suisse.ing

Schweizerische Vereinigung Beratender Ingenieurunternehmungen
Union Suisse des Sociétés d'Ingénieurs-Conseils
Unione Svizzera degli Studi Consulenti d'Ingegneria
Uniun svizra dals biros d'inschigneria consultativs
Swiss Association of Consulting Engineers

Berne, août 2023

FACT-SHEET RELATIVE À LA NOUVELLE LOI SUR LA SÉCURITE DE L'INFORMATION

En décembre 2020, l'Assemblée fédérale a adopté la loi fédérale sur la sécurité de l'information au sein de la Confédération (loi sur la sécurité de l'information, LSI; RO 2022 232). Les dispositions d'exécution afférentes ont été mises en consultation jusqu'au 24 novembre 2022. La LSI ainsi que les quatre ordonnances correspondantes entreront vraisemblablement en vigueur au début 2024. Bien que cette loi concerne en principe uniquement les autorités et organisations, son champ d'application s'étend également à tous les accords et contrats que la Confédération pourrait conclure avec des tiers (cf. art. 9 LSI).

La LSI vise à protéger les intérêts publics suivants (art. 1, al. 2, LSI):

- *la capacité de décision et d'action des autorités et organisations de la Confédération;*
- *la sécurité intérieure et extérieure de la Suisse;*
- *les intérêts de la politique extérieure de la Suisse;*
- *les intérêts économiques, financiers et monétaires de la Suisse;*
- *l'accomplissement des obligations légales et contractuelles des autorités et organisations de la Confédération en matière de protection des informations.*

La présente contribution se propose de donner un aperçu des principales règles de la LSI et de fournir par là un premier point de repère en vue de la collaboration future avec la Confédération.

Applicabilité limitée à la Confédération

La LSI s'applique aux autorités suivantes: l'Assemblée fédérale, le Conseil fédéral, les tribunaux de la Confédération, le Ministère public de la Confédération et son autorité de surveillance ainsi que la Banque nationale suisse; diverses organisations y sont de même soumises, à savoir les Services du Parlement, l'administration fédérale, les services administratifs des tribunaux de la Confédération, l'armée et les personnes chargées de tâches administratives (art. 2, al. 1 et 2, LSI. N.B.: Par souci de lisibilité, les «autorités et organisations soumises à la loi» sont désignées ci-après par la «Confédération»). Certaines dispositions valent aussi pour les cantons, à moins que ces derniers ne garantissent une sécurité au moins équivalente de l'information (art. 3 LSI).

Sont également en partie visées par la loi les organisations de droit public ou privé qui exploitent des infrastructures critiques (art. 2, al. 5, LSI) – étant entendu par infrastructures critiques l'approvisionnement en eau potable et en énergie, les infrastructures d'information, de communication et de transports ainsi que d'autres installations, processus et systèmes essentiels au fonctionnement de l'économie et au bien-être de la population (art. 5, let. c, LSI).

Lorsque la Confédération collabore avec des tiers, elle veille à ce que les exigences et mesures prévues par la loi soient reprises dans les accords et les contrats qu'elle conclut à cet effet. Elle veille par ailleurs à ce que la mise en œuvre des mesures soit contrôlée de manière adéquate (art. 9 LSI). Des entreprises appelées à exécuter un mandat sensible pour le compte de la Confédération peuvent être soumises à une procédure de sécurité (art. 50, al. 1, let. a, LSI).

Nota bene: Si dans le principe seule la Confédération est assujettie à la LSI, tout bureau d'ingénieurs qui collabore avec elle sera lui aussi tenu à l'avenir de se conformer aux exigences et mesures de la loi, voire pourra – dans le cadre de mandats sensibles – faire l'objet d'une procédure de sécurité.

Définition des «activités sensibles»

Aux termes de l'art. 5, let. b, LSI, sont considérées comme sensibles du point de vue de la sécurité de l'information les activités suivantes:

- le traitement d'**informations** classifiées «confidentiel» ou «secret» qui, si elles devaient être portées à la connaissance d'une personne non autorisée, sont susceptibles de nuire aux intérêts publics définis ci-avant dans l'introduction (art. 13, al. 2 et 3, LSI);

- l'administration, l'exploitation, la maintenance et le contrôle de **moyens informatiques** relevant des catégories de sécurité «protection élevée» ou «protection très élevée», lorsqu'une violation de la confidentialité, de la disponibilité, de l'intégrité ou de la traçabilité des informations qu'ils traitent risque de nuire considérablement aux intérêts publics définis ci-avant dans l'introduction (art. 17, al. 2 et 3, LSI);

- l'accès à des zones de sécurité, notamment des zones de protection 2 et 3 d'un ouvrage au sens de la législation sur la protection des ouvrages militaires. Les autorités peuvent instituer des zones de sécurité dans des locaux ou des espaces dans lesquels des informations classifiées «confidentiel» ou «secret» sont fréquemment traitées ou des moyens informatiques des catégories de sécurité «protection élevée» ou «protection très élevée» sont exploités (art. 23, al. 1, LSI).

