Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Chancellerie fédérale ChF

2 avril 2025

Ordonnance sur les services numériques et la transformation numérique dans l'administration fédérale (ordonnance sur la numérisation, ONum)

Rapport explicatif

Table des matières

1 Contexte

1.1 Jalons

Le 17 mars 2023, les Chambres fédérales ont adopté la loi fédérale sur l'utilisation de moyens électroniques pour l'exécution des tâches des autorités (LMETA)[1]. La LMETA crée les bases légales requises pour une transformation numérique efficace de l'administration fédérale, ainsi que pour la collaboration entre les autorités de différentes collectivités et les tiers dans le domaine de la cyberadministration.

L'ordonnance du 22 novembre 2023 sur l'utilisation de moyens électroniques pour l'exécution des tâches des autorités (OMETA)[2] est entrée en vigueur en même temps que la LMETA, le 1er janvier 2024. En outre, l'ordonnance du 25 novembre 2020 sur la transformation numérique et l'informatique (OTNI)[3], qui vise en premier lieu à mettre en œuvre la transformation numérique de l'administration fédérale, est en vigueur depuis le 1er janvier 2021.

La nouvelle ordonnance sur la numérisation (ONum) est une fusion de l'OMETA et de l'OTNI. Sur le fond, la plupart des dispositions des deux ordonnances sont reprises. Les modifications sont essentiellement de nature formelle ou linguistique.

Les adaptations des dispositions en vigueur portent d'une part sur le champ d'application, adapté en raison de la fusion, et, d'autre part, sur l'alignement de la définition des services standard de l'OTNI sur celle des moyens informatiques mis à disposition de manière centralisée, conformément à l'art. 11 LMETA.

Lorsque l'ONum entrera en vigueur, l'OMETA et l'OTNI seront abrogées.

1.2 Digression : principe de la priorité au numérique et accès aux prestations des autorités

En vertu du principe de la priorité au numérique[4] adopté par le Conseil fédéral et consacré à l'art. 3, al. 1, LMETA, les autorités fédérales soumises à cette loi utilisent des moyens numériques pour mettre à disposition des informations et des services *chaque fois que c'est possible et lorsque cela est judicieux*. Pour assurer la transition vers la cyberadministration, la Confédération devra proposer à l'avenir un canal électronique doté d'avantages tels qu'il deviendra nécessairement le premier choix de la population et des entreprises : elle proposera systématiquement des informations et des services sous forme électronique, pour autant que cela soit judicieux, en veillant à une compatibilité maximale avec les appareils mobiles. Elle améliorera la diffusion et l'accessibilité de ses services et assurera des processus entièrement électroniques. Elle veillera à ne pas porter atteinte au droit à l'autodétermination informationnelle.

---

1 RS **172.019**
2 RS **172.019.1**
3 RS **172.010.58**
4 Ce principe est établi dans de la stratégie suisse de cyberadministration 2020–2023, adoptée par le Conseil fédéral, FF **2019** 8267.

Lors de l'élaboration de l'OMETA, il est apparu qu'une concrétisation de ce principe au niveau de l'ordonnance n'apportait pas de valeur ajoutée. S'agissant des conditions « chaque fois que cela est possible » et « lorsque cela est judicieux », il n'a pas été possible de définir des critères suffisamment clairs pour créer une incitation concrète. On ne saurait par exemple régler de manière générale et abstraite pour quelles interactions l'utilisation de moyens électroniques serait *judicieuse*. Cette question doit être tranchée en l'espèce, dans les limites du pouvoir d'appréciation de l'autorité concernée ; les autorités fédérales soumises à la LMETA ne doivent toutefois pas user de ce pouvoir pour se retrancher derrière les conditions « chaque fois que cela est possible » et « lorsque cela est judicieux » pour se soustraire au principe de la priorité au numérique. En raison de l'impossibilité de concrétiser de manière générale et abstraite ces deux notions, on a renoncé à assortir l'art. 3, al. 1, LMETA de dispositions d'exécution.

Il en va de même de l'art. 3, al. 4, LMETA, en vertu duquel les autorités soumises à cette loi doivent veiller à ce que leurs prestations soient accessibles à l'ensemble de la population. Il était inutile de le concrétiser dans l'OMETA, notamment parce que les dispositions nécessaires figurent déjà ailleurs : l'ordonnance du 19 novembre 2003 sur l'égalité pour les handicapés (OHand)[5] établit ainsi les exigences requises pour l'aménagement des prestations de la Confédération conforme aux besoins des personnes handicapées. L'art. 10, al. 1, OHand prévoit que l'information et les prestations de communication ou de transaction proposées sur Internet doivent être accessibles aux personnes handicapées « de la parole, de l'ouïe, de la vue ou handicapées moteur ». À cet effet, les sites doivent être aménagés conformément aux standards informatiques internationaux, notamment aux directives régissant l'accessibilité des pages Internet, édictées par le Consortium World Wide Web (W3C) et, subsidiairement, aux standards nationaux. Les directives sont établies en collaboration avec les organisations d'aide aux personnes handicapées et les organisations professionnelles qui sont spécialisées en matière d'informatique et de communication ; elles sont périodiquement mises à jour en fonction des progrès techniques réalisés dans la branche.

2 Commentaire des dispositions

Remarque liminaire concernant la notion de « tâches des autorités »

La LMETA et l'OMETA règlent au niveau fédéral l'utilisation de moyens électroniques pour l'exécution des *tâches des autorités*.

On parle de « tâche des autorités » lorsque la loi prévoit qu'une tâche de l'État doit être exécutée par une autorité[6], qu'elle soit législative, exécutive ou judiciaire.

5 RS **151.31**

6 Cf. HÄFELIN/MÜLLER/UHLMANN, *Allgemeines Verwaltungsrecht*, 7e édition, ch. 24.

Titre

La nouvelle ordonnance s'intitule :

ordonnance sur les services numériques et la transformation numérique dans l'administration fédérale (ordonnance sur la numérisation, ONum)

Préambule

La LMETA prévoit des règles en matière de gouvernance de l'informatique qui se recoupent avec celles de l'OTNI ou qui les complètent. Ce lien étroit impose que les dispositions d'exécution de la LMETA soient fusionnées avec l'OTNI dans la nouvelle ordonnance. Cette dernière se fonde tant sur la LMETA que sur la loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA)[7].

Chapitre 1 Dispositions générales

Art. 1 Objet

L'ONum met en œuvre la LMETA. Elle règle d'autre part les organes, les stratégies et les processus opérationnels nécessaires à la transformation numérique de l'administration fédérale et à la gouvernance de l'informatique.

Elle règle en particulier la mise à disposition de services numériques par l'administration (*let. a*). Ces services doivent répondre aux besoins des utilisateurs, soit des citoyens et des entreprises. La gouvernance de l'informatique au sens de la présente ordonnance vise à garantir que les processus d'affaires puissent être numérisés, automatisés et intégrés dans les unités administratives et au-delà (*business IT alignment*).

L'utilisation et l'exploitation des technologies de l'information et de la communication dans l'administration fédérale (*let. b*) peuvent être gérées de différentes manières. Une partie des moyens informatiques est par exemple mise à disposition de manière centralisée (services standard) par le secteur Transformation numérique et gouvernance de l'informatique de la Chancellerie fédérale (secteur TNI). En vertu de l'art. 11 LMETA, le secteur TNI peut imposer à d'autres unités administratives de mettre à disposition un moyen informatique de manière centralisée (art. 11 ONum). Le chancelier de la Confédération peut en outre, après avoir consulté la Conférence des secrétaires généraux (CSG), imposer aux unités administratives de l'administration fédérale centrale l'utilisation d'un moyen informatique mis à disposition de manière centralisée (art. 11, al. 2, ONum). La gouvernance de l'informatique au sein de l'administration fédérale respecte les principes d'adéquation, d'interopérabilité, d'économicité et de sécurité.

L'ordonnance règle également les stratégies *(let. c*) qui permettent de faire avancer la transformation numérique. Si la *stratégie Administration fédérale numérique* (art. 7, let. a) ne concerne que l'administration fédérale, la *stratégie Suisse numérique* (art. 7, let.

7 RS **172.010**

b) permet d'atteindre d'autres acteurs tels que les cantons, les communes, les milieux économiques et scientifiques et la société civile.

L'ONum règle en outre d'autres domaines, notamment le système de gestion des données de référence (système GDR) et la compétence des départements et de la Chancellerie fédérale concernant le choix des fournisseurs internes de prestations. Le succès de la transformation numérique dépend de la collaboration des services et des unités administratives concernés, celui de la gouvernance de l'informatique commande que les responsabilités et les compétences soient clairement définies (*let. d*).

Art. 2 Applicabilité

L'ONum s'applique aux unités de l'administration fédérale centrale. En vertu de l'art. 2, al. 2, LMETA, qui entrera en vigueur en même temps que l'ONum, la LMETA s'applique aussi aux unités de l'administration fédérale décentralisée ; le Conseil fédéral peut prévoir des exceptions. Le projet du Conseil fédéral prévoyait qu'il pouvait soumettre des unités de l'administration fédérale décentralisée à tout ou partie de la LMETA[8]. Le Parlement a été d'avis que ces unités devaient être soumises à la loi, mais que le Conseil fédéral pouvait prévoir des exceptions[9].

Une exception générale est prévue pour l'art. 11, al. 1 et 2, LMETA. Aux termes de l'art. 11, al. 3, ONum, les unités de l'administration fédérale décentralisée ne peuvent pas être obligées de mettre à disposition de manière centralisée un moyen informatique ou d'utiliser un moyen informatique mis à disposition de manière centralisée. Ce serait absurde, ne serait-ce qu'en raison de la taille de certaines de ces unités. Par ailleurs, la plupart des unités administratives décentralisées ont fait valoir leur autonomie, garantie par la loi, pour rejeter une telle obligation.

Une restriction s'applique en outre aux logiciels à code source ouvert des unités de l'administration fédérale décentralisée et à l'obligation de respecter les normes (cf. art. 3 ONum). Par contre, les autres dispositions de la LMETA leur sont toutes applicables. Les dispositions d'exécution de la LMETA prévues dans l'ONum s'appliqueront donc aussi aux unités décentralisées.

Plusieurs dispositions de l'ONum prévoient cependant un champ d'application spécifique, qui prime l'art. 2, pour ces unités (par ex. art. 11, al. 3, 15, al. 1, 24, al. 2, et 39, al. 2). La section 3 (Système GDR), par exemple, ne s'applique qu'aux unités décentralisées qui utilisent le système GDR pour exécuter leurs processus d'affaires (art. 22, al. 1, let. b).

En règle générale, les unités décentralisées ne sont pas soumises à des instructions et jouissent d'une certaine autonomie institutionnelle. Elles sont donc elles-mêmes responsables du respect des exigences de la LMETA, telles que les normes contraignantes (art. 12 LMETA).

Les unités décentralisées qui, en vertu de l'art. 2, al. 2, LMETA, ne sont pas soumises à certaines dispositions de cette loi, sont mentionnées dans l'annexe 1 ONum. Le Conseil fédéral décide des éventuelles adaptations de cette annexe.

---

8 FF **2022** 805

9 BO **2022** N 1599

Art. 3 Exceptions pour les unités de l'administration fédérale décentraliséeAl. 1 : conformément à l'art. 2, al. 2, LMETA, les exceptions prévues ne s'appliquent qu'aux unités de l'administration fédérale décentralisée. Celles-ci décident elles-mêmes si les conditions auxquelles sont soumises les exceptions sont remplies.

Let. a : le principe *public money, public code* ne s'applique pas lorsque le développement d'un logiciel n'a pas été financé ou cofinancé par des fonds de la Confédération. C'est notamment le cas lorsqu'une unité décentralisée développe un logiciel sur mandat de tiers et donc avec les fonds de ceux-ci.

Let. b : les logiciels développés dans le cadre de la recherche ne doivent pas non plus être accessibles comme des logiciels à code ouvert. Il en va de la liberté de la recherche.

Al. 2 : les normes visées à l'art. 12 LMETA ont pour but de favoriser l'interopérabilité des systèmes utilisés par les autorités pour accomplir leurs tâches. Seules quelques normes fondamentales qui sont indispensables pour l'interopérabilité avec les systèmes des autorités mentionnées à l'al. 5 sont déclarées contraignantes pour les unités de l'administration fédérale décentralisée (let. a). Au demeurant, les unités décentralisées sont souvent soumises à des normes nationales ou internationales de tiers qui doivent primer les normes visées à l'art. 12 LMETA en cas de concurrence avec ces dernières (let. b).

Le dialogue est indispensable à la réussite de la normalisation. Il est donc prévu que les unités décentralisées participent à la procédure permettant de déclarer ces normes contraignantes pour que les besoins réels de normalisation puissent être établis en commun, dans la mesure du possible. Le cas échéant, les normes existantes peuvent être adaptées pour qu'elles ne soient plus en concurrence avec d'autres normes.

Si une unité décentralisée ne peut pas respecter, pour un des motifs mentionnés à l'al. 2, une norme déclarée contraignante, elle doit l'annoncer au secteur TNI et demander une dérogation à la norme. Le secteur TNI statue sur l'octroi de la dérogation en suivant les processus existants[10].

Art. 4 Publication des conventions conclues en vertu de l'art. 2, al. 3, LMETA

Al. 1 : le champ d'application de la LMETA s'étend à toute l'administration fédérale, centrale et décentralisée; la loi prévoit par ailleurs des possibilités d'assujettissement pour certaines autres autorités fédérales (art. 2, al. 3, LMETA).

L'assujettissement reposant sur une convention conclue avec le Conseil fédéral est réservé aux Services du Parlement, aux tribunaux fédéraux et au Ministère public de la Confédération, compte tenu de leur autonomie administrative. Si ces autorités fédérales décident de se soumettre à la LMETA, elles peuvent décider de le faire en tout ou partie. Elles doivent alors adresser une demande au Conseil fédéral afin de conclure une convention. La convention doit préciser à quelles parties de la loi l'autorité se soumet et doit être publiée dans la Feuille fédérale.

[10] www.chf.admin.ch > Transformation numérique et gouvernance de l'informatique > Directives informatiques > Toutes les directives > P035 - Gestion des exigences et des directives relatives à la transformation numérique et à la gouvernance de l'informatique

Al. 2 : afin que les instances chargées d'appliquer le droit puissent s'informer rapidement, le secteur TNI publie sur Internet une liste des autorités fédérales soumises à la loi en vertu d'une convention. Cette liste précise à quelles dispositions de la LMETA chaque autorité est soumise. Si l'autorité est soumise à la loi dans son ensemble, la liste renvoie directement à la LMETA, sans en citer toutes les dispositions.

L'ordonnance ne précise pas de critères justifiant la soumission des autorités susmentionnées à la LMETA. Leur subordination est particulièrement indiquée pour garantir l'interopérabilité ou renforcer la collaboration entre l'administration fédérale et les autorités que l'on souhaite assujettir à la LMETA, ou lorsqu'il est nécessaire que celles-ci puissent exploiter les possibilités prévues par la LMETA en matière d'utilisation de moyens électroniques (par ex. utilisation de logiciels libres, mise à disposition de moyens informatiques pour les cantons, les communes et des organisations).

Art. 5 Non-soumission des prestations informatiques indispensables aux engagements de l'armée

Bien que les prestations informatiques indispensables aux engagements de l'armée doivent également être standardisées et automatisées, le succès des engagements dans des conditions difficiles (par ex. en cas de crise, de situation d'urgence ou de guerre) l'emporte sur les réflexions purement économiques. Les critères de qualité des moyens informatiques mis à disposition de manière centralisée dans l'administration fédérale ne correspondent donc pas à ceux des moyens indispensables à l'armée et ne satisfont généralement pas aux exigences des engagements. L'affaiblissement potentiel de la capacité de défense justifie qu'on distingue les moyens mis à disposition de l'administration fédérale des moyens indispensables à l'armée. Afin de garantir que cette distinction soit également judicieuse du point de vue civil et que les éventuelles synergies entre les systèmes civils et militaires puissent être identifiées et exploitées dans la mesure du possible, le secteur TNI, chargé de veiller à la cohérence et à l'efficacité des processus d'affaires numériques et de l'utilisation de la technologie, doit être consulté ; en cas de différend, le Département fédéral de la défense, de la protection de la population et des sports (DDPS) consultera le Conseil de la transformation numérique et de la gouvernance informatique de la Confédération (Conseil TNI) et, si nécessaire, la CSG avant de prendre une décision.

Plusieurs projets de l'armée ont déjà été identifiés comme des projets clés au sens de l'art. 35 ONum et sont gérés dans le portefeuille. Ce processus doit être conservé pour pouvoir comparer les projets clés et, en particulier, établir une vue d'ensemble destinée au Parlement (haute surveillance).

Art. 6 Responsabilité

En optant pour le nouveau modèle de gouvernance, le Conseil fédéral s'est prononcé contre une centralisation de la transformation numérique et de la gouvernance de l'informatique. Dans ce modèle, les acteurs principaux de la transformation numérique sont les offices et les départements. Ces derniers, en particulier, jouent un rôle charnière important entre le secteur TNI et les offices. Aussi sont-ils appelés à adapter leurs structures aux nouvelles exigences, notamment, au-delà de la gouvernance de l'infor-

matique et à créer ou renforcer les rôles et responsabilités dans le domaine de l'architecture d'entreprise (harmonisation entre toutes les unités administratives des processus d'affaires et des modèles de données).

