
GIBSON DUNN
GDPR's First Five Months:
Emerging Trends and
Implementation Challenges
Panelists: Ahmed Baladi
Penny Madden
Alexander H. Southwell
Michael Walther
Moderator: F. Joseph Warin
October 15, 2018

MCLE Certificate Information

- Most participants should anticipate receiving their certificate of attendance in four weeks following the webcast.
- Virginia Bar Association members should anticipate receiving their certificate of attendance in six weeks following the webcast.
- All questions regarding MCLE Information should be directed to Jeanine McKeown (National Training Administrator) at 213-229-7140 or jmckeown@gibsondunn.com.

Today's Topics

- GDPR: A Brief Reminder
- Recent Regulatory Guidance
- Enforcement and Litigation to Date
- Common Implementation Challenges
- The U.S. Government's Position
- The "Next GDPR": Emerging Privacy Compliance Issues

GDPR: A Brief Reminder

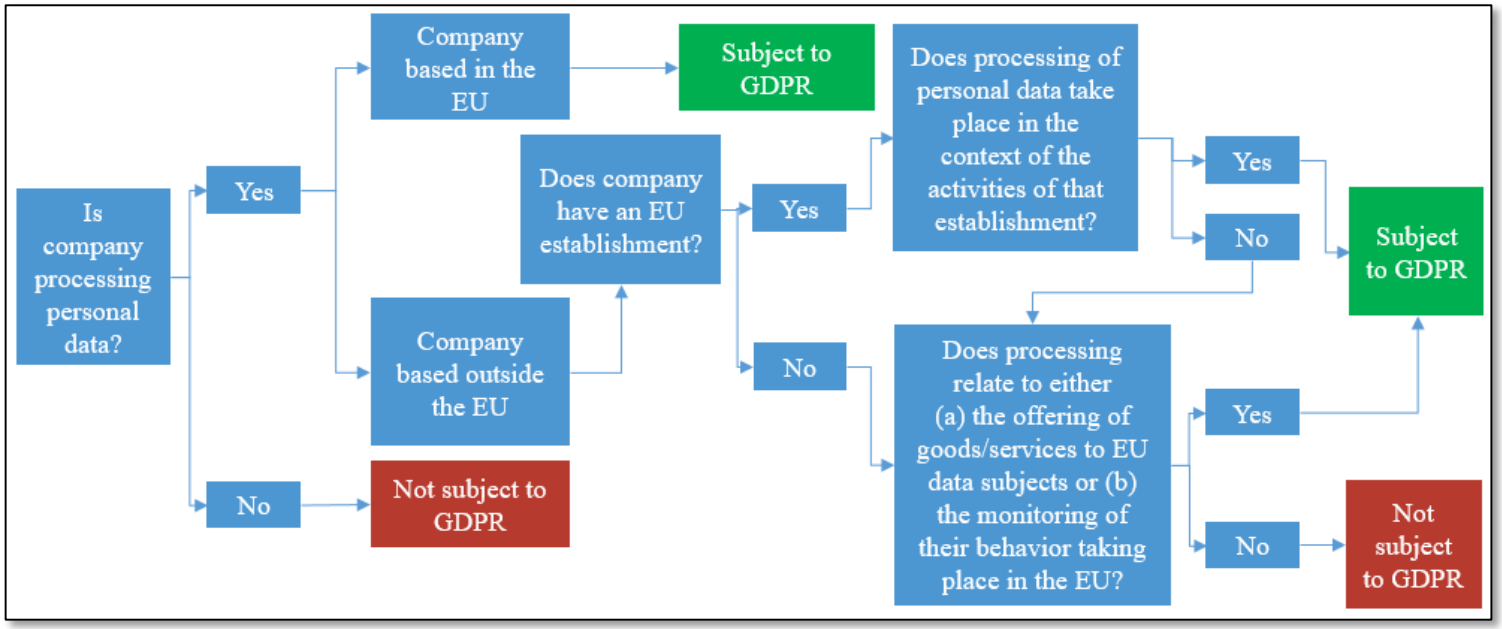
GDPR Overview

- The General Data Protection Regulation ("GDPR") is the EU's new omnibus data protection law.
- Adopted in April 2016 and applicable since May 25, 2018.
- Replaces 1995 Data Protection Directive.
- Regulation (not Directive) that applies without national legislation in all EU Member States.
- Builds from principles in 1995 Directive and creates new requirements for processing personal data.
- Permits EU Member States to enact additional requirements in defined areas.
- Enforceable by administrative fines of up to €20 million or 4% of total worldwide annual turnover.

Territorial Scope

In general, GDPR applies to:

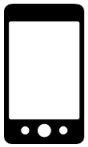
- Companies established in the EU; and
- Companies established outside the EU processing personal data of individuals in the EU, where the processing relates to offering goods or services to the individuals or monitoring their behavior in the EU.



Substantive Scope

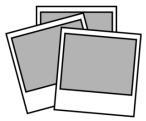
GDPR applies to "processing" of "personal data."

- "Processing" includes, among other things, "collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure . . . , alignment or combination, restriction, erasure or destruction."



- "Personal data" generally includes "any information relating to an identified or identifiable natural person."
  - A natural person can be identified "by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that . . . Person."

  - Broader definition than generally used in the U.S. for Personally Identifiable Information ("PII") or Protected Health Information ("PHI").



- GDPR requires extra protection for "sensitive" personal data.
  - E.g., racial/ethnic origin, political opinions, religious/philosophical beliefs, trade-union membership, health or sex life, sexual orientation, genetic/biometric data.

