Ordonnance sur les systèmes de gestion des données d'identification et les services d'annuaires de la Confédération (OIAM)

du 19 octobre 2016 (État le 1er janvier 2024)

Le Conseil fédéral suisse,

vu les art. 26 et 84, al. 1, de la loi du 18 décembre 2020 sur la sécurité de l'information (LSI)[1],
vu la loi fédérale du 17 mars 2023 sur l'utilisation de moyens électroniques pour l'exécution des tâches des autorités (LMETA)[2],
vu la loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA)[3],
vu l'art. 27, al. 5 et 6, de la loi du 24 mars 2000 sur le personnel de la Confédération[4],
vu l'art. 186 de la loi fédérale du 3 octobre 2008 sur les systèmes d'information de l'armée et du DDPS[5],[6]

arrête:

Section 1 Dispositions générales

Art. 1 Objet

La présente ordonnance régit les compétences, le traitement et la publication de données personnelles ainsi que les exigences concernant la sécurité de l'information pour les systèmes de gestion des données d'identification (systèmes IAM[7]), les services d'annuaires et la base centralisée des identités de la Confédération.

RO **2016** 3623

1 RS **128**
2 RS **172.019**
3 RS **172.010**
4 RS **172.220.1**
5 RS **510.91**
6 Nouvelle teneur selon le ch. I de l'O du 8 nov. 2023, en vigueur depuis le 1er janv. 2024 (RO **2023** 738).
7 IAM = *Identity and Access Management* (gestion des identités et des accès)

Art. 2[8] Champ d'application

[1] Les art. 24 et 25 LSI ainsi que la présente ordonnance s'appliquent:

a. aux unités de l'administration fédérale centrale au sens de l'art. 7 de l'ordonnance du 25 novembre 1998 sur l'organisation du gouvernement et de l'administration (OLOGA)[9];

b. à l'armée.

[2] L'application de la présente ordonnance aux unités de l'administration fédérale décentralisée visées à l'art. 2, al. 3, LOGA et aux organisations visées à l'art. 2, al. 4, LOGA est régie par l'art. 2, al. 2, let. b, et al. 3, de l'ordonnance du 8 novembre 2023 sur la sécurité de l'information (OSI)[10].

Section 2 But et fonction principale des systèmes

Art. 3 Systèmes IAM

[1] Un système IAM sert à gérer conjointement des données sur l'identité et les autorisations de personnes, de machines et de systèmes pour les mettre, sur demande, à la disposition des systèmes en aval et d'autres systèmes IAM.

[2] Les systèmes en aval sont des applications techniques ou des dispositifs permettant d'accéder à des informations, des moyens informatiques, des locaux et d'autres infrastructures.

[3] Placé en amont, le système IAM vérifie l'identité et certains critères d'accès des personnes, des machines et des systèmes qui souhaitent accéder à un système en aval; il transmet à ce dernier les résultats de la vérification afin que celui-ci puisse délivrer les autorisations.

Art. 4 Services d'annuaires

Un service d'annuaires sert à gérer des informations sur les utilisateurs des infrastructures de la Confédération pour pouvoir identifier les personnes et administrer les appareils, les raccordements, les coordonnées et les éléments similaires qui leur ont été attribués.

8 Nouvelle teneur selon le ch. I de l'O du 8 nov. 2023, en vigueur depuis le 1er janv. 2024 (RO **2023** 738).
9 RS **172.010.1**
10 RS **128.1**

Section 3 Organes responsables

Art. 5[11] Systèmes IAM

[1] Les organes de la Confédération suivants sont responsables des systèmes IAM de l'administration fédérale centrale ci-après:

a. le secteur Transformation numérique et gouvernance de l'informatique de la Chancellerie fédérale (secteur TNI de la ChF), pour:
   1. tous les systèmes IAM proposés comme services standard et tous les systèmes IAM relevant explicitement du secteur TNI de la ChF, y compris leur mise à la disposition des cantons et des communes ainsi que d'organisations et de personnes de droit public ou de droit privé conformément à l'art. 11, al. 3, LMETA,
   2. le système IAM des processus de soutien en matière de finances, d'acquisition, de gestion immobilière et de logistique, y compris le raccordement aux services d'informatique en nuage *(cloud)*;