Le respect des directives dans le domaine de la transformation numérique et de la gouvernance de l'informatique est une tâche d'exécution, qui relève dès lors également de la compétence des départements et de la Chancellerie fédérale.

Cette responsabilité générale s'entend sous réserve des dispositions de l'ONum et des directives fondées sur elle. Les règles de compétences prévues par d'autres actes tels que l'ordonnance GEVER du 3 avril 2019[11] ne sont pas touchées.

Par ailleurs, les unités administratives de l'administration fédérale décentralisée doivent également faire progresser la transformation numérique dans leur domaine de compétence. Elles doivent se concerter avec les départements auxquels elles sont rattachées.

Chapitre 2 Stratégies

Art. 7 Contenu

Le Conseil fédéral a la compétence de fixer les objectifs stratégiques dans le domaine de la transformation numérique et de l'informatique dans l'administration fédérale (stratégie Administration fédérale numérique) et les lignes directrices de la transformation numérique de la Suisse (stratégie Suisse numérique). Les autorités et organes qui interviennent plus tard dans la procédure, notamment la CSG et le délégué TNI, accomplissent leurs tâches dans le cadre stratégique fixé par le Conseil fédéral.

Les travaux de mise en œuvre de la stratégie Administration fédérale numérique sont définis par un plan directeur. Celui-ci est régulièrement mis à jour par le délégué TNI et soumis au Conseil fédéral pour information.

La stratégie Suisse numérique se compose d'une partie générale et durable qui donne une vue d'ensemble des domaines importants pour la transformation numérique de la Suisse. Elle expose en outre quelques thèmes prioritaires qui revêtent une importance particulière à l'heure actuelle. Le Conseil fédéral redéfinit périodiquement les thèmes prioritaires.

Art. 8 Mise en œuvre

Les stratégies sont contraignantes pour l'administration fédérale centrale. Les départements et les unités administratives contribuent activement à leur mise en œuvre et à la réalisation des objectifs qu'elles contiennent dans leur domaine de compétence (art. 6).

La stratégie Suisse numérique donne aux autres acteurs de la numérisation, tels que les cantons, les communes, les milieux économiques et scientifiques et la société civile

11 RS **172.010.441**

un cadre sur lequel s'appuyer afin que tous puissent profiter au mieux des opportunités de la transformation numérique.

Le Conseil fédéral exerce la surveillance sur la mise en œuvre des stratégies dans le cadre de sa compétence de surveillance générale. Si nécessaire, il peut adopter des mesures pour garantir la réalisation des objectifs contenus dans les stratégies.

Al. 1 : l'administration fédérale collabore à la mise en œuvre de la stratégie Administration fédérale numérique (*let. a*). Le secteur TNI coordonne les mesures de mise en œuvre qu'il prévoit avec les départements et les unités administratives.

La stratégie Suisse numérique touchant d'autres acteurs (*let. b à e*), elle est mise en œuvre de manière décentralisée, au moyen d'un plan d'action qui donne une vue d'ensemble des mesures concrètes définies par l'administration fédérale ou des acteurs externes pour atteindre les objectifs de la stratégie. Leur avancement est régulièrement mis à jour par les acteurs concernés.

Al. 2 : le secteur TNI élabore la stratégie Administration fédérale numérique ; le délégué TNI consulte à cet effet le Conseil TNI.

Dans la mesure où des éléments de la stratégie Suisse numérique touchent des compétences des cantons ou des communes, le délégué TNI devra se coordonner étroitement avec le chargé de mission de la Confédération et des cantons auprès de l'Administration numérique suisse tant pour l'élaboration que pour la mise en œuvre de la stratégie, raison pour laquelle une consultation du chargé de mission est prévue.

La consultation du Conseil TNI n'est pas prévue en ce qui concerne la stratégie Suisse numérique ; elle est possible en cas de besoin. La stratégie peut par contre avoir une incidence sur les politiques sectorielles, aussi le délégué TNI doit-il consulter la CSG pour son élaboration et sa mise en œuvre.

Chapitre 3 Fourniture de prestations

Art. 9 Compétence

La compétence des départements et de la Chancellerie fédérale s'entend sous réserve des dispositions de l'ONum et des directives qui se fondent sur elle. Si l'utilisation d'un service standard est déclarée obligatoire, les départements et la Chancellerie fédérale doivent impérativement l'utiliser : aucune dérogation n'est possible.

Les départements et la Chancellerie fédérale consultent les bénéficiaires et les fournisseurs de prestations concernés.

Art. 10 Fournisseurs internes de prestations informatiques

Il n'y a qu'un seul fournisseur interne de prestations informatiques par département (*al. 1*). Actuellement, la Chancellerie fédérale ne dispose pas d'un tel fournisseur, mais il n'est pas exclu qu'elle en ait un à l'avenir. Le Conseil fédéral peut, sur demande, autoriser des dérogations *(al. 2*).

Art. 11 Mise à disposition centralisée de moyens informatiques

Al. 1 : les services standard gérés par le secteur DTI correspondent à un moyen informatique mis à disposition de manière centralisée au sens de l'art. 11 LMETA. Six services standard (SS) sont déjà établis :

- SS Transmission de données (DAKO)
- SS Bureautique (BA)
- SS Service d'annuaire (DIR)
- SS Gestion de l'identité et de l'accès (y c. AGOV)
- SS Gestion électronique des affaires (GEVER)
- SS Sites Internet Confédération (WEB)

Pour les SS, le secteur TNI gère les exigences et la fourniture des prestations conformément à la directive du 18 décembre 2023 sur le pilotage et la gestion des services standard conformément à l'OTNI (W008)[12].

Le secteur TNI continuera de gérer les services standard actuels selon le même système. Par services standard, on entend les moyens informatiques dotés de fonctionnalités et présentant une qualité identique ou similaire, dont toutes les unités de l'administration fédérale centrale ont besoin. Le secteur TNI est responsable de la trans-

12 www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/ikt-vorgaben/grundlagen/w008-weisungen_zur_steuerung_und_fuehrung_der_standarddienste_gemaess_vdti.html

formation numérique et de la gouvernance de l'informatique au niveau interdépartemental et gère donc en tant que services standard les moyens informatiques qui sont prioritaires et concernent tous les départements.

En vertu de l'art. 11, al. 1, LMETA, d'autres unités peuvent se voir imposer de mettre à disposition de manière centralisée des moyens informatiques déterminés. Contrairement aux services standard gérés par le secteur TNI, ces moyens ne sont généralement pas pertinents pour tous les départements. Il s'agit notamment de moyens informatiques qui ne concernent qu'un secteur déterminé de l'administration fédérale et qui remplissent une tâche spécifique ou limitée ou qui ne sont utilisés que par une partie de l'administration fédérale dans un domaine spécifique (par ex. Sedex, COSIG). Ils ne sont pas gérés en tant que services standard. Si un moyen informatique n'est utilisé que dans un seul département, ce dernier en est responsable.

Le secteur TNI décide quelle unité administrative peut ou doit mettre à disposition de manière centralisée un moyen informatique. Il consulte au préalable l'unité concernée. La gestion d'un moyen informatique mis à disposition de manière centralisée, mais que le secteur TNI n'a pas défini comme un service standard, relève de l'unité concernée qui l'utilise le plus et dispose donc de l'expérience et des connaissances techniques adéquates. Si un département n'est pas d'accord avec une décision du secteur TNI concernant la gestion d'un moyen informatique mis à disposition de manière centralisée, le différend est réglé conformément à la procédure prévue par l'ONum (art. 42, al. 1, let. a).

Al. 2 : tous les services standard actuels sont assortis d'une obligation d'achat pour les unités administratives de l'administration centrale, mais les fonctionnalités requises, l'approvisionnement et le modèle de commande et de facturation des prestations sont définis en concertation avec les départements. L'obligation d'achat vise à garantir l'interopérabilité, la standardisation recherchée et l'exploitation des synergies dans l'administration fédérale. Dans ce contexte, l'obligation d'achat signifie qu'une unité de l'administration fédérale centrale doit commander les prestations dont elle a besoin au fournisseur prédéfini. Elle est généralement libre de choisir les caractéristiques et la quantité des prestations qu'elle souhaite commander. L'obligation d'achat se fonde sur l'art. 11, al. 2, LMETA. La LMETA permet également d'assortir d'une obligation d'achat les moyens informatiques mis à disposition de manière centralisée par d'autres autorités, à condition toutefois que cette obligation soit judicieuse sur le plan économique pour l'ensemble de l'administration fédérale. Il appartient au chancelier de la Confédération de déterminer si une obligation d'achat s'impose ; il consulte au préalable la CSG.

Al. 3 : en vertu de l'art. 2, al. 2, 2e phrase, LMETA, les al. 1 et 2 ne s'appliquent pas aux unités décentralisées. On ne peut donc pas leur imposer d'utiliser un moyen informatique mis à disposition de manière centralisée. Selon la pratique actuelle, l'organe de compensation de l'assurance-chômage, rattaché au SECO, ne peut pas non plus être obligé d'utiliser un moyen informatique ou de le mettre à disposition de manière centralisée. La commission de surveillance du fonds de compensation de l'assurance-chômage, qui fait partie de l'administration fédérale décentralisée (cf. art. 7*a*, al. 1, let. a,

de l'ordonnance du 25 novembre 1998 sur l'organisation du gouvernement et de l'administration [OLOGA][13]), dispose en effet de compétences particulières pour donner des instructions dans le domaine de l'informatique pour l'assurance-chômage.*Al. 4* : l'art. 2, al. 2, OTNI prévoit que les unités de l'administration fédérale décentralisée et d'autres autorités ou organisations peuvent se soumettre à l'ordonnance par un accord ; cette possibilité n'est pas reprise dans l'ONum. Les intéressés pourront toutefois encore utiliser des services standard et d'autres moyens informatiques mis à disposition de manière centralisée. Le secteur TNI peut en effet conclure avec eux des conventions à cet effet. Par « autres autorités fédérales » (*let. b*), on entend par exemple les tribunaux fédéraux et les Services du Parlement. Les organisations et les personnes de droit public ou privé extérieures à l'administration fédérale visées à la *let. c* comprennent les cantons, mais aussi des sociétés telles que RUAG MRO ou Swissgrid.

Art. 12 Accès aux données pour les fournisseurs externes de prestations

Par principe, les données non accessibles au public ne peuvent être rendues accessibles à des fournisseurs externes de prestations que s'il est inévitable en pratique et donc nécessaire qu'ils y aient accès pour fournir les prestations informatiques *(let. a*), pour autant que l'autorité fédérale responsable ait donné son accord (*let. b*). L'administration doit prendre les mesures nécessaires et raisonnablement exigibles pour prévenir le risque que ces données soient transmises plus loin (*let. c*).

L'accord visé à la *let. b* ne saurait être assimilé au consentement au sens de l'art. 320, ch. 2, du code pénal (CP)[14]. L'accord prouve uniquement que le bénéficiaire a été informé par le fournisseur interne qu'il fait appel à des fournisseurs externes pour la fourniture de services informatiques déterminés.

Lorsqu'un secret de fonction est touché, l'accord doit satisfaire aux conditions fixées à l'art. 320, ch. 2, CP et aux principes généraux reconnus par la jurisprudence. Dans les cas où il s'agit exclusivement — ou du moins également — d'un secret de service (par ex. dispositifs pour des bâtiments de la Confédération sécurisés, inscriptions au casier judiciaire des procédures pénales en cours), l'accord visé à *let. b* doit également satisfaire aux conditions du consentement au sens de l'art. 320, al. 2, CP.

La déclaration de consentement du bénéficiaire ou l'autorisation de l'autorité supérieure devrait, en règle générale, faire l'objet d'un document à caractère contractuel entre le fournisseur interne de prestations et le fournisseur des prestations informatiques et au moins être documentée de manière traçable. Il faut décrire aussi concrètement que possible les cas dans lesquels une violation du secret pourrait se produire (p. ex. maintenance du système par XY ; mise en place du système et sa mise en service par XY) et qui, *a minima* quel domaine, pourrait la commettre.

Pour déterminer « l'autorité fédérale responsable » visée à la *let. b*, on se référera à qui décide de la finalité et des moyens du traitement. Au sein de l'administration fédérale, on se fondera sur la responsabilité initiale des données. Le droit d'organisation applicable détermine l'autorité supérieure dans ce contexte. Par exemple, si l'Office fédéral de l'informatique et de la télécommunication (OFIT) doit rendre accessibles les données d'une banque de données d'un office à un prestataire externe, l'accord de cet

13 RS **172.010.1**
14 RS **311.0**

office est nécessaire. Dans un tel cas, le consentement visé à l'art. 320, ch. 2, CP doit être également considéré sous l'angle de la responsabilité des données au sens de la *let. b* : ce n'est pas la perspective hiérarchique qui prime. L'autorité responsable des données a les connaissances requises pour procéder à la pesée des intérêts indispensable.

Le signataire des conventions (convention de prestations, accord de projet, accord sur les prestations) avec les prestataires internes, en règle générale le directeur de l'office ou son suppléant, peut donner son accord.

Le fournisseur externe de prestations doit avoir accès uniquement aux données strictement nécessaires (*let. c*).

Le cas d'espèce commande les mesures contractuelles, organisationnelles et techniques adéquates. Il n'est donc pas possible d'établir des règles concrètes, valables dans tous les cas ou contraignantes, et il n'est pas non plus obligatoire de prendre ces trois types de mesures. L'autorité qui donne accès aux données doit évaluer, de concert avec l'autorité fédérale responsable des données, quelles sont les mesures judicieuses en l'espèce, c'est-à-dire nécessaires, économiquement supportables et réalisables.

- Les obligations d'effacement, les peines conventionnelles et les obligations de documentation doivent être fixées contractuellement avec les externes. Dans certains cas, il peut être nécessaire de mentionner le nom des collaborateurs externes dans le contrat (ou dans son annexe), par exemple pour des projets nécessitant un contrôle de sécurité conformément à la loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure[15].

- Des moyens organisationnels doivent être mis en place pour garantir que les externes (par ex. en accès à distance ou sur place) soient surveillés ou contrôlés lorsqu'ils traitent des données sensibles.

- Lorsqu'une telle mesure est raisonnablement exigible et techniquement réalisable, il faut également envisager d'anonymiser les données personnelles avant de les porter à la connaissance des externes.

L'inclusion des auxiliaires à l'art. 320 CP[16] a réduit considérablement le risque qu'un fournisseur interne de prestations soit punissable. La règle prévue à l'art. 11, al. 2, OTNI n'est donc pas reprise.

Art. 13 eOperations Suisse SA

Cette disposition crée la base légale concrète de la participation de la Confédération dans la société anonyme de droit privé eOperations Suisse SA. La participation elle-même fera l'objet d'une décision du Conseil fédéral et se concrétisera ensuite par l'achat d'une action eOperations Suisse SA.

Lorsque la Confédération détiendra une participation dans eOperations Suisse SA, cette dernière sera placée sous la responsabilité partagée de la Confédération, des cantons, des villes et des communes. Au-delà du fait qu'elle sera soutenue par les trois

15 RS **120**

16 En vigueur depuis le 1er janvier 2023

échelons de l'État fédéral, elle se présentera comme une structure organisationnelle et un prestataire compétent pour réaliser les projets de coopération de l'administration en matière d'informatique. Elle contribuera à l'achat groupé de solutions informatiques par les cantons et les communes et, au besoin, à leur utilisation commune pour éviter les redondances et les dépenses supplémentaires. Le siège de la société, fondée en 2018, est à Berne.

L'entreprise eOperations Suisse SA dispose d'un capital-actions de 100 000 francs. L'action a une valeur de 300 francs (valeur nominale de 100 francs et réserve de 200 francs, issue des apports en capitaux).

L'entreprise doit couvrir durablement ses coûts, mais n'a pas de but lucratif. Le fait qu'elle ne vise pas à réaliser des bénéfices est une condition fondamentale de la participation de la Confédération, en vertu du principe de la neutralité concurrentielle. La Confédération ne peut toutefois pas empêcher l'assemblée générale d'inscrire dans les statuts que l'entreprise a un but lucratif ou qu'une augmentation de capital est prévue. Si c'était le cas, la Confédération ne pourrait plus prendre de participation dans l'entreprise.

La participation dans cette entreprise est dans l'intérêt de la Confédération : faire partie d'une communauté d'achat ou d'exploitation composée de collectivités de différents niveaux lui permet de bénéficier d'économies d'échelle et donc de conditions d'achat préférentielles pour l'acquisition de produits ou de prestations informatiques. La Confédération prend une participation dans eOperations Suisse SA en acquérant une action afin de réaliser des économies lors de l'acquisition de solutions informatiques.

La participation dans eOperations Suisse SA vise en particulier à réaliser, par l'intermédiaire de l'entreprise, des projets et des procédures d'appel d'offres conjointes avec d'autres collectivités. Il s'agira essentiellement d'achats dans le domaine de l'informatique et de la fourniture de prestations informatiques. L'*al. 1, let. a et b*, définit plus précisément le catalogue des prestations d'eOperations Suisse SA. L'acquisition de moyens informatiques visée à *la let. a* renvoie en particulier à l'achat d'infrastructures numériques, de matériel informatique, de logiciels et de service de base, pour autant qu'ils soient achetés conjointement avec les cantons ou les communes. En outre, eOperations Suisse SA propose à la Confédération, aux cantons et aux communes des prestations (ou leur acquisition) liées à l'informatique (*let. b*). Au sein de l'administration fédérale, les départements et la Chancellerie fédérale sont compétents pour charger eOperations Suisse SA de fournir les prestations mentionnées.

