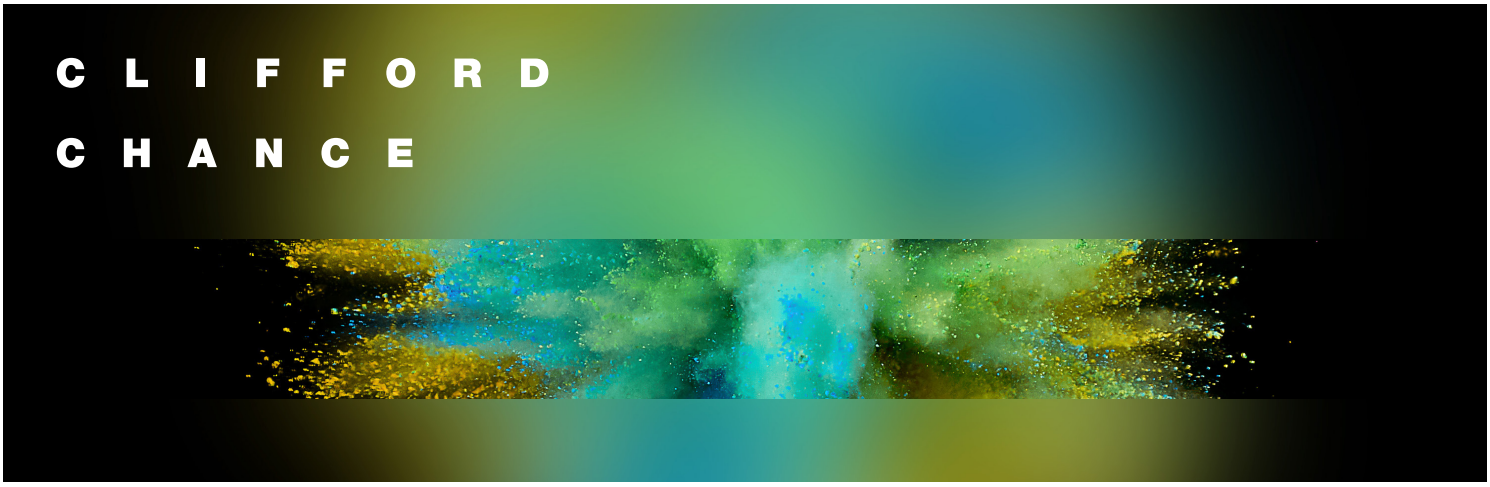
CLIFFORD

CHANCE



NEXT STEPS AFTER U.S. PRESIDENT BIDEN ISSUES EXECUTIVE ORDER ON U.S. DATA TRANSFERS FROM 'QUALIFIED STATES'

On 7 October 2022, U.S. President Joe Biden issued an Executive Order "**On Enhancing Safeguards for United States Signals Intelligence Activities**" (the Order) to effectuate the preliminary agreement between U.S. President Biden and European Commission President Ursula von der Leyen for facilitating trans-Atlantic data flows. The Order aims to address concerns raised by the Court of Justice of the European Union (CJEU) in the 'Schrems II' decision of 16 July 2020, which invalidated the previous EU-U.S. Privacy Shield (for additional background, see our more detailed briefing: **US and EU Agree on Framework for Privacy Shield Replacement**). In particular, the Order adds additional safeguards and redress mechanisms for persons in certain qualifying countries or regional economic integration organizations to protect and preserve privacy rights and civil liberties in relation to data collection practices and procedures of the U.S. intelligence community.

The Order does not establish a mechanism for transfers of personal data from the EEA to the U.S., but is expected to pave the way for an adequacy decision from the European Commission in due course, which would permit such trans-Atlantic personal data flows. In the meantime, it remains necessary for organizations to comply with requirements applicable to such data transfers under the EU General Data Protection Regulation (the GDPR) and the CJEU 'Schrems II' decision, including carrying out 'transfer impact assessments', implementing appropriate safeguards (e.g., Standard Contractual Clauses or Binding Corporate Rules) and, if necessary, supplementary measures to secure the transfer. The rights and safeguards created by the Order would in many cases be relevant to these transfer impact assessments.

