DÉCISION (UE) 2021/1486 DE LA BANQUE CENTRALE EUROPÉENNE

du 7 septembre 2021 portant adoption de règles internes concernant les limitations des droits des personnes concernées en lien avec les missions de la Banque centrale européenne en matière de surveillance prudentielle des établissements de crédit

(BCE/2021/42)

LE DIRECTOIRE DE LA BANQUE CENTRALE EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu les statuts du Système européen de banques centrales et de la Banque centrale européenne, et notamment leur article 11.6,

vu le règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE ([1]), et notamment son article 25,

considérant ce qui suit:

(1) La Banque centrale européenne (BCE) exerce ses missions conformément aux traités et au règlement (UE) nº 1024/2013 du Conseil ([2]).

(2) Conformément à l'article 45, paragraphe 3, du règlement (UE) 2018/1725, la décision (UE) 2020/655 de la Banque centrale européenne (BCE/2020/28) ([3]) établit les règles générales d'application du règlement (UE) 2018/1725 pour ce qui concerne la BCE. Elle précise notamment les règles relatives à la désignation et au rôle du délégué à la protection des données de la BCE, y compris ses tâches, ses fonctions et ses compétences.

(3) Dans l'accomplissement des missions qui lui sont confiées, la BCE, et notamment l'unité organisationnelle concernée, agit en qualité de responsable du traitement dans la mesure où elle détermine, seule ou conjointement avec d'autres, les finalités et les moyens du traitement des données à caractère personnel.

(4) Conformément à l'article 4, paragraphe 1, du règlement (UE) nº 1024/2013, la BCE est seule compétente pour exercer, à des fins de surveillance prudentielle, et en ayant pour objectif de garantir la sécurité et la solidité des établissements de crédit et la stabilité du système financier, des missions spécifiques à l'égard de tous les établissements de crédit établis dans les États membres participant au mécanisme de surveillance unique (MSU).

(5) Dans l'accomplissement de ces missions spécifiques, la BCE traite plusieurs catégories d'informations qui peuvent se rapporter à une personne physique identifiée ou identifiable telles que les données d'identification, les coordonnées, les données professionnelles, les détails financiers ou administratifs, les données provenant de sources spécifiques, les données relatives aux communications électroniques et au trafic des communications électroniques, les casiers judiciaires, une description des intérêts financiers et non financiers, les détails des relations d'une personne ou de ses parents proches avec des entités soumises à la surveillance prudentielle ou des membres de l'organe de direction d'une telle entité, et les données relatives au poste auquel une personne a été nommée ou est susceptible de l'être. Les données à caractère personnel pourraient également faire partie d'une évaluation, y compris une évaluation réalisée: aux fins de l'agrément d'un établissement de crédit, du retrait de l'agrément d'un établissement de crédit et d'une procédure relative à une participation qualifiée; en ce qui concerne le droit d'établissement d'une entité importante soumise à la surveillance prudentielle; pour déterminer si les exigences d'honorabilité, de connaissances, de compétences et d'expérience sont remplies; en ce qui concerne les politiques de rémunération d'une entité importante soumise à la surveillance prudentielle et les crédits accordés par une telle entité à ses cadres dirigeants et aux personnes liées à ces cadres; et en ce qui concerne des allégations relatives à d'éventuelles infractions aux actes juridiques visés à l'article 4, paragraphe 3, du règlement (UE) nº 1024/2013.

([1]) JO L 295 du 21.11.2018, p. 39.

([2]) Règlement (UE) nº 1024/2013 du Conseil du 15 octobre 2013 confiant à la Banque centrale européenne des missions spécifiques ayant trait aux politiques en matière de surveillance prudentielle des établissements de crédit (JO L 287 du 29.10.2013, p. 63).