b. la Direction des ressources du Département fédéral des affaires étrangères (DFAE), pour le système IAM exploité par l'unité Informatique DFAE;

c. le Secrétariat général du Département fédéral de la défense, de la protection de la population et des sports, pour les systèmes IAM exploités par le Groupement Défense (Groupement D);

d. l'Administration fédérale des finances, pour le système IAM de gestion des systèmes d'assurances sociales du premier pilier et de soutien à leurs processus exploité par la Centrale de compensation;

e. le Secrétariat général du Département fédéral de l'économie, de la formation et de la recherche (DEFR), pour le système IAM exploité par le Centre de services informatiques du DEFR (ISCeco);

f. l'Office fédéral des routes, pour son système IAM de gestion des équipements d'exploitation et de sécurité des routes nationales.

[2] Ils veillent à ce que le traitement des données personnelles figurant dans les systèmes IAM dont ils sont responsables soit contrôlé au moins tous les quatre ans par un organe externe.

[3] Les organes suivants sont responsables des systèmes IAM ci-après:

a. le Groupement D, pour les systèmes IAM de l'armée;

b. les unités administratives concernées, pour les systèmes IAM des unités de l'administration fédérale décentralisée;

c. les organisations concernées, pour les systèmes IAM des organisations visées à l'art. 2, al. 4, LOGA.

11 Nouvelle teneur selon le ch. I de l'O du 8 nov. 2023, en vigueur depuis le 1er janv. 2024 (RO **2023** 738).

4 Les autorités visées à l'art. 2, al. 1, let. a et c à e, LSI auxquelles la présente ordonnance s'applique en vertu de l'art. 84, al. 3, LSI déterminent quels organes de la Confédération sont responsables dans leur domaine.

5 La responsabilité du système en aval, et en particulier de l'accès à celui-ci, continue d'incomber au service technique responsable du système.

Art. 6 Services d'annuaires

Les organes de la Confédération responsables des services d'annuaires extérieurs aux systèmes IAM sont:

a. pour les services standard, le secteur TNI de la ChF[12];

b. pour les autres annuaires, les fournisseurs de prestations informatiques qui exploitent ces systèmes, à savoir:

1. l'unité Informatique DFAE de la Direction des ressources du DFAE,
2. le Centre de services informatiques (CSI) du Département fédéral de justice et police (DFJP),
3.[13] le Groupement D,
4. l'Office fédéral de l'informatique et de la télécommunication (OFIT),
5. l'ISCeco.

Art. 7 Exercice des droits

Les personnes concernées font valoir leurs droits relatifs aux systèmes IAM et aux services d'annuaires auprès des organes suivants:

a. droit d'accès: auprès des organes responsables;

b.[14] droit de rectification et de suppression:

1. auprès du service du personnel de leur unité administrative ou de leur organisation ou auprès du service chargé de gérer leurs données,
2. dans le cas de l'art. 9, let. b: auprès des organes responsables.

12 Nouvelle expression selon l'annexe ch. 8 de l'O du 25 nov. 2020 sur la transformation numérique et l'informatique, en vigueur depuis le 1er janv. 2021 (RO **2020** 5871). Il a été tenu compte de cette mod. dans tout le texte.

13 Nouvelle teneur selon le ch. I de l'O du 8 nov. 2023, en vigueur depuis le 1er janv. 2024 (RO **2023** 738).

14 Nouvelle teneur selon le ch. I de l'O du 8 nov. 2023, en vigueur depuis le 1er janv. 2024 (RO **2023** 738).

Section 4
Données traitées, collecte des données et délai de conservation

Art. 8 Personnes gérées dans les systèmes IAM et les services d'annuaires

1 Les données concernant les personnes suivantes peuvent être traitées dans les systèmes IAM et les services d'annuaires:

a. membres de l'administration fédérale centrale au sens de l'art. 7 OLOGA[15];

b. membres de l'administration fédérale décentralisée au sens de l'art. 7*a* OLOGA;

c. membres de l'Assemblée fédérale et des Services du Parlement au sens du titre 4, chap. 7, de la loi du 13 décembre 2002 sur le Parlement[16];

