Skadden

Privacy & Cybersecurity Update

President Biden Issues Executive Order To Implement EU-US Data Privacy Framework

President Joe Biden has signed an executive order regulating how U.S. intelligence agencies collect and use personal data, in an effort to reestablish a legal regime for transfers of personal data from the EU to the U.S.

On October 7, 2022, President Biden signed an executive order on "Enhancing Safeguards for the United States Signals Intelligence Activities," which establishes new regulations for the collection and use of personal data by U.S. intelligence agencies.[1] The executive order is intended to provide greater privacy protection to help reestablish an EU-U.S. framework for the legal export of personal data from the EU to the U.S. under EU laws, following the 2020 *Schrems II* decision that invalidated the prior privacy framework (Privacy Shield) between the two jurisdictions.[2] The executive order implements into U.S. law the agreement in principle on a new EU-U.S. Data Privacy Framework, which was announced by President Biden and European Commission (EC) President Ursula von der Leyen on March 25, 2022. Shortly after President Biden signed the executive order, the EC announced its intention to prepare a draft adequacy decision in favor of the U.S.

Background

In *Schrems II*, the Court of Justice of the EU (CJEU) invalidated the EU's Privacy Shield decision (Decision 2016/1250 on the adequacy of the protection provided by the Privacy Shield), citing concerns over U.S. public authorities' access to and use of EU personal data, and the lack of adequate redress mechanism available to EU data subjects against such public authorities. As a result of the decision, transfers of personal data from the EU to the U.S. on the basis of the Privacy Shield framework became illegal immediately. Companies were therefore obliged to implement a valid data transfer mechanism (such as the European Commission's Standard Contractual Clauses (SCCs)) for the transfer of personal data from the EU to the U.S. and to conduct a transfer impact assessment (TIA) for each transfer. The decision equally applied to the transfer of personal data from the U.K. to the U.S., as the CJEU decision was made during the Brexit transition period and the U.K. GDPR is materially aligned with the EU GDPR.

[1] The executive order can be accessed here.

[2] Skadden's analysis of *Schrems II* is available here.

Enhanced Privacy and Civil Liberties

The executive order introduces a series of reforms to U.S. privacy laws and practices that seek to address the concerns regarding individuals' privacy and civil liberties raised by the CJEU in *Schrems II*. These include both specific limitations and requirements imposed on the intelligence community (as defined below) and a two-step process through which data subjects in a "qualifying state" (as discussed below) can seek legal redress for violations.

Requirements for the Intelligence Community

The executive order's reforms of intelligence community actions include the following:

- **Personal Data Handling Requirements.** The executive order restricts the bulk collection of personal data by the U.S. intelligence community, which was defined in a prior executive order to cover a wide range of US government intelligence agencies, including the Central Intelligence Agency, the National Security Agency, the Defense Intelligence Agency and the Department of Homeland Security, as well as Army, Air Force, Marine Crops and Navy Intelligence. In addition, signals intelligence (which involves collecting foreign intelligence from information and communication systems and providing the information to the intelligence community) can only be collected through bulk collection where the relevant element of the intelligence community has determined that the information is "necessary" for the pursuit of a validated intelligence priority that cannot be achieved through targeted collection of personal data. Where signals intelligence is collected through bulk collection, the executive order restricts the use of any information collected to an exhaustive list of pursuits, including protecting against terrorism and cybersecurity threats created or exploited by a foreign government, organization or person.
- **Additional Safeguards.** The executive order introduces a series of safeguards for individuals in respect of U.S. signals intelligence activities. For instance, such activities may only be undertaken where necessary to advance "legitimate national security objects" that have been validated by the civil liberties protection officer (CLPO) (who is appointed by the director of national intelligence, the head of the intelligence community) and must not disproportionately impact the protection of individual privacy and civil liberties (including the privacy and civil liberties of non-U.S. citizens and residents).
- **Policy and Procedure Updates.** The executive order requires the intelligence community to update its policies and procedures to ensure they are aligned with the safeguards for privacy and civil liberties set out in the order (such as the restriction on bulk collection, the requirement to conduct signals intelligence in pursuit of a legitimate objective (*e.g.*, protecting against terrorism), and the right to seek redress under the new two-tier redress mechanism (discussed below)), and to make such policies and procedures available to members of the public. In addition, the executive order introduces new compliance mechanisms, such as the designation of legal oversight, and compliance officials to oversee signals intelligence activities and the introduction and maintenance of "appropriate" training for employees with access to signals intelligence to ensure they are aware of and understand the requirements set out in the executive order and the policies and procedures for reporting and remediating incidents of noncompliance with applicable U.S. laws. No further information is provided on the nature or frequency required of such training.

