Circulation effective des données à caractère personnel après le Brexit

Implications pour les marchés de capitaux

Avril 2018

Association for Financial Markets in Europe
www.afme.eu

Table des matières

Résumé

Le Règlement général sur la protection des données (RGPD) expose les principes de la protection des personnes physiques au regard du traitement et de la circulation de données à caractère personnel. Le divorce imminent entre le Royaume-Uni et l'Union européenne génère d'importantes incertitudes quant à la capacité des entreprises, dont les banques et les sociétés d'investissement, à continuer de transférer des données à caractère personnel entre l'EEE et le Royaume-Uni après le Brexit.

Cette note d'information aborde les points suivants :

1. Les exigences pertinentes imposées par le RGPD pour le traitement de données et les mécanismes de transfert de données entre l'EEE et des pays tiers.
2. Les incertitudes relatives à la capacité des entreprises à transférer des données à caractère personnel entre l'EEE et le Royaume-Uni après le Brexit.
3. L'importance du partage des données à caractère personnel pour faire bénéficier les clients professionnels et institutionnels d'un service efficace et sécurisé.
4. Solution proposée par l'AFME – que la Commission européenne (CE) et le Royaume-Uni se fixent les priorités suivantes :
    - Engager des pourparlers pour préparer les Décisions d'adéquation dans les meilleurs délais et
    - Concevoir une solution transitoire pendant les évaluations d'adéquation.

1 Contexte du RGPD

Contexte du RGPD

- Le RGPD s'appliquera dans toute l'UE (y compris au Royaume-Uni) à compter du 25 mai 2018. La CE affirme que le RGPD :

  « renforcera la protection du droit des personnes à la protection des données à caractère personnel les concernant, reflétant la place accordée par l'Union européenne à la protection des données en tant que droit fondamental…. il garantira le libre flux des données à caractère personnel entre les États membres de l'UE et renforcera la confiance et la sécurité des consommateurs… le règlement laisse ainsi entrevoir de nouvelles perspectives pour les entreprises et les sociétés, en particulier celles de plus petite taille, en rendant également plus claires les règles régissant les transferts internationaux de données. »[1]

- Deux grands concepts sont évoqués dans cette note : le traitement de données et les Décisions d'adéquation.

Traitement de données

- Le RGPD énonce de nouvelles règles relatives au mode de « traitement » des données à caractère personnel, un terme employé par les informaticiens pour désigner essentiellement toutes les formes de collecte, d'enregistrement, de stockage, de modification, d'utilisation et de transmission de données. Le RGDP (tout comme la précédente directive sur la protection des données) établit une distinction entre le traitement de données à caractère personnel à l'intérieur et à l'extérieur de l'EEE.

- Le traitement de données à caractère personnel au sein de l'EEE doit satisfaire les conditions visées aux chapitres I à IV du RGPD, notamment celles-ci :

  - Principes relatifs au traitement de données à caractère personnel
  - Légalité du traitement
  - Droits des personnes concernées

Décisions d'adéquation

- Le transfert de données à caractère personnel dans un pays situé hors de l'EEE doit, en outre, satisfaire les conditions énoncées au chapitre V. La plus simple de ces conditions – et la seule qui puisse, à notre sens, être mise en œuvre dans le contexte du Brexit – autorise le transfert de données sans autre autorisation lorsque la CE a pris une « Décision d'adéquation », c'est-à-dire qu'elle estime que le pays tiers en question garantit un niveau « adéquat » de protection.

- En l'absence de Décision d'adéquation de la CE, les contrôleurs de données doivent se conformer à l'un des autres instruments recensés au chapitre V, à savoir :

  - Clauses contractuelles types (pour les flux externes)
  - Règles d'entreprise contraignantes (pour les transferts intragroupe)
  - Code de conduite approuvé
  - Mécanisme de certification approuvé

[1] « Une meilleure protection et de nouvelles perspectives - Orientations de la Commission relatives à l'application directe du règlement général sur la protection des données à partir du 25 mai 2018 ». Disponible à cette adresse (version anglaise) : https://ec.europa.eu/commission/sites/beta-political/files/data-protection-communication-com.2018.43.3_en.pdf [Dernière consultation le 15 mars 2018], p. 1.