Nota bene: La Confédération veillant elle-même à la classification des informations (cf. art. 11 LSI), l'on peut présumer que la majeure partie des contrats conclus avec cette dernière ne seront pas considérés comme sensibles du point de vue de la sécurité.

Contrats futurs conclus avec la Confédération pour des activités non sensibles

La LSI aura une incidence sur l'ensemble des contrats conclus avec la Confédération. Les autorités fédérales sont en effet tenues de stipuler la garantie de la sécurité de l'information dans le cadre de la collaboration avec des tiers et de veiller à un contrôle adéquat du respect des directives (cf. art. 9 LSI et rapport explicatif sur la législation d'exécution relative à la loi sur la sécurité de l'information [ci-après: rapport explicatif], pp. 45-46, du Secrétariat général du DDPS, Digitalisation et cybersécurité). Quelles sont les obligations de la Confédération les plus pertinentes pour la sécurité et quel est leur potentiel impact sur les mandats fédéraux? Tour d'horizon:

- **Sécurité de l'information:** Les informations, en fonction de leur besoin de protection, doivent n'être accessibles qu'aux personnes autorisées (confidentialité), être disponibles en cas de besoin (disponibilité), ne pas être modifiables sans droit ou par mégarde (intégrité) et être traitées de manière à être traçables (traçabilité) (art. 6, al. 2, LSI). Les moyens informatiques doivent en outre être protégés contre les utilisations abusives et les perturbations (art. 6, al. 3, LSI). Les principes de la proportionnalité, de l'économicité et de la simplicité d'emploi doivent également prévaloir à cet égard (art. 6, al. 4, LSI). Par conséquent, il est fort probable que la Confédération obligera ses partenaires contractuels à garantir cette sécurité, par exemple en prévoyant dans les contrats des mesures concrètes qu'ils seront tenus de mettre en œuvre.

- **Procédure en cas de violation de la sécurité de l'information:** Les violations de la sécurité de l'information doivent être décelées rapidement, leurs causes clarifiées et leurs conséquences limitées au maximum (art. 10, al. 1, LSI). Partant, la Confédération attendra certainement de ses partenaires contractuels qu'ils signalent dans les plus brefs délais toute violation de la sécurité de l'information.

- **Contrôle:** La mise en œuvre des mesures prévues par la loi doit être contrôlée de manière adéquate (art. 9, al. 2, LSI). Là encore, il y a fort à parier qu'à l'avenir, la Confédération convienne contractuellement à chaque fois d'un droit d'audit.

La Conférence des achats de la Confédération (CA) a mis à la disposition des services d'achat de l'administration fédérale une clause contractuelle type de protection contre les cyberattaques, consultable sous ce lien. Le document donne un aperçu de la portée des nouvelles obligations sur les différents contrats. La CA précise néanmoins que la clause type convient en premier lieu aux achats comportant un risque élevé de cyberattaque. Ainsi des contrats présentant un risque moindre devraient-ils aussi rencontrer moins d'obstacles à ce niveau.

Nota bene: Même les contrats futurs conclus avec la Confédération pour des activités non sensibles contiendront certaines clauses supplémentaires, notamment l'obligation probable pour les partenaires contractuels de garantir la sécurité de l'information (confidentialité, disponibilité, intégrité et traçabilité) ou encore de déclarer des violations de cette sécurité. La Confédération devrait en outre se réserver un droit d'audit.

Contrats futurs conclus avec la Confédération pour des activités sensibles

La fiabilité des entreprises à qui des mandats sensibles de la Confédération sont confiés sera examinée dans le cadre d'une procédure dite de sécurité relative aux entreprises (rapport explicatif, p. 46).

Cette procédure se déroule de la manière suivante:

1. **Demande d'ouverture de la procédure:** Lorsque la Confédération envisage d'attribuer un mandat sensible, elle adresse au service spécialisé chargé de mener la procédure de sécurité relative aux entreprises (service spécialisé PSE) une demande d'ouverture de la procédure (art. 52, al. 1, LSI).

2. **Ouverture de la procédure ou renonciation:** Le service spécialisé PSE examine la demande et ouvre la procédure (art. 53, al. 1, LSI). Il peut aussi renoncer, en accord avec l'adjudicateur, à ouvrir une procédure lorsque d'autres mesures – qu'il aura lui-même recommandées – permettent de ramener le risque pour la sécurité à un niveau acceptable (art. 53, al. 2, LSI).

3. **Évaluation des entreprises:** Le service spécialisé PSE fixe, en accord avec l'adjudicateur, les exigences en matière de sécurité de l'information pour la procédure d'adjudication et la phase d'exécution du mandat (art. 54 LSI).

   L'adjudicateur indique au service spécialisé PSE quelles entreprises entrent en considération pour l'exécution du mandat sensible (art. 55, al. 1, LSI).