d. personnes élues par l'Assemblée fédérale au sens de l'art. 168 de la Constitution[17];

e. membres du Tribunal fédéral, du Tribunal administratif fédéral, du Tribunal pénal fédéral et du Tribunal fédéral des brevets, sauf disposition contraire de la législation;

f. membres du Ministère public de la Confédération au sens des art. 7 à 22 de la loi du 19 mars 2010 sur l'organisation des autorités pénales (LOAP)[18];

g. membres du Secrétariat de l'Autorité de surveillance du Ministère public de la Confédération au sens de l'art. 27, al. 2, LOAP;

h.[19] les militaires et les membres de la protection civile.

2 Peuvent en outre être traitées les données concernant les membres des entreprises suivantes, pour autant que ceux-ci soient régulièrement en contact avec des organes au sens de l'al. 1:

a. Chemins de fer fédéraux;

b. La Poste Suisse;

c. RUAG;

d. Caisse nationale suisse d'assurance en cas d'accidents.

3 Par ailleurs, les données concernant les personnes suivantes peuvent être traitées dans les systèmes IAM et les services d'annuaires:

a. personnes externes exerçant une activité pour des organes au sens des al. 1 ou 2;

15 RS **172.010.1**
16 RS **171.10**
17 RS **101**
18 RS **173.71**
19 Introduite par le ch. I de l'O du 14 nov. 2018, en vigueur depuis le 1er janv. 2019 (RO **2018** 4739).

b. personnes externes qui, pour d'autres motifs, ont accès à des informations, des moyens informatiques, des locaux et d'autres infrastructures de l'administration fédérale.

Art. 9 Personnes gérées dans les systèmes IAM

Les données concernant les personnes suivantes peuvent être traitées dans les systèmes IAM en plus des données au sens de l'art. 8:

a. membres d'autorités cantonales ou communales, si ces personnes utilisent des systèmes d'information mis à disposition par la Confédération;

b.[20] particuliers et représentants d'organisations qui accèdent à des systèmes d'information mis à disposition par la Confédération ou, pour l'exécution du droit cantonal, par les cantons et les communes ainsi que par des organisations et personnes de droit public ou de droit privé, tels que les applications de cyberadministration.

Art. 10 Personnes gérées dans les services d'annuaires

Les données des membres d'autorités cantonales ou communales et d'autres entreprises liées à la Confédération que celles mentionnées à l'art. 8, al. 2, qui utilisent un certificat numérique de la Confédération peuvent être traitées dans les services d'annuaires en plus des données au sens de l'art. 8.

Art. 11 Catégories de données personnelles

[1] Les données personnelles énumérées dans l'annexe peuvent être traitées dans les systèmes IAM, les services d'annuaires et la base centralisée des identités visée à l'art. 13.

[2] Aucun profilage au sens de l'art. 5, let. f et g, de la loi fédérale du 25 septembre 2020 sur la protection des données[21] ne peut être effectué dans ces systèmes.[22]

[3] En l'absence d'une base légale particulière en la matière, aucune donnée sensible ne peut être traitée dans ces systèmes. Fait exception le traitement de données biométriques par les systèmes IAM à des fins d'identification des personnes visées aux art. 8 et 9, let. a, en fonction du risque (art. 20, al. 2, LSI).[23]

[4] Les données assorties d'un astérisque dans l'annexe concernant des personnes mentionnées à l'art. 8 peuvent être publiées dans un service d'annuaires qui est accessible à toutes les personnes y figurant.

20 Nouvelle teneur selon le ch. I de l'O du 8 nov. 2023, en vigueur depuis le 1er janv. 2024 (RO **2023** 738).
21 RS **235.1**
22 Nouvelle teneur selon le ch. I de l'O du 8 nov. 2023, en vigueur depuis le 1er janv. 2024 (RO **2023** 738).
23 Nouvelle teneur selon le ch. I de l'O du 8 nov. 2023, en vigueur depuis le 1er janv. 2024 (RO **2023** 738).

