Ordonnance de la ChF sur le vote électronique (OVotE)

du 13 décembre 2013 (Etat le 1er juillet 2018)

La Chancellerie fédérale suisse (ChF),

vu les art. 27*c*, al. 2, 27*e*, al. 1, 27*f*, al. 1, 27*g*, al. 2, 27*i*, al. 3, et 27*l*, al. 3, de l'ordonnance du 24 mai 1978 sur les droits politiques (ODP)[1],

arrête:

Art. 1 Objet et définitions

[1] La présente ordonnance fixe les conditions régissant l'octroi de l'agrément pour le vote électronique.

[2] Les définitions applicables sont celles qui figurent au ch. 1.3 de l'annexe.

Art. 2 Conditions générales régissant l'octroi de l'agrément pour chaque scrutin où l'on aura recours au vote électronique

L'agrément est accordé pour chaque scrutin où l'on aura recours au vote électronique si les conditions suivantes sont remplies:

a. le système de vote électronique (système) est conçu et exploité de telle sorte qu'il garantit la sûreté et la fiabilité du vote (annexe, ch. 2 et 3);

b. le système est facile à utiliser pour les électeurs. Les besoins particuliers de tous les électeurs, si possible, sont pris en compte;

c. le système et les opérations d'exploitation sont décrits dans une documentation de manière à ce qu'il soit possible de comprendre en détail toutes les opérations techniques et organisationnelles qui sont pertinentes du point de vue de la sécurité.

Art. 3 Appréciation des risques

[1] Le canton doit effectuer une appréciation des risques visant à établir par écrit, de manière détaillée et compréhensible, que tous les risques pour la sécurité se situent à un niveau suffisamment bas. L'appréciation doit être effectuée en fonction des objectifs de sécurité suivants:

a. garantir l'exactitude des résultats;

b. protéger le secret du vote et faire en sorte qu'il soit impossible d'établir des résultats partiels de manière anticipée;

RO **2013** 5371

1 RS **161.11**

c. assurer la disponibilité des fonctionnalités;

d. protéger les informations personnelles concernant les électeurs;

e. protéger contre les manipulations les informations destinées aux électeurs;

f. faire en sorte qu'il soit impossible d'établir des preuves relatives au comportement de vote.

2 Chaque risque doit être identifié et décrit clairement en fonction des objectifs de sécurité, des éventuelles données liées à ces objectifs, des menaces, des vulnérabilités et de la documentation relative au système et à son exploitation. Sur cette base, le canton indique les raisons pour lesquelles il évalue les risques comme étant suffisamment faibles.

3 La réduction des risques ne doit pas reposer sur le fait que l'on garde secrètes des informations sur le système et son exploitation qui sont pertinentes du point de vue de la sécurité.

Art. 4 Exigences à remplir pour que plus de 30 % de l'électorat cantonal puisse voter par voie électronique

1 Pour qu'un système permettant à plus de 30 % de l'électorat cantonal de voter par voie électronique soit agréé, les votants doivent avoir la possibilité de déterminer si le suffrage qu'ils ont exprimé a été manipulé ou intercepté sur la plate-forme utilisateur ou pendant la transmission (vérifiabilité individuelle; annexe, ch. 4.1 et 4.2).

2 Pour qu'il y ait vérification individuelle, le votant doit recevoir la preuve que la partie serveur du système a enregistré le suffrage tel que le votant l'a exprimé sur la plate-forme utilisateur, conformément à la procédure prévue par le système. La preuve doit attester, pour chaque suffrage partiel, que l'enregistrement a été effectué correctement.

3 Si les données d'authentification client sont envoyées par voie électronique, les électeurs qui n'ont pas voté par voie électronique doivent pouvoir demander, après la fermeture du canal permettant de voter par voie électronique, durant les délais de recours légaux, la preuve que le système n'a enregistré aucun suffrage exprimé moyennant l'utilisation de leurs données d'authentification client.

4 Le caractère concluant d'une preuve ne doit pas dépendre de la fiabilité de la plate-forme utilisateur ou du canal de transmission.

5 Il peut se fonder sur les éléments suivants:

a. la fiabilité de la partie serveur du système;

b. la fiabilité des dispositifs techniques particuliers des votants; ces dispositifs doivent répondre à des exigences de sécurité particulièrement élevées;

c. la confidentialité des données envoyées sur support papier; la confidentialité de ces données doit être garantie par des mesures particulières en dehors du cadre de l'infrastructure.

Art. 5 Exigences à remplir pour que plus de 50 % de l'électorat cantonal puisse voter par voie électronique

[1] Pour qu'un système permettant à plus de 50 % de l'électorat cantonal de voter par voie électronique soit agréé, les votants ou les vérificateurs doivent avoir la possibilité, dans le respect du secret du vote, d'identifier toute manipulation aboutissant à une falsification des résultats (vérifiabilité complète; annexe, ch. 4.3 et 4.4).

