Kanton Bern
Canton de Berne

Bureau pour la surveillance de la protection
des données du canton de Berne (BPD)

Poststrasse 25
3072 Ostermundigen
+41 31 633 74 10
protectiondesdonnees@be.ch
www.dsa.be.ch

Protection des données: examen périodique des applications informatique: CONDITION GÉNÉRALES

(également valables lors de recours à des sociétés d'audit)

Table des matières

Quiconque souhaite charger une société d'audit d'un contrôle de la protection des données est tenu de respecter les conditions générales suivantes. Il en va de même pour toute autorité de surveillance de la protection des données qui prévoit de mener elle-même ce contrôle.

1. Délégation du mandat de contrôle à une société d'audit[1]

Il convient de conclure un contrat écrit fondé sur les conditions générales (CG) de la Conférence suisse sur l'informatique (CSI[2]).

2. Teneur du contrôle

2.1 Principe: contrôle de l'application

- Il s'agit d'examiner, en relation avec l'application, le respect des prescriptions juridiques (contrôle par les autorités, pas d'audit de la protection des données, pas de certification).
- Si les normes applicables laissent une marge d'appréciation suffisante, seul le bien-fondé de la solution retenue sera vérifié.

2.2 Objet du contrôle

Il y a lieu de vérifier les points suivants de manière individuelle ou combinée.

2.2.1 Protection des données (sans la sécurité informatique)

La société d'audit procède de la manière suivante:

- Elle examine les bases légales nécessaires au traitement des données de manière générale et, plus particulièrement, celles qu'exige une procédure d'appel.
- Elle examine si les droits d'accès ont été définis de manière à respecter la légalité et proportionnalité, et s'ils ont été mis en œuvre de manière correcte.
    - S'il s'avère que les mesures préventives ne garantissent pas un accès proportionné, la société d'audit examine si l'exercice légal des droits d'accès est assuré par des mesures de contrôle telles qu'une journalisation (art. 6 OPD[3]) et vérifie la façon dont celles-ci sont mises en œuvre.
- Elle examine la mise en œuvre des prescriptions concernant
    - Le droit de blocage,
    - Le droit de rectification,
    - La destruction des données, l'archivage ainsi que
    - Le droit de consultation.

[1] Selon l'ACE 1668/04 du 26 mai 2004
[2] https://sik.swiss/fr/
[3] Ordonnance du 22 octobre 2008 sur la protection des données; OPD, RSB 152.040.1

2.2.2 Sécurité informatique

La société d'audit vérifie la sécurité informatique en procédant de la manière suivante:

- Elle examine si les mesures de sécurité informatiques prescrites par le conseil communal et, le cas échéant, les nouvelles mesures prévues à la période de l'examen, sont appliquées.
- Elle examine si les prescriptions spécifiques à la sécurité informatique, inscrites dans des règles de droit, en particulier celles des articles 4 et 5 OPD, sont mises en œuvre.
- Elle fait des propositions sur les consignes de sécurité qu'elle entend utiliser lors de son contrôle s'il n'existe pour l'application aucune consigne propre à la commune, tenant suffisamment compte de l'état de la technique; elle contrôle leur mise en œuvre.

2.2.3 Organisation de la protection des données

- La société d'audit examine si les responsabilités au sens de l'article 8 LCPD[4] sont claires et vérifie de manière sommaire si les responsables assument leurs tâches de direction, et de quelle manière.

3. Exigences posées aux sociétés d'audit

3.1 Exigences technique

La société d'audit doit disposer de connaissances spécifiques dans les domaines de la technique informatique, du droit et de l'organisation de contrôles (révision). Elle doit le prouver en montrant qu'elle dispose de collaborateurs ayant terminé des études universitaires de droit, de personnes au bénéfice d'une formation en informatique suivie dans une haute école spécialisée ou d'une autre formation de niveau équivalent ou encore d'une longue expérience professionnelle dans ce domaine. Elle doit enfin pouvoir recourir à des personnes disposant d'une formation en audit informatique ou d'une longue expérience professionnelle dans ce domaine.