Two-Tier Redress Mechanism

The executive order introduces a new two-tier redress mechanism for privacy violations. This mechanism replaces the U.S. data ombudsman redress mechanism under the Privacy Shield framework, which was criticized for its lack of independence, investigative powers and binding authority.

Under the first tier of the redress mechanism, individuals — through the appropriate public authority from a "qualifying state" — will be able to lodge a complaint with the CLPO (the EU is intended to be a "qualifying state" and therefore EU data subjects will be able to utilize this new two-tier redress mechanism). The CLPO will conduct an initial investigation to determine whether the executive order's enhanced safeguards or other applicable U.S. laws have been violated and to determine an appropriate remediation.

If dissatisfied with the outcome, the complainant or element of the intelligence community can appeal the decision by the CLPO to a Data Protection Review Court (DPRC) under the second tier of the redress mechanism. The DPRC is a new court under which the attorney general, as directed under the executive order, is responsible for establishing under new regulations. These regulations, which were published on the same date as the executive order, require a three-panel judge to review applications to the DPRC. These judges must not be members of the U.S. government, must have relevant experience in data privacy and national security law, and must be protected against removal (except where there is a serious cause for dismissal such as a conviction of a criminal offence). In addition, the DPRC must appoint a "special advocate" to represent the complainant at the court. However, while judges at the DPRC are supposed to provide "independent and impartial review[s] of applications," the regulations note that the attorney general is responsible for appointing judges to the DPRC (although such judges will not work under the supervision of the attorney general) and the DPRC will be established within the Department of Justice. Though similar to the status of a special counsel (who operates independently but is appointed and can be dismissed by the attorney general), the level of involvement of the attorney general and the Department of Justice has led some to express skepticism as to whether the DPRC will be truly independent.

Additionally, the Privacy and Civil Liberties Oversight Board (PCLOB), a bipartisan, five-member board that is appointed by the president and confirmed by the Senate and which sits within the executive branch, will have a right to review this two-tier redress mechanism on an annual basis, including whether the intelligence community has complied with decisions made by the CLPO and DPRC. However, the executive order notes that such annual reviews by the PCLOB are "encouraged," but not mandatory.

Next Steps

In response to the executive order, the EC announced that it would prepare a draft adequacy decision that, if adopted, would allow personal data to flow freely between the EU and U.S. companies that have been certified by the Department of Commerce under the EU-U.S. Data Privacy Framework. The adoption procedure, which the EC has launched, could take up to six months and involves various stages. These steps include the European Data Protection Board (EDPB) issuing a non-binding opinion and a committee of representatives from EU member states approving the adequacy decision. In addition, the European Parliament may exercise its right of scrutiny over the draft decision and issue a nonbinding resolution. Following this review procedure, the EC can adopt a final adequacy decision in favor of the U.S. for businesses that are certified under the EU-U.S. Data Privacy Framework. Such organizations would no longer have to rely on a separate valid data transfer mechanism (*e.g.*, SCCs) for the transfer of personal data from the EU to the U.S. The European Commission has said that companies will be able to join the EU-U.S. Data Privacy Framework by committing to comply with a set of privacy obligations.

Separately, the U.K. government has said that it is working "expeditiously" to review the enhanced safeguards and redress mechanism in the executive order as part of its assessment of U.S. data protection laws and practices. The U.K. government has said that it intends to lay adequacy regulations in Parliament in early 2023 to restore the free flow of personal data between the two jurisdictions. Meanwhile, the U.S. government has said that it intends to designate the U.K. as a "qualifying state" under the executive order, which would mean that U.K. data subjects could also utilize the enhanced privacy and civil liberties outlined in the executive order (*e.g.*, the multi-layered redress mechanism).

Max Schrems, who brought the *Schrems II* case before the CJEU, has said that, at first sight, the executive order does not address the concerns of the court's decision in that case. In particular, Mr. Schrems has criticized the independence of the DPRC, which, according to him, will not be a court within the legal meaning of Article 47 of the EU's Charter of Fundamental Rights or the U.S. Constitution. Mr. Schrems has further said that NOYB – European Center for Digital Rights, a nonprofit organization of which he is the chair, will review the executive order and publish a detailed legal analysis with a view to potentially bringing another legal challenge before the CJEU.