- Ces instruments sont expliqués ci-après. Lorsqu'aucun de ces instruments ne s'applique, les transferts ne sont possibles que dans des situations spécifiques (énoncées ci-après au paragraphe 3.1.6)[2].

2 Incertitudes : pourra-t-on transférer des données entre l'EEE et le Royaume-Uni après le Brexit ?

Incertitudes : pourra-t-on transférer des données entre l'EEE et le Royaume-Uni après le Brexit ?

2.1 Législation britannique post-Brexit

Le RGPD s'appliquera en UE, y compris au Royaume-Uni, à compter du 25 mai 2018. Le Royaume-Uni prévoit également de transposer le RGPD dans la législation britannique à compter de la date à laquelle le Royaume-Uni quittera officiellement l'UE, en vertu du Projet de loi de l'UE (retrait). Après le départ du Royaume-Uni, le cadre de protection des données au Royaume-Uni sera donc identique ou quasi identique au cadre de protection des données de l'UE.

2.2 Conséquences pour les transferts de données

- Partant du principe que le Royaume-Uni ne sera plus membre de l'EEE après le Brexit, la question se pose de savoir si les entreprises et organismes de régulation pourront continuer de transférer des données à caractère personnel entre l'EEE et le Royaume-Uni. À ce jour, l'UE n'a pas pris de Décision d'adéquation au regard du Royaume-Uni (il n'y a pas de mécanisme officiel pour ce faire puisque le Royaume-Uni n'est pas encore un pays tiers).

- Naturellement, le problème inverse se pose aussi, concernant le transfert de données depuis le Royaume-Uni vers l'EEE, à supposer que le Royaume-Uni reprenne à son compte les dispositions du RGPD relatives aux transferts internationaux. En d'autres termes, il s'agit de déterminer si, avant le Brexit, le Royaume-Uni est en mesure de reconnaître le cadre de protection des données de l'EEE.

2.3 Incertitudes subséquentes

- Les entreprises ont un besoin urgent d'explications sur le cadre juridique qui sera mis en œuvre pour réguler la circulation transfrontalière des données, comme indiqué ci-après.

- Plusieurs sources d'incertitude subsistent en effet :
    - L'UE pourra-t-elle utiliser le mécanisme existant avant le Brexit pour reconnaître l'adéquation du Royaume-Uni ?
    - L'UE choisira-t-elle (dans tous les cas) d'engager une évaluation de l'adéquation du cadre britannique de protection des données ?
    - L'UE rencontrera-t-elle et choisira-t-elle par principe de résoudre des questions litigieuses avant de décider du caractère adéquat du cadre britannique de protection des données ?
    - L'UE aura-t-elle le temps de prendre une décision avant le Brexit ?

- La CE a publié le 9 janvier 2018 une note d'information à l'intention des parties prenantes, qui attire leur attention sur ce problème potentiel et précise que des « garanties supplémentaires » existent en l'absence de décision d'adéquation (c'est nous qui soulignons) :

[2] Voir l'article 49 du RGPD.

« Sous réserve des dispositions transitoires qui pourraient figurer dans un éventuel accord de retrait, les dispositions du règlement relatives aux transferts de données à caractère personnel vers des pays tiers s'appliqueront. Hormis la "décision d'adéquation"… les dispositions de protection des données de l'UE… autorisent un transfert si le contrôleur ou sous-traitant a mis en place des "garanties appropriées". Ces garanties peuvent consister en ce qui suit :

- **Clauses contractuelles types :** la Commission a adopté trois ensembles de clauses types, disponibles sur le site Internet de la Commission.
- **Règles d'entreprise contraignantes :** règles de protection de données juridiquement contraignantes approuvées par l'autorité de protection des données compétente et applicable au sein d'un groupe d'entreprises.
- **Codes de conduite** approuvés, assortis d'engagements contraignants et exécutoires du contrôleur ou sous-traitant dans le pays tiers.
- **Mécanismes de certification** approuvés, assortis d'engagements contraignants et exécutoires du contrôleur ou sous-traitant dans le pays tiers.

En l'absence de « décision d'adéquation » ou de « garanties appropriées », un transfert ou un ensemble de transferts peut être effectué sous le couvert de « **dérogations** » : ces dérogations autorisent les transferts dans des cas spécifiques, par exemple sur la base d'un consentement, pour l'exécution d'un contrat, pour faire valoir des revendications juridiques ou pour des raisons importantes d'intérêt public.