3.2 Indépendance

- La société d'audit doit être indépendante.
- Cela signifie en particulier qu'il n'est pas possible d'engager en qualité de société d'audit:
    - Des anciens collaborateurs qui étaient responsables de l'application informatique;
    - Des services intégrés à la direction de projet;
    - Des organismes qui avaient assumé des mandats partiels dans le domaine de l'exploitation de l'application informatique;
    - Des partenaires ayant travaillé avec l'application dans le cadre d'une externalisation.

4. Respect du secret de fonction

- Dans la mesure où il s'agit de données personnelles, la société d'audit est considérée comme une autorité en vertu de l'article 2, alinéa 6, lettre b LCPD. De ce fait, elle est tenue au secret de

[4] Loi du 19 février 1986 sur la protection des données, LCPD; RSB 152.04

fonction. S'agissant des autres données, les société d'audit assument, sur la base de l'article 64 LCo[5], un mandat officiel et sont par conséquent également soumises au secret de fonction.

- Dans un contrat écrit, l'autorité délivrant le mandat de contrôle attire l'attention de la société d'audit sur le fait qu'elle est soumise au secret professionnel et sur les suites pénales du non-respect de celui-ci. Elle exige dans ce contrat que la société d'audit fasse signer à toutes les personnes impliquées dans les activités de contrôle une déclaration de confidentialité, qui mentionne le secret professionnel et les suites pénales du non-respect de celui-ci.

5. Obligation d'élaborer un programme d'examen

Avant que la société d'audit ne procède aux actes de contrôle proprement dits, elle doit remettre au service responsable un plan d'examen qui mentionne

- Le but et l'étendue du contrôle;
- La période sur laquelle portent les traitements de données à contrôler (p. ex. aussi les données archivées, etc.);
- Les prescriptions de la loi sur la protection des données à prendre en considération;
- Les autres dispositions et instructions à prendre en considération;
- La classification des données;
- Les consignes de sécurité informatique à prendre en considération;
- Les moyens de contrôle prévus conformément au chiffre 6, en particulier le modèle sur les échantillons ainsi que leur nombre, leur contenu et le but de la vérification;
- L'accès nécessaire aux moyens informatiques;
- L'estimation du temps nécessaire au contrôle;
- Les personnes prévues pour effectuer les contrôles;
- Les délais pour les contrôles et le délai final pour la remise du rapport d'audit.

6. Moyens de contrôle

Les moyens de contrôle auxquels la société d'audit doit recourir sont les questions posées oralement ou par écrit aux collaborateurs, les documents, les démonstrations d'applications informatiques, les accès aux moyens informatiques, les fichiers, en particulier les procès-verbaux de journalisation ainsi que des mesures et des tests techniques réalisés sous la forme d'un « piratage éthique ». Généralement, l'examen se fonde uniquement sur des échantillons.

7. Résultat

La société d'audit doit rédiger un rapport exposant de manière détaillée les résultats que les contrôles mentionnés dans le plan d'examen ont permis d'atteindre. Ce rapport doit porter sur l'accomplissement des tâches et sur le taux de conformité aux consignes, mais aussi proposer une évaluation globale. Si le rapport fait état de lacunes, il doit contenir des recommandations sur les mesures d'améliorations à prendre. Le rapport est commenté à l'intention du service responsable au cours d'une séance.

[5] Loi du 16 mars 1998 sur les communes, LCo; RSB 170.01

0. EXPLICATIONS

1. Généralités

1.1 Contexte

Le document intitulé « CONDITIONS GÉNÉRALES » fixe les conditions qui permettent de procéder au contrôle d'une application informatique ainsi que, le cas échéant, de recourir à des sociétés d'audit chargées du contrôle de la protection des données.

1.2 Justification juridique permettant de recourir à une société d'audit

Le recours à une société d'audit correspond à la délégation à des services externes d'un contrôle incombant aux autorités. Le transfert des tâches à des tiers se fonde légalement sur l'article 64, alinéa 1 LCo.