Key Takeaways

- The executive order is welcome news for businesses that transfer personal data from the EU to the U.S. While such transfers of personal data are not illegal, they are more cumbersome to implement than previously under the Privacy Shield framework. However, the adoption of an adequacy decision by the EC is not guaranteed, and any such decision may be subject to fresh legal challenges.
- In the meantime, it remains business as usual for companies that transfer personal data from the EU to the U.S., meaning companies must continue to rely on a valid data transfer mechanism and conduct a TIA for each transfer of European personal data to the U.S.

Return to Table of Contents

European Commission Publishes Draft Cyber Resilience Act

The EC has published a draft law establishing cybersecurity requirements for products with digital elements.

On September 15, 2022, the EC published its proposal for a regulation on cybersecurity requirements for products with digital elements, known as the Cyber Resilience Act). The EC describes the act as "the first regulation of its kind," and the draft will now be examined by the European Parliament and the European Council, a process which could take up to two years.

Background

The act was first announced by EC President Ursula von der Leyen during her State of the EU address on September 15, 2022, and builds on the EU Cybersecurity Strategy and EU Security Union Strategy. Since the act would be an EU regulation and not a directive, if the EC implements it, the act will automatically be enforceable and applicable in all EU member states, ensuring the uniformity of cybersecurity requirements across all represented jurisdictions.

Rules and Requirements

The proposed act notes the global cost of cybercrime in 2021 as €5.5 trillion and attributes this to the fact that (1) hardware

and software products suffer from a low level of cybersecurity and (2) individuals lack an understanding of the cybersecurity properties of such products. To address these concerns, the act outlines:

- rules for placing products with digital elements (defined further below) on the EU market;
- requirements for the design, development and production of products with digital elements and obligations for manufacturers, importers and distributors regarding such products;
- requirements for manufacturers to establish vulnerability handling processes; and
- rules on market surveillance and enforcement.

Scope

The act would apply to manufacturers, importers and distributors of products with digital elements with intended or reasonably foreseeable use that includes a direct or indirect link to a device or network. "Products with digital elements" are broadly defined to include *any* software or hardware and their associated remote data processing operations. There is a carve-out for certain products with digital elements, including medical products and devices that are subject to Regulation (EU) 2017/745 and Regulation (EU) 2017/746.

Conformity Assessment

Under the act, before introducing a product with digital elements on the EU market, manufacturers would have to perform a two-fold "conformity assessment." Under this requirement, the manufacturer would have to:

- Ensure the product meets the security requirements set out in Section 1, Annex I of the act (*e.g.*, ensure protection from unauthorized access, ensure the confidentiality of processed data and provide security related information by recording and/or monitoring internal activity); and
- Establish vulnerability handling processes pursuant to Section 2, Annex I of the act (*e.g.*, apply effective and regular tests and reviews of the security of the product with digital elements, establish and enforce a policy on coordinated vulnerability disclosure, provide security updates to products with digital elements).

Where the conformity assessment demonstrates compliance with the requirements in Section 1, Annex 1 and Section 2, Annex 1 of the act, the manufacturer would have to then draw up an EU declaration of conformity that notes the fulfilment of the applicable essential requirements in accordance with Article 20 of the act and affix the "CE" marking to the declaration in accordance with Article 22 of the act (this marking indicates that the product has been assessed by the manufacturer and deemed to meet EU safety, health and environmental protection requirements). By making such a declaration and affixing the CE marking, the manufacturer would assume responsibility for conformity with the a. Manufacturers also would have to provide the EU declaration of conformity packaged along with the product, or instead include a website address where the EU declaration of conformity could be accessed in the instructions and/or other printed information provided to users. Lack of compliance with these requirements could result in enforcement actions from market surveillance authorities (defined below).

'Critical' Products With Digital Elements

Annex III of the act contains a list of "critical" products with digital elements that are divided into two classes:

- Class I ("lower risk"): This includes password managers, network management systems and update/patch management; and
- Class II ("higher risk"): This includes operating systems for servers, desktops, mobile devices, smart meters and robot controllers.