La Confédération ne détient qu'une participation minoritaire dans la société eOperations Suisse SA et elle n'est donc pas autorisée à lui donner des directives sur son but ou ses objectifs stratégiques. Cependant, elle pourra exercer ses droits en qualité d'actionnaire. L'*al. 3* règle l'exercice des droits de l'actionnaire. Ceux-ci étant essentiellement d'ordre financier, le Département fédéral des finances (DFF) est chargé de les exercer. Afin de garantir que les considérations d'ordre technique sont prises en compte, le DFF doit agir en accord avec la Chancellerie fédérale (secteur TNI).

Concrètement, les droits de l'actionnaire s'exercent comme suit : en accord avec la Chancellerie fédérale, le DFF détermine qui participera à l'assemblée générale et soumet au Conseil fédéral l'ordre du jour, assorti de ses recommandations de vote. À l'assemblée générale, le représentant du DFF vote conformément à la décision du Conseil fédéral.

Conformément à l'art. 21, al. 1, let. a, de l'ordonnance du 1er mai 2024 sur l'organisation des marchés publics de l'administration fédérale (Org-OMP)[17], l'exécution des procédures d'adjudication peut être déléguée à eOperations Suisse SA en cas d'acquisitions communes de moyens informatiques et de services en lien avec les moyens informatiques de la Confédération, des cantons et des communes.

Par souci d'exhaustivité, on notera que la LTrans s'applique tant à la participation de la Confédération qu'à l'exécution des tâches déléguées. De plus, eOperations Suisse SA est soumise à l'obligation d'archivage sur la base de l'art. 1, al. 1, let. h, de la loi fédérale du 26 juin 1998 sur l'archivage[18] en relation avec l'art. 2, al. 3, de l'ordonnance du 8 septembre 1999 relative à la loi fédérale sur l'archivage[19].

Chapitre 4 Données des autorités fédérales

Section 1 Données ouvertes

Art. 14

L'art. 10, al. 2, LMETA définit les données qui ne sont pas soumises à l'obligation de publication prévue à l'al. 1. Entrent notamment dans cette catégorie les données dont la publication n'est pas autorisée ou n'est autorisée que de manière restreinte par des actes cantonaux (art. 10, al. 2, let. b, LMETA). Les autorités cantonales et fédérales collaborent afin de garantir l'application correcte des dérogations à l'obligation de publication.

L'art. 10, al. 4, LMETA énonce les principes qui régissent les données ouvertes : celles-ci sont mises en ligne gratuitement, en temps utile, sous une forme lisible par une machine et dans un format ouvert. Ces différentes notions étant elles aussi sujettes à interprétation — exception faite de la notion de gratuité, qu'il n'est pas nécessaire de définir plus avant dans les dispositions d'exécution —, il faut en préciser le sens dans l'ordonnance. Le législateur suisse se fonde pour ce faire sur le droit européen[20].

Les principes suivants s'appliquent à la publication des données ouvertes :

Let. a : les données sont publiées en temps utile. À l'époque de la numérisation, où tout va très vite, le facteur temps est extrêmement important et constitue par conséquent une exigence fondamentale en matière de données ouvertes. Cela étant, en fonction du type de données et du domaine dont elles relèvent, la notion de « temps utile » peut revêtir des significations très différentes. On ne peut donc pas en donner une définition absolue. Afin de répondre au mieux aux attentes de l'économie, de la société et de la recherche, il faut néanmoins publier les données aussi rapidement que possible, voire en temps réel. Cette rapidité est particulièrement importante pour les données dynamiques (notamment les données environnementales, les données du trafic, les don-

17 RS **172.056.15**
18 RS **152.1**
19 RS **152.11**
20 Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public, JO L 172 du 26.6.2019, p. 56

nées satellitaires et météorologiques et les données provenant de capteurs), qui évoluent en permanence et dont la valeur économique dépend de leur mise à disposition immédiate et de leur actualisation régulière. Il faudrait mettre à disposition les données dynamiques immédiatement après leur collecte ou leur création ou, en cas de mise à jour manuelle, directement après la modification du jeu de données, au moyen d'une API, afin de faciliter le développement d'applications Internet, mobiles et en nuage fondées sur ces données. Lorsque des contraintes techniques ou financières s'y opposent, les organismes du secteur public devraient mettre les données à disposition dans un délai permettant d'en exploiter pleinement le potentiel économique[21].

Toutes les autres données qui entrent dans le champ d'application de l'art. 10, al. 1, LMETA ne doivent pas nécessairement être publiées *immédiatement* pour ne rien perdre de leur plus-value. Dans la mesure du possible, elles doivent cependant elles aussi être publiées directement après leur collecte, leur création, leur traitement et leur compilation sous forme structurée. Il appartient à l'unité administrative concernée de déterminer quelles données doivent être publiées et dans quel délai. Elle doit tenir compte à cet effet de la nature, de la structure et de la complexité des données (données qui changent rapidement et fréquemment ou qui ne changent pas, ou dont la création exige le recours à des processus de traitement complexes), ainsi que de leur plus-value potentielle pour l'économie, la société et la recherche. Plus le cycle de modification des données est court et plus leur plus-value est élevée, plus elles doivent être publiées rapidement en tant que données ouvertes.

Il ne faut toutefois pas que les unités administratives soient contraintes de développer ou d'acquérir des systèmes hautement disponibles dans le seul but de respecter les exigences applicables aux données ouvertes. La publication des données ouvertes ne constituera pas une tâche autonome de l'administration entraînant des demandes de ressources spécifiques (cf. message LMETA[22]).

Let. b : une publication a lieu sous une forme lisible par machine. Les données lisibles par machine ou par ordinateur sont des données structurées dans un format qui permet leur traitement par un ordinateur. L'expression « lisible par une machine » n'est pas synonyme de « numérique ». Les données accessibles par voie numérique peuvent se trouver en ligne, de sorte que les personnes peuvent y accéder plus facilement au moyen d'un ordinateur. Cependant, elles peuvent difficilement être extraites, transformées et traitées par la logique de programmation informatique si elles ne sont pas également lisibles par une machine. L'un des principaux objectifs de la publication de données ouvertes est de permettre à des machines de les traiter aisément et d'éviter notamment les erreurs d'affectation et de formatage qui peuvent se produire lors de la lecture de textes ou d'informations proposés au format PDF. Les formats de fichiers publiés doivent donc être structurés de telle manière que des applications logicielles puissent facilement identifier, reconnaître et extraire des données spécifiques, notamment chaque énoncé d'un fait et sa structure interne. On épargne ainsi une charge de travail disproportionnée aux utilisateurs des données[23]. Les données, la structure des données et les modèles de données qui expliquent les variables doivent être publiés dans un format normalisé, tel que csv ou XML, ou dans des formats bien établis (c'est-à-dire répandus et acceptés par la communauté des utilisateurs), qui permettent une

21 Directive (UE) 2019/1024, consid. 31
22 FF **2022** 804
23 Cf. https://handbook.opendata.swiss/fr/content/vorbereiten/publikationsrichtlinien.html.

lecture et un traitement directs par des machines. On tiendra compte des éventuelles directives du secteur TNI (cf. art. 40, al. 1, let. d). Afin de maximiser l'utilité des données, il faut également, dans la mesure du possible, les mettre à disposition dans des interfaces lisibles par une machine, telles que celles qui figurent à l'adresse https://api3.geo.admin.ch ou https://lindas.admin.ch. Ces interfaces assurent une flexibilité maximale pour la gestion et l'utilisation des données.

Let. c : les données doivent être publiées dans un format ouvert. Conformément à la définition qui figure dans les directives de l'UE, cela signifie qu'il faut proposer les données dans un format de fichier indépendant des plateformes utilisées et mis à la disposition du public sans restriction empêchant la réutilisation des documents.

Au format ouvert s'oppose le format propriétaire : les formats de fichiers sont dits « propriétaires » lorsqu'ils ne peuvent pas être mis en œuvre par des tiers, ou seulement avec difficulté, et qu'ils ne peuvent donc pas être ouverts ou lus, par exemple du fait de l'existence de restrictions découlant de droits de licence, du savoir-faire propre au fabricant ou de brevets. Ces formats se prêtent donc moins à la réutilisation des données par des tiers. À titre d'exemples, on peut citer le format MS-Word, le format WMA ou les formats de fichiers de Lotus SmartSuite. Parmi les formats de fichiers ouverts figurent notamment les formats OpenDocument, Ogg Vorbis, Portable Network Graphics et HTML.

L'Office fédéral de la statistique (OFS), plus précisément le secrétariat pour l'Open Government Data[24] qui lui est rattaché, tient une liste des formats ouverts les plus répandus qui peuvent être utilisés pour publier des données ouvertes. Il actualise régulièrement la liste et la publie sur Internet. Les autres unités administratives peuvent à tout moment informer le secrétariat des formats ouverts qu'elles emploient. Ce dernier les ajoute à la liste s'ils remplissent les exigences auxquelles doit répondre un format ouvert.

L'al. 2 consacre la précision contenue dans le message LMETA[25] : les données provenant de travaux de recherche financés par des fonds publics ne sont pas des données administratives et, en conséquence, elles n'entrent pas dans le champ d'application de l'art. 10, al. 1, LMETA. Il en va évidemment de même de la recherche financée par des fonds privés. Les données administratives sont des données que les autorités collectent ou produisent dans l'exécution des tâches qui leur sont dévolues par la loi, c'est-à-dire des données traitées dans tous les cas et de manière systématique. Tel n'est pas le cas des données issues de la recherche, qui représentent au contraire le résultat d'un travail scientifique spécifique et ne sont donc pas traitées dans tous les cas et de manière systématique. Dans certaines circonstances, elles résultent en outre d'un processus créatif et sont protégées par le droit d'auteur.

Les lois spéciales qui régissent le domaine de la recherche (par ex. la loi fédérale du 14 décembre 2012 sur l'encouragement de la recherche et de l'innovation[26]) sont déterminantes et priment en règle générale la LMETA et l'ONum. D'autres moyens permettent par ailleurs d'offrir un accès aussi libre que possible aux données provenant des travaux de recherche, et donc de satisfaire un intérêt public majeur : sur mandat

24 Voir l'art. 10, al. 4, let. d, de l'ordonnance du 28 juin 2000 sur l'organisation du Département fédéral de l'intérieur (Org DFI ; RS **172.212.1**).
25 FF **2022** 804, p. 68 s.
26 RS **420.1**

du Secrétariat d'État à la formation, à la recherche et à l'innovation, swissuniversities a élaboré la Stratégie Nationale Suisse Open Research Data[27] et le Fonds national suisse de la recherche scientifique a publié des directives pour les chercheurs (Data Management Plan[28]), qui couvrent largement les besoins en données ouvertes issues de la recherche.

Section 2 Harmonisation

L'harmonisation des données des autorités fédérales se fonde essentiellement sur l'art. 14 LMETA et en partie sur les art. 12 et 13 LMETA. Les dispositions de la présente section s'appliquent donc aux autorités fédérales soumises à la LMETA.

Art. 15 Principes

Pour qu'un relevé conforme au principe de la collecte unique des données et une utilisation multiple soient possibles, les données doivent être interopérables sur les plans juridique, organisationnel, technique et sémantique. La présente section ne couvre que l'harmonisation des données d'un point de vue *sémantique*.

L'*al. 1* précise cet aspect. Il faut garantir que toutes les données des autorités fédérales soumises aux art. 12 à 14 LMETA qui ont la même signification soient décrites de la même manière afin d'être sémantiquement interopérables.

Pour y parvenir, on a mis en œuvre le modèle de rôles de l'administration des données (*data stewardship*), qui prévoit entre autres, sous la coordination de l'administrateur suisse des données rattaché à l'OFS, une étroite coopération entre toutes les unités concernées, notamment entre les services spécialisés qui disposent de connaissances spécifiques. Ce modèle garantit que la coordination et la coopération nécessaires à la mise en place de normes sémantiques uniformes pour les données des autorités fédérales suivent un schéma clairement défini et qu'elles contribuent à la mise en œuvre des principes de la collecte uniqueet de l'utilisation multiple des données. L'autorité fédérale compétente reste chargée de la gestion effective des données, afin d'éviter que toutes les données de la Confédération soient conservées en un seul lieu.

Le modèle de rôles prévoit en particulier les rôles suivants :

a. Administrateur suisse des données (swiss data steward) : rattaché à l'OFS sur la base de l'art. 10, al. 4, let. a, Org DFI, ce rôle est, dans les faits, assumé par le directeur de l'OFS, qui peut le déléguer à une ou plusieurs autres personnes. Assigner cette tâche aux autorités fédérales compétentes dans le domaine spécialisé concerné comporterait le risque que chaque unité fasse avancer unilatéralement l'harmonisation et la standardisation des données de son domaine, sans prendre suffisamment en compte les besoins transversaux. Dans de telles conditions, il serait difficile d'assurer l'interopérabilité des données et de mettre en œuvre les principes de la collecte et de l'utilisation multiple des données. Il ne serait donc guère pertinent, en l'état actuel des

27 Publiée en juillet 2021 : https://www.swissuniversities.ch/fr/themes/open-science/open-research-data/strategie-nationale

28 https://www.snf.ch/fr/FAiWVH4WvpKvohw9/dossier/points-de-vue-politique-de-recherche

choses, de confier le rôle d'administrateur suisse des données à l'autorité fédérale compétente dans le domaine spécialisé concerné.

L'administrateur suisse des données a pour tâche de faire avancer et d'accompagner le processus d'harmonisation des données de la Confédération de sorte que toutes les données dont la signification (sémantique) est identique soient décrites de la même manière et soient donc échangeables. Cependant, il ne lui incombe pas de définir le contenu de certaines données. Par exemple, s'agissant de véhicules, il n'appartient pas à l'OFS de définir ce qu'est précisément un véhicule. Cette tâche est du ressort des spécialistes et des services spécialisés. Par contre, il appartient à l'OFS de définir une norme sémantique commune, qui soit comprise de la même manière par toutes les autorités fédérales et permette à celles-ci d'harmoniser leurs données dans l'ensemble des services de la Confédération. Pour y parvenir, l'OFS doit encourager le développement et le bon fonctionnement du modèle de rôles et de processus de l'administration des données (*data stewardship*), de même que la publication de toutes les métadonnées. L'interopérabilité des données de la Confédération ne sera garantie qu'à cette condition. Cependant, comme les différents domaines (sémantique, technique, organisationnel et juridique) de l'interopérabilité ne peuvent pas être totalement dissociés, une étroite coopération entre l'OFS et le secteur TNI s'impose. Cette coopération est notamment assurée par la direction conjointe de l'organe spécialisé Conseil des données de la Confédération.

b. Administrateur des données transversales : de nombreux aspects concernent toutes les autorités fédérales ou du moins nombre d'entre elles, en particulier les services spécialisés, de la même manière, quel que soit leur domaine. Il faut donc garantir que les intérêts de ces domaines transversaux sont également pris en compte dans l'harmonisation et la standardisation des données axées sur les domaines spécialisés. Neuf thèmes transversaux ont été identifiés :

- statistique
- gestion des données
- données de référence
- sécurité de l'information
- science des données
- données ouvertes
- géoinformations
- archivage des données
- structure et sauvegarde des données.

Pour chacun de ces thèmes transversaux, il faut une ou plusieurs personnes qui se chargent d'administrer les données transversales. Ces personnes sont des membres permanents de l'organe spécialisé. Le rôle d'administrateur des données transversales est rattaché à l'autorité fédérale responsable du domaine concerné :

Statistique : OFS

Gestion des données : OFS

Données de référence : secteur TNI

Sécurité de l'information : DDPS

Science des données : OFS, centre de compétences en matière de science des données (DSCC)

Données ouvertes : OFS, secrétariat OGD

Géoinformations : organe de coordination de la géoinformation au niveau fédéral (GCS) qui délègue une unité administrative

Archivage des données : Archives fédérales suisses

Structure et sauvegarde des données : Conférence des prestataires de services informatiques (CPSI)

c. Administrateur local des données (local data steward) : ce rôle consiste à gérer les métadonnées et les données de son unité d'organisation (y compris les départements), à les harmoniser conformément aux normes sémantiques fixées pour un domaine thématique spécifique (métadonnées) et à rendre les métadonnées correctement et complètement accessibles dans le catalogue de métadonnées de la plateforme d'interopérabilité (14Y-IOP[29]), visé à l'art. 14, al. 2, LMETA. L'administrateur local des données s'acquitte de cette tâche selon les instructions données par la personne responsable du traitement des données dans son domaine (propriétaire des données ou *data owner*). Il est responsable de la description correcte et complète des contenus et des structures des données ainsi que de leur qualité au sein de son unité d'organisation. Il lui incombe aussi de définir les exigences par rapport à la conservation, à la qualité et à l'utilisation des données que le consignataire local des données (*local data custodian*) met en œuvre sur le plan technique. L'administrateur local des données collabore étroitement avec le propriétaire des données de son unité d'organisation et avec le consignataire des données. La personne qui assume ce rôle est aussi responsable de la préparation et de la publication des données ouvertes. Puisque, lors de l'élaboration des normes au sein des groupes de travail thématiques, les demandes des domaines transversaux sont prises en compte, leurs besoins sont intégrés dans les normes harmonisées. Par conséquent, l'administrateur local des données participe aussi dans tous les cas à la mise en œuvre des exigences liées à la publication des données ouvertes, à la production statistique ou aux géoinformations.

d. Responsable du traitement des données (propriétaire des données) : dans le jargon international de l'administration des données, ce rôle est appelé *data owner*. Il est assumé par une ou plusieurs personnes de l'autorité fédérale compétente. Cette dernière correspond au responsable du traitement visé à l'art. 5, let. j, de la loi fédérale du 5 25 septembre 2020 sur la protection des données (LPD)[30], mais renvoie en l'occurrence par analogie à toutes les autorités, indépendamment du fait qu'elles traitent uniquement des données personnelles ou uniquement des données non personnelles. Le responsable du traitement est entièrement soumis à la LPD et exécute ses tâches, en particulier le traitement des données visé à l'art. 5, let. d, LPD conformément à la LPD

29 L'abréviation « I14Y » symbolise le terme anglais *interoperability* : la première lettre est « i », elle est suivie de « 14 » lettres et la dernière lettre est « y ».