([3]) Décision (UE) 2020/655 de la Banque centrale européenne du 5 mai 2020 portant adoption de dispositions d'application en ce qui concerne la protection des données à la Banque centrale européenne et abrogeant la décision BCE/2007/1 (BCE/2020/28) (JO L 152 du 15.5.2020, p. 13).

(6) Le but de la BCE dans l'accomplissement de ces missions spécifiques est de poursuivre des objectifs importants d'intérêt public général de l'Union. Pour cette raison, il convient de garantir l'accomplissement de ces missions comme le prévoit le règlement (UE) 2018/1725, et notamment son article 25, paragraphe 1, points c) et g). En particulier, dans l'accomplissement de ces missions, la BCE agit dans l'intérêt public général de l'Union en tant qu'autorité publique chargée d'exercer, à des fins de surveillance prudentielle, des missions spécifiques à l'égard de tous les établissements de crédit établis dans les États membres participant au MSU. Ces missions incluent les fonctions de contrôle, d'inspection ou de réglementation liées à l'exercice de l'autorité publique en ce qui concerne la surveillance prudentielle des établissements de crédit.

(7) Dans ce contexte, il convient de préciser les motifs pour lesquels la BCE peut limiter les droits des personnes concernées relatifs aux données obtenues dans l'accomplissement de ses missions de surveillance prudentielle au titre du règlement (UE) n° 1024/2013.

(8) Conformément à l'article 25, paragraphe 1, du règlement (UE) 2018/1725, des limitations à l'application des articles 14 à 22, 35 et 36, ainsi que de l'article 4 de ce règlement dans la mesure où ses dispositions correspondent aux droits et obligations prévus aux articles 14 à 22, devraient être établies dans des règles internes ou des actes juridiques adoptés sur la base des traités. Par conséquent, il convient que la BCE définisse les règles en vertu desquelles elle peut limiter les droits des personnes concernées dans l'accomplissement de ses missions de surveillance prudentielle.

(9) Bien que la présente décision établisse les règles en vertu desquelles la BCE peut limiter les droits des personnes concernées dans l'accomplissement de ses missions de surveillance prudentielle, le directoire a l'intention d'adopter une décision distincte portant adoption de règles internes concernant la limitation de ces droits lorsque la BCE traite des données à caractère personnel en lien avec son fonctionnement interne.

(10) La BCE peut appliquer une exception conformément au règlement (UE) 2018/1725, ce qui rend inutile la nécessité d'envisager une limitation, y compris en particulier une de celles énoncées à l'article 15, paragraphe 4, à l'article 16, paragraphe 5, à l'article 19, paragraphe 3, et à l'article 35, paragraphe 3, de ce règlement. En ce qui concerne le traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, la BCE peut appliquer une exception prévue à l'article 16, paragraphe 5, point b), ou à l'article 19, paragraphe 3, point d), du règlement (UE) 2018/1725.

(11) L'exercice des droits des personnes concernées visés aux articles 17, 18, 20, 21, 22 et 23 du règlement (UE) 2018/1725 peut rendre impossible ou entraver sérieusement la réalisation de certaines finalités, y compris, selon le cas, des fins archivistiques dans l'intérêt public, des fins de recherche scientifique ou historique ou des fins statistiques. Par conséquent, il convient que la présente décision prévoie une dérogation à ces droits conformément à l'article 25, paragraphes 3 ou 4, du règlement (UE) 2018/1725, sous réserve de garanties appropriées.

(12) Il convient que la BCE justifie les motifs pour lesquels ces limitations des droits des personnes concernées sont strictement nécessaires et proportionnées dans une société démocratique pour garantir les objectifs poursuivis dans l'exercice de son autorité publique et des fonctions qui y sont liées, et la manière dont la BCE entend respecter l'essence des droits et libertés fondamentaux tout en imposant de telles limitations.

