

# Ordonnance de la FINMA sur les données – révision totale

Rapport explicatif

9 mars 2022

# Table des matières

<b>Éléments essentiels .....</b>	<b>3</b>
<b>1 Contexte.....</b>	<b>4</b>
<b>2 Explications concernant les différentes dispositions .....</b>	<b>4</b>
2.1 Remarque préliminaire .....	4
2.2 Dispositions individuelles .....	5
<b>3 Suite de la procédure .....</b>	<b>12</b>

## Éléments essentiels

1. L'ordonnance de la FINMA sur les données est en vigueur depuis le 1<sup>er</sup> octobre 2011. Elle a été complétée et précisée lors de plusieurs révisions partielles. Sa version actuellement en vigueur règle d'une part la tenue d'un fichier de données contenant des indications sur des personnes qui peuvent être utiles pour l'examen des garanties d'une activité irréprochable (fichier de données sur les garanties d'une activité irréprochable, autrefois appelé *watch list*) et d'autre part le traitement des données par des tiers dans le cadre de la surveillance.
2. Le 25 septembre 2020, le Parlement a adopté la révision totale de la loi sur la protection des données. La base légale formelle pour le traitement des données par la FINMA et par des tiers dans le cadre de la surveillance (art. 23 LFINMA) a ainsi été précisée. Comme ce fut le cas jusqu'ici, le législateur a prévu que la FINMA règle les détails du traitement des données.
3. La révision totale de l'ordonnance de la FINMA sur les données a pour but de compléter et de préciser les dispositions d'exécution existantes de la FINMA à la lumière de la nouvelle réglementation fédérale. La FINMA veut ainsi honorer le mandat que lui a confié le législateur, qui consiste à régler les détails du traitement des données qu'elle effectue dans le cadre de la surveillance. Dans le même temps, il s'agit également de mettre en œuvre le droit de la protection des données qui a été révisé.

## 1 Contexte

Le 25 septembre 2020, le Parlement a adopté la révision totale de la loi fédérale sur la protection des données (LPD, nLPD ; FF 2020 7397). Il est prévu que la nLPD entre en vigueur en même temps que les dispositions d'exécution correspondantes qui figurent dans l'ordonnance relative à la loi fédérale sur la protection des données (OLPD ; RS 235.11), laquelle est également en cours d'adaptation.

En vertu de l'art. 23 de la loi sur la surveillance des marchés financiers (LFINMA ; RS 956.1), dans la version entièrement révisée de la loi fédérale sur la protection des données (nLFINMA ; FF 2020 7481 ss), la FINMA peut, dans le cadre de la surveillance selon la LFINMA et les lois sur les marchés financiers, traiter ou faire traiter des données personnelles, y compris des données sensibles (al. 1). Elle peut le faire en particulier pour (al. 2) : le contrôle de l'assujetti (let. a) ; la surveillance (let. b) ; la conduite de procédures (let. c) ; l'évaluation des garanties d'une activité irréprochable (let. d) ; l'évaluation du comportement d'une personne qui exerce une activité pour l'assujetti ou sur le marché financier (let. e) ; l'entraide administrative et judiciaire nationale et internationale (let. f). Pour le traitement des données effectué aux fins de l'al. 2 let. e, la FINMA est habilitée à faire du profilage selon la nLPD, y compris du profilage à risque élevé (al. 3). La FINMA règle les modalités (al. 4).

La présente révision totale vise à compléter et à préciser l'ordonnance de l'Autorité fédérale de surveillance des marchés financiers sur le traitement des données (ordonnance de la FINMA sur les données ; RS 956.124) à la lumière de la nouvelle réglementation fédérale sur le droit de la protection des données. Le but est de mettre en œuvre le mandat légal confié à la FINMA à l'art. 23 al. 4 nLFINMA et de tenir compte des exigences qui découlent de la révision du droit de la protection des données.

## 2 Explications concernant les différentes dispositions

### 2.1 Remarque préliminaire

La version entièrement révisée de l'ordonnance de la FINMA sur les données comprend les parties suivantes : dispositions générales (section 1), dispositions sur le traitement des données en général (section 2) et dispositions relatives à la banque de données nécessaire à l'examen des garanties d'une activité irréprochable en particulier (section 3).

Les dispositions applicables au fichier de données sur les garanties d'une activité irréprochable (section 2, art. 1 a à 9 de l'ordonnance de la FINMA sur

les données) sont conservées pour l'essentiel sans modification matérielle et constituent la section 3 intitulée « Banque de données nécessaire à l'examen des garanties d'une activité irréprochable ». La terminologie doit être adaptée en raison de la révision du droit de la protection des données. Le terme « fichier de données » est supprimé car la notion de « fichier » n'est plus utilisée dans la nLPD (cf. message nLPD, FF 2017 6643 ss) et doit donc être remplacé.