30 RS **235.1**

et aux ordonnances pertinentes. Il en va de même des données dont il confie le traitement à un sous-traitant (art. 5, let. k, LPD). Il collabore avec le conseiller à la protection des données de l'office ou du département.

L'al. 2 prévoit que les données ne doivent pas être harmonisées à n'importe quel moment, mais en fonction du cycle de vie de l'ensemble de données.

Art. 16 Coordination des autorités

L'*al. 1* décrit les tâches clefs de l'OFS dans son rôle d'administrateur suisse des données. Assumant un rôle dirigeant dans l'administration des données, il développe les instruments nécessaires à l'harmonisation. Il a notamment pour tâches de développer et d'exploiter la plateforme d'interopérabilité I14Y et de créer des organes aptes à coordonner et à intégrer, dans une large mesure, toutes les autorités concernées. Ces organes n'ont généralement pas la compétence de prendre des décisions contraignantes.

L'organe *spécialisé dans la gestion et l'interopérabilité des données de l'administration fédérale* est déjà en place.

Il a été créé pour accompagner la mise en œuvre opérationnelle de la gouvernance des données au sein des unités des autorités fédérales. Cet organe spécialisé se réunit sous la présidence de la Chancellerie fédérale et du DFI. Il répond au besoin de coordonner efficacement les projets et les tâches dans le domaine de la gestion et de l'interopérabilité des données. Il s'agit d'exploiter les éventuelles synergies et d'encourager l'apprentissage conjoint ainsi que l'échange de connaissances, notamment en s'appuyant sur les bonnes pratiques existantes. L'organe spécialisé sera chargé de tâches liées spécifiquement à la gestion et à l'interopérabilité des données de l'administration fédérale et encouragera ainsi simultanément la mise en œuvre des directives stratégiques du Conseil fédéral et des organes du modèle de gouvernance de l'informatique de la Confédération. À cet effet, les organes suivants seront intégrés à cet organe spécialisé :

- le groupe de travail interdépartemental Gestion nationale des données (NaDB) ;
- le groupe de travail interdépartemental Données ouvertes ;
- la Gestion commune des données de base de la Confédération ;
- en outre, l'organe spécialisé sera responsable des aspects stratégiques de la science des données (pour lequel il n'existe pas encore de groupe de travail interdépartemental).

Trois éléments déterminent le travail et la composition de l'organe spécialisé :

- Les thèmes transversaux, intégrés dans l'organe spécialisé sur le plan institutionnel (c'est-à-dire par un siège propre au sein de l'organe). Neuf thèmes transversaux sont définis aujourd'hui (cf. commentaire de l'art. 15). Il existe pour chaque thème transversal une sous-structure indépendante pour la mise en œuvre opérationnelle, qui est organisée différemment selon les responsabilités des offices et des départements. Autrement dit, selon le thème transversal, il se peut qu'il n'y ait qu'un seul organisme, qui réunit des représentants régionaux et

nationaux, ou qu'il y ait plusieurs organismes, comme dans le domaine des géodonnées (la GCS au niveau fédéral et la Conférence des services cantonaux de la géoinformation et du cadastre au niveau des cantons) ou de la statistique (Fedestat pour le niveau fédéral et Regiostat pour le niveau régional).

- Les thèmes pertinents : des secteurs spécialisés (par ex. la mobilité) sont intégrés à l'organe spécialisé en fonction de la situation politique actuelle. En conséquence, des membres supplémentaires siègent temporairement au sein de l'organe.

- Une série d'aspects thématiques généraux seront discutés au sein de l'organe spécialisé : l'éthique des données ; la protection des données ; l'intégrité des données ; la qualité des données ; les normes (internationales) ; les processus (réutilisabilité) ; la maintenance des données ; la conformité des données ; l'accès technique et juridique aux données (valeur ajoutée fondamentale de la gestion des données).

L'organe spécialisé est opérationnel depuis le 1er janvier 2023. Il faudra peut-être l'adapter en raison des expériences acquises, par exemple en ce qui concerne sa composition et ses domaines de tâches.

Autres organes

Dans son rôle d'administrateur suisse des données, l'OFS doit développer les instruments et outils adéquats pour harmoniser et standardiser les données. Cette responsabilité peut aussi impliquer l'institution d'organes ou de groupes de travail supplémentaires chargés d'accomplir une tâche concrète. Comme tous les besoins ne sauraient être identifiés d'emblée et que certaines tâches ne requièrent pas forcément des organes ou des groupes de travail sur le long terme, il ne serait pas logique de définir d'ores et déjà des organes supplémentaires dans l'ordonnance. Cette tâche incombe à juste titre à l'administrateur suisse des données, qui a des tâches concrètes. Par exemple, à long terme, un organisme pourrait être institué dans le contexte international pour assurer l'échange de connaissances entre les unités administratives de la Confédération et les autres acteurs éventuels. Une telle mesure permettrait à la Confédération de suivre une ligne uniforme sur le plan international en matière de gestion des données. On pourrait également citer d'autres domaines, par exemple la science des données ou les données ouvertes. Le cas échéant, l'OFS aura la responsabilité de coordonner les travaux des divers organismes.

La pertinence de l'organe de coordination pour l'harmonisation des données de la Confédération est à l'étude. Cet organe est présidé par l'administrateur suisse des données. Ses membres, à savoir la personne responsable de la division Interopérabilité et registres de l'OFS et les administrateurs de données des départements, se réunissent quatre fois par an. Ils assument diverses tâches :

- soutenir activement les travaux d'harmonisation prévus ;

- informer sur des projets pertinents au sein de leur unité d'organisation ;

- élaborer la feuille de route des travaux d'harmonisation spécifique à chaque thème ;

- assurer la circulation des informations entre les départements et les offices ;
- s'informer de l'état d'avancement des groupes de travail opérationnels ;
- détacher des représentants dans les groupes de travail opérationnels au niveau des offices et des départements ;
- s'informer, dans le cadre des séances régulières, des discussions menées au sein de l'organe spécialisé dans la gestion des données et de l'interopérabilité ;
- définir, dans le cadre des séances régulières, le contenu des rapports établis par l'organe de coordination à l'intention de l'organe spécialisé.

L'*al. 2* rappelle que l'OFS, dans son rôle d'administrateur suisse des données, n'impose pas aux autres autorités fédérales la manière de présenter les métadonnées (normes) : il leur propose seulement son aide pour trouver, si possible dans tous les domaines, des formes de présentation communes et pour rendre toutes les métadonnées accessibles sous la forme la plus appropriée à un cercle d'utilisateurs aussi large que possible. Par exemple, les géodonnées sont d'ores et déjà référencées sur geocat.ch selon une autre norme que celle utilisée sur la plateforme d'interopérabilité de l'OFS.

Art. 17 Coordination dans les domaines transversaux

Les intérêts et les besoins d'harmonisation des domaines transversaux sont couverts par le rôle de l'administrateur des domaines transversaux. Ce rôle est nécessaire pour garantir que les compétences déjà clairement définies par la loi dans certains domaines n'entrent pas en conflit avec le modèle de rôles généralement applicable dans l'administration des données. Par exemple, la loi du 5 octobre 2007 sur la géoinformation (LGéo)[31] prévoit une réglementation claire pour l'harmonisation des géodonnées, laquelle conserve toute sa validité. Afin de garantir l'harmonisation, tous domaines et autorités confondus, il est nécessaire d'intégrer les besoins d'harmonisation du domaine transversal « géodonnées » dans les besoins d'harmonisation globaux. Pour ce faire, il faut que, sous la houlette du GCS, le domaine transversal soit pris en compte dans les travaux et les organes de l'administration des données.

Les compétences concernant les neuf domaines transversaux ont été définies en collaboration avec tous les départements au sein du groupe de travail temporaire sur la nouvelle « ordonnance sur le traitement des données »[32].

Art. 18 Procédure

Al. 1 : l'OFS présente régulièrement à l'organe spécialisé dans la gestion et l'interopérabilité des données une feuille de route (liste) contenant les besoins d'harmonisation actuels. Il tient compte du cycle de vie des données (dans quel domaine elles doivent

31 RS **510.62**

32 Les articles relatifs à l'harmonisation des données ont été initialement intégrés dans la révision totale de l'ordonnance concernant l'exécution des relevés statistiques fédéraux et de l'ordonnance concernant l'organisation de la statistique fédérale, dont le titre court était « ordonnance sur le traitement des données ».

être harmonisées et quand). Il n'est pas possible d'harmoniser tous les domaines simultanément. La première fois, ce sera le Conseil fédéral qui demandera l'établissement de cette feuille de route relative à l'harmonisation. Par la suite, l'OFS la tiendra à jour, en accord avec les départements, de manière à pouvoir la soumettre régulièrement à l'organe spécialisé dans la gestion et l'interopérabilité des données.

L'*al. 2* prévoit que l'OFS crée des groupes de travail thématiques qui assumeront concrètement les tâches d'harmonisation et de standardisation dans un domaine thématique (par ex. la santé, l'agriculture). Il est essentiel que les connaissances spécialisées du domaine à harmoniser soient représentées dans ces groupes de travail, raison pour laquelle les administrateurs locaux de données concernés doivent absolument être impliqués dans le projet. Comme mentionné plus haut, un groupe de travail thématique dans le domaine des géodonnées existe déjà au niveau fédéral, le GCS, qui est un organe de coordination au sens de l'art. 55 LOGA. En tant qu'administrateur suisse des données, l'OFS informe d'une manière adéquate les autorités fédérales qui doivent être informées et celles qui sont intéressées de même que les représentants des thèmes transversaux de la création des groupes de travail. Il doit veiller à ce que tous soient représentés dans le groupe de travail. Les autorités fédérales concernées désignent la ou les personnes qui assumeront le rôle d'administrateur local des données et seront détachées dans les groupes de travail.

L'*al. 3* précise que les groupes de travail thématiques élaborent *ensemble* les normes et qu'ils se mettent si possible d'accord sur une norme unique. Cependant, il peut très bien arriver que plusieurs normes doivent être définies, puisque les besoins des unités administratives concernées sont très différents. Dans de tels cas, il doit être possible d'admettre plusieurs normes. De plus, l'unité d'organisation responsable du domaine visé devrait en principe prendre la décision concernant la norme sémantique qui doit être définie. L'OFS, en sa qualité d'administrateur suisse des données, ne fixe donc pas seul, ni de sa propre initiative, les nouvelles normes sémantiques. Il doit seulement veiller à ce que les spécialistes et services spécialisés concernés se réunissent et qu'ils élaborent ensemble une norme unique. Dans ce contexte, il faut aussi tenir compte des normes existantes, notamment de celles établies à l'échelle internationale. En règle générale, il n'est ni possible ni souhaitable de remplacer celles-ci par de nouvelles normes. Par contre, on peut les étendre à d'autres domaines. Il se peut aussi qu'il ne soit pas pertinent d'appliquer une seule norme en raison de besoins très divergents. Dans de tels cas, il doit rester possible de définir plusieurs normes. Toutefois, pour autant que cela soit possible et judicieux, on tentera de rechercher *une* norme commune.

L'al. 4 définit les responsabilités quant à la publication et à l'actualisation des métadonnées. Pour que l'harmonisation et la standardisation des données des autorités fédérales puissent effectivement contribuer à leur utilisation multiple, il est indispensable que leurs descriptions (métadonnées) soient accessibles à tous de manière centralisée. C'est la seule façon pour une unité d'organisation de savoir si les données dont elle a besoin pour remplir ses tâches sont déjà disponibles — dans la forme et la qualité adéquates — auprès d'une autre unité d'organisation. La publication et la gestion effectives des métadonnées sur la plateforme I14Y-IOP de l'OFS incombent aux autorités fédérales compétentes. Toutefois, en tant qu'administrateur suisse des données,

l'OFS a pour tâche de promouvoir la publication des métadonnées harmonisées sur I14Y-IOP et, le cas échéant, d'apporter son soutien.

L'*al. 4* précise en outre que la description et l'harmonisation des données sont des tâches récurrentes. Pour que ces tâches de description et d'harmonisation puissent être accomplies de manière aussi efficiente et efficace que possible, elles doivent être effectuées progressivement par domaine thématique. L'administrateur suisse des données informe régulièrement l'organe spécialisé des thèmes et domaines faisant l'objet d'une harmonisation et du moment où celle-ci est effectuée. À des fins de planification, les départements élaborent une feuille de route sous la coordination de l'administrateur suisse des données. Il faut éviter que des cimetières de données ne soient créés et que des données continuent d'être décrites et sauvegardées alors qu'elles ne sont plus utilisées. L'expérience montre que le cycle de vie des données est d'environ cinq ans. Passé ce délai, il faut vérifier si les données conservent leur pertinence et, le cas échéant, si leur description reste correcte ou si elle doit être adaptée. L'art. 18 règle concrètement le processus d'harmonisation et de standardisation des données fondé sur le modèle de rôles de l'administration des données (*data stewardship*), déjà connu à l'étranger.

Al. 5 : en tant qu'administrateur suisse des données, l'OFS n'a pas pour tâche de gérer toutes les données des autorités fédérales devant être harmonisées selon le modèle de processus et de rôles. Il se limite à coordonner le processus d'harmonisation des données : la gestion effective des données et donc leur harmonisation effective incombent aux unités d'organisation. Celles-ci appliquent les normes à leurs données conformément aux spécificités locales. De ce fait, les unités d'organisation ont la responsabilité d'adapter *leurs* données selon les normes définies conjointement dans les groupes de travail, d'en publier la description sur la plateforme I14Y-IOP et de l'actualiser. Conformément au modèle de rôles, cette tâche incombe aux administrateurs locaux de données en collaboration avec les consignataires locaux des données. Pour que l'interopérabilité obtenue grâce à l'harmonisation et à la standardisation porte vraiment ses fruits, les données doivent toujours être actuelles. Cette tâche est également du ressort de l'administrateur local des données, qui peut publier les métadonnées standardisées de son domaine directement sur la plateforme I14Y-IOP. Il peut aussi les publier sur une plateforme distincte, pour autant que celle-ci soit directement reliée à I14Y-IOP.

Art. 19 Métadonnées

Al. 1 : l'OFS met le catalogue des métadonnées à la disposition du public sur la plateforme I14Y-IOP pour que celui-ci puisse être connu et utilisé par tous (art. 14, al. 2, LMETA). Pour des raisons de sécurité juridique et de transparence, le Conseil fédéral doit au moins déterminer le contenu de ces métadonnées, mais leur forme concrète sera définie dans le cadre du processus décrit aux art. 15 à 18. Les métadonnées doivent notamment contenir l'unité d'organisation responsable des données, le type d'accessibilité (les données sont-elles ouvertes et, si tel n'est pas le cas, pourquoi ne le sont-elles pas ?), les conditions concrètes de l'accès aux données ou l'information qu'elles ne sont pas accessibles (*let. a*). Les contenus des métadonnées figurant sur

la plateforme I14Y-IOP doivent répondre aux normes nationales et internationales établies, soit actuellement au DCAT-AP-CH. Toutefois, ces normes ne sont pas immuables et peuvent changer de nom. C'est pourquoi l'ordonnance ne définit pas une norme précise. L'OFS, qui exploite la plateforme I14Y-IOP, a la responsabilité de garantir la compatibilité de la description des métadonnées enregistrées sur la plateforme avec les normes nationales et internationales.

La structure des données, les nomenclatures et les critères de qualité doivent aussi être indiqués dans les métadonnées. Comme les critères de qualité requis sont encore en voie d'élaboration, qu'ils changent constamment et qu'ils ne s'appliquent parfois qu'à certains domaines, on a renoncé à les décrire plus précisément dans l'ordonnance. L'OFS les décrira dans un règlement de traitement des données qui pourra être adapté chaque année. Un critère de qualité peut par exemple être l'actualité des métadonnées ou l'indication que les données ont été contrôlées ou non. L'OFS expliquera en outre de manière plus détaillée dans le règlement de traitement des données ce qu'il faut entendre par structure des données (art. 14, al. 2, LMETA).

La Confédération ne peut édicter des prescriptions dans le domaine de la gestion (générale) des données qu'au niveau fédéral. Hors du domaine de la statistique publique, elle ne dispose d'aucune compétence constitutionnelle lui permettant de prescrire aux cantons, aux communes et aux particuliers comment ils doivent décrire et gérer leurs données. De ce fait, l'art. 14 LMETA ne s'applique qu'aux autorités fédérales, c'est-à-dire à l'administration fédérale centrale et à l'administration fédérale décentralisée, dans la mesure où celle-ci ne s'est pas exclue totalement ou partiellement du champ d'application de la loi, et, le cas échéant, aux Services du Parlement, aux tribunaux fédéraux et au Ministère public de la Confédération. Or, la transition numérique doit, à long terme, s'effectuer à tous les niveaux fédéraux, c'est pourquoi la plateforme I14Y-IOP doit être aussi à la disposition des cantons et des communes (cf. art. 14, al. 3, LMETA). La publication des métadonnées des services cantonaux et communaux est importante notamment parce qu'elle représente une plus-value manifeste pour les échanges électroniques de données au niveau régional.

