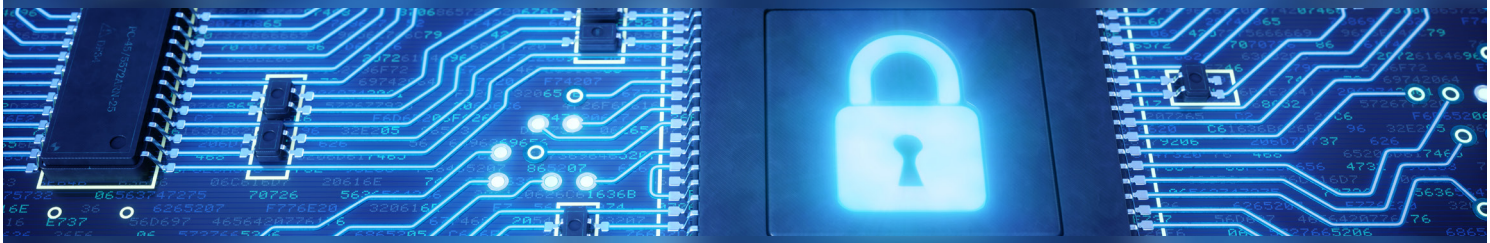
CLIFFORD

CHANCE



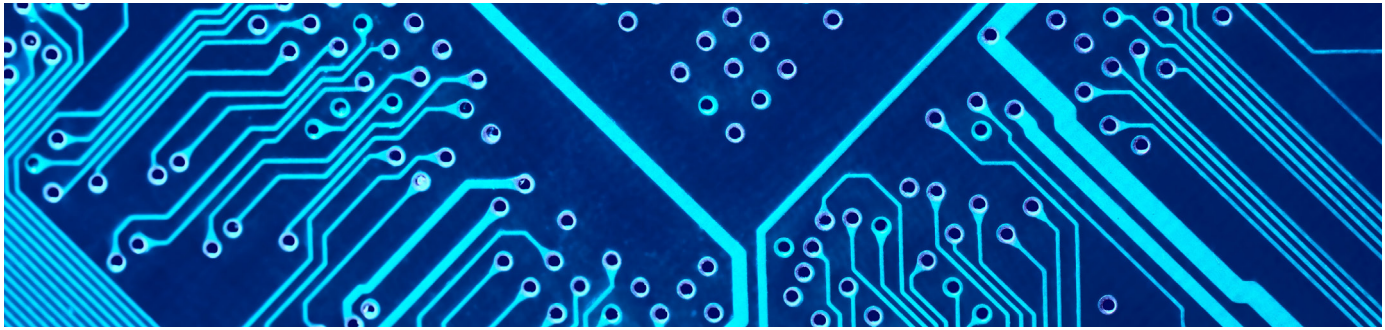
# GENERAL DATA PROTECTION REGULATION (GDPR)
## COMPLIANCE FOR US CORPORATIONS, FUNDS, AND BROKER-DEALERS

# WHAT ARE THE IMMINENT EXTRATERRITORIAL EFFECTS OF THE EU GENERAL DATA PROTECTION REGULATION ?

- The GDPR takes effect on May 25, 2018.
- The GDR is a sweeping EU data privacy law with broad extraterritorial effect that applies to the personal data of EU residents.
- Under the GDPR, “personal data” is broadly defined and includes all information relating to identifiable individuals held in electronic form.
- The GDPR includes a significant expansion of obligations of non-EU companies that control or process data of EU residents.
- Non-EU companies must identify any personal data of EU residents they control or process, and ensure they are GDPR compliant prior to May 25th.

## What are the Penalties for Non-Compliance?

- Penalties for serious breaches can result in fines of up to the greater of 4% of global revenue or €20 million.



# WHAT ARE THE GDPR'S KEY REQUIREMENTS?

- Imposes limitations on data transfer outside the European Economic Area (EEA).[1]
- Imposes reporting and auditing requirements.
- Sets a short deadline of 72 hours for notification of security breaches to the relevant data protection authority.
- Gives data subjects control over their personal data.
- Requires that all data processing be justified by:
  - The data subject's informed consent;
  - Compliance with obligations arising under the law; or
  - The data controller's legitimate interests outweighing prejudice to the privacy of the data subject.
- Requires that processing be proportionate to the purposes for which the data was collected and deleted when no longer needed.
- Requires designation of a representative based in an EU member state who will act as the point of contact for the relevant data protection authority.

## Key Terms

- **"Personal data"** – all information relating to an identifiable EU resident, particularly by reference to an identifier such as a name
- Data **"controller"** – entities who determine the purposes and means of processing of personal data
- **"Processing"** – any operation performed on personal data such as collection, recording, organization, retrieval, etc.
- Data **"processor"** – service providers who process data on behalf of their controller-customers
- **"Consent"** – freely given, specific, informed, and unambiguous indication of a data subject's wishes (a higher standard than under the previous EU privacy directive)
- **"Transparency"** – data subjects must be told about the processing of their information and given other necessary information so that the processing is "fair"

1 The EEA includes EU Member States and Iceland, Liechtenstein, and Norway.

# WHO DOES THE GDPR APPLY TO OUTSIDE OF THE EU?

- Data processors processing data for an entity in the EU.
- Data controllers who monitor the behavior of or offer goods or services to individuals in the EU.
  - "Monitoring" includes cookies or apps that track usage if the information collected renders an individual identifiable.
  - "Offering" means *intentionally* targeting EU residents. An intention can be evidenced from offering goods in a specific language or currency.