As part of the act's requirements, manufacturers would have to satisfy stricter conformity assessments before placing these critical products with digital elements on the EU market. For instance, Class II critical products manufacturers would have to engage a third party as part of the conformity assessment discussed above.

Reporting Obligations

In addition to the conformity assessment (discussed above), manufacturers would be required to notify the European Union Agency for Cybersecurity (ENISA) within 24 hours of becoming aware of (1) any actively exploited vulnerability contained in products with digital elements, and (2) any incident having an impact on the security of products with digital elements. Manufacturers also would have to inform users about any such incidents without undue delay and, where necessary, what actions they can take to mitigate the impact of such incidents.

The act also would require importers and distributors to (1) inform manufacturers without undue delay of any vulnerability in such products, and (2) immediately notify market surveillance authorities in member states where such products present a "significant" cybersecurity risk. A significant cybersecurity risk is defined as one that, based on its technical characteristics, can be assumed to have a high likelihood of an incident that could result in a severe negative impact, such as causing considerable material or non-material loss or disruption.

The act includes a 24-month grace period for compliance with the requirements starting from the date of implementation.

However, there is a shorter 12-month grace period for manufacturers for compliance with their respective reporting obligations discussed earlier.

Enforcement and Penalties

The act would require each member state to designate an existing or new authority to act as a market surveillance authority. Such authorities would be required to cooperate with other surveillance authorities, including ENISA and data protection authorities.

In cases where market surveillance authorities would have sufficient reasons to believe a product with digital elements presents a significant cybersecurity risk (as described above), the act grants authorities the power to conduct evaluations of the product and, in the case of a finding of noncompliance with the act, to take all corrective action necessary to ensure compliance, to withdraw the product from the market or to recall the product within a reasonable period of time. The act also would grant market surveillance authorities the power to conduct simultaneous "sweeps" of products with digital elements to check for compliance with the act (*e.g.*, an EU declaration of conformity has not been drawn up or the CE marking has not been affixed to the EU declaration of conformity (as discussed above)). The results of the sweep could be made public, which could have significant reputational implications for companies that are subject to such sweeps.

The act sets out administrative fines for noncompliance; the highest level of administrative fine would be at €15 million or 2.5% of worldwide annual turnover for the previous financial year, whichever is higher. However, similar to the General Data Protection Regulation (GDPR), the method for imposition of administrative fines is left to the discretion of each member state, which could result in a lack of harmonization across each country. On May 12, 2022, the EDPB adopted guidelines for the calculation of administrative fines under the GDPR in an attempt to harmonize the methodology that supervisory authorities use when calculating administrative fines. It remains to be seen whether similar guidelines will be published for the Cyber Resilience Act.

Parallel Effort in the UK

Separately, the U.K. government also is focusing on cybersecurity requirements for connectable products (*e.g.*, smartphones, connected cameras, smart home assistants), as set out in the Product Security and Telecommunications Infrastructure Bill. As in the act, the bill, once passed, would place duties on manufacturers, importers and distributers; however, the scope of the products, duties, enforcement powers and penalties outlined in the bill differs from those in the act. For instance, the bill is limited to connectable products and the administrative fines for noncompliance are set at £10 million or 4% of worldwide revenue, whichever is higher. However, manufacturers, importers and distributors would be given a grace period of at least 12 months before the legislative framework fully comes into force.

The bill is currently at the final stage in the Houses of Parliament (consideration of amendments) before receiving Royal Asset. We are closing monitoring future developments.

Key Takeaways

- The act is ambitious in its objective, and it has the potential to enhance and harmonize cybersecurity measures across the EU and become a gold standard for cybersecurity legislation globally. However, the act also may create significant operational and financial challenges for organizations and manufacturers, in particular, which may be required to overhaul their processes and products (in a relatively short period of time) in order to comply with the act.
- From a consumer perspective, the act would ensure greater protection and enhance consumers' understanding of the cybersecurity properties of the products they purchase. It may, however, negatively impact the availability of products on the EU market, particularly if companies struggle to adapt to the new requirements or are subject to "sweeps" that impede their operations.
- In light of the additional parallel effort in the U.K., manufacturers, importers and distributors across the continent may have to grapple with two potentially conflicting sets of legislation.