À *l'al. 2*, le Conseil fédéral habilite l'OFS, en accord avec la Chancellerie fédérale, à décrire plus en détail les métadonnées qu'il a définies et à en préciser la forme pour leur publication sur la plateforme I14Y-IOP (cf. art. 14, al. 2, LMETA).

Al. 3 : en qualité d'exploitant de la plateforme d'interopérabilité, l'OFS définit les conditions concrètes d'utilisation de celle-ci et les modalités du processus (demande, examen, décision, publication, liens, modes d'accès, heures d'accès, responsabilité en cas de panne, fenêtres de maintenance, etc.). Il peut ainsi, à moindre coût, assurer également un contrôle général de la qualité.

Dans le domaine des géodonnées de base, il existe déjà des dispositions légales spécifiques. Pour les métadonnées des géodonnées de base qui relèvent du droit fédéral,

c'est-à-dire qui se fondent sur un acte législatif fédéral, la norme SN 612050[33] s'applique dans toute la Suisse depuis le 1er juillet 2008[34]. Afin de garantir l'harmonisation à l'échelle nationale, l'interopérabilité avec les infrastructures de géodonnées cantonales et la compatibilité internationale, cette réglementation dérogatoire des géométadonnées doit être maintenue conformément à *l'al. 4* et primer l'art. 19. Les géométadonnées sont accessibles au public à l'adresse geocat.ch et doivent pouvoir être reliées à partir de la plateforme I14Y-IOP. En créant ce lien, l'OFS et swisstopo garantissent la publication sur la plateforme I14Y-IOP et la libre accessibilité des métadonnées. Cette dérogation est mentionnée de manière transparente à l'*al. 4*.

Section 3 Système GDR

Art. 20 But du système et responsabilité de l'exploitation

Dans le système de gestion des données de référence (GDR), les données de personnes et d'organisations qui exécutent des processus d'affaires en matière de finances et de comptabilité, de trafic des paiements, d'acquisition, de gestion immobilière et de logistique sont gérées de manière centralisée au niveau fédéral (*al. 1*). Ces données sont définies de manière uniforme et gérées pendant toute la durée de leur utilisation. Elles sont saisies une seule fois, gérées et actualisées au fur et à mesure, afin d'être ensuite mises à la disposition des diverses applications informatiques spécialisées dans une qualité et une actualité aussi élevées que possible. Grâce à la gestion centralisée des données et à la mise en œuvre aussi poussée que possible du principe de collecte unique des données dans le traitement des processus de soutien utilisés à l'échelle fédérale, la charge de travail diminue pour la Confédération comme pour les entreprises.

Les processus d'affaires en matière de finances et de comptabilité, de trafic des paiements, d'acquisition, de gestion immobilière et de logistique sont des processus opérationnels transversaux internes à l'administration, qui facilitent l'exécution des tâches (processus de soutien).

Les processus de soutien de la Confédération suivants sont pris en charge par le système GDR :

- processus financiers au sens du droit sur les finances de la Confédération ;
- processus d'acquisition au sens du droit des marchés publics ;
- gestion immobilière et logistique (y compris distribution) au sens de la législation militaire et de l'ordonnance du 5 décembre 2008 concernant la gestion de l'immobilier et la logistique de la Confédération[35].

---

33 Art. 6 de l'ordonnance du 26 mai 2008 de l'Office fédéral de topographie sur la géoinformation (RS **510.620.1**)

34 Édition 2005-05, Mensuration et information géographique — Modèle de métadonnées GM03 — Modèle de métadonnées suisse pour les géodonnées. Cette norme est compatible avec l'ancienne norme ISO 19115:2003, Information géographique — Métadonnées et la norme actuelle ISO 19115-1:2014 Information géographique Métadonnées.

35 RS **172.010.21**

Le processus de soutien « distribution » » est compris comme faisant partie intégrante du processus de soutien « logistique » et peut exploiter les données centralisées du système GDR.

Les processus de soutien en matière de personnel ne sont pas pris en charge par le système GDR. Le système SAP de l'administration fédérale ne prévoit pas d'interface entre le système GDR et les systèmes d'information concernant le personnel pour des motifs liés à la protection des données, raison pour laquelle le domaine du personnel n'est pas touché par la centralisation des données de référence dans le système GDR.

Les processus spécifiquement fiscaux de l'Administration fédérale des contributions (AFC) ne sont pas non plus pris en charge par le système GDR. Afin de protéger au mieux le secret fiscal, l'AFC travaille avec une solution séparée pour la gestion de ses données de référence, raison pour laquelle aucune interface avec le système GDR n'est actuellement mise en place pour la prise en charge de ce processus.

L'*al. 2* prévoit que l'Administration fédérale des finances (AFF) est responsable de l'exploitation du système GDR. Cette tâche est prévue à l'art. 9, al. 2 ^{bis}, de l'ordonnance du 17 février 2010 sur l'organisation du Département fédéral des finances[36]. L'exploitation de l'ensemble du système, sa sécurité, sa maintenance et l'assistance relèvent de donc de la compétence de l'AFF, qui sera assistée par des tiers. La responsabilité du système (propriété et exploitation technique) est assumée par différents domaines de l'AFF. Cette dernière établit l'analyse des besoins de protection et, si nécessaire, le plan de sécurité de l'information et de protection des données. Elle a en outre établi un règlement de traitement, conformément à l'art. 6 de l'ordonnance du 31 août 2022 sur la protection des données (OPDo)[37].

Art. 21 Données

Le domaine central du système GDR contient exclusivement des données de référence nécessaires à l'exécution de processus de soutien pris en charge. Ces « données centralisées » constituent le « fichier d'adresses électroniques » de l'administration fédérale : Elles sont nécessaires aux opérations d'affaires des processus de soutien pris en charge. En font partie les données visées aux *let. a à i*, c'est-à-dire le numéro d'identification non personnel généré par le système GDR lors de la saisie de la personne ou de l'organisation (*let. a*), les données d'identification (*let. b*), la langue de communication avec la personne ou l'organisation (*let. c*) et les coordonnées personnelles (*let. d*). Pour les entreprises, la saisie comprend également la forme juridique (*let. e*) et les informations sur le secteur (*let. f*). Ces dernières résultent en particulier de la reprise du code de la nomenclature générale des activités économiques (NOGA) figurant dans le registre des numéros d'identification des entreprises (IDE) ou dans celui des entreprises et des établissements (REE). Pour les entreprises du domaine de l'armement, le code CAGE est en outre saisi. Les coordonnées bancaires (*let. g*) sont également saisies en tant que données de référence centralisées. En font partie toutes les indications qui permettent à un service (ci-après « utilisateur ») qui utilise le système GDR pour exécuter des processus d'affaires d'effectuer des virements bancaires à une personne ou une organisation, par exemple le nom de la banque, le nom du titulaire du

36 RS **172.215.1**
37 RS **235.11**

compte, le numéro du compte ou le numéro IBAN. Les relations entre d'autres personnes ou organisations saisies dans le système *(let. h*) peuvent également être saisies dans le système GDR, pour autant qu'elles soient nécessaires aux processus de soutien pris en charge. La saisie des coordonnées des personnes à contacter : si une entreprise indique une personne à contacter qui est juridiquement indépendante d'elle (par ex. une fiduciaire qui tient sa comptabilité), cette personne doit être saisie séparément dans le système et mise en relation avec l'entreprise. Dans ce cas également, seules doivent être saisies les données de la personne qui sont nécessaires à l'exécution du processus de soutien pris en charge. En règle générale, les données nécessaires sont nettement moins nombreuses que celles de l'entreprise qui a déclenché le processus de soutien. Autre exemple de saisie d'un lien avec une autre personne ou organisation saisie dans le système : les consortiums ou les communautés de soumissionnaires dans les procédures de marchés publics. Chaque membre de la communauté de soumissionnaire est saisi séparément dans le système, puis mis en relation avec les autres membres de cette communauté. Les numéros de registre visés à la *let. i* sont nécessaires pour identifier une personne ou une organisation de manière univoque. Les numéros sont repris des registres existants. Il est actuellement prévu d'enregistrer les numéros de registre suivants : IDE, numéros REE, numéros DUNS (*Data Universal Numbering Système* du prestataire privé Dun & Bradstreet) et numéro d'identification fiscale pour les entités IDE ayant leur domicile ou leur siège à l'étranger. Pour les personnes et les organisations ayant leur siège en Suisse, le numéro TVA est saisi en même temps que l'IDE. La *let. i* permet également de saisir le numéro AVS pour identifier les personnes physiques.

Selon le processus de soutien pris en charge, d'autres données de référence sont nécessaires (*let. j*), par exemple les données de périmètre comptable pour les processus de soutien en matière de finances. En font partie les données comptables internes à la Confédération telles que le périmètre comptable ou le compte collectif et les données de rappel (délais de paiement, destinataire du rappel, etc.) qui ont été convenues avec la personne ou l'organisation. Les données de périmètre comptable sont nécessaires pour que le justificatif de comptabilisation relatif à la réception ou à la sortie du paiement puisse être établi et que la comptabilisation puisse être effectuée sur cette base. D'autres données de référence sont au surplus nécessaires pour le traitement automatique des opérations d'affaires des processus de soutien en matière d'acquisition, de gestion immobilière ou de logistique. Il s'agit en l'occurrence d'informations d'achat et de distribution telles que le nom de l'organisation de vente, le mode de distribution ou le groupe d'imputation sur lequel le système GDR comptabilise automatiquement le justificatif d'achat ou de vente. Une liste détaillée de toutes les données traitées dans le domaine central du système GDR figurera dans le règlement de traitement au sens de l'art. 6 OPDo et pourra être demandée en tout temps à l'AFF. Toutes les données centralisées du système GDR proviennent exclusivement des sources mentionnées à l'art. 22.

La conception des processus de soutien pris en charge évolue avec le progrès technique. En fonction de cette évolution, il se peut que de nouvelles données de référence deviennent nécessaires ou que des données saisies dans le système GDR deviennent superflues pour le traitement des processus de soutien pris en charge. Le catalogue de données devrait évoluer constamment. Des champs de données supplémentaires ne pourront toutefois être ajoutés qu'à la condition qu'ils portent sur des données non

sensibles (cf. à ce sujet l'*al. 3*) et qu'ils soient effectivement nécessaires pour le traitement de processus de soutien pris en charge. Dans le cadre du processus de gestion des changements, le comité spécialisé (comité consultatif sur les changements) décide de l'ajout de champs de données après avoir entendu le spécialiste du processus de soutien. En raison de l'évolution permanente du catalogue des données gérées dans le système GDR, le texte de l'ordonnance ne détaille pas les champs.

Le système GDR est un système de gestion des données de référence à la disposition de toute l'administration fédérale. Il sert en premier lieu à la gestion centralisée des données dont des personnes ou des organisations ont besoin pour traiter les processus de soutien pris en charge (cf. commentaire de l'*al. 1*). Cependant, les capacités du système GDR permettent de gérer bien d'autres données de référence comme le plan comptable, les fichiers des banques ou les monnaies étrangères et même des données qui ne servent qu'à un cercle restreint d'utilisateurs (*custom objects*) et ne sont donc pas gérées de manière centralisée. L'Office fédéral de la douane et de la sécurité des frontières, par exemple, gère les tarifs des douanes dans un domaine du système GDR à accès limité. L'*al. 2* rappelle que l'utilisateur doit veiller lui-même à la création d'une base légale s'il veut gérer des données personnelles dans le système GDR. Cette base légale doit tenir compte de tous les aspects pertinents en matière de protection des données, tels que le but du traitement, la désignation des données saisies dans le système GDR, les sources des données, les droits d'accès et la responsabilité en matière de protection des données. Aucune base légale n'est nécessaire pour la gestion de données purement techniques. En pareil cas, l'utilisateur reste cependant responsable de la prise en charge des coûts et du respect des éventuelles prescriptions en matière de protection de l'information. Responsable de l'ensemble du système GDR (cf. art. 20, al. 2), l'AFF est également responsable, jusqu'à un certain point, de la licéité du traitement des données saisies dans le système. Elle peut par conséquent exiger du futur utilisateur la preuve que les bases légales nécessaires ont été créées. Par ailleurs, l'utilisateur qui a l'intention de saisir des données de référence pour son propre compte dans le système GDR doit prendre contact avec l'AFF à un stade précoce, afin de procéder aux clarifications techniques nécessaires.

Seules les données personnelles au sens de l'art. 5, let. a, LPD peuvent être traitées dans le système GDR. Aucune donnée sensible ne peut être gérée dans le système et aucun profilage ne peut être effectué avec les données saisies (*al. 3*). Les mesures techniques et organisationnelles qui le permettraient font encore défaut.

Art. 22 Sources de données

Les données de personnes et d'organisations sont saisies dans le système GDR en vue d'une utilisation transversale dès qu'une relation déclenchant un processus de soutien pris en charge est établie. Peu importe que le premier contact émane d'une autorité fédérale, d'un particulier ou d'une entreprise et qu'il aboutisse à un résultat concret. C'est par exemple le cas d'une demande d'offres dans une procédure d'acquisition. La personne ou l'organisation peut déjà être saisie dans le système GDR, bien qu'on ne sache pas encore si elle remettra une offre.

Les données de référence peuvent être saisies ou modifiées de deux manières dans le domaine central du système GDR :

- Une personne ou une organisation dépose une demande de saisie ou de modification de ses données de référence dans un portail électronique en amont du système GDR. Après que les données saisies dans la demande ont fait l'objet d'une vérification automatique ou effectuée par un collaborateur spécialisé, elles sont transférées dans le système GDR au moyen d'une interface (*let. a*).
- Un collaborateur spécialisé d'un utilisateur établit une demande de modification en vue de la saisie ou de la modification de données de référence et un autre collaborateur spécialisé approuve la demande de modification dans le système GDR (*let. b*).

Afin d'améliorer la qualité de données centralisées dans le système GDR et de garantir l'identification univoque, les données de référence saisies sont comparées avec des données provenant de différentes sources externes (*let. c à e*) et le cas échéant complétées par certains champs de données pendant la saisie. Les sources externes utilisées pour la comparaison sont d'une part des registres fédéraux (IDE, REE, banques de données de swisstopo, système d'information géographique de l'Office fédéral de l'agriculture, système d'information central sur la migration et registre central des assurés AVS/AI ; ce dernier n'est pas encore relié au système GDR). D'autre part, les données du service de validation des adresses de personnes et d'entreprises de la Poste Suisse et de banques de données accessibles au public, le cas échéant payantes (telles que DUNS pour la comparaison avec de personnes et d'organisations domiciliées ou sises à l'étranger) sont également utilisées. Le nouveau registre fédéral « Service national des adresses » est par ailleurs en développement. Il permettra de consulter les adresses de personnes physiques. Des éclaircissements sont en cours pour déterminer dans quelle mesure des données de ce nouveau registre pourront être utilisées pour le système GDR. Avant d'utiliser des registres comme sources de données, il faut toujours vérifier si le registre concerné entre dans le champ d'application de l'art. 21 ou si la disposition doit être adaptée.

La comparaison des données de référence avec les différents registres peut être définie jusqu'au niveau du champ. Les registres ne peuvent servir de sources que pour les données visées à l'art. 21, let. b à f et i. Toutes les autres données (art. 21, let. g, h et j) sont soit fournies directement par la personne ou l'organisation (par ex. coordonnées bancaires ou indications telles que délais de paiement convenus contractuellement), soit saisies directement par les utilisateurs (par. ex. périmètre comptable, compte collectif, mode de paiement). Le numéro d'identification non personnel visé à l'art. 21, let. a, est généré automatiquement lors de la saisie de la personne ou de l'organisation.

La comparaison et la reprise des données à partir des registres sont, dans la mesure du possible, automatisées. Les données sont transférées dans le système GDR au moyen d'une interface (*al. 2*). Le règlement de traitement précisera dans quelles circonstances les données sont reprises automatiquement et quand elles doivent être vérifiées par quelqu'un.

Art. 23 Responsabilité

L'AFF est responsable du traitement au sens de l'art. 5, let. j, LPD et de la protection des données suivantes :

- le numéro d'identification non personnel issu du système GDR et les données personnelles étendues (art. 21, al. 1, let. a à f) ;
- les coordonnées bancaires (art. 21, al. 1, let. g) ;
- les données concernant relations avec d'autres personnes ou organisations enregistrées dans le système (art. 21, al. 1, let. h) ;
- les numéros de registre permettant l'identification univoque (art. 21, al. 1, let. i).

Ces données sont utilisées de la même manière par tous les utilisateurs pour l'exécution des processus de soutien.

L'enregistrement des données de référence dans le système GDR et leur gestion sont assurés par une équipe spécialisée du Centre de services en matière de finances du DFF. Si nécessaire, le centre peut recourir à des collaborateurs spécialisés des utilisateurs pour effectuer ces tâches. En leur qualité de consignataires (*local data custodians*), ces collaborateurs sont dotés d'un droit d'accès en écriture. Ils soutiendront l'équipe du Centre de services en matière de finances, par exemple en saisissant de manière décentralisée un changement d'adresse notifié. Cette possibilité n'est pas encore exploitée. Afin d'éviter les abus, on veillera à ce que les collaborateurs qui saisissent et modifient les personnes et les organisations dans le système GDR ne puissent en rien influencer les opérations de paiement. D'autres règles du système de contrôle interne, telles que le respect du principe du double contrôle pour les modifications dans le système GDR, sont consignées dans le schéma d'autorisation.