# GDPR VS US REGULATIONS

- The GDPR contains a broader and more expansive view of “personal data” than most US laws do.
  - US requirements vary by state and sector, but are generally limited to protections of specific discrete pieces of information (e.g. Social Security numbers) related to an individual.
- The GDPR contains stricter breach notification requirements than most US laws.
- The GDPR contains more rigorous data transfer and processing restrictions than US laws.

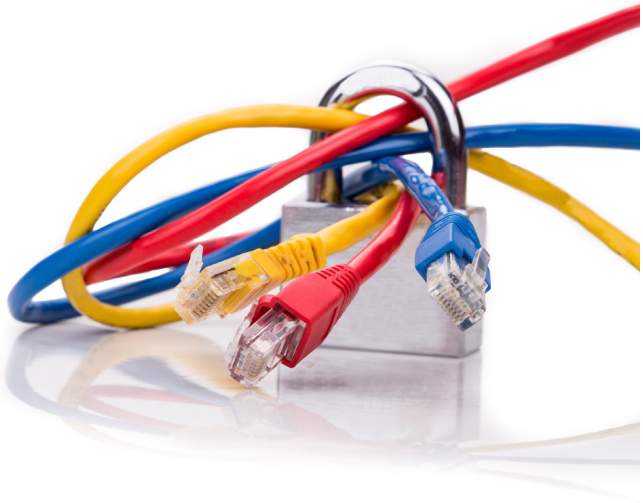
## Privacy Shield

Data can only be transferred from the EU to a country with equal or better data protection laws (which does not currently include the US). The EU-US Privacy Shield Framework attempts to remedy this by providing a self-certification and registration mechanism to comply with EU data transfer requirements, but various EU data protection authorities have questioned whether Privacy Shield does in fact comply with GDPR. The Article 29 Working Party, an advisory body made up of representatives of each EU member state, has stated that the Privacy Shield is deficient and that if the deficiencies are not addressed by the time the GDPR is implemented, the group may pursue legal challenges to its adequacy.

To avoid risk as a result of the uncertainty surrounding the Privacy Shield, companies should either develop internal Binding Corporate Rules (BCRs) or employ approved contractual data protection clauses to ensure that data transferred between corporate affiliates will enjoy adequate protection. BCRs are policies and guidelines that are meant to assure data protection authorities that data transferred outside the EU will have the same protections as under GDPR.

# SPECIFIC RISKS FOR FUNDS AND BROKER-DEALERS

- Funds and broker-dealers may function as data "controllers" through collection of:
  - Investor and potential investor information:
    - AML/KYC
    - Investor suitability
    - FATCA
  - Human resources data for employees
  - Supplier data from vendors/ service providers and their employees
  - Data from members of the public in the EU (e.g. website visitors)
  - Data collected for direct marketing purposes.



# QUESTIONS TO ASK TO PREPARE FOR GDPR IMPLEMENTATION

- Do we control or process any data for EU residents?
  - If so, what types of data and in what form?
- Do we have a security breach response plan? Is it compliant with GDPR? (e.g. are we prepared to identify, escalate and notify breaches to the relevant data protection authority within 72 hours)
- Do we keep adequate records of the data processing we do?
- Do we have adequate records to demonstrate that we understand the risks of our data processing and have taken adequate steps to address those risks?
- Is designation of a data protection officer required based on our specific data profile? Is designation of an EU member state representative required?
- Do we have a process to allow individuals to object to processing of their data?
- Do we have a process to allow individuals to request to have their data transferred to them or passed to a new controller?
- How do we obtain consent from data subjects? Is that consent adequate?
- What data processing do we do based on consent?
- Can we use legitimate interest instead? If so, do our legitimate interests outweigh any prejudice to privacy?

# HOW CLIFFORD CHANCE CAN HELP

- Analyze whether you fall within the GDPR's scope.
- Determine whether the data you hold qualifies as personal data pursuant to GDPR.
- Review your current data privacy and cybersecurity policies and determine what gaps need to be addressed to ensure compliance with GDPR.
- Update or create data breach response plans and other protocols necessary to satisfy GDPR's requirements.
- Run simulations to ensure you are prepared to identify, escalate and remediate data breaches or other cybersecurity incidents.
- Draft internal policies and standard data protection clauses to allow data to be transferred out of the EU.
- Review agreements with vendors and service providers to ensure any data processing is GDPR compliant.
- Assist in minimizing or avoiding GDPR compliance costs by eliminating or outsourcing unnecessary data processing.
- Conduct due diligence in connection with M&A transactions or JVs to ensure GDPR and other data security requirements are met.
- Leverage our global expertise to provide expert local advice from specialists throughout the EU and other regions.

