Conditions générales du canton de Berne

relatives à la

sécurité de l'information et à la protection des données

CG SIPD BE

du 26 août 2024

révisées le 16 décembre 2024

Version 2.0

Table des matières

1. But

1.1 Les présentes conditions générales relatives à la sécurité de l'information et à la protection des données (CG SIPD) ont pour but de garantir la sûreté de l'information et des données et, partant, la protection des données lors de l'acquisition et de l'utilisation de ressources TIC par les autorités du canton de Berne.

1.2 La mise en œuvre des CG SIPD et le respect des exigences posées dans le cadre de l'instruction de l'Office d'informatique et d'organisation (OIO) sur la protection de base en matière de sécurité de l'information et de cybersécurité (IPSIC)[1] du 16 décembre 2024 permet d'assurer la protection de base pour les ressources TIC, les informations et les données personnelles, y compris par les fournisseurs de prestations.

2. Définitions

Au sens des présentes CG, on entend par :

2.1 **Autorités :** les autorités cantonales mandantes, les autorités communales ainsi que les organes chargés de tâches publiques du canton et des communes, quelle que soit leur forme juridique (art. 4, al. 1 et 2 de la loi du 7 mars 2022 sur l'administration numérique [LAN][2]).

2.2 **Fournisseur de prestations :** une personne physique ou morale qui fournit des ressources TIC à une autorité sur mandat de celle-ci.

2.3 **Ressources TIC :** les biens et services des technologies de l'information et de la communication (TIC), y compris le matériel et les logiciels (art. 4, al. 3, lit. a LAN).

2.4 **Informations :** données, sous quelque forme que ce soit, relatives à des faits et non à des personnes (art. 4, lit. b IPSIC).

2.5 **Données personnelles :** données, sous quelque forme que ce soit, relatives à une personne physique ou morale, identifiée ou identifiable (art. 2, al. 1 de la loi du 19 février 1986 sur la protection des données [LCPD][3]).

2.6 **Sécurité de l'information et des données :** état de garantie de la confidentialité, de la disponibilité, de l'intégrité et de la traçabilité des ressources TIC, des informations et des données personnelles (art. 4, lit. d IPSIC).

2.7 **Traitement :** toute activité ayant directement trait à des informations ou des données personnelles, notamment le fait de recueillir, de conserver, de modifier, de combiner, de communiquer ou de détruire des données personnelles (art. 2, al. 4 LCPD).

2.8 **Communication :** le fait de rendre des informations ou des données personnelles accessibles, notamment de les transmettre, de les publier, d'autoriser leur consultation ou de fournir des renseignements (art. 2, al. 5 LCPD).

2.9 **Incident de sécurité :** événement qui compromet la confidentialité, la disponibilité, l'intégrité ou la traçabilité des ressources TIC, des informations ou des données personnelles (art. 4, lit. f IPSIC).

[1] IPSIC ; Site Internet de l'OIO sur la protection des données, la sécurité de l'information et la cybersécurité
[2] LAN ; RSB 109.1
[3] LCPD ; RSB 152.04

3. Assujettissement à la loi cantonale sur la protection des données

3.1 Le fournisseur de prestations prend acte que, par son activité de traitement de données sur mandat d'une autorité au sens de l'article 16 LCPD, il est soumis à la LCPD dans la même mesure que l'autorité mandante. En particulier, la communication des données personnelles à des tiers requiert l'accord exprès de l'autorité.

4. Rapport avec le contrat et avec les CG CSI

4.1 Les CG SIPD font partie intégrante du contrat conclu entre le fournisseur de prestations et l'autorité. Les accords dérogatoires sont réservés.

4.2 Les conditions générales TIC-Services de la Conférence suisse sur l'informatique (CG ANS)[4] en vigueur au moment de la conclusion du contrat font également partie du contrat. Néanmoins, les dispositions contractuelles et les CG SIPD priment.

5. Sécurité de l'information et des données

5.1 Responsabilité

5.1.1 L'autorité conserve le pouvoir décisionnel en lien avec les informations et les données personnelles traitées dans le cadre de son mandat ; cela vaut aussi bien pour les données de contenu que pour les données secondaires de communication au sens de l'article 1, alinéa 1, lettres a et b de l'ordonnance du 20 novembre 2019 sur les données secondaires de communication (ODSC)[5]. Elle conserve également la responsabilité de la protection des données et est habilitée à donner des instructions en la matière (responsabilité en matière de garantie, art. 8, al. 1 LCPD).

5.1.2 Le fournisseur de prestations veille, dans le cadre de son domaine de compétence, à la sécurité des ressources TIC, informations et données personnelles qui lui sont confiées.