Puisque les données de référence visées à l'art. 21, let. j, peuvent différer en fonction de l'affaire et du processus de soutien, l'utilisateur qui a saisi ces données dans le système GDR doit assumer la responsabilité de leur protection ; la *let. b* le prévoit expressément.

Art. 24 Utilisation et accès

L'al. 1 établit que les unités de l'administration fédérale centrale doivent utiliser le système GDR et les données gérées dans ce système pour exécuter leurs processus de soutien conformément à l'art. 20, al. 1. Cette règle est indispensable pour que la comptabilisation dans le compte d'État des opérations de paiement soutenues par le système GDR soit largement automatisée. Comme pour la plupart des obligations, des exceptions peuvent se justifier ici aussi. Des problèmes techniques peuvent rendre une connexion difficile, voire impossible, notamment à cause de l'ancienneté de l'application métier. Par ailleurs, les interfaces recèlent toujours un risque, aussi vaut-il parfois mieux renoncer à une connexion pour protéger les données de certaines applications. Les motifs d'exception sont trop nombreux pour être énumérés. Une exception ne doit toutefois être accordée que si elle est objectivement justifiée et l'emporte nettement sur le gain d'efficacité que la comptabilisation automatique des opérations de paiement dans le compte d'État permettrait.

En tant que responsable du système GDR et en vertu de l'art. 59 de la loi du 7 octobre 2005 sur les finances[38], l'AFF est habilitée à accorder une dérogation à l'obligation

38 RS **611.0**

d'utilisation, sur demande d'une unité administrative. Elle décidera après avoir convenu d'une solution plus adéquate avec l'unité concernée.

Les unités de l'administration fédérale décentralisée, les Services du Parlement, les tribunaux fédéraux et le Ministère public de la Confédération faisant partie du périmètre comptable de la Confédération, ils pourront également utiliser le système GDR pour leurs processus de soutien. Lorsque des organisations ou des personnes de droit public ou de droit privé qui ne font pas partie de l'administration fédérale sont chargées de tâches administratives et exécutent dans ce cadre des processus de soutien pour la Confédération, il est justifié qu'elles puissent utiliser les données enregistrées de manière centralisée dans le système. L'*al. 2* prévoit donc cette possibilité. L'AFF leur accorde en général l'accès au système sur demande. Il se peut toutefois, comme pour l'al. 1, que des circonstances techniques empêchent d'accéder aux données ou rendent cet accès très difficile ou que des dispositions juridiques s'opposent à un tel accès. Il faut donc que l'AFF ait la possibilité de refuser la demande d'accès.

D'autres conditions doivent encore être remplies pour que les organisations et personnes chargées de tâches administratives obtiennent un droit d'accès, étant donné qu'elles n'ont pas un lien aussi étroit avec l'administration fédérales que les autres utilisateurs mentionnés à l'al. 2. Selon les circonstances, ces organisations et personnes exécutent également des mandats de droit privé et sont soumises, dans ce cadre, aux dispositions du droit privé. L'al. 3 prévoit dès lors que ces organisations et personnes se voient accorder l'accès aux données enregistrées de manière centralisée dans le système GDR uniquement si elles en ont besoin pour accomplir leurs tâches administratives. Cette condition est remplie si elles exécutent également dans ce cadre des processus de soutien pour la Confédération. Les données ne peuvent cependant être utilisées à des fins plus larges que celles qui sont autorisées pour les unités administratives de la Confédération ou les autorités fédérales mentionnées à l'al. 2. Les organisations et personnes en question ne peuvent par exemple accéder aux données du système pour exercer leurs activités de droit privé.

La demande d'accès pour les organisations et personnes visées à l'art. 2, al. 4, LOGA doit être soumise à l'AFF par l'unité administrative compétente du département qui a le lien le plus étroit avec le système. Cette unité est en contact permanent avec l'organisation ou la personne concernée. Elle convient avec elle des modalités de l'exécution des tâches administratives, règle les questions financières (par ex. les indemnités éventuelles) et joue le rôle d'interlocuteur et de superviseur dans ce domaine. Elle est donc la mieux placée pour juger si l'organisation ou la personne exécute également des processus de soutien pour la Confédération et si elle a besoin, à cet effet, d'un accès aux données du système. Elle dispose par ailleurs de connaissances spécifiques sur l'‘infrastructure dont dispose l'organisation ou la personne et peut donc juger si une protection adéquate des données et des informations est garantie lors du traitement des données personnelles enregistrées dans le système. Elle est le cas échéant également la mieux placée pour obtenir les informations manquantes. La demande adressée à l'AFF doit par conséquent contenir les informations suivantes :

- la raison pour laquelle un accès aux données doit être accordé et la mention des processus de soutien qui doivent être exécutés ;

- une confirmation que l'organisation ou la personne respecte les dispositions pertinentes de la législation fédérale sur la protection des données et des informations, afin de pouvoir lui donner accès à toutes les données personnelles enregistrées dans le systèmes (numéro AVS compris).

L'AFF vérifiera que la raison avancée est plausible et que la confirmation demandée a bien été jointe à la demande. Compte tenu des éléments exposés plus haut, elle ne procédera cependant pas à contrôle plus poussé : c'est l'unité administrative qui soumet la demande et qui a un lien direct avec l'organisation ou la personne qui est responsable de l'exactitude des informations fournies.

Actuellement, seule la société RUAG MRO dispose d'un tel accès dans l'exercice de ses activités pour le DDPS.L'al. 4 prévoit que les utilisateurs chargés de processus de soutien ont accès aux données qu'ils ont saisies et à celles dont le traitement et la protection relèvent de la compétence de l'AFF.

Ils disposent d'un droit de lecture des données visées à l'art. 21, al. 1, let. a à i. Ce droit leur permet de vérifier si les données d'une personne ou d'une organisation sont déjà saisies dans le système GDR. Ils peuvent, par l'intermédiaire d'un masque de saisie du système GDR, demander une modification qui leur permettra automatiquement d'utiliser les données de référence dont ils ont besoin. Toutes les données d'une personne ou d'une organisation qui peuvent être lues peuvent être utilisées. Il n'y a pas de restriction concernant certains attributs de données.

Depuis la migration vers S/4HANA en septembre 2023, la grande majorité des unités de l'administration fédérale centrale qui participent à des processus de soutien pris en charge, ont accès aux données de référence du système GDR et les utilisent pour ces processus[39]. Près de 595 000 partenaires commerciaux sont aujourd'hui gérés dans le système GDR (état en septembre 2024). Environ 5000 nouveaux partenaires sont saisis chaque mois, à la demande des utilisateurs.

Aux termes de l'al. 5, l'accès au système GDR peut être accordé au moyen d'une interface.

Art. 25 Interface pour la mise à jour d'autres systèmes d'information

En plus de la gestion centralisée des données de référence à l'échelle de la Confédération, le système GDR permettra de tenir à jour les données des registres de la Confédération. Seules les données de référence saisies dans le système GDR peuvent être utilisées pour comparer des données. Cette comparaison porte donc en premier lieu sur les registres fédéraux dont les données sont organisées comme celles du système GDR (en particulier registre IDE et REE). La comparaison nécessite cependant des mesures techniques et organisationnelles transversales visant à clarifier ses modalités (hiérarchie, règles de reprise, etc.). Tant que ces mesures transversales ne seront pas mises en œuvre, les données du système GDR ne pourront être utilisées pour mettre à jour un autre système d'information que si la base légale régissant ce dernier prévoit la reprise des données du système GDR. L'unité administrative responsable du

39 État au 1er octobre 2024 : encore aucune connexion avec les offices civils du DDPS et avec quelques applications métiers non SAP

système d'information doit estimer elle-même les conséquences éventuelles de la comparaison des données (par ex. des écrasements involontaires lors de la reprise automatique) et les supporter. L'actualisation aussi rapide que possible des données des registres de la Confédération est dans l'intérêt général et contribue par ailleurs à la mise en œuvre du principe de la collecte unique des données, aussi la mise à disposition des données gérées dans le système GDR est-elle autorisée dans ce but. Les données seront reprises automatiquement au moyen d'une interface.

Art. 26 Conservation et radiation des données

Les données centralisées du système GDR servent de base aux utilisateurs pour l'exécution de leurs processus de soutien. Ces derniers sont déclenchés dans une multitude de situations différentes, telles que le versement de subventions, l'octroi de droits spéciaux donnant lieu au paiement d'un émolument (octroi de licences ou de concessions), l'acquisition de biens et services par la Confédération, pour n'en citer que quelques-unes. Il est probable qu'au fil du temps les données centralisées concernant des personnes et des organisations seront utilisées plusieurs fois par différents services fédéraux. Pour mettre en œuvre le principe de la collecte unique des données et en tirer le plus grand bénéfice possible, les données doivent être entretenues activement pendant une période relativement longue. Conformément à l'art. 7, al. 1, de l'ordonnance du 30 juin 1993 sur le registre des entreprises et des établissements[40], la présente disposition prévoit un délai de conservation de 30 ans pour les ensembles de données de référence. Ce délai serait toutefois absurde si l'organisation ou la personne concernée disparaissait dans l'intervalle. Les données ne seront donc conservées que pendant 10 ans au plus après la mort d'une personne, la radiation d'une entreprise du registre du commerce ou la fermeture définitive d'une succursale.

Le délai de conservation commence à courir au moment du dernier traitement dans un jeu de données de référence (dernière communication à un utilisateur ou dernière mutation). Si le jeu de données n'est pas modifié pendant le délai de conservation, il est radié à l'expiration de celui-ci et archivé dans le système (*al. 2*). Les données de référence (sauf si le droit de demander la destruction en vertu de la législation sur la protection des données l'exige) ne peuvent pas être détruites pour les raisons suivantes : les utilisateurs recourent aux données du système GDR dont ils ont besoin pour une opération d'affaires particulière, laquelle déclenche un processus de soutien pris en charge ; les données centralisées du système GDR et les données des applications spécialisées de l'utilisateur sont appariées par l'utilisation des données. Si on détruisait les données traitées par les applications métiers dans le système de base GDR, il pourrait y avoir des conséquences indésirables sur les données se trouvant dans les applications spécialisées. Les données de référence utilisées dans ces applications pourraient être introuvables ou impossibles à retracer. Pour éviter ces problèmes, les données ne peuvent pas être détruites dans le système GDR. À l'expiration du délai de 30 ans, par analogie avec la procédure visée à l'art 12 de la loi fédérale du 18 juin 2010 sur le numéro d'identification des entreprises[41], les données qui ne sont plus nécessaires sont « radiées » et conservées dans le système GDR, pour autant qu'aucune réserve juridique ne s'oppose à la radiation. Les données radiées ne peuvent plus être

40 RS **431.903**
41 RS **431.03**

utilisées pour de nouvelles opérations ou l'actualisation de registres de la Confédération (*al. 3*). Cependant, si dans un cas d'espèce un document fondé sur d'anciennes données d'un utilisateur a été endommagé ou ne peut plus être retracé pour une autre raison liée aux données tirées du système GDR, l'AFF communique les données pertinentes conservées dans le système. Cette approche permet de résoudre de façon pragmatique les éventuels problèmes techniques imprévisibles qui peuvent se produire lors de l'appariement de données provenant de deux systèmes d'information.

Lorsqu'une personne ou une organisation fait légitimement valoir un droit de destruction fondé sur des dispositions en matière de protection des données, les données concernées doivent être détruites.

Chapitre 5 Secteur TNI

Art. 27 Direction

Le secteur TNI fait partie de la Chancellerie fédérale et donc de l'administration fédérale centrale (art. 7, al. 1, let. a, OLOGA) ; il est composé de plusieurs sections et il est dirigé par le délégué TNI (*al. 1*) ; il encourage le regroupement des acquisitions de marchandises et de services dans le domaine des technologies de l'information et de la communication conformément à l'art. 7, al. 3, Org-OMP. Le délégué TNI est membre de la direction de la Chancellerie fédérale.

Art. 28 Tâches

Le secteur TNI est le centre de compétences de la Confédération pour les questions liées à la numérisation qui touchent l'ensemble de l'administration fédérale, voire tout le pays. Il veille à ce que les normes dans le domaine de l'architecture d'entreprise (pour les prestations de l'administration, les données, les processus, les applications et les technologies) soient définies, au niveau interdépartemental, de manière cohérente, de façon à optimiser les résultats et afin que les projets, moyens informatiques et prestations au niveau transversal de l'administration fédérale soient pilotés et gérés dans un portefeuille. Responsable de la gestion des services informatiques standard, le secteur TNI regroupe les exigences des unités administratives à l'intention des fournisseurs de prestations informatiques. Il joue le rôle d'état-major de la délégation du Conseil fédéral « Transformation numérique et informatique » et prépare les propositions au Conseil fédéral relatives à la transformation numérique de l'administration fédérale. Il coordonne les travaux des départements en matière de numérisation de l'administration au niveau de la Confédération, dirige le conseil TNI et prépare les affaires à l'intention de la CSG. Il gère les services standard mis à disposition de manière centralisée. Il est responsable de la coordination et du développement de la stratégie Suisse numérique du Conseil fédéral et coordonne la collaboration de l'administration fédérale avec l'organisation appelée à succéder à Cyberadministration suisse (projet Administration numérique : mise en œuvre de l'optimisation du pilotage et de la coordination au sein de l'État fédéral).

Dans la mesure où l'accomplissement de ses tâches le requiert, il établit et entretient des contacts internationaux dans le domaine TNI (*al. 4*).

Chapitre 6 Organes dans le domaine de la transformation numérique et de la gouvernance de l'informatique

Section 1 Conseil TNI

Art. 29 Tâche

Le Conseil TNI est un organe consultatif interdépartemental du délégué TNI. Il veille de manière centralisée à l'harmonisation interdépartementale de projets, stratégies et décisions dans le domaine de la numérisation (processus d'affaires, données, applications, technologie). Il constitue une plateforme au sein de laquelle tous ses membres peuvent faire des propositions pour promouvoir la transformation numérique ou critiquer des décisions ou des développements qui touchent leur domaine de compétences ou les entravent ; ces propositions et critiques pouvant au besoin déboucher rapidement sur une décision.

Le Conseil TNI assiste le délégué TNI et les départements dans les projets de numérisation interdépartementaux, ainsi que dans le cadre de la coordination de la transformation numérique et de la gouvernance de l'informatique. Cet organe a besoin d'une vision globale de la numérisation pour pouvoir la piloter efficacement, ce qui suppose notamment que le Conseil TNI soit informé des projets interdépartementaux qui ne sont pas gérés par la Chancellerie fédérale (par ex. la gestion nationale des données) ou des instructions qui concernent la numérisation, mais qui ne sont pas édictées par le secteur TNI.

Art. 30 Composition

Tous les départements sont représentés au sein du Conseil TNI ; ils peuvent y déposer des propositions et y disposent chacun d'une voix (art. 31, al. 1 et 2). La Chancellerie fédérale est représentée par le délégué TNI, qui a lui aussi un droit de proposition et de vote. Si nécessaire, les départements et la Chancellerie fédérale peuvent participer aux séances avec deux représentants.

Le chargé de mission de la Confédération et des cantons auprès de l'Administration numérique suisse siège lui aussi au Conseil TNI, avec un droit de proposition (art. 31, al. 1), afin d'assurer une harmonisation étroite des travaux du délégué TNI avec la future plateforme politique de la Confédération et des cantons chargée de développer des normes.

Le délégué TNI et le chargé de mission de la Confédération et des cantons auprès de l'Administration numérique suisse peuvent se faire représenter par leur remplaçant ou, à défaut, par une personne de leur choix au sein de leur unité.

L'application du modèle de gouvernance à tous les niveaux de la transformation numérique a changé le rôle des fournisseurs de prestations informatiques de l'administration fédérale. Ces derniers ont un rôle élargi de prestataires de services et apportent leurs

idées, connaissances et savoir-faire dans le domaine des technologies et du développement de celles-ci, y compris au niveau stratégique. Pour cette raison, un représentant de l'organe de coordination des fournisseurs internes de prestations informatiques siégera également au Conseil TNI, avec un droit de proposition. Il rassemble dans ce but les connaissances, requêtes et intérêts de l'ensemble des fournisseurs de prestations informatiques de l'administration fédérale de manière transparente (cf. art. 32).

Afin que les intérêts liés à la sécurité de l'information soient pris en compte, un représentant du Secrétariat d'État à la politique de sécurité (SEPOS), avec droit de proposition (art. 31, al. 1), est représenté au Conseil TNI.

Le DFI (OFS) a été chargé de créer les outils et instruments nécessaires pour instaurer et mettre en œuvre la standardisation, l'harmonisation et l'uniformisation des données (système de métadonnées, catalogue de données). Dans ce contexte, l'OFS a institué le nouveau centre national de compétences en science des données (DSCC). Compte tenu des tâches transversales que l'OFS doit assumer dans le domaine de la gestion des données et de la politique en matière de données, un représentant de l'OFS siège également au Conseil TNI, avec un droit de proposition (art. 31, al. 1).

En cas de besoin et afin de garantir la compatibilité des moyens informatiques de l'armée avec ceux de la Confédération, un représentant du commandement Cyber peut participer aux séances du Conseil TNI.

