Observation des obligations contractuelles en vue du maintien de la protection informatique de base

Madame, Monsieur,

Votre entreprise fournit des prestations informatiques à notre Commune de ou à l’une de nos unités organisationnelles.

L’incident lié à la sécurité de l’information de l’entreprise Xplain a mis en lumière qu’une plus grande importance devait être accordée au maintien de la protection informatique de base[[1]](#footnote-1). Il en va de même au regard des différents incidents de sécurité qui ont pu se produire ces dernières années dans des communes en Suisse. La protection informatique de base définit de manière contraignante les mesures minimales de sécurité de l’information devant être obligatoirement garanties, les prescriptions en matière de sécurité des données (21 nLIPDA[[2]](#footnote-2)) et de respect des règles en matière de sous-traitance (l’article 28bss nLIPDA) devant être dans tous les cas respectés, ce qui devrait également être prévu dans les contrats que nous avons conclus avec vous. Les éventuelles dispositions contractuelles complémentaires visant le maintien de la sécurité de l’information qui iraient au-delà de la protection informatique de base doivent évidemment aussi être observées.

Nous partons du principe que votre entreprise honore ces obligations. À titre de mesure proactive et préventive, notre commune a néanmoins décidé de demander à ses principaux prestataires externes de lui confirmer par écrit qu’ils mettent bel et bien en œuvre la protection informatique de base, en expliquant *comment* ils s’y prennent. Nous nous attendons à ce que des mesures de protection supplémentaires soient mises en place en cas de besoin de protection accru, c’est-à-dire en fonction de l’importance des données et des documents, et en vue de l’entrée en vigueur de la nouvelle Loi sur l’information du public, la protection des données et l’archivage, le 1er janvier 2024 (ci-après : « nLIPDA »). C’est notamment le cas pour la gestion des données de production qui vous sont transmises dans le cadre de l’exécution de vos tâches. À titre d’exemple, les cas d’usage suivants sont importants pour nous (cette liste n’est pas exhaustive, elle vise uniquement à vous donner un aperçu des problématiques pertinentes) :

* Les données de production sont-elles régulièrement effacées après qu’un cas de support a été fermé ?
* Au cas où elles seraient impératives pour les travaux de projet, les bases de données de production sont-elles conservées conformément à la nLPIDA ? Font-elles l’objet d’une protection particulière et sont-elles effacées définitivement à la fin des travaux selon ces mêmes dispositions ?
* Est-il garanti que les bases de données de test ne contiennent en aucun cas des données de production ? Les bases de données de test doivent être systématiquement anonymisées. Si des données de production devaient toutefois être contenues dans ces bases, ces données sont-elles protégées en conséquence, notamment par le chiffrement, le contrôle d’accès et la journalisation des accès ?
* Est-il garanti que les environnements d’intégration ne nécessitent aucune donnée de production ? Si des données de production sont toutefois requises, des dispositions supplémentaires sont-elles prévues pour ces cas ?
* Les données, bases de données et environnements de test ainsi que les captures d’écran contenant des données de test ou anonymisées sont-ils clairement désignés comme tels pour pouvoir être différenciées des données de production ?
* Les captures d’écran issues des systèmes de production sont-elles rigoureusement anonymisées pour les travaux de projet et les cas de support ? Les originaux sont-ils systématiquement effacés ? Les expéditeurs sont-ils régulièrement sensibilisés au fait qu’ils ne doivent envoyer que des captures d’écran anonymisées ?
* Les fichiers de journalisation sont-ils conçus de manière à ne contenir aucune donnée de production de clients ? Offrent-ils la possibilité de filtrer ou d’anonymiser les données de production de clients en toute simplicité pour que celles-ci puissent être transmises sans mesure spécifique en cas de support ? Les fichiers de journalisation sont-ils effacés une fois l’analyse effectuée ?
* Les données de production (ou des extraits de ces données) sont-elles protégées de telle sorte qu’elles ne sont accessibles qu’aux collaborateurs qui en ont absolument besoin pour exécuter leurs tâches ? Sont-elles effacées une fois la tâche effectuée ? Ce procédé est-il régulièrement contrôlé ?
* Les documents de notre commune sont-ils protégés contre les accès non autorisés et les fuites de données et enregistrés de manière sécurisée selon leur niveau de sensibilité ? Ce procédé est-il régulièrement contrôlé ? Les documents qui ne sont plus nécessaires sont-ils régulièrement effacés ?
* Est-il garanti qu’aucune donnée de connexion ni aucun mot de passe ne sont lisibles en texte clair dans le code source lors du développement logiciel ?
* Est-il garanti que les informations relatives à l’accès au système (identifiants, mots de passe, adresses IP, ports, etc.) ne sont en aucun cas enregistrées en texte clair dans les fichiers de configuration ou d’autres fichiers ?
* Comment est-il garanti que les certificats utilisés pour effectuer des tests ne sont pas utilisé par la suite en production et sont effacés une fois la phase de test terminée ?
* Existe-t-il un canal sécurisé via lequel il est possible d’échanger des données sensibles lorsque cela est strictement nécessaire (par ex : via un courriel chiffré ou un portail sécurisé) ?
* Les informations d’accès aux systèmes de notre commune (comptes, mots de passe, données d’authentification, adresses IP, etc.) sont-elles enregistrées sous une forme chiffrée ?
* Les accès des équipes support aux systèmes productifs sont-ils protégés par une authentification forte à double facteur, systématiquement journalisés et les communications chiffrées ?
* Des clés de 256 bits au moins sont-elles utilisées pour chiffrer les informations de notre commune ?
* Est-ce que vos collaborateurs sont sensibilisés et formés aux risques cyber et à la sensibilité des données de notre commune ?

Nous vous prions de bien vouloir nous faire parvenir d’ici au [délai de 30 jours dès envoi du courrier] 2023 par lettre recommandée vos explications détaillées (y.c. description des processus, liste des données de production de clients (également les artéfacts tels que les fichiers de journalisation ou les captures d’écran non anonymisées issues des systèmes de production), etc.) en tenant compte des questions ci-avant (adresse postale : Commune de [XXX], adresse, n° postale, Commune).

[Madame ou Monsieur] se tient à votre disposition pour toute question au moyen des coordonnées suivantes :

* [n° de téléphone]
* [adresse de courriel].

Veuillez agréer, Madame, Monsieur, nos meilleures salutations.

1. https://www.ncsc.admin.ch/ncsc/fr/home/dokumentation/sicherheitsvorgaben-bund/sicherheitsverfahren/grundschutz.html [↑](#footnote-ref-1)
2. https://lex.vs.ch/app/fr/texts\_of\_law/170.2/versions/3229. [↑](#footnote-ref-2)