(13) Dans ce cadre, la BCE est tenue de respecter, dans toute la mesure du possible, les droits fondamentaux des personnes concernées, notamment ceux relatifs au droit à l'information, au droit d'accès et de rectification, au droit à l'effacement, à la limitation du traitement, au droit à la communication d'une violation de données à caractère personnel à la personne concernée ou à la confidentialité des communications, comme le prévoit le règlement (UE) 2018/1725.

(14) Toutefois, la BCE peut être obligée de limiter les informations fournies aux personnes concernées et les droits des personnes concernées afin de protéger l'accomplissement de ses missions de surveillance prudentielle, en particulier ses propres enquêtes et procédures, les enquêtes et procédures d'autres autorités publiques, ainsi que les droits et libertés fondamentaux d'autres personnes liées à ses enquêtes ou à d'autres procédures.

(15) Il convient que la BCE lève une limitation qui a déjà été appliquée lorsque celle-ci n'est plus nécessaire.

(16) Il convient que le délégué à la protection des données de la BCE procède au réexamen de l'application des limitations afin de garantir la conformité avec la présente décision et le règlement (UE) 2018/1725.

(17) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 41, paragraphe 2, du règlement (UE) 2018/1725 et a rendu un avis le 12 mars 2021,

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

Objet et champ d'application

1. La présente décision établit des règles relatives à la limitation des droits des personnes concernées par la BCE lorsque celle-ci exerce des activités de traitement de données à caractère personnel, telles qu'enregistrées dans le registre central, dans l'accomplissement de ses missions de surveillance prudentielle au titre du règlement (UE) n° 1024/2013.

2. Les droits des personnes concernées qui peuvent faire l'objet d'une limitation sont précisés aux articles suivants du règlement (UE) 2018/1725:

a) article 14 (transparence des informations et des communications et modalités de l'exercice des droits de la personne concernée);

b) article 15 (informations à fournir lorsque des données à caractère personnel sont collectées auprès de la personne concernée);

c) article 16 (informations à fournir lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée);

d) article 17 (droit d'accès de la personne concernée);

e) article 18 (droit de rectification);

f) article 19 [droit à l'effacement («droit à l'oubli»)];

g) article 20 (droit à la limitation du traitement);

h) article 21 (obligation de notification en ce qui concerne la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement);

i) article 22 (droit à la portabilité des données);

j) article 35 (communication à la personne concernée d'une violation de données à caractère personnel);

k) article 36 (confidentialité des communications électroniques);

l) article 4 dans la mesure où ses dispositions correspondent aux droits et obligations prévus aux articles 14 à 22 du règlement (UE) 2018/1725.

Article 2

Définitions

Aux fins de la présente décision, on entend par:

1) «traitement»: le traitement au sens de l'article 3, point 3), du règlement (UE) 2018/1725;

2) «données à caractère personnel»: les données à caractère personnel au sens de l'article 3, point 1), du règlement (UE) 2018/1725;

3) «personne concernée»: une personne physique identifiée ou identifiable; une personne identifiable est une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;

4) «registre central»: le recueil, accessible au public, de toutes les activités de traitement des données à caractère personnel effectuées à la BCE qui est tenu par le délégué à la protection des données de la BCE et visé à l'article 9 de la décision (UE) 2020/655 (BCE/2020/28);

5) «responsable du traitement»: la BCE, et notamment l'unité organisationnelle compétente au sein de la BCE, qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données à caractère personnel et qui est responsable de l'opération de traitement;

6) «institutions et organes de l'Union»: les institutions et organes de l'Union au sens de l'article 3, point 10), du règlement (UE) 2018/1725.

Article 3

Application des limitations

1. Le responsable du traitement peut limiter les droits visés à l'article 1er, paragraphe 2, afin de garantir les intérêts et objectifs visés à l'article 25, paragraphe 1, du règlement (UE) 2018/1725, notamment lorsque l'exercice de ces droits pourrait compromettre ou porter atteinte à:

a) l'accomplissement des missions de surveillance prudentielle de la BCE au titre du règlement (UE) no 1024/2013, y compris le bon fonctionnement du système de surveillance;

b) la sécurité et la solidité des établissements de crédit et la stabilité du système financier au sein de l'Union européenne et de chaque État membre;

c) l'efficacité du signalement des infractions conformément à l'article 23 du règlement (UE) no 1024/2013.