Roles and Responsibilities

Entities processing personal data may be **"Data Controllers"** or **"Data Processors."**

	Data Controller	Data Processor
Definition	Entity that determines the purposes and means of processing personal data.	Entity that processes personal data on behalf of controller.
Responsibilities	Primary responsibility to ensure compliance with all data protection requirements.	Comply with controller's instructions; ensure security; report breaches to controller.
Liability	Liable to data subjects.	Limited liability to data subjects.

Where two or more entities jointly determine the purposes and means of processing, they are **"Joint Controllers."**

Key GDPR Principles

- **Fairness and transparency:** Personal data should be processed lawfully, fairly, and in a transparent manner.
- **Purpose limitation:** Personal data should be collected only for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
- **Legal basis:** Personal data should be processed with a valid legal basis (consent, contract, legal obligation, vital interest, public task, or legitimate interest).
- **Individual rights:** Data subjects have the right to be informed regarding the processing of their data; rights of access, rectification, erasure, restriction, and data portability; and rights related to automated decisionmaking and profiling.
- **Data retention:** Personal data should not be retained for any longer than necessary in relation to the purposes for which it was collected.

Key GDPR Principles (cont'd)

- **Accountability and governance:** Organizations processing personal data should implement appropriate technical and organizational measures to demonstrate compliance, maintain documentation of processing activities, implement privacy by design and privacy by default principles, and appoint a DPO and conduct data protection impact assessments where appropriate.
- **Security:** Appropriate technical and organizational security measures should be taken to protect personal data against unauthorized processing and accidental disclosure, access, loss, destruction, or alteration.
- **Data transfers:** Personal data should not be transferred outside the EU without adequate safeguards.
- **Data breaches:** Breaches involving personal data may trigger requirements to notify supervisory authorities and affected data subjects.

Recent Regulatory Guidance

WP29/EDPB Guidance

- Article 29 Working Party ("WP29") and its replacement, the European Data Protection Board ("EDPB") have published guidance on several GDPR requirements.

Topic	Reference	Adoption (Last Revision)
Derogations of Article 49	2/2018	25 May 2018
Certification in accordance with Articles 42 and 43	1/2018	25 May 2018
Transparency	WP260 rev.01	12 Dec. 2017 (11 April 2018)
Consent	WP259 rev.01	28 Nov. 2017 (10 April 2018)
Automated individual decision-making and profiling	WP251 rev.01	3 Oct. 2017 (6 Feb. 2018)
Data breach notification	WP250 rev.01	3 Oct. 2017 (6 Feb. 2018)
Data Protection Impact Assessments ("DPIAs")	WP248 rev.01	4 April 2017 (4 Oct. 2017)
Application and setting of administrative fines	WP253	3 Oct. 2017
Right to data portability	WP242 rev.01	13 Dec. 2016 (5 April 2017)
Data Protection Officers ("DPOs")	WP243 rev.01	13 Dec. 2016 (5 April 2017)
Identifying a controller or processor's lead supervisory authority	WP244 rev.01	13 Dec. 2016 (5 April 2017)

Obtaining Consent for Processing

- The WP29 published the *Guidelines on Consent under Regulation 2016/679* on April 10, 2018.
- These rules apply to "consent" obtained for different purposes under the GDPR: (i) consent as a legal basis to process personal data (Article 6(1)(a)), (ii) explicit consent as an exception to the prohibition to process sensitive personal data (Article 9(2)(a)), (iii) explicit consent as a derogation to the prohibition on exporting personal data outside the EU (Article 49(1)(a)), and (iv) explicit consent for automated individual decisionmaking, including profiling (Article 22(2)(c)).
- Valid "consent" under the GDPR requires fulfilment of a series of conditions:
  - Free: "Free" consent implies real choice and control for data subjects. "Consent" is not a suitable legal basis where the controller needs to process the personal data for other reasons (e.g., compliance with the law), or where the data subject is constrained to provide his/her consent.
  - Specific: The consent of the data subject must be given in relation to "one or more specific" purposes, and data subjects must have a choice in relation to each of them.
  - Informed: Consent must only be provided after having obtained the information legally required under the GDPR (Articles 13 and 14).
  - Unambiguous: Consent requires a statement from the data subject or a clear affirmative act.
- Obtaining explicit consent: This means that the data subject must give an express statement of consent (in writing, or electronically).
- Demonstrating consent: The controller must be able to prove that a data subject in a given case has consented. As long as a data processing activity in question lasts, the obligation to demonstrate consent exists.
- Obtaining consent for under-16 children: Since the GDPR requires that consent of under-16 children be obtained from parents or guardians, a proportional approach should be used in the consent process, obtaining a limited amount of information, such as contact details of a parent or guardian.

Cookies and Website Analytics

- Cookies are still regulated by the ePrivacy Directive 2002/58, which requires implementation at the national level. The ePrivacy Regulation has not yet been enacted.
- The GDPR also contains provisions that have a bearing on the processing of data related to cookies and website analytics (e.g., Article 22 regarding automated decision-making and profiling).
- Numerous guidelines of the EU authorities apply to cookies and website analytics – they require consent where cookies are used beyond what is "strictly necessary" to provide a service requested by the user:
  - *Opinion 4/2012 on Cookie Consent Exemption*
  - *Opinion 2/2010 on Online Behavioural Advertising*, and *Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising*
- Article 22 of the GDPR further indicates that automated decisionmaking and profiling require: (i) necessity to perform a contract, (ii) authorization by EU or national law, or (iii) explicit consent.
- EU authorities' stated view is that analytics cookies may not require consent only when they are:
  - First-party cookies (i.e., not set by third-party analytics providers);
  - Strictly limited to first-party aggregated statistical purposes;
  - Used by websites that already provide clear information about these cookies in their privacy policy; and
  - Combined with safeguards, including a user-friendly mechanism to opt-out from any data collection and comprehensive anonymization mechanisms that are applied to other collected identifiable information (e.g., IP addresses).