Ces instruments sont bien connus des exploitants d'entreprises dans les États membres, car ils sont déjà employés aujourd'hui pour les transferts de données à caractère personnel vers des pays non membres de l'UE. »[3]

3 Solution proposée

3.1 Inconvénients des « garanties supplémentaires »

La note d'information évoque les différents instruments susceptibles d'être employés pour étayer certains transferts de données vers des pays situés hors de l'EEE. Si ces instruments sont certes utiles, et certains d'entre eux sont effectivement employés aujourd'hui, ils ont aussi leurs inconvénients, comme indiqué ci-après.

- Clauses contractuelles types (CCT)

  - Il est très compliqué de mettre en place un réseau de CCT pour un groupe multinational (ex. : une banque), qui a plusieurs entités légales et succursales dispersées dans le monde. C'est en effet un processus lent et complexe, qui exige de cartographier les flux de données et d'établir des CCT distinctes pour chaque connexion intersociétés.
  - De surcroît, les CCT approuvées par la Commission ont aussi leur lot d'incertitudes juridiques, puisque ces clauses sont actuellement contestées au plan judiciaire[4]. Si des CTT devaient être invalidées par la CJUE, les entreprises s'appuyant sur des CCT perdraient du jour au lendemain toute base légale pour transférer des données à caractère personnel vers des pays tiers. Cela s'est déjà produit avant.

- Règles d'entreprise contraignantes (REC)

  - Les REC permettant aux grandes organisations internationales de transférer des données. Cela étant, elles se révèlent très complexes et fastidieuses à mettre en œuvre. Les

[3] « Notice to stakeholders: withdrawal of the United Kingdom and EU rules in the field of data protection ». Disponible à cette adresse (version anglaise) : https://eubusinesslaw.wordpress.com/2018/01/12/notice-to-stakeholders-withdrawal-of-the-united-kingdom-and-eu-rules-in-the-field-of-data-protection/ [Dernière consultation le 15 mars 2018].
[4] 2016 N° 4809 P. *The Data Protection Commissioner and Facebook Ireland Limited and Maximillian Schrems*. Disponible à cette adresse (version anglaise) : https://dataprotection.ie/documents/judgements/DPCvFBSchrems.pdf [Dernière consultation le 10 avril 2018].

multinationales doivent satisfaire plusieurs critères avant de pouvoir mettre des REC en place, notamment : conclure des accords intragroupe entre des entreprises exerçant des activités économiques communes, rédiger de nouvelles politiques et engager une phase de négociation avec les autorités de protection des données, ce qui peut prendre une à deux années. Les sociétés renâclent donc à engager la procédure de demande et, faute de moyens, renoncent aux REC.

- À l'heure actuelle, seules 33 entités ont été autorisées par le Commissariat à l'information britannique à transférer des données à caractère personne hors de l'EEE en vertu de REC[5]. Dans l'UE-27, seules 67 sociétés ont accompli cette procédure sous couvert de REC[6]. Il est fort peu probable que les autorités de protection des données en UE-27 soient en mesure de répondre à un afflux de demandes de REC dans des délais suffisants pour autoriser la poursuite des affaires courantes.

- Codes de conduite

  - Il serait très compliqué pour l'industrie de concevoir un code de conduite et de le faire approuver, en l'état actuel des choses. Il n'existe aucun exemple de code de conduite actuellement utilisé en base légale au transfert de données à caractère personnel depuis l'EEE vers un pays tiers. Il est donc très peu probable que les codes de conduite puissent constituer une solution viable.

- Mécanismes de certification

  - À l'instar des codes de conduite, les mécanismes de certification sont sans précédent. Pour l'heure, nous ne connaissons aucun organisme d'accréditation susceptible d'administrer les régimes de certification ; rien ne garantit donc avec certitude que des mécanismes de certification pourront être mis sur pied à temps.

- Dérogations

  - Comme indiqué au paragraphe 2.3 ci-avant, en l'absence de décision d'adéquation ou de garanties appropriées, un transfert ou un ensemble de transferts peut être effectué sous le couvert de dérogations, autorisant les transferts dans des cas spécifiques. Le projet d'orientation du Groupe de travail Article 29 stipule que les dérogations doivent être interprétées au sens restrictif afin que les exceptions ne confirment pas la règle. Par conséquent, les dérogations ne constituent pas au sens large une solution au problème.