Art. 31 Séances

Si tous les membres du Conseil TNI peuvent déposer des propositions (*al. 1*), seuls le délégué TNI et les représentants des départements ont le droit de vote (*al. 2*), afin d'éviter la surreprésentation d'un département lors des votes.

D'autres unités peuvent participer ponctuellement aux séances du Conseil TNI à titre consultatif (*al. 3*), en particulier le Préposé fédéral à la protection des données et à la transparence (PFPDT), l'AFF et les Services du Parlement ; ils seront consultés sur les sujets qui les concernent ou pour lesquels ils peuvent apporter une contribution précieuse. Même si ces unités ne sont pas représentées en permanence au Conseil TNI, rien n'empêchera donc une collaboration fructueuse.

Section 2 Conférence des prestataires de services informatiques

Art. 32

Le rôle des fournisseurs de prestations dans le pilotage stratégique de la transformation numérique doit être renforcé (cf. commentaire de l'art. 29). Pour cette raison, la disposition de l'OTNI concernant la Conférence des prestataires de services informatiques (CPSI) et les tâches qui lui incombent est reprise à l'identique dans la présente ordonnance.

Seuls des fournisseurs internes sont représentés dans la CPSI. La coordination efficace de tous les fournisseurs de prestations informatiques commande d'impliquer de manière appropriée les autres fournisseurs spécifiques de certaines unités qui ont ob-

tenu une dérogation conformément à l'art. 10, al. 2 (swisstopo, Météosuisse ou la Centrale de compensation). À l'avenir, il faudra veiller à ce que ces prestataires soient mieux intégrés.

Section 3 Comité de pilotage des processus de soutien

Art. 33

Le Comité de pilotage des processus de soutien vise à coordonner les décisions de l'AFF, de l'Office fédéral du personnel, de l'Office fédéral des constructions et de la logistique, d'armasuisse et du délégué TNI concernant l'appui informatique aux processus de soutien utilisés dans l'ensemble de l'administration fédérale en matière de finances, de personnel, d'acquisition, de gestion immobilière et de logistique. Depuis la mise en service de la nouvelle plateforme SAP S/4HANA en automne 2023, le programme SUPERB assume provisoirement l'intégralité des tâches du comité de pilotage. Il continuera d'assumer la tâche de coordination visée à l'al. 1, conformément au ch. 3.4., al. 2, des directives du Conseil fédéral du 19 août 2020 concernant le programme « SUPERB »[42], jusqu'à la mise en place de la nouvelle gouvernance.

Les dispositions concernant le Comité de pilotage des processus de soutien sont conservées provisoirement, étant donné que la durée de validité des directives du Conseil fédéral est explicitement liée à celle du programme SUPERB.

La nouvelle gouvernance et les adaptations juridiques qu'elle appelle sont élaborées dans le cadre du programme SUPERB, compte tenu de la gouvernance supérieure. Les dispositions relatives à la nouvelle gouvernance seront soumises au Conseil fédéral d'ici à la fin de l'année 2025.

Le chef du DFF abrogera les directives du Conseil fédéral à la fin du programme SUPERB (ch. 5.2, al. 2, des directives). La présente ordonnance ne les modifie pas puisqu'elles restent applicables jusqu'à cette date.

Section 4 Collaboration entre les unités administratives qui gèrent des systèmes d'information dans les domaines de la justice ou de la police

Art. 34

L'art. 31 OTNI, qui permet de conclure des conventions entre la Confédération et les cantons concernant l'harmonisation des moyens informatiques des domaines judiciaire et policier, est sans objet depuis l'entrée en vigueur de l'art. 4 LMETA.

Une partie de cette disposition est néanmoins conservée pour mettre en évidence l'obligation de collaboration des unités administratives qui gèrent des systèmes d'information dans les domaines de la justice et de la police (*al. 1*). Par ailleurs, les départements doivent pouvoir continuer à conclure des conventions d'exécution pour des projets (*al. 2*).

42 FF **2020** 6527

Chapitre 7 Projets clés et projets pilotes

Section 1 Projets clés

Art. 35 Objet

Ce chapitre réunit les principaux éléments concernant les projets clés de l'administration fédérale. Il appartient à l'unité administrative compétente et à son département de renforcer la surveillance des projets clés et de prendre les mesures nécessaires pour assurer le succès des projets. Les critères énumérés aux *let. a à d* ne sont pas cumulatifs.

Art. 36 Responsabilité

Al. 1 : avant de déterminer un projet clé, le chancelier de la Confédération consulte la CSG. Le règlement de la CSG prévoit la consultation préalable des unités administratives intéressées.

Al. 2 : si nécessaire, le chancelier de la Confédération peut régler les modalités dans une directive.

Art. 37 Rapports et mesures correctives

Le contenu et la périodicité des rapports à fournir sont réglés dans une directive du secteur TNI visée à l'art. 40. Après que la CSG a traité les rapports, la Chancellerie fédérale les transmet à la Délégation des finances, aux Commissions des finances et aux Commissions de gestion des Chambres fédérales.

Section 2 Projets pilotes

Aux termes de l'art. 15, al. 4, LMETA, la réalisation d'un projet pilote nécessite l'accord de la Chancellerie fédérale. Cette dernière dispose donc d'un pouvoir de contrôle et peut, en dernier recours, opposer son *veto*. L'ordonnance du département qui règle le projet pilote doit être soumise en temps utile à la Chancellerie fédérale ; les organes compétents en matière de coordination et de surveillance doivent être également consultés (cf. message LMETA[43]).

Pour des raisons pratiques, le rapport annuel du Conseil fédéral à l'Assemblée fédérale visé à l'art. 15, al. 7, LMETA sera fait par un canal d'information existant.

Art. 38 Obligation d'informer et de documenter

Le service responsable du projet pilote doit rendre compte de l'avancement du projet au secteur TNI et aux autorités compétentes.

43 FF **2022** 804, p. 87 s.

Les conditions de réalisation des projets pilotes menés au titre de la LMETA doivent être réglées. Il incombe au département chargé du projet ou à la Chancellerie fédérale de régler, par une ordonnance au sens de l'art. 48, al. 1, LOGA, le cadre dans lequel le projet pilote doit s'inscrire. Par ailleurs, le département devra soumettre l'ordonnance, avant qu'elle soit signée par le chef de département, au secteur TNI pour que celui-ci puisse se prononcer et assumer pleinement sa tâche de pilotage et de coordination dans le domaine de la transformation numérique et de la gouvernance de l'informatique au sein de l'administration fédérale. En pratique, la Chancellerie fédérale a un droit de *veto* ; si elle ne parvient pas à un accord avec le département concerné sur le contenu de la réglementation du projet pilote, ce dernier ne peut pas être réalisé. Elle peut donc proposer des adaptations de la réglementation pour parvenir à un accord. On notera que la réglementation que le département soumet au secteur TNI doit respecter la protection informatique de base, qui définit de manière contraignante les directives de sécurité minimales sur les plans de l'organisation, du personnel et de la technique en matière de sécurité informatique dans l'administration fédérale. La réglementation exigée ne permet pas de s'écarter des directives de base pertinentes.

Dans la mesure où les essais pilotes doivent être soumis aux organes de surveillance (Conseil TNI, PFPDT, OFCS), rien ne s'oppose à ce que la Chancellerie puisse s'octroyer des autorisations. La surveillance est suffisamment garantie par ces organes.

L'office concerné doit en outre informer le secteur TNI et les autorités compétentes de l'état actuel du projet pilote, c'est-à-dire des ressources financières déjà utilisées, de celles dont il dispose encore et de celles dont il aura besoin à l'avenir, mais aussi des avancées significatives du projet, des problèmes rencontrés et de toute modification de la planification initiale. Cette obligation de faire rapport doit permettre aux autorités compétentes d'assumer efficacement leurs tâches de contrôle et de surveillance prévues par la loi. La périodicité de cette obligation a été fixée à une fois par an pour que les projets pilotes ne soient pas entravés par des obligations administratives excessives, mais que les autorités de surveillance puissent tout de même suivre de près l'avancement des projets.

À l'obligation périodique de rendre compte s'ajoute une obligation extraordinaire d'informer en cas d'événement particulier. Si la situation est critique, le secteur TNI et les organes compétents doivent être informés dans le mois qui suit l'événement, afin que des mesures puissent être prises rapidement. Par événement particulier on entend tous les événements dont l'importance pourrait compromettre la poursuite du projet pilote ou la réalisation de ses objectifs ou porter atteinte aux droits de tiers.

La violation des dispositions du droit de la protection des données et de la sécurité de l'information peut constituer un événement particulier qui doit être annoncé dans le mois qui suit sa survenance. Toute violation des obligations qui découlent de ces dispositions, comme celle du responsable du traitement et du sous-traitant de veiller à la sécurité des données (art 8 LPD et 1 à 6 OPDo) doit également être signalée. Ce devoir d'information a une portée autonome et vaut indépendamment d'autres obligations similaires telles que celle de l'art. 24 LPD (obligation d'annoncer les cas de violation de la sécurité des données) ou celle de signaler les cyberattaques contre les infrastructures critiques, qui s'applique depuis le 1er avril 2025[44].

44 Ordonnance du 7 mars 2025 sur la cybersécurité (OCyS, RS **128.51**)

L'obligation d'informer et de documenter s'inscrit pleinement dans le dispositif visant à permettre aux autorités de surveillance d'assumer effectivement leurs tâches. Les obligations légales ordinaires de documenter et d'informer restent applicables, indépendamment de la présente disposition.

Art. 39 Financement

Si les conditions prévues par les directives du secteur TNI sont remplies, le financement des projets pilotes peut être assuré par les ressources affectées de manière centralisée, dans la mesure où elles sont disponibles. La directive informatique P053, qui règle la procédure relative à l'affectation des ressources centrales destinées aux projets pilotes de transformation numérique dans l'administration fédérale et complète l'art. 44, s'applique. Un projet pilote ne doit toutefois pas forcément être financé au moyen des ressources affectées de manière centralisée. La réalisation d'essais pilotes doit demeurer possible lorsqu'on ne peut plus obtenir d'argent par cette source de financement ou qu'il n'est pas nécessaire d'y recourir parce que le département concerné peut fournir les fonds nécessaires.

Chapitre 8 Directives

Art. 40 Directives du secteur TNI

Le secteur TNI peut édicter des directives sur la transformation numérique de l'administration fédérale et la gouvernance de l'informatique ou sur les outils et méthodes qui sont nécessaires pour assurer le pilotage et la gestion. Il s'agit principalement de dispositions de nature générale et abstraite qui définissent de manière contraignante la pratique des unités soumises à l'ordonnance (« ordonnances administratives »). Les directives peuvent ne concerner qu'un (petit) nombre de destinataires déterminés ou des décisions prises au cas par cas, si leur contenu est en rapport avec le domaine d'activité du secteur TNI. Les unités administratives, ou plus précisément les personnes et organes qui sont à leur tête, sont seules responsables du respect des directives. Les ordonnances administratives n'ont en général pas d'effet à l'extérieur de l'administration fédérale et ne créent donc pas de droits ou d'obligations pour des tiers.

Les directives visées peuvent porter tant sur l'exécution des tâches que sur certains aspects touchant l'organisation interne des unités administratives, notamment lorsque, dans les modèles de pilotage et de gouvernance, il faut définir certains rôles dans des sous-domaines et la manière dont ils s'articulent (par ex. création de groupes d'experts afin d'assurer la gouvernance d'un service standard ou, dans le domaine de la gestion des données, création de rôles tels que celui d'administrateur des données) ou lorsqu'il faut définir des outils et des processus de contrôle de gestion et de rapport pour assurer la coordination transversale.

Il est possible d'édicter des directives et des normes dans tous les domaines de l'architecture d'entreprise qui sont nécessaires pour assurer le succès de la transformation numérique de l'administration fédérale au niveau interdépartemental et pour la gouvernance de l'informatique. Aux directives informatiques s'ajoutent des directives qui portent essentiellement sur la conception des processus d'affaires transversaux (par ex.

modèles, configuration ou rôles) ou qui permettent aux unités administratives d'échanger et d'utiliser les données de manière transversale. Ce type d'échange et d'utilisation des données exige que celles-ci soient interopérables sur le plan technique (recherche, évaluation, interprétation) et sur le plan sémantique (signification des données et relations entre elles, modèles de données).

Les directives et normes concernant la protection contre les cyberrisques doivent être édictées en accord avec l'OFCS.

En vertu de l'art. 47, al. 4, LOGA, le chancelier de la Confédération peut en tout temps prendre la responsabilité d'un dossier qui relève du délégué TNI pour décision. Dans ce cas, il consultera au préalable la CSG et tiendra compte de la recommandation de celle-ci.

Let. a : les stratégies partielles servent à établir en commun les lignes directrices qui définissent l'orientation générale des activités à moyen terme dans des sous-domaines. Elles peuvent notamment porter sur la bureautique, sur l'harmonisation de données de référence ou sur l'intégration de processus d'affaires. Elles servent en général à fixer une orientation commune et donc à la coordination générale, mais elles peuvent aussi contenir des principes directeurs et des éléments normatifs.

Let. b : les processus de pilotage du secteur TNI définissent la manière dont les tâches liées à la transformation numérique ou à la gouvernance de l'informatique sont accomplies. Ils peuvent inclure la création de rôles ou de fonctions au sein des unités administratives. Ils servent aussi à définir les modèles de gouvernance lorsqu'un pilotage ou une gestion est nécessaire au niveau transversal dans des sous-domaines.

Let. c : les directives portant sur l'architecture d'entreprise décrivent la manière de concevoir les processus d'affaires, les informations et les technologies et sur la manière dont ils s'articulent au sein de l'administration fédérale. Elles peuvent revêtir un caractère indicatif, voire incitatif, et contenir des éléments détaillés de nature normative.

Let. d : les normes découlent en règle générale de l'architecture d'entreprise. Elles déterminent les circonstances dans lesquelles il faut concevoir et utiliser de manière standardisée tels ou tels technologies, produits, outils, prestations informatiques, interfaces, modèles de données ou modèles de processus d'affaires pour assurer l'économicité, l'interopérabilité, la flexibilité et la sécurité. Cette obligation se fonde sur l'art. 12 LMETA : les normes au sens de cette disposition englobent toutefois les normes organisationnelles et techniques qui pourraient relever de la let. b ou c.

Si une norme vaut également pour les unités administratives décentralisées, une directive ou une décision relative à cette norme doit le préciser.

Let. e : le secteur TNI continuera de gérer les moyens informatiques mis à disposition de manière centralisée comme des services standard. D'autre part. l'art. 11, al. 1, permet de mettre à disposition de manière décentralisée d'autres moyens informatiques et imposer leur utilisation lorsque cette obligation se justifie (art. 11, al. 2).

La présente disposition habilite le secteur TNI à édicter des directives concernant les moyens informatiques mis à disposition de manière centralisée. Il l'a déjà fait pour les services standard existants en édictant la directive du 18 décembre 2023 sur le pilotage

et la gestion des services standard conformément à l'OTNI (W008)[45], qui règle le modèle de service, le modèle d'obtention, le modèle de prix et le contrôle de qualité. Il sera dorénavant possible d'édicter des directives sur les moyens informatiques mis à disposition de manière centralisée par d'autres unités administratives.

Let. f : les directives portant sur la gestion du portefeuille visent à garantir que les informations nécessaires au pilotage et à la gestion de la transformation numérique et de la gouvernance de l'informatique sont disponibles et à mises à jour régulièrement et qu'elles sont, le cas échéant, corrigées. La gestion du portefeuille va donc de pair avec l'architecture d'entreprise et permet de comparer la situation souhaitée et la situation effective. Elle peut porter sur différents aspects (technologie, applications, prestations, projets, programmes, matériel, modèles de données ou processus d'affaires).

Let. g : les directives portant sur le contrôle de gestion visent à garantir que le délégué TNI peut accomplir ses tâches, notamment en ce qui concerne le contrôle des acquisitions et l'établissement des rapports dans le cadre du compte d'État, pour le compte des autorités auxquelles il est subordonné.

Al. 2 : le secteur TNI consulte le Conseil TNI avant d'édicter une directive. Il peut consulter d'autres organes pour les directives de portée mineure, en particulier le Conseil de l'architecture de la Confédération et le Comité de gestion des services standard. Par directives d'importance mineure, on entend par exemple les décisions relatives à la planification des versions ou au catalogue des services standard. Si ces décisions sont contestées au sein d'organes subordonnés, elles sont mises à l'ordre du jour du Conseil TNI, qui vote.

La délégation de compétence prévue à l'*al. 4* ne peut porter que sur des décisions de portée mineure, telles que des dérogations concernant les services standard qui n'ont pas d'influence sur des tiers.

Art. 41 Directives interdépartementales des départements

Avant d'édicter une directive dans le domaine de la numérisation ou de la gouvernance de l'informatique, un département doit consulter le Conseil TNI (cf. commentaire de l'art. 40).

Art. 42 Règlement des différends

Conformément au modèle de gouvernance prévu par cet article, les décisions du délégué TNI qui sont contestées, malgré la consultation préalable et l'élimination des divergences au Conseil TNI, peuvent être portées rapidement devant l'autorité supérieure par tous les départements.

---

45 www.bk.admin.ch > Transformation numérique et gouvernance de l'informatique > Directives informatiques > Toutes les directives > W008 - Directive sur le pilotage et la gestion des services standard conformément à l'OTNI

Cette possibilité n'est pas ouverte à tous les membres du Conseil TNI, seuls les départements ont le droit de lancer une procédure d'intervention par paliers. Les autres membres du Conseil TNI doivent passer par la voie hiérarchique afin que leur département de tutelle lance la procédure.