La disposition en vigueur concernant le traitement des données par des tiers (section 3, art. 9a de l'ordonnance de la FINMA sur les données) n'est pas reprise. Le fait de confier le traitement de données personnelles par un responsable du traitement à un sous-traitant est réglé dans la législation générale relative à la protection des données (art. 10a LPD et 9 nLPD ainsi que art. 22 OLPD et 6 et 7 P-OLPD) et est possible pour tout responsable du traitement d'une façon générale. Avec l'art. 23 al. 1 nLFINMA, la possibilité pour la FINMA de confier le traitement des données à des sous-traitants (c'est-à-dire des personnes mandatées par la FINMA au sens de l'art. 14 al. 4 LFINMA et des prestataires mandatés sous le régime du droit privé) est en outre expressément prévue à l'avenir sur une base légale formelle (cf. message nLPD, FF 2017 6765).

Dans le cadre de son activité de surveillance, la FINMA est amenée à travailler régulièrement avec des tiers pour des raisons d'efficience. Il s'agit en l'occurrence de personnes mandatées par la FINMA pour effectuer des tâches de droit public (chargés d'audit, chargés d'enquête, délégués à l'assainissement, liquidateurs, gérants) ou des fournisseurs de prestations externes travaillant pour la FINMA sur une base contractuelle. L'accomplissement de leur mandat et la fourniture de leurs services implique que des données non accessibles au public soient portées à la connaissance de ces tiers. La FINMA veille à ce que les personnes qu'elle mandate et ses fournisseurs de prestations externes n'aient accès qu'aux données nécessaires à l'exécution de leur mandat et à la fourniture de leurs services, et qu'ils ne puissent traiter que ces données.

## 2.2 Dispositions individuelles

### Section 1 Dispositions générales

#### Art. 1 Objet

L'ordonnance s'applique au traitement de données personnelles par la FINMA dans le cadre de la surveillance prévue par la LFINMA et par les lois sur les marchés financiers et règle les modalités sur la base de l'art. 23 al. 1 LFINMA et de l'art. 23 al. 4 nLFINMA.

## **Art. 2 Compétences**

La division Technologies de l'information et de la communication (ICT) de la FINMA assure l'exploitation technique des systèmes d'information et peut, dans le cadre de l'administration et de la maintenance des systèmes, avoir accès à des données personnelles dans la mesure où cela est nécessaire à l'exécution de ses tâches (al. 1).

La direction de la FINMA fixe, dans un ou plusieurs règlements de traitement au sens de l'art. 21 OLPD et de l'art. 5 P-OLPD, les mesures techniques et organisationnelles requises pour garantir la sécurité des données conformément aux dispositions de l'OLPD et du P-OLPD, le contrôle du traitement des données, et les droits d'accès et de regard des différentes catégories de collaborateurs de la FINMA (al. 2).

Les personnes concernées peuvent faire valoir les droits prévus par la nLPD, notamment les droits d'accès, de rectification et d'effacement, auprès de la division Droit et compliance de la FINMA (al. 3). La division Droit et compliance assume la fonction de conseiller à la protection des données selon les art. 27 à 30 P-OLPD et est l'interlocuteur des personnes concernées. Les collaborateurs et collaboratrices de la FINMA lui transmettent les requêtes ayant pour objet l'exercice des droits des personnes concernées selon la LPD.

## **Section 2 Traitement des données**

### **Art. 3 But**

Pour accomplir son mandat légal, la FINMA traite des données personnelles de personnes physiques et morales, y compris des données sensibles. Elle le fait notamment dans les buts cités à l'art. 23 al. 2 nLFINMA : *a. le contrôle de l'assujetti ; b. la surveillance ; c. la conduite de procédures ; d. l'évaluation des garanties d'une activité irréprochable ; e. l'évaluation du comportement d'une personne qui exerce une activité pour l'assujetti ou sur le marché financier ; f. l'entraide administrative et judiciaire nationale et internationale*. Le but premier du traitement des données par la FINMA est de protéger les créanciers, les investisseurs et les assurés, et d'assurer le bon fonctionnement des marchés financiers (art. 4 LFINMA).

### **Art. 4 Compétence**

Chaque unité d'organisation de la FINMA est responsable de ses données et de leur traitement.

L'exploitation technique des systèmes d'information est garantie par la division ICT (cf. art. 2 al. 1).