3.2 Importance du partage de données

- Les régulateurs des pratiques financières attendent des entreprises qu'elles aient une vue consolidée de leurs clients professionnels et institutionnels afin d'honorer les exigences réglementaires, notamment l'identification des transactions douteuses, l'évaluation de la pertinence et la lutte contre le blanchiment de capitaux, le financement du terrorisme et les abus de marché. Pour que ces entreprises servent au mieux leurs clients, elles ont besoin de partager des données à caractère personnel sur les employés, administrateurs et actionnaires de leurs clients avec toutes leurs entités affiliées. En particulier, une entreprise ayant son siège social en UE-27 doit être en mesure de partager de telles données avec ses affiliés au Royaume-Uni, et inversement. Les entreprises doivent également partager en interne des données à caractère personnel sur leurs propres employés, par exemple pour garantir la cohérence des processus de ressources humaines ou pour vérifier la conformité des

[5] Information Commissioner's Office, « Binding Corporate Rules ». Disponible à cette adresse (version anglaise) : https://ico.org.uk/for-organisations/guide-to-data-protection/binding-corporate-rules/ [Dernière consultation le 14 mars 2018].
[6] Commission européenne, « Binding corporate rules ». Disponible à cette adresse (version anglaise) : https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/binding-corporate-rules_en [Dernière consultation le 15 mars 2018].

déplacements des employés avec les politiques de frais et loisirs.

- Nombre d'entreprises ont établi des plateformes centralisées de traitement sur de multiples sites afin de faciliter leur collecte et analyse de données, ainsi que pour des raisons de sécurité des données et de résilience commerciale. Le flux de communication se fait à double sens. Les affiliés fournissent des informations aux plateformes, lesquelles diffusent à leur tour des informations pertinentes dans tout le groupe. Les plateformes constituent un moyen sûr et efficace de stocker et de traiter des données à caractère personnel.

- Au Royaume-Uni, le directeur général de la Financial Conduct Authority (FCA) a admis qu'il importait de résoudre la question du transfert de données, en indiquant le 5 février que :

> « Les entreprises de l'UE et du Royaume-Uni détiennent et partagent un très important volume de données sur leurs citoyens respectifs. On estime que trois quarts environ des données transfrontalières transitant par le Royaume-Uni sont destinées à des États membres de l'UE. Le Royaume-Uni est un gros exportateur de services de données numériques (ex. : hébergement et traitement de données) et constitue le point d'entrée en Europe de nombreuses entreprises mondiales dépendant des données. La FCA est elle-même un important exportateur de données sur les activités boursières, aidant les autres organes de régulation européens à surveiller les entreprises et les marchés. De fait, lors d'un mois moyen, nous exportons plus de 250 millions de rapports commerciaux, alors que nous n'en recevons que 12 millions. Si le Royaume-Uni devait quitter l'UE sans mesures d'atténuation de part et d'autre, le simple fait de détenir et de partager les données d'un autre pays pourrait violer le droit national. »[7]

- Si l'on veut que les entreprises poursuivent leurs activités transfrontalières, des dispositions doivent être prises pour garantir la libre circulation constante de données à caractère personnel après le Brexit. Comme l'a indiqué l'Autorité bancaire européenne (ABE), « les risques liés... au transfert de données et à la protection de données avec un pays tiers pourraient perturber la stabilité financière et la confiance des marchés. »[8]

3.3 Proposition d'une solution : vers une Décision d'adéquation

- Une possibilité pourrait être un Bouclier de protection des données UE-Royaume-Uni, analogue à celui conclu entre l'UE et les États-Unis. Un tel mécanisme serait toutefois susceptible de poser des problèmes juridiques, comme ce fut le cas pour le dispositif de sphère de sécurité.

- Une autre possibilité pourrait, en principe, consister à insérer des dispositions horizontales pour la circulation des données transfrontalières et la protection des données à caractère personnel dans les futures relations entre l'UE-27 et le Royaume-Uni. Une solution provisoire a pu être trouvée avec la conclusion d'un accord transitoire. Nous notons que l'accord conclu au Conseil européen le 23 mars 2018 sur les conditions d'une période de transition commençant le 29 mars 2019 et se terminant à la fin 2020 comporte la formulation suivante, potentiellement utile : « sauf disposition contraire du présent Accord, la législation de l'Union sera applicable au Royaume-Uni durant la période de transition ». Cela étant, l'interprétation pratique de cette formule demeure sujette à caution.