Key points of the Order

The Order seeks to address the tension between U.S. national security interests in intelligence gathering and the privacy interests of individuals in limiting access to their personal information. As an attempt to mitigate this tension, the Order implements the following guiding principles, objectives and policies:

- *Authorization of activities* – All U.S. signals intelligence activities must be authorized by statute or presidential directive in accordance with U.S. law, be subject to appropriate safeguards, and be balanced with the privacy rights and civil liberties of "all persons, regardless of their nationality." For example, the U.S. intelligence community may only conduct signal intelligence activities that are necessary and proportionate to a validated and authorized intelligence priority. The Director of National Intelligence will also obtain an assessment from the Civil Liberties Protection Officer of the Office of the Director of National Intelligence (the CLPO) that the signals intelligence activities align with the objectives of the Order, which are described in greater detail below.
- *Types of activities* – The Order requires that the U.S. only conduct specific signals collection activities after a determination that such activity advances a "validated intelligence priority" based on all relevant factors. The U.S. intelligence community must also consider "the availability, feasibility and appropriateness of other less intrusive sources and methods for collecting [such] information… including from diplomatic and public sources." Such activities must also be tailored "as feasible" to advance national security interests while not disproportionately impacting a person's privacy rights and civil liberties. The U.S. intelligence community may also conduct "bulk" collection signals intelligence (i.e., acquiring large quantities of signals intelligence data without the use of discriminants or specific identifiers) only if such information cannot be obtained through targeted signals intelligence collection activities.
- *Permitted objectives* – U.S. signals intelligence activities must satisfy at least one of the enumerated objectives set forth in the Order. Such objectives include understanding the "capabilities, intentions, or activities" of a (1) foreign government, military arm, faction, or political organization in order to protect U.S. national security interests, (2) a foreign organization (e.g., international terrorist organization) that poses a current or potential U.S. national security threat, and (3) global security threats (e.g., climate change, public health risks, humanitarian risks, political instability and geographic rivalries). In addition, the Order permits signals intelligence collection activities to protect against foreign cybersecurity threats and to maintain the integrity of U.S. political processes and infrastructure.
- *Prohibited objectives* – The Order also explicitly prohibits signals intelligence collection activities to (1) suppress criticism, dissent or political opinions of any individuals or the press, (2) suppress legitimate privacy interests, (3) restrict an individual's right to legal counsel, or (4) disadvantage an individual based on their ethnicity, race, gender, gender identity, sexual orientation or religion. Moreover, signals intelligence collection activities must be limited to advancing national security interests and may not be conducted to create or bolster a competitive economic advantage for U.S. companies or industry sectors.

- *Physical and technical safeguards* – The Order contains technical and physical safeguards "to minimize the dissemination and retention of personal information collected through signals intelligence", including limiting the ability of the U.S. intelligence community to disclose such data within the U.S. government (e.g., only to authorized personnel on a "need-to-know" basis) and to other foreign governments or organizations (e.g., requiring an assessment of the potential impact of the disclosure on the applicable data subject(s)). The U.S. intelligence community may only retain a non-U.S. person's personal information if the retention of comparable information of U.S. persons would be permitted under "applicable law" and must promptly delete all such information after the applicable retention period lapses. All personal information collected through signals intelligence activities must be processed in accordance with relevant presidential orders and associated policies. Each member of the U.S. intelligence community that engages in such intelligence collection must also maintain (1) adequate documentation that describes the nature, type and context of such intelligence activities and (2) sufficient legal, oversight and compliance officials and policies for such intelligence activities.

In the event a "qualifying state" believes that any element of the U.S. intelligence community violated the Order or its related regulations, then the qualifying state (on behalf of the affected data subjects) may file a complaint and seek redress pursuant to the following mechanisms:

- *Qualifying state designation* – As a threshold matter, the U.S. Attorney must first designate a foreign country or regional economic integration organization as a "qualifying state" for the redress mechanisms described in the Order to apply. In making such determination, the Attorney General, in consultation with other departments of the Executive Branch, must determine that (1) the country or regional economic organization maintains laws that require appropriate safeguards for signals intelligence activities for personal information of U.S. persons transferred from the U.S. to the applicable country or organization, (2) the country or regional economic organization permits the transfer of personal information between the U.S. and such country or organization member countries for commercial purposes, and (3) the designation advances U.S. national interests.
- *Initial CLPO determination* – The Order requires the U.S. Attorney General to formulate procedures for an initial layer of review of complaints by the CLPO from qualified states. For each complaint, the CLPO will review all information necessary to investigate the complaint; determine whether a covered violation occurred by assessing national security interests, privacy protection and giving "appropriate deference" to national security officials; and impartially apply the law. After such review is completed, the CLPO will inform the complainant (through the applicable public authority of the qualifying state) that "the review did not identify any covered violations or [the CLPO]issued a determination requiring appropriate remediations." The CLPO will also prepare and maintain "appropriate documentation" of its review, including a classified report of violations and an explanation of its decision based on factual findings and the appropriate remediation efforts. Subject to the appeal process described below, the CLPO's findings and determinations will be binding on each element of the U.S. intelligence community. Notably, the CLPO will also be free from interference from the U.S. Director of National Intelligence and may not be removed from office, except for "misconduct, malfeasance, breach of security, neglect of duty or incapacity."

