de journalisation.

Art. 19 d) Exercice par les personnes concernées de leurs droits

Les applications et fichiers doivent permettre aux personnes d'exercer leur droit d'accès aux données les concernant (art. 23 à 25 LPrD), ainsi que leurs droits en cas de traitement illicite (droit à la rectification ou à la destruction des données ou droit à l'inscription d'une mention appropriée, art. 26 LPrD).

Art. 20 Réseaux et communications
a) Données confidentielles ou secrètes

[1] Les données personnelles classées confidentielles ou secrètes doivent être protégées par cryptage ou par d'autres mesures appropriées lors de leur transmission et de leur stockage.

[2] S'il est impossible de ramener à un niveau raisonnable les risques posés par le réseau principal, le trafic des données doit être isolé de ce dernier par la création d'un réseau virtuel ou par une autre mesure adéquate.

Art. 21 b) Procédure d'appel

[1] Lors de la mise en place d'une procédure d'appel, les autorisations individuelles d'accès sont définies par le responsable du fichier, en accord avec les destinataires des données.

[2] Le responsable du fichier veille à ce que les destinataires ne puissent pas modifier les données ni en entrer de nouvelles et qu'ils n'aient accès qu'aux données correspondant aux autorisations d'accès.

[3] La procédure d'appel doit être documentée dans un règlement d'utilisation, qui précise notamment les personnes autorisées à accéder aux données, les données mises à leur disposition, la fréquence des interrogations, la procédure d'authentification, les autres mesures de sécurité ainsi que les mesures de contrôle. Une copie du règlement est transmise à l'autorité cantonale ou communale de surveillance en matière de protection des données.

Art. 22 c) Internet et Intranet

[1] Les dispositions du présent chapitre s'appliquent aussi au traitement de données effectué sur un réseau de type Internet ou Intranet.

[2] En accord avec l'Autorité cantonale de la transparence et de la protection des données, le SITel et l'Université veillent à fournir aux utilisateurs et utilisatrices qui sont raccordés à ce type de réseau une information générale sur les risques qui y sont liés, notamment en ce qui concerne la messagerie électronique ; cette information est également adressée aux communes.

Art. 23 Appareils périphériques et maintenance

Des mesures spéciales doivent être prises pour éviter toute atteinte à la confidentialité et tout traitement non autorisé lors de la sortie des données sur des appareils périphériques ainsi que lors des opérations de maintenance.

Art. 24 Procédures de journalisation

[1] Lorsqu'un système ou une application informatique est doté d'une procédure de journalisation des événements, les fichiers de journalisation sont soumis aux règles de la protection des données, notamment en ce qui concerne la déclaration mentionnée à l'article 19 LPrD.

[2] La conservation, l'exploitation et la destruction des fichiers de journalisation font l'objet d'instructions dans le concept de sécurité informatique prévu par les dispositions sur la gestion de l'informatique de l'Etat.

CHAPITRE 4

Surveillance

Art. 25 Contrôle hiérarchique

L'autorité supérieure contrôle l'application, par les organes publics qui lui sont subordonnés, des dispositions du présent règlement.

Art. 26 Contrôle par l'autorité de surveillance

[1] L'autorité cantonale ou communale de surveillance en matière de protection des données exerce la surveillance externe conformément aux articles 29 et suivants LPrD.

[2] L'organe public contrôlé collabore avec l'autorité de surveillance et lui fournit tous les renseignements nécessaires, notamment ceux qui concernent l'évaluation des risques, la détermination des autorisations

d'accès, la définition des mesures organisationnelles et techniques ainsi que les vérifications effectuées.

Art. 27 Compétences du SITel

[1] Les compétences en matière de contrôle de la sécurité informatique du SITel ou, le cas échéant, du service informatique compétent sont réservées.

[2] Lorsque les contrôles effectués mettent au jour des lacunes dans la sécurité des données personnelles, le SITel ou le service informatique compétent en avise le ou la supérieur-e hiérarchique de l'organe public concerné ainsi que l'autorité cantonale ou communale de surveillance en matière de protection des données.

Art. 28 Constatations fortuites

Les collaborateurs et collaboratrices qui, dans l'accomplissement de leurs tâches, constatent des lacunes dans la sécurité des données personnelles d'un autre organe public que celui dont ils relèvent en informent leur chef-fe de service, qui avise l'organe responsable des données.

CHAPITRE 5

Dispositions transitoires et finales

Art. 29 Droit transitoire

Les communes qui sont dotées d'équipements et d'applications informatiques anciens et difficilement adaptables aux exigences de la sécurité informatique peuvent, jusqu'au remplacement de ces équipements et applications, se contenter de mesures d'ordre physique pour assurer la sécurité des données personnelles lors de traitements informatisés.

Art. 30 Modification

L'arrêté du 22 décembre 1987 concernant la gestion de l'informatique dans l'administration cantonale, l'enseignement et les établissements de l'Etat (RSF 122.96.11) est modifié comme il suit :

...

Art. 31 Entrée en vigueur et publication

[1] Le présent règlement entre en vigueur le 1er janvier 2000.

[2] Il est publié dans la Feuille officielle, inséré dans le Bulletin des lois et imprimé en livrets.