2. Explications détaillées

2.1 Questions organisationnelles (chiffre 1 des CONDITIONS GÉNÉRALES)

En cas de recours à une société d'audit, les contrats conclus avec celle-ci doivent se fonder sur les conditions générales (CG) de la Conférence suisse sur l'informatique (CSI).

2.2 Contenu du contrôle (chiffre 2 des CONDITIONS GÉNÉRALES)

2.2.1 Contrôle de l'application (chiffre 2.1 des CONDITIONS GÉNÉRALES)

L'article 43 de la loi sur la protection de l'environnement (LPE)[6] prévoit pour le domaine dont elle traite que les autorités exécutives peuvent confier à des particuliers l'accomplissement de tâches d'exécution. Cette procédure connue dans le domaine de l'environnement est désormais également proposée par des prestataires privés pour des contrôles de la protection des données effectués auprès d'autorités et de personnes privées. C'est la gestion de la protection des données qui figure au cœur même de ces contrôles, l'examen détaillé d'une application informatique ne représentant en fait qu'une petite partie de l'ensemble des procédures de contrôle. Les prestataires de tels contrôles, qui se voient généralement octroyer un certificat de protection des données, peuvent parfaitement jouer le rôle de société d'audit, mais il faut clairement préciser que leur mandat se limite au contrôle d'une application par une autorité. Le droit cantonal prévoit que les certifications ne concernent que les contrôles préalables, ce qui n'exclut pas que des services administratifs s'intéressent à une telle certification. S'ils le font, ils sortent dès lors du cadre prévu par les CONDITIONS GÉNÉRALES. Par conséquent, prendre en charge l'ensemble d'un contrôle prévu en vue d'une certification n'est généralement pas opportun.

A l'instar des contrôles effectués dans le domaine de la protection de l'environnement, ceux dont se charge la société d'audit laissent la place à des marges d'appréciation. Celles-ci peuvent être dues à des

[6] Loi fédérale du 7 octobre 1983 sur la protection de l'environnement, LPE; RS 814.01

notions juridiques imprécises ou à des réglementations que le service responsable de l'application informatique devra évaluer. La société d'audit doit donc toujours reprendre les évaluations et les d'appréciation si celles-ci respectent le cadre fixé par la norme. Il n'y a pas lieu de procéder à un contrôle de l'évaluation ou de l'appréciation[7].

2.2.2 Contrôle de la protection des données sans contrôle de la sécurité informatique (chiffre 2.2.1 des CONDITIONS GÉNÉRALES)

S'agissant du contrôle de la protection de la personnalité décrit ici, il y a lieu d'examiner si les prescriptions prévues par la loi sur la protection des données sont respectées. En revanche, il n'est pas nécessaire de vérifier si la disposition de cette même loi sur la sécurité informatique (art. 17 LCPD) a été prise en compte. Les points devant faire l'objet d'un contrôle sont donc les suivants: le droit de blocage est-il appliqué dans le système, un droit à la rectification peut-il être mis en œuvre, les données peuvent-elles être archivées puis détruites, et de quelle manière, et enfin, comment le droit de consultation peut-il être appliqué?

Le contrôle pourrait par exemple révéler qu'il manque un champ de données permettant de procéder à un blocage, qu'une destruction des données dans le système est impossible ou qu'elle n'est pas prévue pour des raisons d'organisation.

L'examen des droits d'accès existants est particulièrement important. Il s'agit de déterminer si les collaborateurs utilisant l'application n'ont accès qu'aux informations dont ils ont besoin pour accomplir leur tâche. Il peut s'avérer que la simple description théorique des droits d'accès soit rédigée de manière trop ouverte. Et même si elle est correcte, il est possible que le système ne respecte pas les limites imposées ou qu'il existe des possibilités de les contourner.

Un examen non négligeable est celui qui concerne l'existence des bases légales, et en particulier celles qui portent sur la procédure d'appel (accès par un service tiers dans le cadre de la procédure du libre accès).