Conducting Data Protection Impact Assessments

- The WP29 published *Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679* on October 4, 2017.
- A DPIA is required when processing is "likely to result in a high risk to the rights and freedoms of natural persons" (Article 35(1) GDPR). A decision on whether or not to conduct a DPIA must be made when two of nine criteria are met: (i) evaluation or scoring; (ii) automated decisionmaking with a legal or similar effect; (iii) systematic monitoring; (iv) sensitive data or data of a highly personal nature; (v) data processed on a large scale; (vi) matching or combining data sets; (vii) data concerning vulnerable data subjects; (viii) innovative use or applying new technological or organizational solutions; (ix) data processing preventing a data subject from exercising a right or using a service.
- A DPIA is not required: (i) when a DPIA has already been performed for a similar processing operation; (ii) when a supervisory authority has already "checked" an operation; (iii) where the legal basis for data processing includes a DPIA; or (iv) when a DPIA has been declared optional by a supervisory authority.
- A DPIA requires: (i) analyzing the description of the processing; (ii) assessing necessity and proportionality; (iii) reviewing the risks to rights and freedoms and the safeguards in place; and (iv) hearing from the DPO and the data subjects concerned.
- Further guidance at national level:
  - DPIA software offered by CNIL and DPIA template offered by ICO; and
  - Guidance offered by Spanish AEPD and Polish GIODO.

Data Security

- There are two main guidelines adopted by EU regulators that address security of personal data:
  - The *Handbook on Security of Personal Data Processing* of the EU Agency for Network and Information Security, dated January 29, 2018; and
  - The 2018 *Security of Personal Data* guidance of the CNIL.
- Both documents address specific security measures that are advised for data processing operations regularly carried out by businesses, such as:
  - User authentication, access control, and tracking;
  - Workplace security, including security of mobile and IT networks, servers, and websites;
  - Safeguarding the continuity of business operations, including archiving, maintenance, and data retention;
  - Handling data processors, including the security of personal data and maintaining documentation to ensure confidentiality and compliance with legal obligations; and
  - Ensuring data security (encryption) and integrity.

Anticipated Future Guidance

Anticipated future guidance from the EDPB includes:

- Opinion on the list of data processing operations that always require a DPIA under the GDPR (Articles 64(1)(a) and 35(4))
  - Expected to further narrow down the situations identified in the WP29's *Guidelines on DPIA*.
- Guidelines on the application of the territorial scope of the GDPR (Article 3)
  - Important to determine the level of risk of non-EU businesses that incidentally process personal data of data subjects in the EU, or systematically monitor EU data subjects' personal data.
- Position paper on GDPR Article 6.1(b) in the context of 'free' online services
  - Many online service providers rely on the use of personal data in order to offer free services.
  - The Position paper is expected to clarify the views of the EU supervisory authorities regarding reliance on "performance of a contract" as a legal basis to process user data (Article 6(1)(b)), and the relationship with other provisions (e.g., regarding automated decisionmaking and profiling under Article 22(2)(a)).

Enforcement and Litigation to Date

Enforcement – United Kingdom

In July 2018, the Information Commissioner's Office ("ICO") filed its first GDPR Enforcement Notice (no fine) against Canadian data analytics firm AggregateIQ ("AIQ").

- ICO alleged AIQ violated GDPR Articles 5 and 6 by processing personal data in a manner that "the data subjects were not aware of, for purposes that they would not have expected, and without a lawful basis for that processing."
- Terms: AIQ must "cease processing any personal data of UK or EU citizens obtained from UK political organizations or otherwise for the purposes of data analytics, political campaigning or any other advertising purposes."
- AIQ has filed appeal.

Elizabeth Denham, Information Commissioner

ICO Enforcement Powers and Current Focus

- The 2018 U.K. Data Protection Act gives ICO authority to enforce the GDPR in the U.K. and expands ICO's evidence-gathering powers.
  - Broadens ICO's powers to issue assessment notices, requires companies to respond to requests for information in 24 hours, and gives ICO broader "dawn raid" powers to enter and inspect premises with little or no notice at a "reasonable hour."
- Complaints to up 160% under GDPR – 6,291 complaints in first 40 days.
- "Enforcement is a last resort. . . . Hefty fines will be reserved for those organizations that persistently, deliberately or negligently flout the law. Those organizations that self-report, engage with us to resolve issues and can demonstrate effective accountability arrangements can expect this to be a factor when we consider any regulatory action."
- "When we do need to apply a sanction, fines will not always be the most appropriate or effective choice. Compulsory data protection audits, warnings, reprimands, and enforcement notices are all important enforcement tools. The ICO can even stop an organization processing data."

Implementation Challenges in the U.K.

- Post-Brexit, GDPR likely will apply in the U.K. as it currently applies outside the EEA.
- 2018 Data Protection Act will provide GDPR-like protections in U.K. post-Brexit, regardless.
- Extensive revisions to the Data Protection Act are possible, but not anticipated, post-Brexit.
- Interpretations of GDPR and Data Protection Act may diverge over time.
  - U.K. not subject to CJEU or EDPB decisions post-Brexit.
  - ICO not part of EDPB post-Brexit; will lose influence on EBDP decisions.
- For companies with operations in U.K. and elsewhere in EU, ICO will no longer serve as supervisory DPA in EU (e.g., coordinating breach investigations).
- DPOs in the U.K. may continue to serve as DPOs for purposes of the GDPR, but must expend additional effort to liaise with supervisory DPAs in EU.