2. Afin de garantir les intérêts et objectifs visés à l'article 25, paragraphe 1, du règlement (UE) 2018/1725, le responsable du traitement peut limiter les droits visés à l'article 1er, paragraphe 2, concernant les données à caractère personnel obtenues auprès d'autres institutions et organes de l'Union et d'autorités compétentes d'États membres ou de pays tiers ou d'organisations internationales, dans les cas suivants:

a) lorsque l'exercice de ces droits pourrait être limité par d'autres institutions et organes de l'Union auprès desquels les données à caractère personnel ont été obtenues, sur la base d'autres actes prévus à l'article 25 du règlement (UE) 2018/1725 ou conformément au chapitre IX de ce règlement ou aux actes fondateurs d'autres institutions et organes de l'Union;

b) lorsque l'exercice de ces droits pourrait être limité par les autorités compétentes des États membres auprès desquelles les données à caractère personnel ont été obtenues, sur la base des actes visés à l'article 23 du règlement (UE) 2016/679 du Parlement européen et du Conseil ([4]) ou dans le cadre de mesures nationales transposant l'article 13, paragraphe 3, l'article 15, paragraphe 3, ou l'article 16, paragraphe 3, de la directive (UE) 2016/680 du Parlement européen et du Conseil ([5]);

c) lorsque l'exercice de ces droits pourrait compromettre ou porter atteinte à la coopération de la BCE avec des pays tiers ou des organisations internationales auprès desquels les informations ont été obtenues, dans l'accomplissement de ses missions, sauf si les intérêts ou les droits et libertés fondamentaux des personnes concernées surpassent l'intérêt de la BCE à la coopération.

([4]) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

([5]) Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO L 119 du 4.5.2016, p. 89).

3. Avant d'appliquer une limitation dans les cas visés au paragraphe 2, points a) et b), le responsable du traitement:

a) prend acte des accords conclus avec les institutions et organes de l'Union pertinents ou les autorités compétentes des États membres;

b) consulte les institutions et organes de l'Union pertinents ou les autorités compétentes des États membres, à moins qu'il ne soit évident pour le responsable du traitement que l'application de cette limitation est prévue par l'un des actes ou l'une des mesures visés au paragraphe 2, points a) et b).

4. Le responsable du traitement ne peut appliquer une limitation que s'il conclut, sur la base d'une évaluation au cas par cas, que la limitation:

a) est nécessaire et proportionnée compte tenu des risques pour les droits et libertés de la personne concernée; et

b) respecte l'essence des droits et libertés fondamentaux dans une société démocratique.

5. Le responsable du traitement documente son évaluation dans une note d'évaluation interne qui inclut la base juridique, les motifs de la limitation, les droits des personnes concernées faisant l'objet d'une limitation, les personnes concernées, la nécessité et la proportionnalité de la limitation et la durée probable de la limitation.

6. Toute décision de limiter les droits d'une personne concernée conformément à la présente décision, qui doit être prise par le responsable du traitement, est établie au niveau du responsable ou du responsable adjoint du service dans lequel l'opération principale de traitement des données à caractère personnel est effectuée.

Article 4

Dérogations

1. En ce qui concerne le traitement à des fins de recherche scientifique ou historique ou à des fins statistiques, le responsable du traitement peut appliquer des dérogations conformément à l'article 25, paragraphe 3, du règlement (UE) 2018/1725. À cette fin, le responsable du traitement peut déroger aux droits visés aux articles 17, 18, 20 et 23 du règlement (UE) 2018/1725, dans les conditions énoncées à l'article 25, paragraphe 3, de ce règlement.