Art. 12 Obtention de données personnelles

1 Les systèmes IAM et les services d'annuaires peuvent obtenir automatiquement les données relatives aux personnes gérées dans le système d'information pour la gestion des données du personnel (IGDP) au sens de l'art. 34 de l'ordonnance du 22 novembre 2017 concernant la protection des données personnelles du personnel de la Confédération[24].[25]

2 Ils peuvent obtenir automatiquement auprès des organes concernés au sens de l'art. 8 les données des personnes ne figurant pas dans IGDP[26], dans la mesure où ces groupes de personnes ont besoin d'accéder à des systèmes d'information ou à d'autres ressources de la Confédération.

3 Ils peuvent obtenir automatiquement auprès des systèmes d'information concernés les données des personnes externes qui accèdent régulièrement aux ressources de la Confédération.

4 Ils peuvent obtenir automatiquement les données de personnes externes auprès des systèmes IAM externes raccordés aux systèmes IAM de la Confédération conformément aux art. 21 à 24.[27]

Art. 13 Base centralisée des identités pour la distribution des données

1 L'OFIT exploite une base centralisée des identités pour distribuer les données des utilisateurs aux différents systèmes IAM et services d'annuaires. Toutes les données personnelles mentionnées dans l'annexe peuvent être traitées dans cette base. Le secteur TNI de la ChF est l'organe responsable au sein de la Confédération.

2 IGDP transmet régulièrement à la base centralisée des identités les données mentionnées dans l'annexe, pour autant que ces dernières soient disponibles. Toute obtention automatique de données personnelles depuis IGDP est réalisée grâce à ce distributeur, à l'exception de l'obtention directe des données de base du personnel dans l'environnement SAP pour les systèmes SAP autorisés.

3 Les données personnelles au sens de l'art. 8, al. 1, let. c, et 3, sont transmises aux Services du Parlement pour y être reprises et harmonisées.

4 Les données peuvent être transmises de manière automatisée à d'autres systèmes d'information internes à l'administration fédérale, dans lesquels elles sont reprises et harmonisées, à condition que le système concerné:

24 RS **172.220.111.4**

25 Nouvelle teneur selon l'annexe 8 ch. II 1 de l'O du 22 nov. 2017 concernant la protection des données personnelles du personnel de la Confédération, en vigueur depuis le 1er janv. 2018 (RO **2017** 7271).

26 Nouvelle expression selon l'annexe 8 ch. II 1 de l'O du 22 nov. 2017 concernant la protection des données personnelles du personnel de la Confédération, en vigueur depuis le 1er janv. 2018 (RO **2017** 7271). Il a été tenu compte de cette mod. dans tout le texte.

27 Introduit par le ch. I de l'O du 8 nov. 2023, en vigueur depuis le 1er janv. 2024 (RO **2023** 738).

a.[28] dispose d'une base légale prévoyant le traitement des données à transmettre et d'un règlement de traitement au sens de l'art. 6 de l'ordonnance du 31 août 2022 sur la protection des données (OPDo)[29], et

b. ait été annoncé au Préposé fédéral à la protection des données et à la transparence conformément à l'art. 12, al. 4, de loi fédérale du 25 septembre 2020 sur la protection des données[30].[31]

4bis Le numéro AVS n'est transmis que si son utilisation est annoncée à la Centrale de compensation conformément à l'art. 134ter du règlement du 31 octobre 1947 sur l'assurance-vieillesse et survivants[32].[33]

5 Les données nécessaires à la publication de l'Annuaire fédéral au sens de l'art. 5 de l'ordonnance du 29 octobre 2008 sur l'organisation de la Chancellerie fédérale[34] sont transmises régulièrement à cette dernière.

Art. 14 Délai de conservation des données personnelles

1 Lorsqu'une personne n'est plus soumise à la présente ordonnance, ses données figurant dans les systèmes IAM et les services d'annuaires sont détruites au plus tard après deux ans.

2 Les dispositions de l'art. 20, al. 2, LSI relatives à la destruction des données biométriques sont réservées.[35]

Section 5 Communication de données inhérente aux systèmes IAM

Art. 15 Communication de données en cas de raccordement d'un système d'information à un système IAM

1 Si un système d'information auparavant autonome est raccordé à un système IAM et si la vérification de l'identité et de certains critères d'accès des personnes est confiée à ce dernier, les données personnelles correspondantes peuvent être importées dans le système IAM.