Enforcement – France

In June 2018, the Commission Nationale de l'Informatique et des Libertés ("CNIL") issued warning (no fine) to two companies regarding use of location data for targeted advertising, alleging:

- Information needed for users to evaluate whether to provide consent was given only *after* installation of app.
- Modifications in privacy policy were applied without adequate notice.
- Consent to use location data was improperly bundled with other terms.
- Retention of location data for 13 months was excessive.

Isabelle Falque-Pierrotin, CNIL President

CNIL: Companies "can expect to be treated leniently initially provided that they have acted in good faith."

Implementation Challenges in France

1. **Harmonizing laws**
   - Act No. 78-17 of January 6, 1978 on information technology, data files and liberties ("FDPA") was modified by Law No. 2018-493 of June 20, 2018 implementing the GDPR.
   - The CNIL has identified difficulties of readability in the new modified Act. Thus, the FDPA is expected to be completely rewritten by December 2018.

   ➔ **Challenge: Evaluating how arguably inconsistent provisions in the FDPA and the GDPR will be applied.**

2. **Shortage of available resources**
   - ~25,000 organizations have appointed a DPO.
   - More than 600 data breach notifications (i.e., about 7 per day) have been received by the CNIL since May 2018.

   ➔ **Challenge: For companies, locating and retaining a skilled DPO; for the CNIL, locating additional FTEs to manage its increased workload.**

3. **Increasing number of complaints triggering investigations and litigation**

   3,767 complaints in first three months, up from 2,294 complaints over same period in 2017 – which was already a record year. Includes two class actions and more than 200 cross-border complaints.

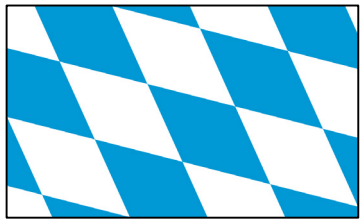
   ➔ **Challenge: Evaluating how to most *efficiently* mitigate increasing risk.**

Enforcement – Germany

- No enforcement actions to date by 16 state DPAs with general jurisdiction over private companies (or federal DPA with limited jurisdiction).
- Legislation includes a "one-stop shop" mechanism so organizations with multiple German locations may report to DPA with jurisdiction over company's "main establishment."
- Sample of activity by state DPAs:
  - In June 2018, Lower Saxony DPA announced it would survey GDPR compliance by sending a compliance questionnaire to 20 large and 30 mid-sized companies.
  - Brandenburg DPA issued warning that failure to provide complete, timely breach reports will generate fines.
  - Bavaria DPA published phased audit plan for September through November 2018 targeting compliance across various industries.
- Per federal DPA, reporting to state DPAs has "exploded."
  - Berlin: 1,380 complaints through July, four times more than same period last year.
  - North Rhine Westphalia: 100 calls / day on average during the first month of GDPR.
  - Hamburg: Complaints doubled during first month of GDPR.

Lower Saxony

Brandenburg



Bavaria

Implementation Challenges in Germany

German law goes beyond the requirements of the GDPR in several respects:

- Stricter requirements for appointment of DPO, e.g. if 10 employees usually engage in the automated processing of personal data.
- Written employee consent for processing – is it required, or permitted, and/or safe?
- Right to access data is restricted where access would require unreasonable effort and data is maintained only for legal, security, or control purposes.
- Processing of special categories of personal data is permissible without consent if e.g. required for social security, health care, employment, or certain public interests – but only if additional strict requirements e.g. regarding conditions of such processing are met.
- 16 different state DPAs in Germany issue privacy-related guidance, making monitoring of new statements and decisions more challenging.

German Regional Court Ruling on "Legitimate Business Purposes"

- On May 29, 2018, German Regional Court (*Landgericht*) Bonn took a narrow view of data processing necessary for "**legitimate business purposes**."
- The Internet Corporation for Assigned Names and Numbers ("ICANN") sought to obligate the German-based, ICANN-accredited Registrar EPAG Domainservices GmbH ("EPAG") to comply with the ICANN "Registrar Accreditation Agreement," which requires registrars to collect administrative and technical contact information for a new domain name registration ("WHOIS data").
- The court ruled that ICANN could not show credibly that the collection of such WHOIS data is "**necessary**" under Art. 5(1) of GDPR.
- ICANN did not succeed in appealing the decision.

Wirtschaftsakademie Decision

- CJEU ruled that fan page administrator is **jointly responsible** with social media platform for the processing of personal data of fan page visitors.
- Court found administrator's creation of fan page made it possible for social media platform to collect personal data of fan page visitors, and that administrator exercised control over whose information was provided to social media platform.
- Decision based on 1995 Data Protection Directive – now replaced by GDPR – but GDPR did not change portion of Directive on which decision was based.

Potential exposure of companies with social media presence to liability for data processing performed by social media platforms.