2. En ce qui concerne le traitement à des fins archivistiques dans l'intérêt du public, le responsable du traitement peut appliquer des dérogations conformément à l'article 25, paragraphe 4, du règlement (UE) 2018/1725. À cette fin, le responsable du traitement peut déroger aux droits visés aux articles 17, 18, 20, 21, 22 et 23 du règlement (UE) 2018/1725, dans les conditions énoncées à l'article 25, paragraphe 4, de ce règlement.

3. Ces dérogations font l'objet de garanties appropriées conformément à l'article 13 du règlement (UE) 2018/1725 et à l'article 8 de la présente décision.

Article 5

Fourniture d'informations générales sur les limitations

Le responsable du traitement fournit des informations générales sur la limitation éventuelle des droits des personnes concernées comme suit:

a) le responsable du traitement précise les droits susceptibles de faire l'objet d'une limitation, les motifs de la limitation et sa durée potentielle;

b) le responsable du traitement inclut les informations visées au point a) dans ses avis relatifs à la protection des données, ses déclarations de confidentialité et son registre des activités de traitement visé à l'article 31 du règlement (UE) 2018/1725.

Article 6

Limitation du droit d'accès des personnes concernées, du droit de rectification, du droit à l'effacement ou à la limitation du traitement

1. Lorsque le responsable du traitement limite, totalement ou partiellement, le droit d'accès, le droit de rectification, le droit à l'effacement ou le droit à la limitation du traitement visés respectivement aux articles 17 et 18, à l'article 19, paragraphe 1, et à l'article 20, paragraphe 1, du règlement (UE) 2018/1725, il informe la personne concernée, dans le délai visé à l'article 11, paragraphe 5, de la décision (UE) 2020/655 (BCE/2020/28), dans sa réponse écrite à la demande, de la limitation appliquée, des principaux motifs de la limitation et de la possibilité d'introduire une réclamation auprès du Contrôleur européen de la protection des données ou de former un recours juridictionnel devant la Cour de justice de l'Union européenne.

2. Le responsable du traitement conserve la note d'évaluation interne visée à l'article 3, paragraphe 5, et, le cas échéant, les documents contenant les éléments factuels et juridiques sous-jacents, et les met à la disposition du Contrôleur européen de la protection des données sur demande.

3. Le responsable du traitement peut différer, omettre ou refuser de fournir des informations sur les motifs de la limitation visée au paragraphe 1 aussi longtemps que cette fourniture d'informations porterait atteinte à la finalité de la limitation. Dès que le responsable du traitement estime que la fourniture des informations ne porte plus atteinte à la finalité de la limitation, il les communique à la personne concernée.

Article 7

Durée des limitations

1. Le responsable du traitement lève une limitation dès que les circonstances qui l'ont justifiée cessent d'exister.

2. Lorsque le responsable du traitement lève une limitation conformément au paragraphe 1, il est tenu, sans délai:

a) dans la mesure où il ne l'a pas déjà fait, d'informer la personne concernée des principaux motifs qui ont motivé l'application d'une limitation;

b) d'informer la personne concernée de son droit d'introduire une réclamation auprès du Contrôleur européen de la protection des données ou de former un recours juridictionnel devant la Cour de justice de l'Union européenne;

c) d'accorder à la personne concernée le droit qui faisait l'objet de la limitation ayant été levée.

3. Le responsable du traitement réévalue tous les six mois la nécessité de maintenir une limitation appliquée en vertu de la présente décision et documente sa réévaluation dans une note d'évaluation interne.

Article 8

Garanties

La BCE applique les garanties organisationnelles et techniques figurant à l'annexe afin de prévenir les abus ou les accès ou transferts illicites.