Return to Table of Contents

US Treasury Department Seeks Public Comment on Potential Federal Cyber Insurance Program

The U.S. Treasury Department's Federal Insurance Office (FIO) and the Cybersecurity and Infrastructure Security Agency (CISA) are soliciting feedback from the public on the need for a potential federal cyber insurance program.

On September 29, 2022, the FIO issued a request for comment in the Federal Register to solicit public comments on whether to implement a federal insurance program for responding to catastrophic cyber incidents and, if desired, how to structure such a program.[3] The regulator will be seeking public comments until November 14, 2022.

[3] The request for comment is available here.

Background Information

The FIO is an office housed within the U.S. Department of the Treasury that provides expertise on insurance matters to the Treasury and other federal agencies, in addition to engaging in international discussions relating to insurance. CISA is an agency of the U.S. Department of Homeland Security that is responsible for strengthening cybersecurity and infrastructure protection, coordinating cybersecurity programs with U.S. states and improving the government's cybersecurity protections against private and nation-state hackers. In September 2022, CISA released its 2023-2025 Strategic Plan, which was issued as a response to the increasing vulnerability of U.S. infrastructure to cyberattacks. In light of their efforts to define and manage the government's role in mitigating cyber threats, CISA and the FIO have agreed to provide Congress with a joint assessment of whether a federal insurance response to catastrophic cyber incidents is warranted.

In May 2021, following a steady stream of cyberattacks in recent years, the Government Accountability Office (GAO) began reviewing how well-suited the government's Terrorism Risk Insurance Program (TRIP) was for dealing with these incidents. The GAO had previously issued a report the previous year that cited a 2020 CISA study that included an analysis of scenario-based estimates of potential losses from severe cyber incidents that ranged from $2.8 billion to $1 trillion per event for the U.S.[4] Following the 2020 report, the GAO issued a second report in 2022 that recommended the FIO and CISA jointly assess the issue, secure public comments related to catastrophic cyber incidents and discuss a potential federal cyber insurance program.[5]

The FIO's Request for Comment

In its request for comment, the FIO noted that cyber insurance is a significant risk-transfer mechanism for businesses, and that the insurance industry has an important role to play in strengthening cyber hygiene and building resiliency. The request also acknowledged that most insurance in the U.S. is regulated at a state level but noted that there are programs where policymakers and regulators saw a need for federal programs to supplement the commercial market and existing state requirements. Examples of such programs include TRIP, the National Flood Insurance Program and the Federal Crop Insurance Program.

In their request, the regulators are specifically seeking comments on:

- The risks of catastrophic cyber incidents to critical infrastructure. Specifically, what type of cyber incidents could have a catastrophic effect on U.S. critical infrastructure and how likely are these types of incidents? Are any particular sectors of U.S. critical infrastructure more susceptible to such incidents?
- The potential quantification of such risks and the extent of existing private market insurance protection for such risks. Specifically, what amount of financial losses should be deemed "catastrophic" for purposes of any potential federal insurance response?
- Whether a federal insurance response is warranted. Specifically, what insurance coverage is currently available for catastrophic cyber incidents and what are the current limitations?
- How such a federal insurance response, if warranted, should be structured. Specifically, what structures should the FIO and CISA consider for a potential federal insurance response and to what extent should reinsurance arrangements, including capital markets participation, be included in the potential response?

The request for comments is open until November 14, 2022. Those seeking to submit comments can do so at the government's website at regulations.gov.

Key Takeaways

The FIO and CISA's request for comment signals a potentially significant shift in the insurance landscape surrounding cybersecurity incidents. One outcome of the shift could be that federal financial support for certain cyber risks could protect insurers against certain catastrophic losses, and thereby encourage them to make cybersecurity insurance more widely available. We will monitor further developments on this topic.

Return to Table of Contents

New York DFS Fines Health Insurer $4.5 Million for Consumer Data Breach

The New York Department of Financial Services (DFS) ordered EyeMed Vision Care LLC, a licensed health insurance company for vision services, to pay a $4.5 million penalty following a data breach that exposed more than six years' of consumers' sensitive nonpublic information.

On October 18, 2022, the New York DFS announced that the agency had settled with EyeMed Vision Care LLC (EyeMed) to end an investigation into the company's violation of New York data protection regulations.[6] Under the settlement, EyeMed agreed to pay DFS a $4.5 million penalty and to undertake significant remedial measures to better secure its data.

[4] The GAO's 2020 report is available here.