5.1.3 Le fournisseur de prestations n'acquiert aucun droit sur les informations et les données personnelles traitées. Il doit mettre en œuvre efficacement les mesures SIPD et suivre les instructions de l'autorité mandante (responsabilité en matière de mise en œuvre).

5.2 Mise en œuvre de la protection de base

5.2.1 Le fournisseur de prestations met en œuvre les mesures de protection de base selon l'IPSIC en vigueur lors de la conclusion du contrat et contrôle leur efficacité de manière vérifiable. Les précisions spécifiques aux prestations sont réglées dans le contrat.

5.3 Mise en œuvre de la protection élevée conformément à l'analyse SIPD et au concept SIPD

5.3.1 S'il ressort de l'analyse SIPD de l'autorité que les informations et les données personnelles à traiter présentent un besoin de protection accru, le fournisseur de prestations doit mettre en œuvre les mesures nécessaires convenues contractuellement conformément au concept SIPD et contrôler leur efficacité de manière vérifiable (art. 5 OD SIPD[6] : analyse SIPD et concept SIPD).

[4] CG ANS
[5] ODSC, RSB 153.011.5
[6] OD SIPD, RSB 152.040.2

6. Traitement des données

6.1 Finalité

6.1.1 Les informations et les données personnelles ne peuvent être traitées que par les collaboratrices et collaborateurs du fournisseur de prestations qui en ont besoin pour l'exécution du contrat. Le traitement des informations et des données personnelles ne peut être effectué que dans le but défini par le contrat.

6.2 Traitement et communication d'informations ou de données personnelles

6.2.1 Sauf autorisation contraire, le fournisseur de prestations ne peut traiter ou communiquer des informations ou des données personnelles de l'autorité que pour le compte de celle-ci. Les requêtes de divulgation de données présentées par des personnes privées ou par d'autres autorités doivent être transmises sans délai à l'autorité.

6.2.2 Les mesures de contrainte prévues par les codes de procédure et ordonnées par d'autres autorités compétentes sont réservées. Dans ces cas également, dans la mesure où la loi le permet, le fournisseur de prestations doit adresser le requérant ou la requérante à l'autorité ou informer immédiatement cette dernière.

6.3 Lieu de traitement des informations et des données personnelles

6.3.1 Sauf disposition contraire du contrat, le traitement des informations et des données personnelles peut avoir lieu uniquement en Suisse ou dans un État offrant un niveau de protection adéquat des données conformément à l'annexe 1 de l'ordonnance fédérale du 31 août 2022 sur la protection des données (OPDo)[7].

7. Sous-traitance

7.1 Le contrat détermine si, et dans quelle mesure, le fournisseur de prestations peut avoir recours à des sous-traitants qui, en exerçant directement les prestations essentielles confiées par le fournisseur de prestations, entreraient eux-mêmes dans le champ d'application des CG SIPD. S'ils sont connus au moment de la conclusion du contrat, ces sous-traitants sont mentionnés dans le contrat et leur intervention est autorisée par l'autorité.

7.2 Le fournisseur de prestations impose contractuellement à ses sous-traitants, selon le chiffre 7, la mise en œuvre des mesures de sécurité conformément au contrat principal, au concept SIPD, ainsi qu'aux CG SIPD et aux CG CSI.

8. Audits

8.1 Contrôle de la légalité

8.1.1 Pour permettre le contrôle du caractère légal de la fourniture des prestations, le fournisseur de prestations accorde un droit d'audit et de contrôle aux organes de surveillance étatique indépendants suivants, dans le cadre de leurs tâches légales :

a) autorité de surveillance compétente en matière de protection des données ;
b) organe de surveillance financière compétent.

[7] OPDo ; RS 235.11

Le fournisseur de prestations est tenu, dans le cadre des bases légales en vigueur, de collaborer avec les organes de surveillance et, en particulier, de fournir les informations et documents requis.

8.2 Contrôle des prestations

8.2.1 L'autorité peut réaliser des audits dans le domaine de la sécurité de l'information, de la protection des données, des processus et de la facturation en lien avec les prestations convenues contractuellement.

8.3 Réalisation des audits

8.3.1 La direction des audits incombe à l'autorité. Après consultation du fournisseur de prestations, elle définit

a) les objets à auditer tels que les processus, les services de base, les logiciels, les fichiers de données, les documentations et codes source, les factures de prestations ;
b) l'organisation chargée de l'audit, qui ne peut pas être un concurrent direct du fournisseur de prestations, et
c) la procédure et les modalités de l'audit.