Etant donné que le concept SIPD pour les projets informatiques qui est également demandé pour le contrôle préalable doit lui aussi respecter les prescriptions de la loi sur la protection des données, les points à contrôler se recoupent pour l'essentiel avec la mise en œuvre des droits de la protection de la personnalité qui doivent être commentés dans un concept SIPD.

A ce jour, les contrôles menés dans le domaine de la protection des données sans lien avec la sécurité informatique ont été fort rares. Il s'agit de remédier au fait que le mandat de contrôle, imposé par la loi, n'a de loin pas été suffisamment respecté.

2.2.3 Contrôle de la sécurité informatique (chiffre 2.2.2 des CONDITIONS GÉNÉRALES)

- Il convient d'examiner ici si les consignes du conseil communal sont respectées (art. 17 LCPD).
- Des dispositions spécifiques, contenues dans des ordonnances, imposent des consignes supplémentaires en matière de sécurité informatique. Celles dont il faut tenir compte sont les articles 4 et 5 OPD, qui décrivent les risques contre lesquels protéger les systèmes ainsi que les mesures techniques et organisationnelles à prendre.
- Il se peut que les consignes existantes, relatives à la sécurité informatique, ne suffisent pas pour l'application informatique à examiner. Dans un tel cas, l'organe de contrôle ou la société d'audit

[7] Voir aussi Alexander Rossnagel, Datenschutzaudit, Konzeption, Durchführung, gesetzliche Regelung, Braunschweig/Wiesbaden, 2000.

doit déterminer quelles normes, comblant des lacunes, doivent être reprises en vue de l'examen. On peut penser par exemple aux exigences de sécurité minimales et aux responsabilités relatives au besoin général de protection de la Confédération[8].

2.2.4 Organisation de la protection des données (chiffre 2.2.3 des CONDITIONS GÉNÉRALES)

L'article 8 LCPD définit l'autorité responsable du traitement des données. Il prévoit en particulier, dans le cas où les traitements de données sont le fait de plusieurs autorités, de désigner une autorité assumant une responsabilité globale. Cette attribution de responsabilité est liée à des tâches de conduite. Dans le cadre de ses contrôles liés aux applications, la société d'audit examine la manière dont l'autorité responsable assume sa tâche de conduite et dresse un rapport sommaire sur ses constatations.

2.3 Exigences posée à la société d'audit (chiffre 3 des CONDITIONS GÉNÉRALES)

2.3.1 Connaissances spécialisées (chiffre 3.1 des CONDITIONS GÉNÉRALES)

- Il y a plus de 20 ans déjà, le rapport relatif à la loi cantonale sur la protection des données expliquait qu'un contrôle de la protection des données nécessitait des connaissances juridiques, de technique de l'information et d'organisation. Les exigences posées aux sociétés d'audit n'ont pas changé.
- Il convient de préciser qu'au savoir-faire en matière organisationnelle doit s'ajouter des connaissances dans le domaine de l'audit (révision).
- En fonction des circonstances, il est difficile de vérifier si les sociétés d'audit disposent de ces connaissances. Elles doivent prouver qu'elles peuvent recourir à des personnes au bénéfice de formations dans les domaines concernés ou d'une longue expérience professionnelle. Le fait qu'il s'agisse de collaborateurs ou de personnes intégrées d'une autre manière (consortiums) n'a pas d'importance. Lors d'examens partiels, des connaissances spécifiques dans le domaine concerné (p. ex. sécurité informatique) sont suffisantes. Il est également possible d'apporter la preuve des connaissances requises en présentant le document attestant qu'une formation a été suivie auprès d'une organisation reconnue (p. ex. ISACA)[9].

