Contrats conclus avec les fournisseurs

Best Practice

Les points clés énumérés ci-dessous constituent une base pour rédiger les contrats conclus avec les fournisseurs. Ces bonnes pratiques doivent en principe être prises en compte notamment pour répondre aux exigences en matière de cybersécurité et de protection des données.

1. Le fournisseur doit protéger ses propres moyens informatiques – c’est-à-dire tous les systèmes informatiques et les réseaux – contre les cyberattaques selon l’état actuel de la technique et le niveau de risque.
2. Le fournisseur doit utiliser des méthodes de chiffrement modernes, régulièrement mises à jour et conformes aux normes de l’industrie. Cette clause permet de protéger les données sensibles lors de leur transfert entre les systèmes et, lorsqu’elles sont stockées, dans les banques de données en ligne et les dispositifs de sauvegarde.
3. Le fournisseur est soumis à l’obligation de transparence en matière d’accès afin de pouvoir déterminer clairement les personnes, les moments de consultation et les données ou systèmes concernés.
4. Le fournisseur doit signaler les cyberattaques, les violations de la protection des données et les vulnérabilités de ses systèmes afin de permettre une réaction rapide et appropriée aux incidents de sécurité. Le contrat doit préciser le délai de signalement en heures ou en jours ainsi que le service auquel le fournisseur doit s’adresser.
5. Le fournisseur doit immédiatement corriger les vulnérabilités détectées et ce, à ses propres frais (coûts liés au matériel, heures de travail et éventuels frais de prestataires externes).
6. Le fournisseur est tenu de respecter les exigences et les prescriptions de la loi sur la protection des données (LPD) lors du traitement d’informations personnelles. Seules les données nécessaires à l’accomplissement des tâches peuvent être collectées et traitées.
7. Le fournisseur doit tenir une liste des types de données sensibles qui sont utilisées dans les applications.
8. Le fournisseur doit tenir à jour un diagramme illustrant comment les données sensibles aboutissent dans les systèmes du fournisseur et où elles sont finalement stockées.
9. Le fournisseur doit régulièrement communiquer les informations qu’il détient sur l’organisation et les détruire lorsqu’elles ne sont plus nécessaires.
10. Le contrat doit définir les accords sur les niveaux de service (p. ex. les critères de prestation concrets, les normes de qualité que le fournisseur doit respecter, les critères d’évaluation des prestations ou les conséquences en cas de non-respect des normes).
11. Si le fournisseur fait appel à des sous-traitants, l’entreprise ainsi que ses employés sont soumis aux mêmes normes de cybersécurité et de protection des données que celles qui s’appliquent au fournisseur principal. Le contrat devrait contenir une clause exigeant du fournisseur l’autorisation de l’organisation s’il souhaite faire appel à un nouveau sous-traitant.
12. Le fournisseur doit tenir une liste des sous-traitants (entreprises tierces) qui ont accès aux données des clients. Cette liste doit pouvoir être consultée à tout moment en cas de demande.
13. Il est possible de demander au fournisseur de présenter deux fois par année une preuve du niveau de cybersécurité au sein de son entreprise afin de garantir la conformité et l’efficacité des mesures de protection. Dans ce cas, le contrat devrait préciser les modalités des audits de sécurité et les exigences sur l’état des mesures de cybersécurité (p. ex. réalisation des audits par une entreprise indépendante et reconnue). Le contrat peut également contraindre le fournisseur à utiliser des systèmes de surveillance pour consigner, enregistrer et conserver des données dans le but d’identifier les activités suspectes ou les violations potentielles de la sécurité. Il peut aussi l’obliger à établir des plans de réponse aux incidents comprenant des directives claires pour notifier, endiguer et investiguer les incidents de sécurité.
14. Il est possible d’inclure une clause dans le contrat rendant le fournisseur responsable des dommages directs et indirects qui découlent du non-respect des obligations contractuelles ainsi que des pénalités en cas de violation des obligations contractuelles en matière de cybersécurité et de protection des données.
15. Il est possible de contraindre le fournisseur à souscrire une assurance responsabilité civile et/ou une assurance cybersécurité couvrant les dommages qui découlent du non-respect des obligations contractuelles ou de violations de la LPD.

\* \* \* \* \*