[2] Il y a vérifiabilité complète quand les exigences étendues applicables à la vérifiabilité individuelle (al. 3) et les exigences applicables à la vérifiabilité universelle (al. 4 à 6) sont remplies.

[3] Pour qu'il y ait vérification individuelle, les exigences suivantes doivent être remplies en plus des exigences fixées à l'art. 4:

a. la preuve doit en outre permettre aux votants de constater que les données pertinentes pour la vérification universelle sont parvenues dans la partie fiable du système (al. 6);

b. après la fermeture du canal permettant de voter par voie électronique, le votant doit pouvoir demander la preuve que la partie fiable du système n'a pas déjà enregistré un suffrage exprimé moyennant l'utilisation de ses données d'authentification client;

c. le caractère concluant d'une preuve ne doit pas dépendre de la fiabilité de l'ensemble de la partie serveur du système. Il peut toutefois se fonder sur la fiabilité de la partie fiable du système.

[4] Pour qu'il y ait vérification universelle, les vérificateurs doivent recevoir la preuve attestant que les résultats ont été établis correctement. Ils doivent évaluer cette preuve au cours d'un processus observable. Pour ce faire, ils doivent utiliser des dispositifs techniques indépendants et séparés du reste du système. La preuve doit attester que l'établissement des résultats a pris en compte:

a. tous les suffrages qui ont été exprimés conformément à la procédure prévue par le système et qui ont été enregistrés par la partie fiable du système;

b. uniquement les suffrages qui ont été exprimés conformément à la procédure prévue par le système;

c. tous les suffrages partiels conformément à la preuve générée dans le cadre de la vérification individuelle.

[5] Le caractère concluant de la preuve ne peut dépendre que de la fiabilité de la partie fiable du système et du dispositif technique utilisé pour le contrôle. Par ailleurs, la garantie du secret du vote et le fait qu'il ne doit pas être possible d'établir des résultats partiels de manière anticipée au sein de l'infrastructure ne peuvent dépendre que de la fiabilité de la partie fiable du système.

[6] La partie fiable du système comprend soit un groupe soit quelques groupes de composants indépendants sécurisés par des mesures particulières (composants de contrôle). L'utilisation de ces composants doit permettre d'identifier n'importe quel abus même si, dans chaque groupe, il n'y a qu'un composant de contrôle qui fonctionne correctement et qui, en particulier, n'est pas manipulé sans qu'on s'en aperçoive. Pour que la fiabilité de la partie fiable du système soit garantie, il faut que les

composants de contrôle diffèrent les uns des autres de par leur conception, mais aussi que leur exploitation et leur surveillance soient indépendantes.

Art. 6 Mesures supplémentaires visant à réduire les risques

Si les risques ne sont pas suffisamment faibles malgré les mesures prises, il convient de prendre des mesures supplémentaires afin de réduire les risques. Cette règle s'applique notamment dans les cas où toutes les exigences fixées aux ch. 2 à 4 de l'annexe ont déjà été mises en œuvre.

Art. 7 Exigences applicables au contrôle

1 Les cantons veillent à ce que des services indépendants contrôlent le respect des conditions fixées. Le contrôle a lieu notamment si le système ou son exploitation a subi une modification qui pourrait remettre en question le respect des conditions ayant abouti à l'octroi de l'agrément.

2 Dans les cas où il s'agit de permettre à plus de 30 % de l'électoral cantonal de participer à un essai (art. 4 et 5), le système et son exploitation doivent être soumis à un contrôle particulièrement approfondi sur la base des critères suivants:

a. le protocole cryptographique (annexe, ch. 5.1);

b. les fonctionnalités (annexe, ch. 5.2);

c. la sécurité de l'infrastructure et de l'exploitation (annexe, ch. 5.3);

d. la protection contre les tentatives d'intrusion dans l'infrastructure (annexe, ch. 5.5);

e. les exigences applicables aux imprimeries (annexe, ch. 5.6);

f.[2] en cas d'utilisation d'un système ayant les propriétés de la vérifiabilité complète définie à l'art. 5: les composants de contrôle (annexe, ch. 5.4).

