Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

Ordonnance de la FINMA sur les données – révision totale

Explications

4 mai 2023

Laupenstrasse 27, 3003 Berne, tél. +41 (0)31 327 91 00, www.finma.ch

Table des matières

Éléments essentiels

1. L’ordonnance de la FINMA sur les données est en vigueur depuis le 1er 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 watchlist) 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 honore ainsi 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 sur la protection des données (ci-après nLPD ; RO *2022* 491). La nLPD entre en vigueur le 1er septembre 2023, en même temps que l'ordonnance sur la protection des données du 31 août 2022, laquelle a également fait l'objet d'une révision totale (ci-après nOPD ; RO *2022* 568).

En vertu du nouvel 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 (RO *2022* 491), 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 au nouvel art. 23 al. 4 LFINMA 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 relatives à l'objet et aux compétences (section 1), dispositions relatives au traitement des données en général (section 2) et dispositions relatives à la banque de données nécessaire à l'évaluation 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'évaluation 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 concernant la nLPD du 15 septembre 2017, FF *2017* 6565, p. 6643 s.) et doit donc être remplacé.

La disposition en vigueur concernant le traitement des données par des tiers (section 3, art. 9*a* 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. 9 nLPD ainsi que art. 7 nOPD) et est possible pour tout responsable du traitement d'une façon générale. Avec le nouvel art. 23 al. 1 LFINMA, 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 concernant la nLPD du 15 septembre 2017, FF *2017* 6565, p. 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 ne traitent que ces données.

2.2 Dispositions individuelles

Section 1 Objet et compétences

Art. 1 Objet

La nLPD est la loi-cadre qui établit les principes généraux du traitement des données et doit être respectée par tous les organes fédéraux (art. 2 al. 1 let. b nLPD). Les modalités concrètes du traitement des données de droit public au niveau fédéral sont en revanche réglées dans les bases légales propres à chaque domaine. La révision totale de l'ordonnance de la FINMA sur les données définit plus précisément la base légale de la FINMA pour les différents domaines d'intervention (nouvel art. 23 LFINMA). L'ordonnance de

la FINMA sur les données 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 du nouvel art. 23 al. 4 LFINMA.

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 dans lesquels des données personnelles sont traitées (al. 1). Dans le cadre de l'administration et de la maintenance des systèmes, la division ICT peut avoir accès à des données personnelles dans la mesure où cela est nécessaire à l'exécution de ses tâches.

La direction de la FINMA fixe, dans un ou plusieurs règlements de traitement au sens de l'art. 6 nOPD, les mesures techniques et organisationnelles requises pour garantir la sécurité des données conformément aux dispositions de la nOPD, le contrôle du traitement des données, et les droits d'accès 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). Les collaborateurs de la FINMA transmettent à cette division les requêtes ayant pour objet l'exercice des droits des personnes concernées selon la nLPD.

Section 2 Traitement des données

Art. 3 Compétence

Chaque unité d'organisation de la FINMA est responsable de ses données et de leur traitement. Il s'agit d'une règle relative aux compétences organisationnelles. La FINMA, en tant qu'organe fédéral, est responsable au sens de l'art. 5 let. j nLPD.

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

Les collaborateurs 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. 4 Accès aux données

Les droits d'accès sont attribués en respectant le principe du *need to know*. Les collaborateursde la FINMA disposent de droits d'accès aux données qui

relèvent de leur fonction de surveillance respective (al. 1). Cela signifie qu'un collaborateur de la division Banques a accès aux données et aux dossiers de la division Banques ; un collaborateur de la division Assurances a accès aux données et aux dossiers de la division Assurances. Les collaborateurs 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.) ont également accès, à d'autres données (par ex. les données d'autres fonctions) dont ils besoin pour exécuter leurs tâches respectives (al. 2), en sus des données accessibles à leur fonction respective (al. 1). Dans la mesure où cela est nécessaire dans le cas d'espèce, les droits d'accès peuvent être restreints à certain(e)s collaborateurs de la FINMA (par ex. pour les données sensibles) ou accordés à d'autres collaborateurs (par ex. pour les données qui doivent être traitées par plusieurs divisions) (al. 3).

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

Art. 5 Catégories de données personnelles traitées

L'art. 5 al. 1 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 concernant la nLPD du 15 septembre 2017, FF *2017* 6565, p. 6765), qui sont énumérées à l'art. 5 al. 1. Il n'est pas possible de prédéfinir de manière abstraite les catégories de données personnelles qui parviennent à la FINMA et qui peuvent être pertinentes pour l'activité de surveillance. Pour cette raison, le catalogue de données de l'art. 5 al. 1 ne contient pas de catégories de données personnelles définies exclusivement de manière abstraite, mais se réfère également en partie à la manière, à la provenance ou aux finalités des données.

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).