2 Il faut gérer dans le système IAM, pour chaque système d'information en aval, une liste des données personnelles pouvant être communiquées à ce dernier en vertu de la présente ordonnance et des bases légales du système en aval.

28 Nouvelle teneur selon le ch. I de l'O du 8 nov. 2023, en vigueur depuis le 1er janv. 2024 (RO **2023** 738).
29 RS **235.11**
30 RS **235.1**
31 Nouvelle teneur selon l'annexe 2 ch. II 18 de l'O du 31 août 2022 sur la protection des données, en vigueur depuis le 1er sept. 2023 (RO **2022** 568).
32 RS **831.101**
33 Introduit par le ch. I de l'O du 4 mai 2022, en vigueur depuis le 1er juin 2022 (RO **2022** 282).
34 RS **172.210.10**
35 Introduit par le ch. I de l'O du 14 nov. 2018 (RO **2018** 4739). Nouvelle teneur selon le ch. I de l'O du 8 nov. 2023, en vigueur depuis le 1er janv. 2024 (RO **2023** 738).

Art. 16 Communication de données en cas d'accès individuel

Le système IAM authentifie les personnes, les machines ou les systèmes qui demandent l'accès à un système d'information en aval; il vérifie les données d'identification requises ainsi que d'autres caractéristiques et attestations nécessaires et transmet au système en aval le résultat de la vérification, avec les données d'identification, les caractéristiques et les attestations déterminées.

Art. 17 Communication de données personnelles à un exploitant externe

1 Si un système d'information de la Confédération est géré par un exploitant externe sur mandat de celle-ci ou si les personnes visées à l'art. 8, al. 1 ou 3, let. a, doivent accéder à des systèmes d'information tiers, les données personnelles requises à cet effet peuvent être communiquées de manière automatisée à l'exploitant externe à partir des systèmes d'information concernant le personnel, de la base centralisée des identités ou des systèmes IAM.

2 Pour ce faire, le service qui est responsable du système d'information confié à un exploitant externe ou qui a besoin d'accéder à un système d'information tiers établit une demande écrite précisant les personnes concernées et la transmet, par l'intermédiaire du conseiller à la protection des données compétent, à l'organe de la Confédération responsable du système d'information fournissant les données requises.

3 Dans la demande, le service responsable au sens de l'al. 2 s'engage par écrit à respecter la législation fédérale sur la protection des données, à utiliser ces dernières exclusivement dans le but prévu et à les protéger conformément à l'état de la technique. Un droit d'inspection doit être accordé à l'organe de la Confédération responsable du système d'information fournissant les données requises.

4 Les personnes concernées doivent être informées au préalable.

Section 6
Mesures de protection des systèmes IAM et des services d'annuaires[36]

Art. 18 Exigences concernant la sécurité de l'information

1 Les exploitants internes et externes d'éléments d'un système IAM ou d'un service d'annuaires doivent avoir des instructions écrites sur la sécurité de l'information et la gestion des risques. En particulier, chaque organe responsable d'un système ou d'un service d'annuaires en vertu de la présente ordonnance établit un règlement de traitement conformément à l'art. 6 OPDo[37,38]

36 Nouvelle teneur selon le ch. I de l'O du 8 nov. 2023, en vigueur depuis le 1er janv. 2024 (RO **2023** 738).
37 RS **235.11**
38 Nouvelle teneur selon le ch. I de l'O du 8 nov. 2023, en vigueur depuis le 1er janv. 2024 (RO **2023** 738).

2 Les systèmes IAM et les services d'annuaires qui ne sont pas gérés par des organes visés à l'art. 2 ou sur mandat de ces derniers peuvent être raccordés à des systèmes IAM ou des services d'annuaires internes à l'administration fédérale uniquement s'ils respectent les exigences minimales concernant la sécurité de l'information.[39]

3 L'organe compétent ou le secteur TNI de la ChF peut demander le respect d'exigences plus élevées et des certifications précises afin d'accorder l'accès à certains systèmes d'information.