- *Appeal process of Data Protection Review Court* – Within sixty days of the Order, the U.S. Attorney General must also establish a "Data Protection Review Court" comprised of private legal practitioners with appropriate experience in data privacy and national security law. Following the CLPO's determination, either the complainant or the applicable element of the U.S. intelligence community may appeal such determination to the Data Protection Review Court. Upon the filing of such appeal, the Data Protection Review Court will convene a three-member panel and appoint a "special advocate" to advocate for the complainant's privacy and civil liberty interests. The Data Protection Review Court then must impartially review the record and the CLPO's determination of whether a covered violation occurred and, if so, whether the remediation efforts are appropriate. The Order requires that the Data Protection Review Court use relevant decisions of the Supreme Court of the United States to guide its review in a manner similar to that of other U.S. courts, including giving "appropriate deference to determinations of national security officials." The Data Protection Review Court will then issue its own determination and inform the CLPO and complainant (through the applicable public authority of the qualifying states) of its decision without "confirming or denying that the complainant was subject to U.S. signals intelligence activities." Similar to the CLPO, the Data Protection Review Court's decisions are binding on the U.S. intelligence community and judges may not be removed, except for "misconduct, malfeasance, breach of security, neglect of duty or incapacity."

Next steps & guidance

With the Order's recent publication, the U.S. government will now move to enacting the implementing policies and regulations associated with the Order. At the same time, the European Commission will commence its adequacy decision process, working to assess the sufficiency of the protections afforded to citizens in the EU under the Order and related U.S. implementing regulations by reference to the 'European essential guarantees' for surveillance measures, notably as identified by the European Data Protection Board (the EDPB) on its Recommendation 02/2020. The adoption of an adequacy decision by the European Commission involves an opinion of the EDPB and an approval from representatives of EU Member States. Historically, such adoption processes have taken several months, and it is expected that any adequacy decision related to the Order will have a similar timeline. As of the date of this publication, the expected target date for the adoption of this adequacy decision is end of Q1 2023.

Also, on 7 October 2022, the UK Secretary of State for Digital, Culture, Media and Sport, the Rt. Hon. Michelle Donelan MP and the U.S. Secretary of Commerce, Gina M. Raimondo issued a **joint statement** on the progress of promoting UK-U.S. cross-border data flows. In the statement, the UK government welcomed the release of the Order and "intends to work expediently to conclude its assessment" and issue an adequacy decision, while the U.S. will work to designate the UK as a "qualifying state" under the Order.

In the meantime, in addition to compliance with any applicable GDPR requirements pertaining to personal data transfers, companies should consider the following in light of the Order, especially if all or a portion of the business relies on cross-border data transfers from the EU and other jurisdictions to the U.S.:

- *Privacy policies* – Companies should engage with data privacy counsel to assess the impact of the Order on their existing privacy policies. For example, if the business collects personal information from "qualified states" and transfers such data to the U.S. for commercial operations, then companies should consider disclosing the rights and redress mechanisms afforded to persons in such qualified states under the Order. Importantly, those applicable data subjects must seek redress from the U.S. government through the appropriate public authority in the qualifying state (i.e., not on an individual basis). Additional guidance from the U.S. government is expected, but U.S. companies should begin preliminary discussions of the Order's effect on their privacy policies.
- *Transfer impact assessments* – companies should also engage with data privacy counsel to take account of the legal changes that the Order will bring to the existing U.S. legal framework, and the impact of this on their 'transfer impact assessments'. Indeed, even before the European Commission adopts its adequacy decision, the implementing policies and regulations associated with the Order (once effectively enacted) are meant to bring the U.S. framework closer to the EU data protection requirements and the 'European Essential Guarantees for surveillance measures'. As a result, it may be necessary to update existing transfer impact assessments to reflect those changes, and companies should factor in those changes when assessing the risk associated with new transfers.
- *Commercial agreements* – In the Order's "**Fact Sheet**", the White House stated that the Order also will "provide greater legal certainty for companies using Standard Contractual Clauses and Binding Corporate Rules to transfer EU person data to the [U.S.]." While companies should continue using the Standard Contractual Clauses and Binding Corporate Rules to facilitate the legal transfer of EU personal data to the U.S. unless and until the European Commission issues an adequacy decision for the U.S., companies should also review their commercial contracts and relationships and assess the potential impact of the Order. For example, U.S. businesses and their contractual partners should engage in preliminary discussions to determine if any contractual amendments should be executed in light of the Order and any related adequacy decisions.