Ongoing Enforcement Activity

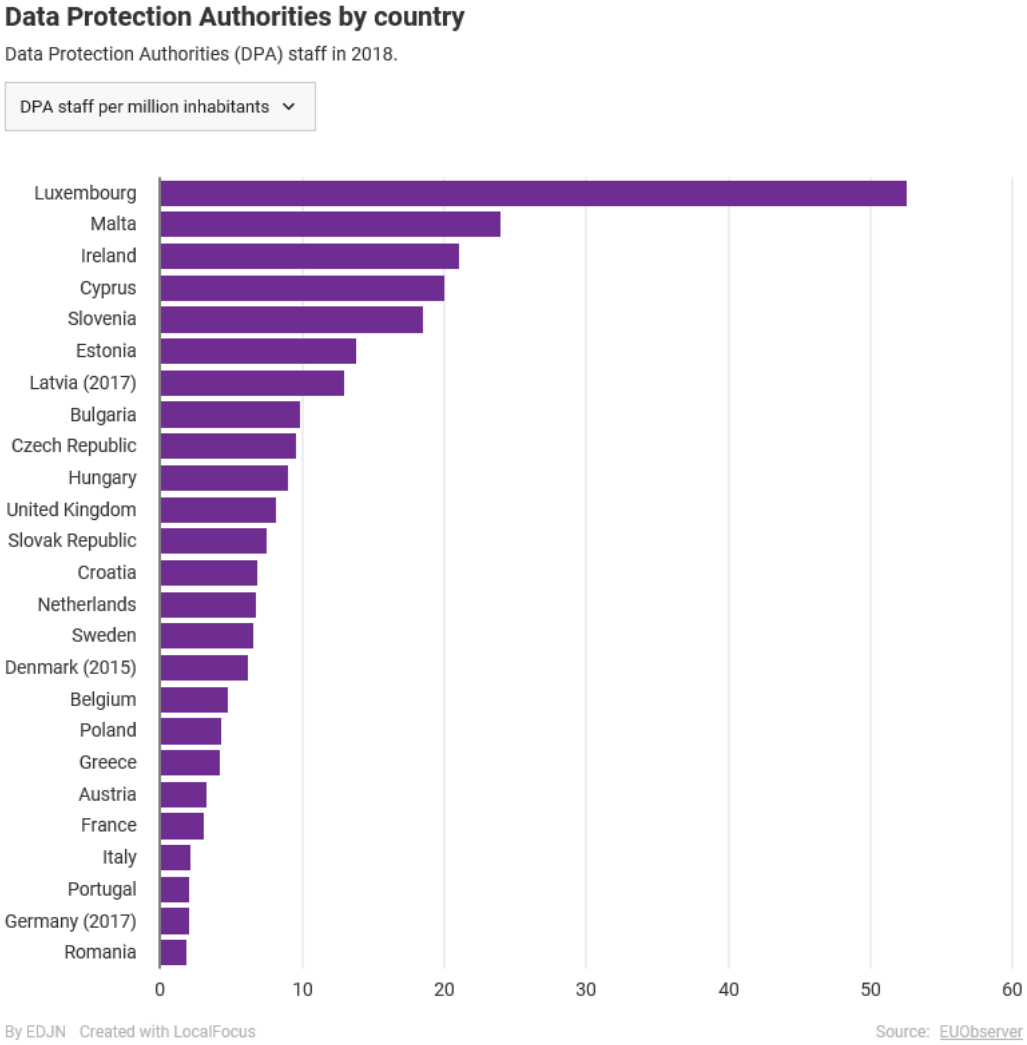
- On October 3, 2018, the Irish DPC announced an investigation of a Facebook security incident that purportedly affected 50 million users. The DPC reports the investigation will focus on whether Facebook had the proper "technical and organisational measures to ensure the security and safeguarding of the personal data it processes." EU Justice Commissioner Vera Jourova termed the investigation the "first big test case" for GDPR.
- In July 2018, the Dutch AP announced an audit of 30 randomly selected large companies (those with more than 250 employees) in 10 sectors: industry, water supply, construction, retail, hospitality, travel, communications, finance, business services, and health care. The investigation focuses on compliance with GDPR Article 30, which requires maintaining a data processing registry.

EU Justice Commissioner Vera Jourova

Increase in DPA Staffing

DPAs are seeking to increase headcount to address increased workload under GDPR.

- Commissioner Jourova reported in May 2018 that she is worried understaffed DPAs will have difficulty enforcing GDPR.
- Number of current staff at DPAs ranges from 11 in Malta to 565 in U.K.
- French CNIL has requested additional staff, beyond current 199 FTEs.
- German federal DPA has requested additional staff, beyond ~160 FTEs in 2017 (plus ~ 480 FTEs at state level).
- Dutch AP has increased from 76 to 113 FTEs.



New Complaints Alleging Violations of Consent Principle

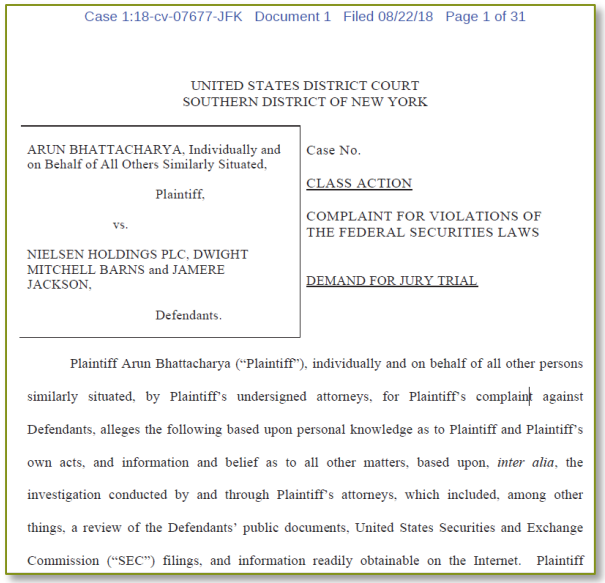
Within days of GDPR's implementation, complaints were filed with multiple DPAs against several tech companies, alleging that requiring users to consent to the collection and use of their personal data as an all-or-nothing prerequisite for use of the services violates the GDPR's "particularized consent" principle.

- In May 2018, Austrian privacy activist Max Schrems' group Noyb.eu filed complaints in Austria, Belgium, Germany, and France against a social media company and a search company.
- French non-profit La Quadrature du Net filed similar complaints against social media, search, marketplace, and device manufacturing companies with the CNIL.
- In September 2018, complaints were filed against a search company with the ICO and Irish DPC, alleging that advertising technology companies inappropriately distribute user data in allowing companies to bid on advertisements.