La procédure de règlement des différends prévue ici ne s'applique qu'aux désaccords concernant des décisions du secteur TNI. Si le différend porte sur une décision du chancelier de la Confédération (cf. art. 11, al. 2), l'affaire peut, conformément à la procédure ordinaire (art. 47, al. 4, LOGA), être portée devant le Conseil fédéral, qui tranche. Il en va de même des décisions prises par le chancelier à l'issue d'une procédure de règlement des différends (*al. 3*).

C'est à dessein que la Chancellerie fédérale n'est pas mentionnée à l'art. 42 : le secteur TNI étant une de ses unités, tout différend avec lui est réglé en interne.

Let. a : conformément à l'art. 11, al. 1, le secteur TNI peut imposer la mise à disposition de manière centralisée d'un moyen informatique. L'art. 11, al. 1, LMETA, est la base légale qui l'habilite à le faire. Il peut donc ordonner à un département de mettre à disposition de manière centralisée un moyen informatique. Si plusieurs départements souhaitent mettre à disposition de manière centralisée un moyen informatique, le secteur TNI peut choisir parmi eux. Il peut soutenir le département responsable par une directive sur les moyens informatiques mis à disposition de manière centralisée (art. 40, al. 1, let. e).

Let. b : seule la décision concernant l'adoption ou non d'une directive peut faire l'objet de la procédure de règlement des différends : celle-ci ne s'applique pas aux désaccords sur l'interprétation ou l'application des directives. Il incombe au Conseil fédéral et aux supérieurs hiérarchiques de veiller à ce que l'administration fédérale se conforme aux directives.

Let. c : les décisions visées sont celles prévues à l'art. 40, al. 3, qu'elles aient été déléguées ou non au sens de l'art. 40, al, 4. La procédure de règlement des différends peut porter sur la décision d'octroyer ou non une dérogation.

Let. d : les divergences concernant la numérisation transversale (par ex. l'utilisation des données) doivent aussi être éliminées par la procédure de règlement des différends, même si elles ne concernent pas une directive du secteur TNI ou concernent une directive édictée par un département en vertu de l'art. 41. Les départements règlent leurs différends *internes* par la voie hiérarchique, conformément à la procédure ordinaire prévue par la LOGA avant de faire usage de la procédure de règlement visée par le présent article. Le droit de proposition des membres du Conseil fédéral au sens de l'art. 3, al. 2, OLOGA est maintenu.

Le délégué TNI ouvre la procédure et prépare une proposition à l'intention de la CSG : il expose les divergences et leurs motifs. Le droit des départements de faire des propositions à la CSG ou au Conseil fédéral n'est pas touché.

Le Conseil TNI s'est déjà prononcé sur les directives contestées (art. 40, al. 2). Pour garantir la célérité de la procédure de règlement des différends, le délégué TNI peut donc informer les membres du conseil par voie de circulation, sans attendre la prochaine séance du conseil.

La célérité visée implique que le délégué TNI transmette l'affaire à la CSG dans les meilleurs délais. Il faut toutefois prévoir un laps de temps raisonnable pour la préparation de dossier. Le nouveau règlement de la CSG prévoit que les unités administratives intéressées sont consultées et que les directives sur les affaires du Conseil fédéral (Classeur rouge) s'appliquent par analogie, notamment en ce qui concerne les services qui doivent être systématiquement consultés et les délais applicables aux consultations des offices. Les offices ne seront donc pas exclus de ce processus.

Chapitre 9 Finances et audit

Art. 43 Gestion financière de la transformation numérique et de l'informatique

Les moyens financiers destinés aux nouveaux développements et aux optimisations, ainsi qu'à l'exploitation des applications métiers sont généralement budgétisés auprès des unités administratives compétentes (*al. 1*). Il en va de même des moyens destinés à l'exploitation des services standard. Les prestations des fournisseurs de prestations informatiques des départements sont refacturées conformément à l'art. 41 de l'ordonnance du 5 avril 2006 sur les finances de la Confédération (OFC)[46].

Pour accomplir les tâches prévues à l'art. 28, le secteur TNI a besoin d'informations à jour et complètes concernant les projets en cours ou planifiés, les applications exploitées et les infrastructures des unités administratives (*al. 2*). Les départements disposent depuis 2014 d'un outil de contrôle de gestion du portefeuille reposant sur SAP (PFCT Confédération) pour gérer les informations nécessaires aux projets de numérisation et aux applications. La Chancellerie fédérale règle les données à saisir, avec le concours des départements, dans une directive au sens de l'art. 40. Ces informations comprennent notamment des descriptions probantes des projets et des applications, leur statut et le montant des coûts uniques et des coûts récurrents. Les projets et les applications mineurs peuvent être exemptés de l'obligation de saisie si l'utilité des informations est faible et si, par exemple, il n'y a pas de besoin accru de protection.

Dans ce contexte, le secteur TNI met notamment à disposition l'outil PFCT Confédération, utilisable par toute l'administration fédérale, qui contient les données issues des systèmes financiers de la Confédération (*al. 3*). Il permet aux unités administratives de planifier et de surveiller l'utilisation de leurs ressources dans le domaine de la numérisation et de l'informatique. Le secteur TNI vérifie les demandes budgétaires dans ce domaine conformément à l'art. 22, al. 1, OFC. Par ailleurs, il répond aux besoins d'information des Commissions des finances des Chambres fédérales concernant le budget et le compte d'État, dans le domaine de la numérisation et de l'informatique (*al. 4*).

Pour accomplit la tâche visée à l'art. 28, al. 1, le secteur TNI a besoin d'informations à jour, complètes et probantes concernant les coûts et les recettes, au titre des services standard, des fournisseurs de prestations informatiques (*al. 5*).

46 RS **611.01**

Art. 44 Inscription au budget centralisée au moyen de crédits de programme

Des moyens financiers sont centralisés au secteur TNI :

a. pour l'introduction et le développement de services standard ;

b. pour des programmes et des projets qui entrent dans le champ d'application de l'ordonnance et qui ne peuvent, selon la planification, être financés par les unités administratives ;

c. pour des projets interdépartementaux dans le domaine de la transformation numérique.

Le Conseil fédéral décide chaque année, dans les limites de ses compétences budgétaires, des montants à affecter de manière centralisée à la transformation numérique et à l'informatique (*al. 1*). En ce qui concerne le cadre du développement du domaine propre, la réglementation dérogatoire décidée par le Conseil fédéral le 21 juin 2023 s'applique. Elle prévoit que les demandes de ressources pour l'ensemble de l'administration fédérale sont recevables, même directement auprès du Conseil fédéral, c'est-à-dire en dehors de l'identification des besoins.

L'attribution des ressources centralisées reste du ressort du chancelier de la Confédération *(al. 2*). Par le passé, les ressources centralisées à affecter à la transformation numérique et l'informatique visées à l'al. 1, ont été attribuées par le Conseil fédéral dans le cadre du processus budgétaire, sur proposition de la Chancellerie fédérale ou du DFF. Conformément à la pyramide de gouvernance de la transformation numérique et de l'informatique, l'art. 33 OTNI est repris. Le ch. 6 du règlement de la CSG prévoit que les unités administratives intéressées (comme l'AFF) sont consultées. Les directives du 8 septembre 2023 concernant les ressources centrales pour la numérisation[47] s'appliquent en particulier à la demande de moyens centralisés dans le cadre de l'évaluation des besoins concernant le cadre de développement du domaine propre.

Les ressources visées à l'*al. 3* comprennent notamment les réserves constituées jusqu'ici de manière centralisée au titre de la stratégie Administration fédérale numérique (par ex. pour les projets pilotes de numérisation) et les projets informatiques imprévisibles. Elles comprennent aussi les ressources qui ont été attribuées, mais qui ont été restituées, par exemple parce que les besoins ont diminué. Il va de soi que le secteur TNI peut aussi décider de ne pas attribuer ces moyens. Si le chancelier de la Confédération attribue les moyens (al. 2) dans le cadre du processus budgétaire, le secteur TNI les attribue tout au long de l'année. Les départements sont consultés avant cette attribution de moyens, généralement par l'intermédiaire du Conseil TNI.

Le secteur TNI gère les ressources financières centralisées. Il assure une gestion administrative, comparable à la tenue du budget.

47 https://intranet.dti.bk.admin.ch/isb_kp/fr/home/ikt-vorgaben/grundlagen/w003-weisungen_bundesrat_finanzielle_fuehrung_ikt-bereich.html (publication prévue sur Internet)

Art. 45 Participation des cantons aux coûts

La participation financière des cantons correspond aux coûts effectivement engendrés par l'utilisation qu'ils font des moyens informatiques mis à disposition. L'ensemble des coûts de matériel et de personnel, y compris l'amortissement, doit ainsi être pris en compte de manière proportionnelle (*al. 1*).

Les cantons prennent notamment en charge les coûts d'exploitation des moyens informatiques mis à disposition qu'ils entraînent (ainsi que ceux engendrés par leurs communes et les organisations et personnes de droit public ou privé qu'ils chargent de tâches publiques, voir *al. 2*). Ils supportent la part des coûts totaux de la fourniture de prestations qui leur est imputable en fonction du volume d'utilisation. Ils prennent également en charge les dépenses découlant de cette utilisation, notamment au titre des « services associés », qui comprennent essentiellement les frais de maintenance et d'assistance liés à ces moyens informatiques ou encore les frais engendrés par les dommages et les problèmes que l'utilisation des moyens informatiques et des services associés pourrait causer.

Les investissements peuvent représenter la part la plus importante des coûts dans le domaine informatique, aussi les autorités fédérales qui mettent les moyens informatiques à disposition facturent-elles également les coûts liés aux investissements et à leur amortissement par les cantons. La participation financière des cantons peut donc s'étendre aux investissements supplémentaires que l'utilisation des moyens informatiques génère, par exemple si la forte demande des cantons nécessite que l'offre soit développée.

Il revient à l'autorité qui met à disposition ses moyens informatiques d'établir la facture détaillant les différents éléments de l'al. 1 concernant l'utilisation de ces moyens par les cantons. Ces derniers sont responsables de la répartition interne des coûts, en particulier vis-à-vis des communes.

La prise en charge des coûts par les cantons est en principe réglée par un contrat liant l'autorité fédérale qui met à disposition le moyen informatique concerné et le canton qui l'utilise. Ce contrat peut aussi régler les obligations respectives de la Confédération et des cantons en cas d'utilisation inappropriée des moyens informatiques. Il peut notamment stipuler que la Confédération ne peut être tenue pour responsable en cas d'indisponibilité du service (définition du niveau de service, notamment en cas de maintenance ou de problèmes techniques).

Le droit fédéral applicable est réservé. Il existe déjà, dans de nombreux domaines juridiques, des réglementations autonomes en matière de prise en charge des coûts. Ces dernières doivent être respectées. La réserve vaut en particulier pour les réglementations différentes prévues par les unités administratives décentralisées, mais peut également toucher l'administration centrale (*al. 3*).

eOperations Suisse SA, à laquelle tant les cantons que la Confédération participent, est expressément nommée pour les contrats mentionnés à l'*al. 3*. Elle est déjà partenaire de la Confédération pour l'utilisation du validateur de signature eGov de la Confédération par les cantons. Le risque que la Confédération ne puisse pas défendre correctement ses intérêts au sein d'eOperations Suisse SA est en outre modeste, dans la mesure où c'est elle qui décide si un moyen informatique est mis à la disposition des

cantons. L'art. 11, al. 3, LMETA prévoit en outre des conditions supplémentaires si ces moyens sont utilisés pour exécuter le droit cantonal.

Les relations entre les cantons et les autorités fédérales qui leur mettent des moyens informatiques à disposition doivent être réglées par une convention (possibilité prévue par l'art. 4 LMETA).

Art. 46 Audit

La disposition est reprise telle quelle de l'art. 34 OTNI. Les tâches et les compétences du CDF sont réglées par la loi du 28 juin 1967 sur le Contrôle des finances (LCF)[48]. Le CDF exerce une activité autonome et indépendante dans les limites des prescriptions légales. Il fixe chaque année son programme de révision, qu'il communique à la Délégation des finances des Chambres fédérales et au Conseil fédéral (art. 1, al. 2, LCF). Il peut refuser les mandats spéciaux qui compromettraient l'indépendance et l'impartialité de ses futures activités de révision ou la réalisation du programme de révision. Il a donc le droit, comme le prévoit l'art. 46, de procéder à des audits dans le domaine de la transformation numérique et de l'informatique, mais il ne réalise pas pour autant tous les audits relevant de l'ONum.

Chapitre 12 Dispositions finales

Art. 47 Abrogation et modification d'autres actes

L'ONum fusionne l'OMETA et l'OTNI, ces dernières sont par conséquent abrogées à l'entrée en vigueur de l'ONum.

La modification d'autres actes concerne essentiellement des renvois aux dispositions de l'OMETA ou de l'OTNI, qui sont remplacés par des renvois à l'ONum. Les modifications plus substantielles d'autres actes sont commentées ci-après.

Art. 48 Disposition transitoire

Les unités administratives, autorités et organisations qui se sont soumises à l'OTNI par un accord avec le secteur TNI, conformément à l'art. 2, al. 2, OTNI, ne sont pas automatiquement soumises à l'ONum. Nombre d'entre elles ont conclu un accord avec le secteur TNI concernant l'utilisation des services standard gérés par celui-ci. Les accords portant sur l'utilisation des services standard restent valables pendant un délai transitoire d'un an à partir de l'entrée en vigueur de l'ONum. Ils devront ensuite être renouvelés ou abrogés pour satisfaire aux conditions de l'art. 11, al. 4, ONum. Une convention ne pourra être conclue que pour l'utilisation de moyens informatiques mis à disposition de manière centralisée.

48 RS **614.0**

Art. 49 Entrée en vigueur

L'ONum entre en vigueur le 1er mai 2025.

Annexe 1

Exceptions au champ d'application de la LMETA pour les unités administratives décentralisées de la Confédération

L'annexe 1 recense les unités administratives décentralisées qui ne sont soumises qu'aux dispositions indiquées de la LMETA et de l'ONum. Toute modification de l'annexe requiert l'autorisation du Conseil fédéral (art. 2, al. 2, LMETA).

Annexe 2

Modification d'autres actes

1. Ordonnance du 8 novembre 2023 sur la sécurité de l'information

L'actuel art. 38 de l'ordonnance du 8 novembre 2023 sur la sécurité de l'information (OSI)[49] règle les compétences en matière de garantie de la sécurité de l'information dans les services standard. Or l'expression *services standard* n'est plus utilisée dans l'ONum ; elle doit donc être remplacée dans cette disposition.

L'art. 38 continuera de ne régler que les responsabilités concernant la sécurité de l'information dans les moyens informatiques mis à disposition de manière centralisée par le secteur TNI, soit les services standard actuels. C'est toutefois la terminologie de la LSI et de l'OSI (moyen informatique) qui est reprise ici, avec le même sens. Lorsqu'un moyen informatique est mis à disposition de manière centralisée par une autre unité administrative, celle-ci est responsable de la sécurité de base en tant que bénéficiaire de prestations et représentante des autres bénéficiaires de prestations (art. 4 OSI). Toute unité qui utilise un moyen informatique mis à disposition de manière centralisée est responsable de la sécurité opérationnelle, puisque ses données et ses processus d'affaires sont concernés. Le fournisseur de prestations, en règle générale l'OFIT, est responsable de la sécurité de l'exploitation (art. 30 OSI).

3. Ordonnance GEVER du 3 avril 2019

[50] L'ordonnance GEVER règle en détail le service standard GEVER et doit être respectée par les autorités, organisations et personnes qui utilisent ce service. Il en va de même des directives fondées sur cette ordonnance.

La possibilité pour les autorités, organisations et personnes visées à l'art. 2, al. 2, OTNI de se soumettre par une convention à l'ordonnance GEVER disparaît. Par contre, les

49 RS **128.1**
50 RS **172.010.441**

unités administratives, autorités et organisations visées à l’art. 11, al. 4, ONum pourront utiliser le système de gestion des affaires proposé par le service TIC standardisé GEVER (GEVER standardisé) en concluant une convention avec le secteur TNI. Si elles le font, elles seront, conformément à la nouvelle formulation, automatiquement soumises à l’ordonnance GEVER.

3 Conséquences

3.1 Conséquences pour la Confédération

La nouvelle ordonnance aura des conséquences sur les unités de l’administration fédérale décentralisée, puisqu’elles sont désormais soumises à la LMETA (à l’exception de son art. 11). Elles devront en particulier respecter les mêmes directives que l’administration fédérale centrale en matière d’interopérabilité, afin que la transformation numérique de l’ensemble de l’administration fédérale soit un succès. Le Conseil fédéral peut cependant exclure du champ d’application de la LMETA, en tout ou partie, telle ou telle unité de l’administration fédérale décentralisée.

La nouvelle ordonnance n’a pas de conséquences pour la Confédération en matière de finances et de personnel.

3.2 Conséquences pour les cantons et les communes

La fusion de l’OMETA et de l’OTNI dans l’ONum n’a aucune conséquence d’ordre financier pour les cantons et les communes et n’aura pas non plus de conséquence sur leur personnel. Les modifications par rapport au droit en vigueur sont minimes et portent principalement sur des processus organisationnels de l’administration fédérale.