In the longer term, companies will also need to monitor the progress of any legal challenges raised in response to an EU adequacy decision. The privacy-focused nonprofit organization NOYB (spearheaded by Max Schrems, the Austrian Lawyer who successfully challenged Privacy Shield) published a statement on 7 October 2022 reacting to the Order. The statement outlines concerns, including as to the meaning of 'proportionality' under the Order and the status of the Data Protection Review Court as a body within the US government's executive branch. It is expected that NOYB will bring a legal challenge to any EU adequacy decision. It remains to be seen whether the Order – referred to as "Privacy Shield 2.0" by some – will fare better than Privacy Shield.

AUTHORS

Devika Kornbacher
Partner
New York
T: +1 212 878 3424
E: devika.kornbacher@cliffordchance.com

Dessislava Savova
Partner
Paris
T: +33 1 4405 5483
E: dessislava.savova@cliffordchance.com

Alexandre Balducci
Avocat
Paris
T: +33 1 4405 5137
E: alexandre.balducci@cliffordchance.com

Ricky Legg
Law Clerk
Washington
T: +1 202 912 5943
E: ricky.legg@cliffordchance.com

Rita Flakoll
Senior Associate
Knowledge Lawyer
London
T: +44 207006 1826
E: rita.fakoll@cliffordchance.com

CONTACTS

Megan Gordon
Partner
Washington
T: +1 202 912 5021
E: megan.gordon@cliffordchance.com

Fernando Irurzun
Partner
Madrid
T: +34 91 590 4120
E: fernando.irurzun@cliffordchance.com

Ines Keitel
Partner
Frankfurt
T: +49 69 7199 1250
E: ines.keitel@cliffordchance.com

Jonathan Kewley
Partner
London
T: +44 207006 3629
E: jonathan.kewley@cliffordchance.com

Celeste Koeleveld
Partner
New York
T: +1 212 878 3051
E: celeste.koeleveld@cliffordchance.com

Simon Persoff
Partner
London
T: +44 207006 3060
E: simon.persoff@cliffordchance.com

Gunnar Sachs
Partner
Düsseldorf
T: +49 211 4355 5460
E: gunnar.sachs@cliffordchance.com

Daniel Silver
Partner
New York
T: +1 212 878 4919
E: daniel.silver@cliffordchance.com

Thomas Voland
Partner
Dusseldorf
T: +49 211 4355 5642
E: thomas.voland@cliffordchance.com

Laia Bertran Manye
Senior Associate
London
T: +44 207006 8919
E: laia.bertranmanye@cliffordchance.com

Sanne Blankestijn
Senior Associate
Amsterdam
T: +31 20 711 9131
E: sanne.blankestijn@cliffordchance.com

Andrea Tuninetti Ferrari
Counsel
Milan
T: +39 02 8063 4435
E: andrea.tuninettiferrari@cliffordchance.com

Arnav Joshi
Senior Associate
London
T: +44 207006 1303
E: arnav.joshi@cliffordchance.com

Alexander Kennedy
Counsel
Paris
T: +33 1 4405 5184
E: alexander.kennedy@cliffordchance.com

Andrei Mikes
Senior Associate
Amsterdam
T: +31 20 711 9507
E: andrei.mikes@cliffordchance.com

Manel Santilari
Senior Associate
Barcelona
T: +34 93 344 2284
E: manel.santilari@cliffordchance.com

Grégory Sroussi
Counsel
Paris
T: +33 1 4405 5248
E: gregory.sroussi@cliffordchance.com

Herbert Swaniker
Senior Associate
London
T: +44 207006 6215
E: herbert.swaniker@cliffordchance.com

Jaap Templeman
Senior counsel and co-head of Tech Group
Amsterdam
T: +31 20 711 9192
E: jaap.tempelman@cliffordchance.com

Susanne Werry
Counsel
Frankfurt
T: +49 69 7199 1291
E: susanne.werry@cliffordchance.com

CLIFFORD

CHANCE

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

2210-003214