2.3.2 Indépendance (chiffre 3.2 des CONDITIONS GÉNÉRALES)

La constatation d'une insuffisance chronique de l'accomplissement du mandat d'audit dans le domaine de la protection des données doit inciter à introduire de tels examens. Pour répondre à ce mandat prescrit par la loi, il faut toutefois que la société d'audit soit crédible, ce qui suppose en premier lieu une indépendance de sa part. Celle-ci ne peut pas vérifier des actes dont elle a personnellement à répondre ni participer à l'exploitation de l'application informatique.

L'article 9 de la loi sur la procédure et la juridiction administratives (LPJA)[10] poursuit les mêmes buts pour la procédure administrative et pour la procédure de justice administrative. Les auteurs des CONDITIONS GÉNÉRALES se sont inspirés de cette disposition pour traiter la question de l'indépendance.

[8] https://www.isb.admin.ch/isb/fr/home/themen/sicherheit.html
[9] Pour obtenir des informations sur l'ISACA, consulter son site Internet à l'adresse http://www.isaca.ch/ (www.isaca.org/french), en particulier ce qui concerne son certificat CISA
[10] Loi du 23 mai 1989 sur la procédure et la juridiction administratives, LPJA; RSB 155.21

2.4 Respect du secret de fonction par les sociétés d'audit (chiffre 4 des CONDITIONS GÉNÉRALES)

Une société d'audit à laquelle on aura le cas échéant recouru exerce des tâches relevant d'une autorité. Il s'agit dans tous les cas de s'assurer que cette société, par ses actes, ne fasse pas courir un risque de non-respect de la confidentialité. L'article 2, alinéa 5 LCPD et l'article 64 LCo constituent la base légale de l'obligation qu'a la société d'audit de respecter le secret de fonction. Elle est donc susceptible d'encourir la peine prévue à l'article 320 CPS[11]. Il doit être prévu, dans les termes du contrat, que la société d'audit est tenue à un devoir de discrétion et qu'elle doit respecter le secret professionnel. Elle doit par ailleurs faire signer à tous les collaborateurs prenant part aux contrôles une déclaration de confidentialité.

2.5 Obligation d'établir un programme d'examen (chiffre 5 des CONDITIONS GÉNÉRALES)

Les CONDITIONS GÉNÉRALES prévoient des consignes détaillées à ce sujet. Les applications informatiques traitent généralement d'importantes quantités de données. Les traitements de données possibles sont nombreux et les questions qui se posent du point de vue du droit de la protection des données présentent souvent une certaine complexité. L'examen d'une application informatique sous l'angle de la protection des données comporte un risque, celui de se perdre, qu'il faut limiter par l'intermédiaire du plan d'examen. La société d'audit doit exposer la façon dont elle entend procéder et fixer les limites de ses vérifications. Il doit être ainsi possible de déterminer, avant le contrôle, si la procédure prévue est judicieuse.

2.6 Moyens de contrôle (chiffre 6 des CONDITIONS GÉNÉRALES)

L'énumération des moyens de contrôle doit montrer à la société d'audit lesquels d'entre eux elle peut ou ne peut pas utiliser. En plus des moyens habituellement employés lors de révisions (questionnaires, consultation de documents), des démonstrations d'applications informatiques, des mesures d'ordre technique, des accès à des moyens informatiques et à des fichiers ainsi que, le cas échéant, le recours à un « piratage éthique » (tentative d'intrusion dans un système informatique afin de montrer à son responsable quelles sont les failles de sécurité) doivent également être possibles.

2.7 Résultat (chiffre 7 des CONDITIONS GÉNÉRALES)

Tout comme il convient d'imposer à la société d'audit un plan d'examen, il s'agit également de lui prescrire la forme sous laquelle ses résultats devront être exposés. Le rapport d'audit doit comporter les points énumérés dans le plan d'examen et contenir une évaluation générale. Il doit évoquer l'accomplissement des tâches et le taux de conformité aux consignes. En cas de lacunes, le rapport présentera des recommandations sur les mesures d'amélioration qui s'imposent. Le rapport doit être commenté oralement, lors d'une séance, à l'intention du service responsable de l'application.

[11] Code pénal suisse du 21 décembre 1937, CPS; RS 311.0