- Cependant, pour avoir une solution pratique avant le Brexit, nous estimons que le meilleur moyen de garantir une certitude juridique aux entreprises prévoyant de transférer des données à caractère personnel entre l'EEE et le Royaume-Uni est de faire en sorte que les Décisions d'adéquation soient prises par la CE et par le Royaume-Uni. Ce mécanisme, conjointement avec la mise en œuvre de solutions provisoires pendant les évaluations d'adéquation, doit être opérationnel avant le Brexit afin

[7] Financial Conduct Authority, « The Future of the City Speech ». Disponible à cette adresse (version anglaise) : https://www.fca.org.uk/news/speeches/future-city [Dernière consultation le 9 avril 2018].
[8] ABE, « Risk Assessment of the European Banking System », 24 novembre 2017, p. 17.

de prévenir toute lacune après le retrait du Royaume-Uni.

- Compte tenu de l'expertise et de l'expérience acquises par la CE pour déterminer si un pays tiers dispose d'un niveau adéquat de protection, nous estimons que les évaluations devraient pouvoir être achevées d'ici un an, pour autant que la question soit traitée en priorité.

- Selon nous, les Décisions d'adéquation sont possibles parce que :
    - Le RGPD s'appliquera au Royaume-Uni à compter du 25 mai 2018 et le Royaume-Uni a affirmé son intention d'adapter la législation nationale britannique au RGPD après le Brexit.
    - Sous réserve des prescriptions de la Loi britannique sur les pouvoirs d'enquête *(Investigatory Powers Act*, voir ci-après), les cadres de protection des données de l'UE et du Royaume-Uni seront au moins aussi proches que les cadres en vigueur dans les pays pour lesquels une Décision d'adéquation a déjà été prise (quoiqu'il soit entendu que la Commission se propose de revoir toutes les décisions d'adéquations précédentes afin de déterminer si elles demeurent « essentiellement équivalentes »).
    - L'autorité britannique de protection des données a des antécédents en matière d'application de la législation sur la protection des données (un critère fondamental pour l'adéquation).
    - Il en est de même pour les autorités de protection des données en Europe.
- De récentes déclarations de la CE ont également mentionné le lien entre l'application du GRPD par le Royaume-Uni et la décision relative à l'adéquation ; le Commissaire à la Justice, aux Consommateurs et à l'Égalité des genres a ainsi déclaré ceci :

« avec les mêmes règles de protection des données, il serait beaucoup plus facile pour l'UE et le Royaume-Uni de prendre des décisions en matière d'adéquation ».[9]

4 La Loi britannique de 2016 sur les pouvoirs d'enquête *(Investigatory Powers Act)*

La Loi britannique de 2016 sur les pouvoirs d'enquête *(Investigatory Powers Act)*

- Concernant une possible Décision d'adéquation, il convient de noter que la Loi britannique de 2016 sur les pouvoirs d'investigation (IPA) est actuellement perçue par certains comme étant incompatible avec la législation de l'UE, suite à l'arrêt de la CJUE du 21 décembre 201610.

- En réponse, le Gouvernement britannique procède à des consultations pour un amendement de la loi IPA, acceptant que :

> « …la loi DRIPA (Loi de 2014 sur la conservation de données et les pouvoirs d'enquête, *Data [Retention] and Investigatory Powers Act)*, et par conséquent certains aspects de la partie 4 de la loi IPA, sont incompatibles avec la législation de l'UE, en ce sens que : a) il n'y a aucune disposition pour l'autorisation indépendante de demandes d'accès à des données conservées et b) la finalité criminelle de la conservation et de la consultation de données n'est pas limitée à une criminalité grave.[11] »

[9] Déclaration de la Commissaire Věra Jourová lors d'une conférence de presse donnée après la publication du document « Orientations de la Commission relatives à l'application directe du règlement général sur la protection des données à partir du 25 mai 2018 » le 24 janvier 2018.

[10] Jurisprudence de la Cour de justice. Arrêt de la Cour (grande chambre) dans les affaires jointes C-203/15 et C-698/15. Disponible à cette adresse (version anglaise) : http://curia.europa.eu/juris/document/document.jsf?docid=186492&doclang=EN [Dernière consultation le 14 mars 2018].