4 Le secteur TNI de la ChF fixe dans des directives les exigences en matière de sécurité et les procédures à respecter.

Art. 19 Traitement des données pour émettre des moyens d'identification électroniques

1 Pour vérifier l'identité de la personne demandeuse, l'émetteur d'un moyen d'identification peut exiger la présentation d'un passeport, d'une carte d'identité suisse ou d'une pièce d'identité reconnue pour entrer en Suisse.

2 Il peut enregistrer une photo ou la signature de la personne ou utiliser des photos ou signatures figurant déjà dans le système pour les comparer avec la pièce d'identité.

3 Les données utilisées pour l'identification sont enregistrées avec celles du moyen d'identification. Si les exigences en matière de sécurité propres au moyen d'identification l'exigent, une copie des pièces d'identité ayant servi à l'identification peut également être sauvegardée.

Section 7 Interconnexion de systèmes IAM

Art. 20[40] Système global IAM

Les systèmes IAM de la Confédération peuvent être reliés entre eux et aux systèmes IAM externes visés à l'art. 21 pour former un système global.

Art. 21 Conditions pour le raccordement de systèmes IAM externes

Les systèmes IAM externes ci-après peuvent être raccordés aux systèmes IAM de la Confédération afin que les personnes gérées dans ces systèmes externes puissent accéder aux ressources de celle-ci, pour autant que les conditions et les procédures énoncées aux art. 22 et 23 soient respectées et que leurs exploitants s'engagent à respecter la présente ordonnance et les prescriptions qui en découlent ou, dans le cas des

39 Nouvelle teneur selon le ch. I de l'O du 8 nov. 2023, en vigueur depuis le 1er janv. 2024 (RO **2023** 738).

40 Nouvelle teneur selon le ch. I de l'O du 8 nov. 2023, en vigueur depuis le 1er janv. 2024 (RO **2023** 738).

cantons, que ces derniers garantissent une sécurité de l'information au moins équivalente:[41]

a.[42] systèmes IAM comprenant des collaborateurs cantonaux et communaux au sens de l'art. 9, let. a, et systèmes IAM de la Principauté de Liechtenstein;

b. systèmes IAM reconnus par le secteur TNI de la ChF qui sont destinés à la fédération d'identités dans le cadre de la cyberadministration;

c. fédérations d'identités ou systèmes IAM étrangers dont le raccordement mutuel est prévu dans un traité international, ou

d. registres des attributs qui mettent à disposition des données relatives à des fonctions professionnelles selon l'annexe, let. b.

Art. 22 Demande de raccordement de systèmes IAM externes

[1] Le service compétent adresse à l'organe de la Confédération responsable en vertu de l'art. 5 une demande de raccordement d'un système IAM externe à un système IAM de la Confédération.

[2] La demande comprend notamment:

a. le but du raccordement;

b. les bases légales et les autres réglementations relatives au système à raccorder;

c. une description technique du système à raccorder;

d. les preuves du respect des exigences concernant la sécurité de l'information au sens de l'art. 18, al. 2 ou 3;

e. l'avis favorable du département compétent;

f. l'avis favorable d'au moins un service responsable d'un système en aval auquel le système IAM à raccorder permettra d'accéder.

Art. 23 Décision concernant la demande de raccordement de systèmes IAM externes

[1] L'organe de la Confédération responsable d'un système IAM de la Confédération est chargé de statuer sur la demande.

[2] Si le système IAM externe est relié aussi à d'autres systèmes IAM de la Confédération par le système auquel il est directement raccordé, l'approbation de la demande requiert l'accord de le secteur TNI de la ChF.

[3] L'organe de la Confédération responsable conclut la convention avec le service demandeur, informe le secteur TNI de la ChF et mandate le fournisseur de prestations concerné en vue du raccordement.