Les collaborateurs et collaboratrices de la FINMA qui travaillent avec des données personnelles prennent des mesures propres à garantir la sécurité des données dans leur domaine d'activité. Ils y sont sensibilisés par des directives et formations internes.

#### **Art. 5 Droits d'accès**

Les droits d'accès sont attribués en respectant le principe du *need to know*. Les collaborateurs et collaboratrices de la FINMA disposent de droits d'accès aux données qui relèvent de leur fonction de surveillance respective (al. 1). Cela signifie qu'un collaborateur ou une collaboratrice de la division Banques a accès aux données et aux dossiers de la division Banques ; une collaboratrice ou un collaborateur de la division Enforcement a accès aux données et aux dossiers de la division Enforcement. Les collaborateurs et collaboratrices de la FINMA qui exercent une fonction transversale (par ex. dans les divisions Enforcement, Recovery et Resolution, Lutte contre le blanchiment d'argent, Droit et compliance, ICT, etc.) peuvent également avoir des droits d'accès à d'autres données dont ils ont besoin pour exécuter leurs tâches respectives (al. 2). Si nécessaire, les droits d'accès peuvent être restreints ou élargis à certain(e)s collaborateurs ou collaboratrices de la FINMA (al. 3).

Les détails concernant la nature et l'étendue des droits d'accès des différentes catégories de collaborateurs et collaboratrices de la FINMA sont réglés dans un règlement de traitement (cf. art. 2 al. 2).

#### **Art. 6 Catégories de données personnelles traitées**

L'art. 6 dresse la liste des catégories de données que la FINMA peut traiter dans le cadre de l'exécution de ses tâches légales.

La surveillance des marchés financiers suppose de disposer d'informations complètes sur les assujettis et sur les acteurs des marchés financiers. Dans le cadre de ses activités de surveillance, la FINMA traite donc une multitude de données (cf. message nLPD ; FF 2017 6765), qui sont énumérées à l'art. 6. Les assujettis ainsi que d'autres personnes sont soumis aux obligations de renseigner et d'annoncer vis-à-vis de la FINMA (par ex. art. 29 LFINMA ; il existe également d'autres obligations découlant des lois sur les marchés financiers et de la loi fédérale sur la procédure administrative, PA ; RS 172.021). L'obligation de renseigner et d'annoncer est l'un des instruments de surveillance fondamentaux de la FINMA qui lui permet d'assumer ses tâches. Des données personnelles peuvent également parvenir à la FINMA en vertu des obligations de renseigner et d'annoncer (let. m).

Dans le cadre de l'exécution de ses tâches, la FINMA reçoit régulièrement des communications provenant de tiers (par ex. des clients d'assujettis) concernant des irrégularités supposées commises par des assujettis. La FINMA

est légalement tenue de mener des investigations sur les irrégularités commises par les assujettis, de veiller à ce qu'elles cessent et à ce que l'ordre légal soit rétabli (art. 31 LFINMA). Des données personnelles peuvent également être portées à la connaissance de la FINMA dans le cadre de ces communications (let. n).

#### **Art. 7 Collecte des données personnelles**

L'art. 7 reprend et complète l'art. 5 de l'ordonnance de la FINMA sur les données actuellement en vigueur, qui est désormais défini à la section 2 de la version entièrement révisée de l'ordonnance sur les données, et s'applique à tous les traitements de données de la FINMA.

Dans le cadre de son activité de surveillance, la FINMA collecte des données personnelles non seulement auprès des personnes concernées, mais aussi auprès de tiers (al. 1).

Des données personnelles sont également collectées par la FINMA lors de recherches qu'elle effectue dans des sources accessibles au public ou non (al. 2). Ainsi, elle collecte et traite des données personnelles issues de recherches sur Internet. Les recherches sur Internet sont réalisées au moyen de moteurs de recherche gratuits (Google, par ex.), de banques de données publiques gratuites (Zefix, par ex.), de banques de données payantes (Teledata ou Worldcheck, par ex.) et en consultant des profils d'utilisateur publics sur les réseaux sociaux (Facebook, Twitter, LinkedIn, Xing, par ex.).

Afin de ne pas compromettre le but d'un traitement de données, il peut s'avérer nécessaire que la FINMA collecte des données personnelles à l'insu de la personne concernée (al. 3). En particulier lors d'investigations préliminaires menées en cas de soupçon d'activité exercée sans droit ou dans le cadre de la surveillance du marché, la FINMA peut être amenée à collecter et à traiter des données personnelles sans que les personnes concernées n'en aient toujours connaissance. Ainsi, par exemple, la FINMA utilise des faux noms ou pseudonymes (appelés « profils XY ») lors de recherches sur Internet afin d'accéder à des profils d'utilisateur publics sur les réseaux sociaux. Cela vise à empêcher que la personne concernée ait connaissance des investigations réalisées par la FINMA afin d'éviter qu'elle ne contrecarre ou empêche la réalisation d'une enquête ultérieure en détruisant ou modifiant des preuves, ou encore en usant de son influence envers des témoins et d'autres parties concernées (risque de collusion).