3 Dans les cas où il s'agit de permettre à 30 % au maximum de l'électorat cantonal de participer à un essai et où le système a les propriétés de la vérifiabilité complète définie à l'art. 5, le système et son exploitation doivent être soumis à un contrôle particulièrement approfondi sur la base des critères suivants:

a. le protocole cryptographique (annexe, ch. 5.1);

b. les fonctionnalités (annexe, ch. 5.2); le contrôle ne doit pas obligatoirement porter sur les logiciels de portails de cyberadministration qui sont reliés à un système;

c. la sécurité de l'infrastructure et de l'exploitation (annexe, ch. 5.3); à cet égard, le contrôle peut porter uniquement sur l'infrastructure qui enregistre le suffrage et qui établit à l'intention du votant la preuve visée à l'art. 4, al. 2;

2 Nouvelle teneur selon le ch. I de l'O de la ChF du 30 mai 2018, en vigueur depuis le 1er juil. 2018 (RO **2018** 2279).

d. la protection contre les tentatives d'intrusion dans l'infrastructure (annexe, ch. 5.5);

e. les composants de contrôle (annexe, ch. 5.4).[3]

Art. 7*a*[4] Publication du code source

[1] Le code source du logiciel du système doit être publié.

[2] La publication a lieu, quand le système a les propriétés de la vérifiabilité complète définie à l'art. 5 et:

a. après le contrôle visé à l'art. 7, al. 2, dans les cas où il s'agit de permettre à plus de 30 % de l'électorat cantonal de participer à un essai;

b. après le contrôle visé à l'art. 7, al. 3, dans les cas où il s'agit de permettre à 30 % au maximum de l'électorat cantonal de participer à un essai.

[3] Ne doit pas obligatoirement être publié le code source:

a. de composants tiers tels que des systèmes d'exploitation, des bases de données, des serveurs web et des serveurs d'application, des systèmes de gestion des droits, des pare-feu et des routeurs, pour autant que ces composants soient utilisés à grande échelle et qu'ils soient mis à jour en permanence;

b. de portails de cyberadministration qui sont reliés à un système.

Art. 7*b*[5] Modalités de la publication du code source

[1] Le code source doit être préparé et documenté conformément aux bonnes pratiques.

[2] L'accès au code source par Internet doit être simple et gratuit.

[3] Une documentation portant sur le système et son exploitation doit indiquer en quoi les différentes parties du code source sont pertinentes pour la sécurité du vote électronique. Elle doit être publiée avec le code source.

[4] Toute personne a le droit non seulement d'examiner, de modifier, de compiler et d'exécuter le code source à des fins idéales, mais aussi de rédiger des études en la matière et de les publier. Le propriétaire du code source peut autoriser l'utilisation de ce dernier à d'autres fins.

Art. 8 Pièces justificatives à l'appui des demandes

[1] Doivent être joints aux demandes présentées en vertu des art. 27*c* et 27*e*, al. 1, ODP:

3 Introduit par le ch. I de l'O de la ChF du 30 mai 2018, en vigueur depuis le 1er juil. 2018 (RO **2018** 2279).
4 Introduit par le ch. I de l'O de la ChF du 30 mai 2018, en vigueur depuis le 1er juil. 2018 (RO **2018** 2279).
5 Introduit par le ch. I de l'O de la ChF du 30 mai 2018, en vigueur depuis le 1er juil. 2018 (RO **2018** 2279).

a. les pièces justificatives ou les certificats attestant que le système et son exploitation ont été contrôlés sur la base des exigences fixées et qu'ils remplissent efficacement toutes les exigences (annexe, ch. 6.1 à 6.3);

b. les pièces justificatives attestant que l'appréciation des risques a été menée avant un scrutin; elles doivent indiquer les raisons pour lesquelles les risques ont été évalués comme étant suffisamment faibles (annexe, ch. 6.4).

2 Il est possible de faire valoir des pièces justificatives que la Chancellerie fédérale a déjà reçues et qui sont encore valables.

Art. 9 Autres dispositions

1 Les exigences techniques et administratives détaillées qu'il faut remplir pour obtenir l'agrément pour le vote électronique figurent dans l'annexe.

2 D'ici au 30 juin 2015, un canton peut être dispensé, à titre exceptionnel, de remplir certaines exigences figurant aux ch. 2 et 3 de l'annexe:

a. s'il n'est pas prévu que plus de 30 % de l'électorat cantonal puisse voter par voie électronique;

b. si les exigences qui ne devront pas être remplies sont indiquées dans la demande; et

c. si le canton décrit les mesures de remplacement qui seront prises et indique, à propos de l'appréciation des risques, les raisons pour lesquelles il évalue les risques comme étant suffisamment faibles.

Art. 10 Entrée en vigueur

La présente ordonnance entre en vigueur le 15 janvier 2014.

Annexe
(art. 9, al. 1)

Exigences techniques et administratives applicables au vote électronique[6]

6 Le texte de l'annexe de la présente ordonnance n'est pas publié au RO (RO **2018** 2279). Il peut être consulté gratuitement à l'adresse www.chf.admin.ch > Droits politiques > Vote électronique > Exigences du droit fédéral, ou obtenu gratuitement à la Chancellerie fédérale, Section des droits politiques, Palais fédéral Ouest, 3003 Berne.