[5] The GAO's 2022 report is available here.

[6] The DFS announcement is available here.

Background

On October 9, 2020, EyeMed reported to DFS that an individual gained unauthorized accessed to its enrollment processing email mailbox, which both EyeMed and certain of its external clients used to communicate enrollment updates. Lasting from June 24 to July 1, 2020, the breach allowed the intruder to access emails and attachments dating back six years before the attack. The attackers were found to have accessed information on over 2 million customers, including children, and the information included names, Social Security numbers and sensitive nonpublic health data such as medical diagnoses and conditions. DFS could not determine how the intruder secured access to the mailbox, but EyeMed suggested that it was likely the result of a successful phishing scheme.

The DFS investigated EyeMed to determine whether the company had violated Cybersecurity Regulation 23 NYCRR Part 500, a New York state regulation that became effective on March 1, 2017, and was designed to promote the protection of customer information and information technology systems of financial service companies.

DFS Consent Order

The DFS investigation, as set forth in its Consent Order, determined that EyeMed committed the following violations[7] of the Cybersecurity Regulation:

- Failure to implement multifactor authentication — a security measure requiring users to provide multiple credentials before accessing a platform — or reasonably equivalent access controls within EyeMed's email network in violation of 23 NYCRR § 500.12(b);
- Failure to limit user access privileges by permitting nine employees to share login credentials for the mailbox in violation of 23 NYCRR § 500.07;
- Failure to implement sufficient data retention and disposal processes in violation of 23 NYCRR § 500.13; and
- Failure to conduct a risk assessment that complied with the requirements of 23 NYCRR § 500.09.

The order further noted that EyeMed violated 23 NYCRR § 500.17(b), which requires regulated entities to annually certify compliance with the Cybersecurity Regulation. Although EyeMed timely certified its compliance with the regulation from 2017-20, DFS concluded through its investigation that the company's certifications were based on inadequate risk assessments. Consequently, DFS found that EyeMed's certification filings for 2017-20 were improper.

In addition to the monetary penalty, EyeMed agreed to conduct a comprehensive cybersecurity risk assessment consistent with the requirements of 23 NYCRR § 500.09, submit the results of the assessment to DFS and present a detailed action plan describing the steps EyeMed will take to address any risks identified in the assessment. The company further agreed that its action plan is subject to DFS review and approval.

The fine paid to DFS was the second fine EyeMed paid in connection with the data breach. The company had previously paid a $600,000 fine to the New York attorney general in connection with a separate inquiry into the incident.

Key Takeaways

The order highlights the continued focus from regulators on cybersecurity precautions, as well as the need for companies that handle sensitive consumer information to ensure that their cybersecurity measures and assessments align with applicable laws and regulations.

Return to Table of Contents

[7] The Consent Order is available here.

Skadden

Contacts

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

James Carroll
Partner / Boston
617.573.4801
james.carroll@skadden.com

Brian Duwe
Partner / Chicago
312.407.0816
brian.duwe@skadden.com

David Eisman
Partner / Los Angeles
213.687.5010
david.eisman@skadden.com

Patrick Fitzgerald
Partner / Chicago
312.407.0508
patrick.fitzgerald@skadden.com

Todd E. Freed
Partner / New York
212.735.3714
todd.freed@skadden.com

Marc S. Gerber
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

Rich Grossman
Partner / New York
212.735.2116
richard.grossman@skadden.com

Ken D. Kumayama
Partner / Palo Alto
650.470.4553
ken.kumayama@skadden.com

Michael E. Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

Jason D. Russell
Partner / Los Angeles
213.687.5328
jason.russell@skadden.com

David Schwartz
Partner / New York
212.735.2473
david.schwartz@skadden.com

Ingrid Vandenborre
Partner / Brussels
32.2.639.0336
ingrid.vandenborre@skadden.com

Helena Derbyshire
Of Counsel / London
44.20.7519.7086
helena.derbyshire@skadden.com

Peter Luneau
Counsel / New York
212.735.2917
peter.luneau@skadden.com

James S. Talbot
Counsel / New York
212.735.4133
james.talbot@skadden.com

Eve-Christie Vermynck
Counsel / London
44.20.7519.7097
eve-christie.vermynck@skadden.com

Skadden, Arps, Slate, Meagher & Flom LLP
One Manhattan West
New York, NY 10001
212.735.3000