# US TEAM

**Daniel Silver**
**Partner (NY)**
**Co-Chair, US Cybersecurity and Data Privacy Group**

Daniel Silver focuses on regulatory enforcement and white collar criminal defense matters. Dan co-chairs the US cybersecurity and data privacy group, and has extensive experience counseling clients on data-related regulatory challenges and responding to cybercrime incidents and data breaches.

Prior to joining Clifford Chance, Dan spent ten years as a federal prosecutor, serving as Chief of the National Security and Cybercrime Section within the United States Attorney's Office for the Eastern District of New York. In the US Attorney's Office, Dan supervised a team of more than one hundred federal prosecutors, led complex cross-border cybercrime investigations and prosecutions, conducted more than a dozen jury trials, and argued numerous appeals.

**Megan Gordon**
**Partner (DC),**
**Co-Chair, US Cybersecurity and Data Privacy Group**

Megan Gordon co-chairs the US cybersecurity and data privacy group. Her practice focuses on risk management, transactional due diligence, compliance and internal investigation matters.

Megan's work encompasses a broad range of regulatory matters pertaining to privacy and data protection laws. She also advises clients on how to manage risk exposure in a wide variety of areas affecting companies conducting international business. She advises multinational companies in connection with transactional risks and in designing and implementing compliance programs.

# GLOBAL CONTACTS

## Australia

**Tim Grave**
**Partner**
**Sydney**
T: +61 28922 8028
E: tim.grave@cliffordchance.com

## Belgium

**Sophie Delwaide**
**Lawyer**
**Brussels**
T: +32 2 533 5074
E: sophie.delwaide@cliffordchance.com

## China

**Tiecheng Yang**
**Partner**
**Beijing**
T: +86 106535 2265
E: tiecheng.yang@cliffordchance.com

## Czech Republic

**Veronika Kinclová**
**Lawyer**
**Prague**
T: +420 22255 5242
E: veronika.kinclova@cliffordchance.com

## France

**Dessislava Savova**
**Partner**
**Paris**
T: +33 14405 5483
E: dessislava.savova@cliffordchance.com

## Germany

**Markus Muhs**
**Partner**
**Munich**
T: +49 8921632 8530
E: markus.muhs@cliffordchance.com

**Anne Britta Haas**
**Counsel**
**Munich**
T: +49 8921632 8472
E: anne.haas@cliffordchance.com

**Ines Keitel**
**Counsel**
**Frankfurt**
T: +49 697199 1250
E: ines.keitel@cliffordchance.com

## Hong Kong

**Anita Lam**
**Consultant, HK**
**Head of Employment**
**Hong Kong**
T: +852 2825 8952
E: anita.lam@cliffordchance.com

## Italy

**Claudio Cerabolini**
**Partner**
**Milan**
T: +39 028063 4248
E: claudio.cerabolini@cliffordchance.com

## Japan

**Natsuko Sugihara**
**Partner**
**Tokyo**
T: +81 3 6632 6681
E: natsuko.sugihara@cliffordchance.com

## Luxembourg

**Isabelle Comhaire**
**Counsel**
**Luxembourg**
T: +352 485050 402
E: isabelle.comhaire@cliffordchance.com

**Udo Prinz**
**Counsel**
**Luxembourg**
T: +352 485050 232
E: udo.prinz@cliffordchance.com

## The Netherlands

**Alvin Khodabaks**
**Partner**
**Amsterdam**
T: +31 20711 9374
E: alvin.khodabaks@cliffordchance.com

## Poland

**Marcin Bartnicki**
**Partner**
**Warsaw**
T: +48 22429 9510
E: marcin.bartnicki@cliffordchance.com

## Poland

**Krzysztof Hajdamowicz**
**Counsel**
**Warsaw**
T: +48 22429 9620
E: krzysztof.hajdamowicz@cliffordchance.com

**Lena Ng**
**Partner**
**Singapore**
T: +65 6410 2215
E: lena.ng@cliffordchance.com

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

## Romania

**Diana Crangasu**
**Senior Associate**
**Bucharest**
T: +40 216666 121
E: diana.crangasu@cliffordchance.com

## UK

**Jonathan Kewley**
**Partner**
**London**
T: +44 20 7006 3629
E: jonathan.kewley@cliffordchance.com

**Alice Kane**
**Counsel**
**New York**
T: +1 212 878 8110
E: alice.kane@cliffordchance.com

**Radu Ropota**
**Senior Associate**
**Bucharest**
T: +40 216666 135
E: radu.ropota@cliffordchance.com

**Richard Jones**
**Director of Data Privacy**
**London**
T: +44 20 7006 8238
E: richard.jones@cliffordchance.com

## Russia

**Alexander Anichkin**
**Partner**
**Moscow**
T: +7 495258 5089
E: alexander.anichkin@cliffordchance.com

**André Duminy**
**Partner**
**London**
T: +44 20 7006 8121
E: andre.duminy@cliffordchance.com

## Singapore

**Luke Grubb**
**Partner**
**Singapore**
T: +65 6506 2780
E: luke.grubb@cliffordchance.com

## US

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




**WWW.CLIFFORDCHANCE.COM**