Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

[Signature]

[QR Code]

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

du …

Le Conseil fédéral suisse,

vu la loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA)[1],
vu les art. 27, al. 2, let. c, et 27*a*, al. 6, de la loi du 24 mars 2000 sur le personnel de la Confédération (LPers)[2],

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[3]), les services d'annuaires et la base centralisée des identités de la Confédération.

Art. 2 Champ d'application

1 La présente ordonnance s'applique 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)[4].

2 Les autorités et services suivants peuvent, sous réserve d'autres dispositions du droit fédéral en matière d'organisation, s'engager par une convention à respecter la présente ordonnance et les prescriptions qui en découlent:

a. les unités de l'administration fédérale décentralisée au sens de l'art. 7*a* OLOGA;

b. d'autres autorités fédérales;

RS .....
1 RS **172.010**
2 RS **172.220.1**
3 IAM = *Identity and Access Management* (gestion des identités et des accès)
4 RS **172.010.1**

c. des organisations et des personnes de droit public ou privé qui sont extérieures à l'administration fédérale, mais auxquelles des tâches de l'administration fédérale peuvent être confiées (art. 2, al. 4, LOGA);

d. des institutions proches de la Confédération qui poursuivent un but d'intérêt public, si leurs systèmes sont reliés à ceux de l'administration fédérale.

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.

Section 3 Organes responsables

Art. 5 Systèmes IAM

1 Les organes de la Confédération responsables des systèmes IAM sont:

a. l'Unité de pilotage informatique de la Confédération (UPIC), pour tous les systèmes IAM proposés comme services standard ou tous les systèmes IAM relevant explicitement de l'UPIC;

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

c. l'État-major de l'armée, pour le système IAM exploité par la Base d'aide au commandement (BAC);

d. 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).

2 Le service technique compétent demeure responsable du système en aval, et en particulier de l'accès à celui-ci.

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, l'UPIC ;

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. la BAC,
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. droit de rectification et de suppression: auprès du service du personnel de leur unité administrative ou de leur organisation ou auprès du service chargé de gérer leurs données.

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[5];

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

5 RS **172.010.1**

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[6];

d. personnes élues par l'Assemblée fédérale au sens de l'art. 168 de la Constitution[7];

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[8];

g. membres du Secrétariat de l'Autorité de surveillance du Ministère public de la Confédération au sens de l'art. 27, al. 2, de la loi sur l'organisation des autorités pénales.

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;

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. particuliers et représentants d'organisations qui accèdent à des systèmes d'information mis à disposition par la Confédération, tels que les applications de cyberadministration.

6 RS **171.10**
7 RS **101**
8 RS **173.71**

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 profil de la personnalité ne peut être traité dans ces systèmes.

3 En l'absence d'une base légale particulière en la matière, aucune donnée sensible ne peut être traitée dans ces systèmes.

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.

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 concernant le personnel de l'administration fédérale (BV PLUS) au sens de l'art. 11 de l'ordonnance du 26 octobre 2011 concernant la protection des données personnelles du personnel de la Confédération[9].

2 Ils peuvent obtenir automatiquement auprès des organes concernés au sens de l'art. 8 les données des personnes ne figurant pas dans BV PLUS, 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.

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

1 L'Office fédéral de l'informatique et de la télécommunication (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. L'UPIC est l'organe responsable au sein de la Confédération.

2 BV PLUS transmet régulièrement à la base centralisée des identités les données mentionnées dans l'annexe, pour autant que ces dernières soient disponibles. Toute

9 RS **172.220.111.4**

obtention automatique de données personnelles depuis BV PLUS 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:

a. dispose d'une base légale et d'un règlement de traitement au sens de l'art. 21 de l'ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données (OLPD)[10], et

b. ait été annoncé au Préposé fédéral à la protection des données et à la transparence ou ne doive pas être déclaré en vertu de l'art. 18 OLPD.

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[11] sont transmises régulièrement à cette dernière.

Art. 14 Délai de conservation des données personnelles

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.

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.

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'identifi-

10 RS **235.11**
11 RS **172.210.10**

cation 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

Art. 18 Exigences concernant la sécurité de l'information

1 Les exploitants internes et externes d'éléments d'un système IAM doivent avoir des instructions clairement documentées sur la sécurité de l'information et la gestion des risques. En particulier, chaque organe responsable d'un système au sens de la présente ordonnance établit un règlement de traitement conformément à l'art. 21 de l'ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données[12].

2 Les systèmes IAM qui ne sont pas gérés par des organes au sens de l'art. 2 ou sur mandat de ces derniers peuvent être raccordés à des systèmes IAM internes à l'administration fédérale uniquement s'ils respectent les exigences minimales prédéfinies concernant la sécurité de l'information.

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

12 RS **235.11**

4 L'UPIC 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 Interconnexion de systèmes IAM de la Confédération

Les systèmes IAM de l'administration fédérale peuvent être reliés entre eux et avec les systèmes IAM des Services du Parlement ou de l'armée pour former un système global.

Art. 21 Conditions pour le raccordement de systèmes IAM externes

1 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:

a. systèmes IAM comprenant des collaborateurs cantonaux et communaux au sens de l'art. 9, let. a;

b. systèmes IAM reconnus par l'UPIC 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 l'UPIC.

3 L'organe de la Confédération responsable conclut la convention avec le service demandeur, informe l'UPIC et mandate le fournisseur de prestations concerné en vue du raccordement.

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. le raccordement sert à octroyer aux personnes visées aux art. 8 ou 9 un accès 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 pouvoir exécuter leurs tâches légales;

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 L'UPIC 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.

2 Les données des procès-verbaux sont détruites au plus tard après deux ans. Elles ne sont pas archivées.

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.

Section 9 Dispositions finales

Art. 29 Exécution

L'UPIC 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[13] est abrogée.

Art. 31 Entrée en vigueur

La présente ordonnance entre en vigueur le 1er janvier 2017

… Au nom du Conseil fédéral suisse:

Le président de la Confédération, Johann N. Schneider-Ammann
Le chancelier de la Confédération, Walter Thurnherr

13 RO **2013** 4553

Annexe
(art. 11, al. 1 et 4, 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(s) de famille actuel(s)*	x	x	x
2. Prénom(s) actuel(s)*	x	x	x
3. Date de naissance		x	x
4. Sexe		x	x
5. Civilité*	x	x	x
6. Titre*	x	x	x
7. Initiales*	x	x	x
8. Identificateurs personnels locaux	x	x	x
9. Profession*	x	x	x
10. Langue de correspondance*	x	x	x
b. Données relatives au rapport avec l'employeur/le mandant			
1. Rapports de travail (interne/externe)*	x	x	
2. Unité d'organisation*	x	x	x
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	
c. Données de contact			
1. Adresse du lieu de travail et adresse postale professionnelle*	x	x	x
2. Numéro du bureau*	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
3. Composantes de l'adresse professionnelle* telles qu'adresse électronique*, numéro de téléphone*, numéro de fax*, adresse VoIP*	x	x	x
4. 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
6. Noms pour la connexion aux systèmes informatiques	x	x	x
7. Mot(s) de passe		x	x
8. Dernière ouverture de session		x	x
9. Échecs lors d'ouvertures de session		x	x
10. Statut (actif/passif)		x	x