[11] Investigatory Powers Act 2016. Consultation sur la réponse proposée du Gouvernement à l'arrêt de la Cour de Justice de l'Union européenne rendu le 21 décembre 2016 concernant la conservation de données de communication. Disponible à cette adresse (version anglaise) :

- Concernant l'accès aux données conservées, le Gouvernement accepte l'arrêt de la CJUE, selon lequel :

  « Il est essentiel que l'accès des autorités nationales compétentes aux données conservées soit, en principe, sauf cas d'urgence dûment justifiés, subordonné à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante, et que la décision de cette juridiction ou de cette entité intervienne à la suite d'une demande motivée de ces autorités présentée, notamment, dans le cadre de procédures de prévention, de détection ou de poursuites pénales [paragraphe 120]. »[12]

  « Les projets de règlement modifient la partie 3 de la loi IPA pour instaurer trois différents régimes d'autorisation des demandes de données de communication. »[13]

- Concernant la criminalité, la consultation note que la CJUE a affirmé ceci :

  « Eu égard à la gravité de l'ingérence dans les droits fondamentaux en cause que constitue une réglementation nationale prévoyant, aux fins de la lutte contre la criminalité, la conservation de données relatives au trafic et de données de localisation, seule la lutte contre la criminalité grave est susceptible de justifier une telle mesure. » [paragraphe 102]. »[14]

  Par conséquent, le Gouvernement britannique amende la législation afin de définir le concept de « criminalité grave » dans ce cadre[15].

- Le Gouvernement britannique reconnaît clairement que la loi IPA doit être amendée pour garantir sa compatibilité avec la législation de l'UE. Partant, l'arrêt de la CJUE ne devrait pas empêcher la Commission et le Royaume-Uni d'engager le processus d'adéquation, qui pourrait se dérouler parallèlement à la mise en œuvre des amendements proposés.

5 Conclusion et recommandations

Conclusion et recommandations

- Pour les raisons exposées ci-avant, il importe de faire toute la lumière sur la capacité des entreprises, dont les banques et les sociétés d'investissement, à continuer de transférer des données à caractère personnel entre l'EEE et le Royaume-Uni après le Brexit.

- Compte tenu de l'alignement des cadres de protection des données de l'UE et du Royaume-Uni, et de la complexité, de la lenteur et des lacunes des autres solutions, nous proposons que la CE et le Royaume-Uni procèdent en priorité comme suit :

- Convenir d'engager des pourparlers pour préparer les Décisions d'adéquation dans les meilleurs délais. Nous pensons qu'un tel processus peut se dérouler indépendamment des négociations sur les futures relations entre l'UE-27 et le Royaume-Uni.
- S'engager à trouver une solution provisoire pour éviter toute lacune pendant le déroulement des évaluations d'adéquation, par exemple l'Accord de retrait, toute autre convention bilatérale ou, si nécessaire, des mesures bilatérales.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/663668/November_2017_IPA_Consultation_-_consultation_document.pdf [Dernière consultation le 15 mars 2018], p. 6.

[12] Ibid, p. 18.

[13] Ibid, p. 18.

[14] Ibid, p. 14.

[15] Ibid, p. 15.

- Nous apprécierions avoir l'opportunité de collaborer avec toutes les parties impliquées dans ce processus, y compris la Commission européenne, les États membres et les autorités nationales de supervision. Nous sommes d'avis que la libre circulation de données est une question intersectorielle, et non pas une question politique, mais qui est vitale pour les entreprises européennes, en particulier les entreprises des marchés de capitaux européens que nous représentons.

Contacts

Richard Middleton
Managing Director, Co-Head of Policy Division
Richard.Middleton@afme.eu
+44 (0)20 3828 2709

Will Dennis
Managing Director, Co-Head of Policy Division
Will.Dennis@afme.eu
+44 (0)20 3828 2683

Oliver Moullin
Managing Director, Brexit
General Counsel and Company Secretary
Oliver.Moullin@afme.eu
+44 (0)20 3828 2712

Stevi Iosif
Associate Director, Advocacy
Stevi.Iosif@afme.eu
+32 2 788 39 76

Aleksandra Wojcik
Associate, Policy, Technology and Operations
Aleksandra.Wojcik@afme.eu
+44 (0)203 828 2734