41 Nouvelle teneur selon le ch. I de l'O du 8 nov. 2023, en vigueur depuis le 1er janv. 2024 (RO **2023** 738).

42 Nouvelle teneur selon le ch. I de l'O du 8 nov. 2023, en vigueur depuis le 1er janv. 2024 (RO **2023** 738).

4 Les demandes de modification ou de déconnexion sont traitées de manière analogue aux demandes de raccordement.

Art. 24 Raccordement de systèmes IAM de la Confédération à des systèmes IAM externes

1 Les systèmes IAM de la Confédération peuvent être raccordés en qualité de fournisseurs de données d'identification et d'authentification à un système IAM externe ou à une fédération d'identités externe aux conditions suivantes:

a.[43] le raccordement sert à octroyer aux personnes visées aux art. 8 ou 9 un accès:

1. à des systèmes d'information qui sont gérés par un exploitant externe sur mandat de la Confédération ou à des systèmes d'information tiers dont elles ont besoin pour exécuter leurs tâches légales, ou
2. à des systèmes d'information qui sont mis à disposition, pour l'exécution du droit cantonal, par les cantons et les communes ainsi que par des organisations et personnes de droit public ou de droit privé, tels que les applications de cyberadministration;

b. la Confédération et l'exploitant du système d'information bénéficiaire concluent une convention régissant les relations sur le plan juridique, organisationnel et technique;

c. la connexion est configurée de façon à permettre uniquement un accès aux systèmes d'information prédéfinis.

2 Le secteur TNI de la ChF fixe dans des directives les exigences à respecter en matière de sécurité, en accord avec l'organe responsable du système IAM correspondant, et vérifie régulièrement si ces exigences sont satisfaites.

3 Il est également possible de participer à une fédération internationale d'identités sur la base d'un traité international, à condition que le respect des exigences concernant la sécurité de l'information soit garanti.

Section 8
Établissement de procès-verbaux, de statistiques et d'une documentation

Art. 25 Établissement de procès-verbaux par les systèmes IAM

1 Le système IAM consigne les authentifications et la publication de données d'identification dans un procès-verbal uniquement pour la durée et dans la mesure nécessaires à une exploitation sûre et ordonnée de ses propres systèmes et de ceux en aval.

43 Nouvelle teneur selon le ch. I de l'O du 8 nov. 2023, en vigueur depuis le 1er janv. 2024 (RO **2023** 738).

2 Les données des procès-verbaux de journalisation sont conservées séparément du système dans lequel les données personnelles sont traitées et sont détruites au plus tard après deux ans. Elles ne sont pas archivées.[44]

3 Demeurent réservés l'établissement d'un procès-verbal plus détaillé, une conservation plus longue ou un archivage des procès-verbaux concernant les accès à un système d'information précis en raison d'une base légale particulière.

Art. 26 Transmission des données des procès-verbaux établis par les systèmes IAM

1 Les exploitants des systèmes IAM de la Confédération peuvent communiquer au service responsable du système en aval concerné les données des procès-verbaux concernant les authentifications et la publication de données d'identification.

2 À cet effet, une demande écrite mentionnant le but et les bases légales doit être adressée à l'organe responsable du système IAM par l'intermédiaire du conseiller à la protection des données compétent. La livraison des données peut faire l'objet d'une convention mentionnant les mêmes informations entre l'organe responsable du système en aval et l'exploitant du système IAM.

3 En vertu des principes en vigueur pour l'acquisition de prestations informatiques au sein de la Confédération, la livraison des données peut être payante.

Art. 27 Statistiques des systèmes IAM

Des statistiques d'accès peuvent être établies pour les besoins du service responsable du système IAM ou du système d'information en aval. Les données personnelles doivent être anonymisées.

Art. 28 Inventaire et documentation

1 Tout organe responsable d'un système IAM, d'un service d'annuaires ou d'un autre système d'information en vertu de la présente ordonnance tient un inventaire:

a. de ses systèmes IAM et services d'annuaires;

b. des systèmes d'information à partir desquels des données sont obtenues automatiquement;

c. des systèmes d'information auxquels des données sont transmises automatiquement;

d. de tous les systèmes IAM auxquels est relié son propre système IAM.

2 Les preuves et les documents importants, en particulier les demandes établies en vertu de la présente ordonnance, doivent être conservés au moins jusqu'à l'expiration de leur durée de validité.

44 Nouvelle teneur selon l'annexe 2 ch. II 18 de l'O du 31 août 2022 sur la protection des données, en vigueur depuis le 1er sept. 2023 (RO **2022** 568).

Section 9 Dispositions finales

Art. 29 Exécution

Le secteur TNI de la ChF édicte les directives administratives et techniques concernant la mise en place et l'exploitation des systèmes IAM de la Confédération.