Article 9

Réexamen par le délégué à la protection des données

1. Lorsque le responsable du traitement limite l'application des droits d'une personne concernée, il doit y associer en permanence le délégué à la protection des données. En particulier, les mesures suivantes sont applicables:

a) le responsable du traitement consulte le délégué à la protection des données dans les meilleurs délais;

b) à la demande du délégué à la protection des données, le responsable du traitement lui donne accès à tout document contenant des éléments factuels et juridiques sous-jacents, y compris la note d'évaluation interne visée à l'article 3, paragraphe 5;

c) le responsable du traitement documente la manière dont le délégué à la protection des données a été associé, y compris les informations pertinentes qui ont été partagées, en particulier la date de la première consultation visée au point a);

d) le délégué à la protection des données peut demander au responsable du traitement de réexaminer la limitation;

e) le responsable du traitement informe le délégué à la protection des données, par écrit, du résultat du réexamen demandé dans les meilleurs délais et, en tout état de cause, avant l'application de toute limitation.

2. Le responsable du traitement informe le délégué à la protection des données lorsque la limitation est levée.

Article 10

Entrée en vigueur

La présente décision entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Fait à Francfort-sur-le-Main, le 7 septembre 2021.

La présidente de la BCE
Christine LAGARDE

ANNEXE

Les garanties organisationnelles et techniques mises en place au sein de la BCE afin de prévenir les abus et les accès ou transferts illicites comprennent:

a) en ce qui concerne les personnes:

   i) le devoir pour toutes les personnes ayant accès à des informations non publiques de la BCE de connaître et d'appliquer la politique et les règles de la BCE en matière de gestion et de confidentialité des informations;

   ii) une procédure d'habilitation de sécurité qui garantit que seules des personnes contrôlées et autorisées ont accès aux locaux de la BCE et à ses informations non publiques;

   iii) des mesures de sensibilisation à la sécurité informatique, à la sécurité de l'information et à la sécurité physique;

   iv) des formations organisées régulièrement pour les membres du personnel et les prestataires de services externes;

   v) l'imposition aux membres du personnel de la BCE de règles strictes en matière de secret professionnel énoncées dans les conditions d'emploi de la BCE et les règles applicables au personnel de la BCE, dont la violation donne lieu à des sanctions disciplinaires;

   vi) des règles et obligations régissant l'accès des prestataires de services externes ou des sous-traitants aux informations non publiques de la BCE, énoncées dans des dispositions contractuelles;

   vii) des contrôles d'accès, y compris un zonage de sécurité, qui sont mis en œuvre pour garantir que l'accès des personnes aux informations non publiques de la BCE est autorisé et limité en fonction des besoins de l'activité et des exigences de sécurité;

b) en ce qui concerne les procédures:

   i) la mise en place de procédures garantissant une mise en œuvre, une exploitation et une maintenance contrôlés des applications informatiques sur lesquelles reposent les activités de la BCE;

   ii) l'utilisation, pour les activités de la BCE, d'applications informatiques conformes aux normes de sécurité de la BCE;

   iii) l'existence d'un programme complet de sécurité physique en fonctionnement qui évalue en permanence les menaces pour la sécurité et comprend des mesures de sécurité physique afin d'assurer un niveau de protection approprié;

c) en ce qui concerne la technologie:

   i) le stockage de toutes les données électroniques dans des applications informatiques conformes aux normes de sécurité de la BCE et ainsi protégées contre tout accès ou toute modification non autorisés;

   ii) la mise en œuvre, l'exploitation et la maintenance des applications informatiques à un niveau de sécurité correspondant aux besoins desdites applications en matière de confidentialité, d'intégrité et de disponibilité, sur la base d'analyses d'impact sur les activités;

   iii) la validation régulière du niveau de sécurité des applications informatiques par des évaluations techniques et non techniques de sécurité;

   iv) l'octroi de l'accès aux informations non publiques de la BCE conformément au principe du «besoin d'en connaître», et un accès privilégié strictement limité et strictement contrôlé;

   v) la mise en œuvre de contrôles pour détecter les failles de sécurité réelles et potentielles et en assurer le suivi.