8.3.2 L'autorité annonce en principe au moins un mois à l'avance l'exercice des droits d'audit, en précisant le thème et le calendrier de l'audit. Ce délai peut être raccourci en cas d'incident de sécurité.

8.3.3 Le fournisseur de prestations participe à l'audit à ses propres frais conformément aux instructions de l'autorité ou de l'organisation chargée de l'audit. Elle octroie à ses collaboratrices et collaborateurs ou à ses mandataires les droits d'accès et de consultation nécessaires et répond à leurs questions.

8.3.4 L'autorité soumet au secret l'organisation chargée de l'audit ainsi que ses collaboratrices et collaborateurs ou ses mandataires.

8.4 Coûts

8.4.1 Les coûts d'un audit réalisé par un tiers mandaté à cet effet sont en principe pris en charge par l'autorité. Par ailleurs, les parties assument en principe elles-mêmes les coûts générés par l'audit.

8.4.2 Si l'audit révèle que des prescriptions légales ou contractuelles ont été violées et que l'autorité chargée de l'audit a fait des constatations d'importance moyenne ou élevée, le fournisseur de prestations est néanmoins tenu de payer au canton, dans les 30 jours suivant la présentation du rapport final approuvé par l'autorité chargée de l'audit,

a) les indemnités indûment perçues (trop-perçu) à la suite de la fourniture insatisfaisante des prestations contractuelles, majorés d'un intérêt de 5 %, ainsi que
b) tous les frais internes et externes supportés par l'autorité dans le cadre de l'audit.

8.4.3 Les frais engagés pour remédier aux manquements constatés dans le cadre de l'audit sont à la charge du fournisseur de prestations.

9. Obligation de signaler et mesures immédiates en cas d'incident de sécurité ou de vulnérabilité

9.1 En cas d'incident de sécurité ou de vulnérabilité au sens de l'article 4, alinéas f et g IPSIC, le fournisseur de prestations est tenu d'informer l'autorité et de collaborer avec elle, en particulier

a) en cas d'incident de sécurité ou de vulnérabilité au sens de l'annexe 2, chiffre 1.1.4 IPSIC ou
b) si une autre autorité extracantonale ou étrangère met en œuvre des actes de contrôle ou des mesures auprès du fournisseur de prestations, dans la mesure où ceux-ci concernent des informations, des données personnelles ou des ressources TIC conformément au contrat conclu ou
c) si des ressources TIC sont retirées au fournisseur de prestations par saisie, faillite ou autre mesure d'exécution forcée ou par d'autres événements ou mesures de tiers. Le fournisseur de prestations informera immédiatement toutes les personnes responsables que le pouvoir décisionnel en lien avec les informations et les données personnelles revient exclusivement à l'autorité conformément au contrat.

Les incidents de sécurité susmentionnés doivent être signalés au plus tard dans les 24 heures et les vulnérabilités dans les 48 heures suivant leur découverte. Le contenu du signalement doit satisfaire aux exigences de l'ordonnance fédérale sur la cybersécurité.

9.2 Dans les cas susmentionnés, le fournisseur de prestations prend sans délai les mesures immédiates requises par la loi conformément à l'état actuel de la technique afin de sécuriser les informations et les données personnelles ainsi que les ressources TIC utilisées pour le traitement de celles-ci et d'éviter ou de réduire au minimum les répercussions négatives.

9.3 Le fournisseur de prestations documente à l'intention de l'autorité les incidents et les éventuelles violations de la sécurité de l'information et des données. En outre, il met en œuvre et documente les mesures qui sont nécessaires, selon l'état actuel de la technique, pour éviter que de telles atteintes ne se reproduisent.

10. Confidentialité et engagement de personnel

10.1 Les chiffres 13 et 14 des CG CSI de janvier 2020 s'appliquent, notamment les sanctions pénales et de droit privé qui y sont décrites.

11. Restitution et effacement à l'échéance du contrat

11.1 À l'échéance du contrat, le fournisseur de prestations doit restituer gratuitement à l'autorité, au format convenu ou dans un format pouvant être traité ultérieurement selon l'état actuel de la technique, l'ensemble des informations et des données personnelles en sa possession.

11.2 Les informations ou les données personnelles traitées par le fournisseur de prestations doivent être effacées gratuitement et de manière irrécupérable par ce dernier conformément aux instructions des autorités et selon les exigences du chiffre 1.2.3 de l'annexe 2 à l'IPSIC. Cette obligation s'applique également au matériel de test et au matériel mis au rebut. Le procès-verbal de l'effacement doit être présenté à la première demande de l'autorité.

* * *