#### **Art. 8 Modalités de la communication de données personnelles**

La FINMA ne peut communiquer de données personnelles que si les conditions énoncées à l'art. 19 LPD ou à l'art. 36 nLPD sont remplies. La FINMA ne communique des données personnelles à des tiers que dans le cadre d'une autorisation légale. En principe, la réponse de savoir à qui et quelles



données la FINMA peut ou doit communiquer (par ex. à d'autres autorités de surveillance ou à des autorités pénales) découle d'une base légale formelle (LFINMA, lois sur les marchés financiers ou autres lois par ex.) .

L'art. 8 énonce les modalités de la communication des données par la FINMA. Celle-ci peut avoir lieu soit sur papier (par ex. par la poste), soit sous forme électronique. Dans ce dernier cas, des systèmes de communication et de transmission électroniques sont utilisés (téléphone, courriel ou outils collaboratifs, par ex.). Lorsqu'elle utilise de tels systèmes, la FINMA prend des mesures appropriées pour garantir la sécurité des données et elle forme ses collaborateurs et collaboratrices en conséquence.

#### **Art. 9 Conservation des données**

En vertu de l'art. 6 de la loi fédérale sur l'archivage (LAr ; RS 152.1) en relation avec l'art. 4 de l'ordonnance sur l'archivage (OLAr ; RS 152.11), la FINMA a l'obligation de proposer aux Archives fédérales les documents (dont font également partie les données personnelles) dont elle n'a plus besoin en permanence (cf. aussi art. 21 LPD et art. 38 nLPD). Les documents (y c. les données personnelles) sont conservés auprès de la FINMA aussi longtemps qu'ils peuvent être utiles pour la surveillance, puis sont proposés aux Archives fédérales pour conservation. Les documents (y c. les données personnelles) que les Archives fédérales désignent comme n'ayant plus de valeur archivistique sont détruits par la FINMA.

### **Section 3 Banque de données nécessaire à l'examen des garanties d'une activité irréprochable**

#### **Art. 10 But**

Les lois sur les marchés financiers exigent comme condition d'octroi d'une autorisation – devant être respectée en permanence – par les établissements assujettis à la surveillance de la FINMA que seules des personnes offrant toutes garanties d'une activité irréprochable assument la gestion ou la direction d'un assujetti ou détiennent une participation qualifiée dans un assujetti.

La FINMA saisit dans une banque de données les données de personnes pour lesquelles les garanties d'une activité irréprochable doivent être examinées si elles étaient appelées à l'avenir à occuper une position pour laquelle elles doivent présenter lesdites garanties. Elle gère la banque de données pour s'assurer que seules les personnes présentant toutes garanties d'une activité irréprochable assument la gestion ou la direction d'un assujetti ou détiennent une participation qualifiée dans un assujetti. Dans le cadre de la gestion de la banque de données, la FINMA ne procède à aucun profilage au sens de la nLPD.

La banque de données est un instrument de travail qui sert exclusivement à la gestion interne des connaissances afin de s'assurer de disposer des données pertinentes au cas où les garanties d'une activité irréprochable doivent être examinées à l'avenir. La saisie de ces données dans la banque de données ne préjuge toutefois en rien la question de savoir si la personne concernée présente ou non toutes garanties d'une activité irréprochable. La FINMA est libre, eu égard aux données saisies dans la banque de données, de porter une appréciation positive sur l'existence de ces garanties dans le cadre d'une fonction concrètement envisagée, par exemple en raison du temps qui s'est écoulé et parce que la personne concernée a durablement fait preuve d'un comportement en affaires adéquat et qu'un pronostic favorable peut donc être émis quant au respect de l'exigence des garanties d'une activité irréprochable. Inversement, l'absence de données au sujet d'une personne dans la banque de données ne signifie pas que la FINMA n'est pas autorisée ou tenue de vérifier sur la base d'autres informations si ladite personne présente toutes garanties d'une activité irréprochable.

#### **Art. 11 Compétence**

La gestion de la banque de données et des traitements de données qui y sont liés relève de la compétence de la division Droit et compliance.

L'exploitation technique de la banque de données est assurée par la division ICT (cf. art. 2 al. 1).