   Le service spécialisé PSE évalue si les entreprises concernées présentent les qualifications requises pour exécuter le mandat sensible ou s'il existe un risque pour la sécurité (art. 55, al. 2, LSI). Pour son évaluation, il peut collecter des données auprès de l'entreprise concernée, du Service de renseignement de la Confédération (SRC) et de toute source d'information publique (art. 56, al. 1, LSI). Il peut également demander à des services étrangers ou internationaux de lui transmettre des données; la demande est adressée par l'intermédiaire du SRC (art. 56, al. 2, LSI). L'existence d'un risque pour la sécurité est considérée comme avérée lorsque des indices concrets fondés sur les données collectées laissent supposer avec une probabilité élevée que l'entreprise exécutera le mandat sensible de manière inadéquate ou contraire aux prescriptions (art. 57, al. 1, LSI). Que le risque pour la sécurité soit imputable ou non à l'entreprise ne joue ici aucun rôle (cf. art. 57, al. 3, LSI).

   Le service spécialisé PSE communique son évaluation à l'adjudicateur et la notifie formellement à l'entreprise (art. 58, al. 1, LSI). Si une entreprise devait présenter un risque pour la sécurité, elle se verra exclue de la procédure d'adjudication (cf. art. 58, al. 2, LSI). Si toutes les entreprises qui entrent en considération posent un risque pour la sécurité, l'adjudicateur peut néanmoins confier le mandat à l'une d'entre elles. Le service spécialisé PSE classe la procédure et l'adjudicateur applique par analogie les mesures de sécurité prévues par la loi (art. 58, al. 3, LSI), à savoir plan de sécurité, avec obligation concomitante de l'appliquer constamment, contrôles de sécurité relatifs aux personnes, obligation d'information de tout changement ou incident dans le domaine de la sécurité, droit d'inspection et de consultation par le service spécialisé PSE et prise de mesures par celui-ci en cas de menace pour la sécurité de l'information (cf. art. 59, 60, 63 et 64 LSI).

4. **Plan de sécurité:** L'adjudicateur indique au service spécialisé PSE quelle est l'entreprise adjudicataire (art. 59, al. 1, LSI). L'entreprise établit un plan de sécurité en suivant les directives du service spécialisé PSE, lequel contrôle ledit plan (art. 59, al. 2 et 3, LSI). Les collaborateurs de l'entreprise qui sont appelés à exercer une activité sensible sont soumis à un contrôle de sécurité (art. 60, al. 1, LSI).

5. **Établissement de la déclaration de sécurité relative aux entreprises:** Le service spécialisé PSE rend formellement une déclaration de sécurité – valable cinq ans – lorsque l'entreprise apporte la preuve qu'elle a mis en œuvre le plan de sécurité (art. 61, al. 1 et 5, LSI). Si celle-ci ne met pas en œuvre le plan de sécurité, il lui refuse la déclaration de sécurité et rend formellement une décision en conséquence (art. 61, al. 2, LSI). Les décisions du service spécialisé PSE sont communiquées à l'adjudicateur, par lesquelles ce dernier se trouve lié (art. 61, al. 3 et 4, LSI).

6. **Exécution d'un mandat:** L'adjudicateur ne peut laisser une entreprise exécuter un mandat sensible qu'une fois que celle-ci a obtenu une déclaration de sécurité (art. 62 LSI). Les entreprises doivent constamment appliquer le plan de sécurité et immédiatement informer le service spécialisé PSE et l'adjudicateur de tout changement et de tout incident dans le domaine de la sécurité (art. 63 LSI). Le service spécialisé PSE dispose d'un droit d'inspection et de consultation, de même qu'il peut prendre les mesures de protection qui s'imposent lorsque des indices concrets plaident en faveur d'une menace pour la sécurité de l'information (art. 64 LSI).

7. **Autres mandats:** Les entreprises qui ont obtenu une déclaration de sécurité sont réputées qualifiées en cas d'adjudication d'autres mandats sensibles. Le service spécialisé PSE examine la nécessité d'adapter le plan de sécurité (art. 65 LSI).

Les entreprises peuvent demander un certificat international de sécurité (art. 66 LSI).

Nota bene: Les mandats requérant une procédure de sécurité relative aux entreprises représenteront selon toute vraisemblance une petite minorité. Les coûts d'une telle procédure s'élèvent généralement à moins de 0,5 % du volume du marché et sont directement ou indirectement répercutés sur l'adjudicateur (rapport explicatif, p. 46).

En résumé: La nécessité d'ouvrir une procédure de sécurité relative aux entreprises restera l'exception. Si une telle procédure implique certes un certain surcroît de travail, elle est aussi porteuse de valeur ajoutée: les entreprises souhaitant concourir à l'étranger à un mandat sensible du point de vue de la sécurité de l'information pourront demander un certificat international de sécurité. Par ailleurs pour ce qui relève de l'aspect financier, les coûts peuvent être répercutés directement ou indirectement sur l'adjudicateur.

Conclusion

La LSI jouera dès son entrée en vigueur un rôle dans les contrats futurs conclus avec la Confédération. Les contrats non sensibles prévoiront une garantie de la sécurité de l'information, assortie d'un contrôle approprié du respect des directives. Quant aux contrats sensibles, ils feront l'objet d'une procédure de sécurité relative aux entreprises.