Aussi bien le catalogue général de l'art. 5 al. 1 que le catalogue relatif à la banque de données nécessaire à l'évaluation des garanties d'une activité irréprochable de l'art.11 énumère le numéro AVS au rang des données relatives à l'identité (let. a). L'utilisation, par la FINMA, du numéro AVS aux fins d'identification dans le cadre de l'exécution des tâches légales de la FINMA fait actuellement l'objet d'un examen ponctuel. Une telle utilisation découlerait de l'habilitation contenue à l'art. 153c al. 1 let. a ch. 2 de la loi fédérale sur l'assurance-vieillesse et survivants (LAVS; RS *831.10*). Elle interviendrait dans le respect des prescriptions légales spéciales des art. 153b ss LAVS et art. 134bis ss du règlement sur l'assurance-vieillesse, survivants et invalidité facultative (RAVS; RS *831.101*).

À des fins de transparence, l'art. 5 al. 2 indique les catégories de données personnelles sensibles selon l'art. 5 let. c ch. 1 à 6 nLPD qui peuvent être contenues dans les données traitées par la FINMA conformément à l'al. 1.

Art. 6 Collecte des données personnelles

L'art. 6 reprend et complète l'art. 5 de l'ordonnance de la FINMA sur les données actuellement en vigueur, qui est désormais ancré 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 à partir d'autres sources non accessibles au public et de sources accessibles au public (al. 2). Ainsi, elle collecte et traite des données personnelles issues notamment 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 de cette nature reposant sur des recherches sur Internet, il peut s'avérer nécessaire que la FINMA collecte des données personnelles sans révéler son identité (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, afin d'éviter le risque de collusion, collecter et traiter des données personnelles sans être alors directement identifiable pour la personne concernée. Ainsi, lors de recherches sur Internet, la FINMA peut utiliser des pseudonymes afin d'accéder à des réseaux sociaux pour voir les informations postées ou mises à disposition par l'utilisateur sur un profil public. Dans ce cas, en revanche, il n'y a pas de prise de contact ni d'interaction plus poussée avec la personne concernée.

Art. 7 Forme de la communication de données personnelles

La FINMA ne peut communiquer de données personnelles que si les conditions énoncées 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 à la question 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. 7 énonce la forme sous laquelle les données sont communiquées par la FINMA. La communication 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 en conséquence.

Art. 8 Conservation et destruction des données personnelles

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. 38 nLPD). Les documents (y c. les données personnelles) sont conservés auprès de la FINMA aussi longtemps qu'ils sont pertinents et nécessaires à la surveillance. Ensuite, les documents (y c. les données personnelles) sont proposés aux Archives fédérales pour archivage et détruites à la FINMA.

Section 3 Banque de données nécessaire à l'évaluation des garanties d'une activité irréprochable

Art. 9 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 tient à jour une banque de données pour assurer l'évaluation des garanties d'une activité irréprochable au sens des lois sur les marchés financiers. À cet effet, elle saisit dans la banque de données les données nécessaires pour le cas où une évaluation future des garanties d'une activité irréprochable serait réalisée. Elle tient à jour 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.

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 évaluées 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 une personne censée présenter lesdites garanties, 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 et tenue de vérifier sur la base d'autres informations si ladite personne présente toutes garanties d'une activité irréprochable.

Art. 10 Accès aux données

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 une division centrale. La division Droit et compliance et les collaborateurs de la FINMA compétents pour l'évaluation des garanties d'une activité irréprochable ont accès à la banque de données (al. 1). Les collaborateurs qui ont accès à la banque de données selon l'al. 1 peuvent fournir

par écrit ou par oral à d'autres collaborateurs de la FINMA qui en font la demande des renseignements sur des données contenues dans la banque de données dans la mesure où l'exécution de leurs tâches l'exige (al. 2).

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

Art. 11 Contenu

L'art. 11 définit les données nécessaires à l'évaluation des garanties d'une activité irréprochable que peut contenir la banque de données. Conformément au but de la banque de données, il s'agit des données dont la FINMA peut avoir besoin pour évaluer 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 *watchlist* 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. 11 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. 12 ci-après), elle est en mesure de faire valoir ses droits en vertu de la nLPD si cela s'avère nécessaire.

Art. 12 Information de la personne concernée

La personne concernée est informée après la première saisie dans la banque de données. L'information porte sur la saisie dans la banque de données 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 faire valoir ses droits en vertu de la nLPD auprès de la division Droit et compliance, notamment à demander des renseignements sur les données saisies (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. 13 Conservation et destruction des données

Cette disposition a été reprise du droit en vigueur sans modification sur le fond et règle la durée de conservation d'une saisie 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

La version entièrement révisée de l'ordonnance de la FINMA sur les données entre en vigueur en même temps que la version entièrement révisée du droit de la protection des données de la Confédération, à savoir le 1er septembre 2023.