Following the complaint of one of its 220,000 tenants, the Vienna communal housing cooperative announced on October 12 that it would anonymize the bell nameplates of all tenants within the next months.

U.S. Shareholder Litigation Regarding GDPR

- In August 2018, a shareholder suit was filed against Nielsen Holdings alleging that executives misled investors about the financial impact that compliance with the GDPR would have on Nielsen's income.



Case 1:18-cv-07677-JFK Document 1 Filed 08/22/18 Page 1 of 31

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

ARUN BHATTACHARYA, Individually and on Behalf of All Others Similarly Situated,

Plaintiff,

vs.

NIELSEN HOLDINGS PLC, DWIGHT MITCHELL BARNS and JAMERE JACKSON,

Defendants.

Case No.

CLASS ACTION

COMPLAINT FOR VIOLATIONS OF THE FEDERAL SECURITIES LAWS

DEMAND FOR JURY TRIAL

Plaintiff Arun Bhattacharya ("Plaintiff"), individually and on behalf of all other persons similarly situated, by Plaintiff's undersigned attorneys, for Plaintiff's complaint against Defendants, alleges the following based upon personal knowledge as to Plaintiff and Plaintiff's own acts, and information and belief as to all other matters, based upon, *inter alia*, the investigation conducted by and through Plaintiff's attorneys, which included, among other things, a review of the Defendants' public documents, United States Securities and Exchange Commission ("SEC") filings, and information readily obtainable on the Internet. Plaintiff

  - Suit filed in the United States District Court for the Southern District of New York.
  - Defendants' Motion to Dismiss is pending.
  - Allegations include claims that Nielsen "recklessly disregarded" the risks of GDPR and understated impact of GDPR given Nielsen's reliance on social media.

Common Implementation Challenges

Maintaining a Data Processing Register

GDPR Requirement

- Article 30 requires controllers to maintain a record of processing activities.

Implementation Considerations

- Regulators often request processing registers early in investigations; failure to maintain an up-to-date registry can prolong an investigation.
- Some regulators (e.g., CNIL) have released register templates.
- For many large organizations, specialized software is invaluable in maintaining the required register.
- A document management system can help with ensuring the accessibility of key documents referenced in the register (e.g., contracts with data processors, data protection impact assessments, model clauses).
- Organizations undertaking the data mapping necessary to develop a register may find an iterative process helpful, as gathering detailed information on the first try is difficult.
- The GDPR exempts from this requirement controllers with fewer than 250 employees, unless processing is high risk, occurs more than occasionally, or includes certain types of data.

Implementing a Data Retention Schedule

GDPR Requirement

- Under Article 5, personal data generally must be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed."

Implementation Considerations

- Implementing a data retention schedule is a difficult aspect of GDPR compliance.
- Consider the impact of Member State-specific requirements that may require long data retention periods (e.g., German requirements for retention of pension-related data, Polish requirements for retention of health care information).
- Consider the effect of non-EU requirements (e.g., U.S. data retention requirements), and the extent to which those requirements can be harmonized with the GDPR.
- Software solutions that scan unstructured data may be helpful in ensuring deletion of data across systems on required timeline, but data transfer implications of the use of these systems should be considered.
- Ongoing attention is necessary to ensure alignment of representations regarding data retention in privacy policies / notices with actual practices.

Responding to Data Subject Requests

GDPR Requirement

- Article 12 requires controllers to disclose information to data subjects regarding their rights, and to facilitate the exercise of those rights.

Implementation Considerations

- Failures in this area are a trigger for potential government investigations: Analysis of GDPR-related complaints by Dutch AP shows nearly 33% related to erasure requests, 5% related to access requests.
- Cross-functional cooperation (e.g., Privacy, IT) is integral to meeting the GDPR's deadline of responding to requests within 30 days.
- GDPR recognizes grounds for not granting certain requests.
  - E.g., request for erasure need not be granted where information is necessary "for the establishment, exercise, or defence of legal claims."
- Clear visibility into the sources and uses of data is integral to being able to respond to access requests.
- Obligation by controller to convey request to third parties?

Designation of a DPO

GDPR Requirement

- Article 37 requires designation of a DPO where, among other things, a controller or processor monitors data subjects or processes sensitive data on a large scale.

Implementation Considerations

- GDPR does not bar an individual from serving as both EU-wide and country-specific DPO.
- GDPR does not bar a DPO from serving as an in-house privacy attorney, including an attorney with responsibilities beyond the EU.
- A company's lead DPA is determined by the location of the company's main establishment in the EU. A company's main establishment is determined by a number of factors, including corporate structure and the number of employees in a country. The location of the company's DPO does not dictate its lead DPA.
- It is often helpful, but not required, for a company to locate its DPO in the country of its lead DPA given the role of the lead DPA in coordinating privacy investigations.
- In some instances Member State law requires appointment of DPO when the GDPR does not.
- DPO departures must be handled carefully, to avoid the appearance of retaliation for privacy-related determinations.

Controller-Processor Contracts

GDPR Requirement

- Article 28 requires controller-processor contracts with specifics regarding the processing performed, security measures, sub-processor engagement, and other issues.

Implementation Considerations

- Identification of whether a company is playing the role of a processor or joint controller is sometimes difficult, warranting careful review of proposed processing contracts for accuracy.
- Limitations on liability proposed by processors may leave controllers with considerable exposure and should be carefully considered.
- In addition to a data processing agreement, a safeguard for transferring data outside the EEA (e.g., model clauses) may be required, depending on the proposed location of processing.
- In assessing proposed locations for processing, controllers should consider not only where data will be stored, but also the locations from which it may be accessed by the processor.
- Pre-GDPR processing contracts in many instances may be amended, not replaced, to meet GDPR requirements.