Art. 30 Abrogation d'un autre acte

L'ordonnance du 6 décembre 2013 sur les services d'annuaires de la Confédération exploités par l'OFIT[45] est abrogée.

Art. 31 Entrée en vigueur

La présente ordonnance entre en vigueur le 1er janvier 2017

45 [RO **2013** 4553]

Annexe[46]
(art. 11 et 13, al. 1 et 2)

Catégories de données

Remarque préliminaire: pour la signification des astérisques (*), voir l'art. 11, al. 4.

	Services d'annuaires	Systèmes IAM avec des personnes au sens des art. 8 et 9, let. a	Systèmes IAM avec des personnes au sens de l'art. 9, let. b
a. Données relatives à la personne			
1. Nom*	x	x	x
2. Prénoms*	x	x	x
3. Date de naissance		x	x
4. Lieu de naissance			x
5. Nationalité			x
6. Sexe		x	x
7. Civilité*	x	x	x
8. Titre*	x	x	x
9. Initiales*	x	x	x
10. Identificateurs personnels locaux	x	x	x
11. Profession*	x	x	x
12. Langue de correspondance*	x	x	x
13. Caractéristiques biométriques personnelles particulières, en particulier scan de l'iris, rétine, scan des veines, empreinte digitale, empreinte palmaire, caractéristiques de la forme du visage et profil de la voix		x	
14. Photo du visage	x	x	x
15. Numéro AVS	x	x	x
b. Données relatives au rapport avec l'employeur / le mandant			
1. Rapports de travail (interne/externe)*	x	x	
2. Informations relatives à l'unité d'organisation et aux postes de travail*	x	x	x

[46] Nouvelle teneur selon le ch. II de l'O du 8 nov. 2023, en vigueur depuis le 1er janv. 2024 (RO **2023** 738).

	Services d'annuaires	Systèmes IAM avec des personnes au sens des art. 8 et 9, let. a	Systèmes IAM avec des personnes au sens de l'art. 9, let. b
3. Futur rattachement à une unité d'organisation	x	x	
4. Catégorie de personnel		x	
5. Numéro personnel (y c. cantonal)	x	x	
6. Fonction*	x	x	
7. Poste*	x	x	
8. Identification du système d'information du personnel (source)	x	x	
9. Date d'entrée et date de départ	x	x	
10. Numéro de pièce d'identité et/ou de badge	x	x	x
c. Données de contact			
1. Lieu de travail et adresse postale professionnelle*	x	x	x
2. Adresse postale privée			x
3. Numéro du bureau*	x	x	
4. Composantes de l'adresse professionnelle* telles qu'adresse électronique*, numéro de téléphone*, numéro de fax*, adresse VoIP*	x	x	x
5. Composantes de l'adresse externe* (pour les collaborateurs et les mandataires*) ou de l'adresse privée	x	x	x
d. Données concernant les fonctions professionnelles			
1. Indications issues des registres professionnels officiels (médecin, personne habilitée à dresser des actes authentiques, avocat, etc.)		x	x
2. Fonction selon le registre du commerce et d'autres registres des représentations		x	x
e. Données techniques			
1. Appareils, raccordements, systèmes, applications, etc.	x	x	x
2. Composantes de l'adresse, numéros d'identification, etc.	x		
3. Langue du système des appareils, des raccordements, etc.	x	x	x
4. Clés publiques des certificats numériques*	x	x	x
5. Groupes d'autorisations	x	x	x

	Services d'annuaires	Systèmes IAM avec des personnes au sens des art. 8 et 9, let. a	Systèmes IAM avec des personnes au sens de l'art. 9, let. b
6. Noms pour la connexion aux systèmes informatiques	x	x	x
7. Mots de passe (sécurisés cryptographiquement)		x	x
8. Dernière ouverture de session		x	x
9. Échecs lors d'ouvertures de session		x	x
10. Statut (actif/passif)		x	x
11. Qualité de l'authentification		x	x
f. Données relatives au contrôle de sécurité relatif aux personnes, si celui-ci a abouti à une déclaration de sécurité sans réserve ou si l'autorité décisionnelle a rendu une décision positive			
1. Degré de contrôle		x	
2. Durée de validité de la déclaration de sécurité		x	