#### **Art. 12 Droits d'accès**

Les droits d'accès à la banque de données sont attribués de manière restrictive selon le principe du *need to know*. Ils sont approuvés et périodiquement contrôlés par la division Droit et compliance. La division Droit et compliance et les collaborateurs et collaboratrices de la FINMA compétents pour l'examen des garanties d'une activité irréprochable disposent de droits d'accès (al. 1). La division Droit et compliance peut fournir par écrit ou par oral aux collaborateurs et collaboratrices de la FINMA qui en font la demande des renseignements sur une entrée (al. 2).

Les détails concernant la nature et l'étendue des droits d'accès des différentes catégories de collaborateurs et collaboratrices de la FINMA sont réglés dans un règlement de traitement (cf. art. 2 al. 2).

#### **Art. 13 Contenu**

L'art. 13 définit les données que la FINMA a le droit de détenir dans la banque de données nécessaire à l'examen des garanties d'une activité irréprochable. Conformément au but de la banque de données, il s'agit des don-

nées dont la FINMA peut avoir besoin pour apprécier les garanties d'une activité irréprochable. La disposition fait une énumération exhaustive des catégories de données que la banque de données peut contenir.

Dans un arrêt du 22 mars 2017 (ATF 143 I 253), le Tribunal fédéral a jugé que l'art. 23 LFINMA en lien avec le but de la banque de données – laquelle était encore désignée par le terme *watch list* dans ces lois – fondé sur les lois sur les marchés financiers (vérification de l'exigence de garantie) représentait une base légale formelle suffisante pour la gestion de la banque de données. Sont autorisées les « données confirmées sur une personne en lien avec des données fiables sur l'activité commerciale ». Sont considérées comme telles selon le Tribunal fédéral les données issues de procédures dans lesquelles la personne concernée a les droits de partie, notamment des procédures pénales et administratives ainsi que des procédures de surveillance et des procédures disciplinaires, ou les données provenant d'autres sources fiables telles que des inscriptions dans des registres ou des résultats d'audits internes ou externes et d'évaluations du personnel réalisés comme il se doit. En revanche, le stockage de données découlant de simples soupçons n'est pas autorisé (ATF 143 I 253, consid. 6.5.3).

La FINMA observe la pratique du Tribunal fédéral et a repris le catalogue de données en vigueur actuellement en y apportant des modifications marginales. En ce sens, l'énumération faite à l'art. 13 contient, outre les données personnelles qui permettent notamment de vérifier l'identité de la personne dont les données ont été saisies et de décrire son activité professionnelle (let. a et b), d'autres catégories de données qui reposent soit sur des procédures fondées sur le droit, soit sur des sources fiables (let. c à m), et qui répondent donc aux exigences définies par le Tribunal fédéral. En outre, la FINMA vérifie toujours au cas par cas si les données enregistrées remplissent les critères qualitatifs retenus par le Tribunal fédéral.

La personne concernée étant informée une fois les données saisies dans la banque de données (cf. art. 14 ci-après), elle est en mesure d'exercer ses droits en vertu de la nLPD si cela s'avère nécessaire.

#### **Art. 14 Information de la personne concernée**

La personne concernée est informée une fois les données saisies dans la banque de données. Les données saisies dans la banque de données lui sont communiquées en précisant la base sur laquelle repose cette saisie. L'information a lieu sous la forme d'une communication à l'adresse de correspondance connue de la FINMA ou à l'adresse de domicile de la personne concernée en Suisse connue de la FINMA. La personne concernée est autorisée à exercer son droit de consultation des données saisies en s'adressant à la division Droit et compliance (cf. art. 2 al. 3).

L'art. 20 nLPD demeure expressément réservé. La FINMA peut notamment restreindre ou différer la communication des informations, ou y renoncer, aux conditions énoncées à l'art. 20 al. 3 nLPD. Cela est notamment le cas si la communication est susceptible de compromettre une investigation ou une enquête de la FINMA ou d'une autre autorité, telle qu'une autorité pénale par exemple.

#### **Art. 15 Conservation des données**

Cette disposition n'est pas modifiée sur le fond et règle la durée de conservation d'une inscription concernant une personne déterminée dans la banque de données et la durée pendant laquelle des données la concernant y sont enregistrées à cet effet.

### **3 Suite de la procédure**

Il est prévu que la version entièrement révisée de l'ordonnance de la FINMA sur les données soit adoptée et entre en vigueur après l'entrée en vigueur de la version entièrement révisée de la loi sur la protection des données ainsi que des dispositions d'exécution correspondantes figurant dans l'ordonnance relative à la loi fédérale sur la protection des données.