Mergers & Acquisitions

- GDPR places limits on an acquiring company's use of personal data held by a target company.
- Key GDPR-related questions after an acquisition are (i) who is the controller of the personal data, and (ii) what is being done with the personal data.
    - If either the controller changes, or the uses of personal data change, it may be necessary to obtain additional consent from data subjects.
    - For example, if the acquiring company plays a role in determining the uses of personal data after the transaction, it may have become a controller – and consent of the data subjects may be required. And if personal data is used by the target company in new ways (e.g., for new types of marketing) post-transaction, consent also may be required.
- Data subjects of a newly acquired company already may have consented to the transfer of their data to a new corporate parent in the event of a transaction. In such instances, additional consent may not be required (depending on the scope of the consent already provided, and assuming the consent was properly obtained).
- Where the transfer of data from a target company to an acquiring company involves a transfer of data out of the EEA, an appropriate safeguard for the transfer may need to be implemented (e.g., model contractual clauses).
- Works Council agreements in the EU frequently limit the uses that may be made of employees' personal data, as an addition to the requirements of the GDPR, and should be considered in the context of any transaction.
- If non-privacy related regulatory approvals are required for an acquisition, the regulator responsible for providing the approval may make a referral to a DPA for a privacy review.

Producing Documents with Personal Data in U.S. Government Investigations

Reviewing and producing documents from the EU in connection with a U.S. government investigation raises a variety of GDPR compliance questions, including:

- What impact does the form of process used by a U.S. regulator have on whether documents may be produced?
- From what location(s) will documents be collected? Will documents be collected from electronic devices issued to employees? From personal electronic devices used for business purposes?
- How will personal records be segregated from business records?
- Where will the documents be processed and reviewed?
- Will personal data in the documents be redacted?
- Do employment and Works Council agreements permit the review and production? Was the possibility of review/production disclosed in an employee privacy notice?
- What collateral uses may be made of the documents discovered by the company?

The U.S. Government's Position

EU-U.S. Privacy Shield Under Fire

- In July 2018, European Parliament adopted resolution calling for suspension of EU-U.S. Privacy Shield, unless U.S. fully complied with all Privacy Shield requirements by September 1, 2018. Resolution was in response to several U.S. actions:
  - January 2017 Enhancing Public Safety Executive Order (Executive Order 13768);
  - Reauthorization of FISA § 702 without safeguards from Presidential Policy Directive 28;
  - Clarifying Lawful Overseas Use of Data ("Cloud") Act; and
  - Privacy Shield certification of entities EU officials contend have not protected privacy.
- European Commission responded by noting its intent to continue working with U.S. to improve, not suspend, Privacy Shield.
- Questions on adequacy of Privacy Shield referred to European Court of Justice in pending litigation regarding adequacy of other data-transfer mechanisms.
- WP29 / EDPB continues seeking information from U.S. Privacy and Civil Liberties Oversight Board ("PCLOB") on bulk data collection by U.S. intelligence agencies, as well as operations and staffing of PCLOB.

U.S. Response to Privacy Shield Criticism

- On August 30, 2018, the Department of Commerce ("DOC") defended the EU-U.S. Privacy Shield in a letter to the European Parliament but did not announce any new initiatives in response to the Parliament's concerns. The letter noted that the DOC is proactively monitoring participating organizations' compliance and has published additional resources on how to comply with Privacy Shield obligations. It also defended FISA Section 702, the CLOUD Act, and Executive Order 13768 as Privacy Shield-compatible.
- In September 2018, the U.S. designated Manisha Singh to serve as permanent Privacy Shield Ombudsperson.
- Status of other Privacy Shield-related appointments varies: all FTC Commissioners have been confirmed, but several high-level DOC positions have no nominee or await Senate confirmation.
- On October 3, 2018, U.S. Ambassador to the EU Gordon Sondland stated:
  - "***There is no non-compliance. We are fully compliant***. . . . As we've told the Europeans, ***we really don't want to discuss this any further***. And their response was 'OK'… Let's discuss things that have true relevance instead of discussing something where there is no problem."
- On October 18 and 19, 2018, EU and U.S. regulators will hold the second annual review of the EU-U.S. Privacy Shield framework.

U.S. Ambassador to EU Gordon Sondland

Recent U.S. Privacy Legislation and Regulation

High-profile federal initiatives:

- 2017 bills: In 2017, the Senate introduced two privacy bills: the ***Consumer Privacy Protection Act*** aimed to improve companies' data security practices, and the ***Online Privacy Act***, which would have strengthened user notice and opt-in. Neither bill proceeded beyond subcommittee.
- 2018 bills: The ***Customer Online Notification for Stopping Edge-provider Network Transgressions (CONSENT) Act*** would require edge providers to notify customers about the collection, use, and sharing of "sensitive customer proprietary information." Other senators proposed the ***Social Media Privacy and Consumer Rights Act***, which would require business to disclose what data it collected/shared; give the right to opt-out; and notify users of data breaches within 72 hours.
- HIPAA: In Spring 2018, the Trump Administration announced that it may seek to revise several parts of HIPAA.

Noteworthy state initiatives:

- California Consumer Privacy Act: In June 2018, California passed a sweeping privacy law, which will require businesses collecting data about California consumers to ***disclose*** the data being collected/shared and purpose of collection, and ***delete*** data upon the consumer's request.
- New York Department of Financial Services cybersecurity regulation: In March 2017, New York's cybersecurity regulation for financial services companies went into effect. Covered entities must establish a ***cybersecurity program***, create a written ***cybersecurity policy***, and conduct regular ***testing and risk assessment***.
- State data breach notification laws: All 50 states have now enacted data breach laws, following passage of data breach statutes in 2018 by Alabama and South Dakota.

Recent Enforcement of U.S. Privacy Law

- U.S. State Attorneys General have cited privacy and cybersecurity as enforcement priorities, and multiple states have created specialized privacy/cybersecurity enforcement units.
- SEC is increasingly active in privacy and cybersecurity enforcement.
- FTC enforcement of privacy and cybersecurity issues continues.

Electronic Toy Maker Settles FTC Allegations that It Violated Children's Privacy Law and the FTC Act

SEC Charges Firm with Deficient Cybersecurity Procedures

California Attorney General and San Francisco District Attorney Announce Settlement Over Data Breach

*** Consumer Alert***

Attorney General Madigan Investigating Massive Data Breach & Urges Illinois Residents to Be Vigilant

Mobile Phone Maker Reaches Settlement with FTC over Deceptive Privacy and Data Security Claims

The "Next GDPR": Emerging Privacy Compliance Issues

EU Network and Information Security Directive

- EU-wide legislation on cybersecurity, but must be transposed to national law; adoption of required laws by Member States is ongoing.
- Requires companies to implement technical and organizational measures to manage threats to networks and information systems and to report cybersecurity incidents to authorities.
- Applicable to providers of essential services (e.g., transportation, energy, financial services, health care, water) and digital services (e.g., cloud providers, search engines, online marketplaces).
- Applies to multinationals and other companies doing business in the EU.
- In some member states, penalties may be aligned to GDPR (i.e., €20 million or 4% of worldwide annual turnover).
- Requirements for companies complemented by requirements for member states to implement CSIRT or similar teams to coordinate response to reported attacks.

120 million

Estimated new malware variants created by hackers yearly

$124 billion

Predicted 2019 spending on information security products/services

($114 billion in 2018)

$400 billion

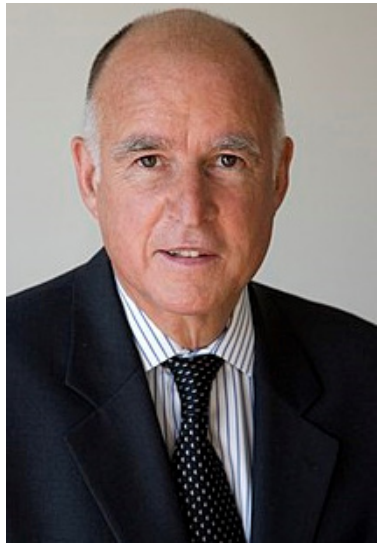
Estimated yearly breach-related losses

EU ePrivacy Regulation

- Regulation intended to replace existing ePrivacy Directive and align ePrivacy requirements more closely to GDPR.
- Regulates electronic communications, direct marketing, website audience measurement, the transmission of information across devices and browsers, and the setting of cookies.
- Provides more specific rules regarding these issues than the high-level GDPR.
- Unlike GDPR, covers both personal and non-personal data.
- EDPB has called for quick implementation: EC published initial draft in January 2017 and most recent amended draft in July 2018; final version is expected in 2019.

California Consumer Privacy Act of 2018

- Enacted June 2018 and amended September 2018, with further amendments anticipated.
- Anticipated to become enforceable in July 2020.
- Intended to provide increased transparency to consumers regarding companies' use and sharing of personal information, broadly defined.
- Applies to companies doing business in California with AGRs > $25 million, or that meet thresholds for selling personal information.
- Requirements similar, but not identical, to those for GDPR, including:
  - Consumers have right to access and delete data, and may opt out from the sale of their personal information; and
  - Companies must provide additional disclosures on websites and in privacy policies.
- Directs California Attorney General's Office to promulgate implementation regulations.



California Governor Jerry Brown

China Privacy and Cybersecurity Legislation

Cyber Security Law - *in force since June 1, 2017*

- Applies to establishment, operation and use of "networks" in China, which is defined as any system consisting of "*computers or other information terminals and related equipment*" that collects, stores, transmits exchanges or processes information.
- Restricts the transfer of un-anonymized personal information without the data subject's consent.
- Operators of "*Critical Information Infrastructure Equipment*" must store personal information and "*important*" data onshore. This data cannot be transferred out of China without carrying out a security assessment in a form prescribed by the Cyber Space Administration and State Council.

Draft Guidelines for Cross-Border Data Transfer - *released on August 25, 2017*

- Compliance with the principles of **legality, legitimacy** and **necessity**.
- Subject to narrow exceptions, the principle of legitimacy requires the **consent** of the data subject.
- Data users must undertake a **security assessment**. This assessment shall consider, among other things, the sender's ability to protect the data and the legal and political environment where the recipient is located.
- In some circumstances, the assessment must be provided to the relevant industry supervisory body or the National Cyberspace Administration.

China Privacy and Cybersecurity Legislation

Personal Information Security Specification – *in effect since May 1, 2018*

- Non-binding guidelines but highly regarded source of rules.
- Standards very **similar to the ones provided by the GDPR** (principle of accountability, data minimization, concept of data controller, conduct of impact assessment…).
- Expands the definition of **personal information** to include information that reflects the activities of individuals.
  Examples: location information or online browsing history information.
- Introduction of the concept of **sensitive personal information**, which includes information that, if disclosed or illegally processed, will likely threaten personal and property safety and can easily harm personal reputation, physical or mental health or lead to discriminatory treatment.
  Examples: a person's ID card number or a bank account number.
- **Consent** of data subjects is the key legal basis for collection and processing of personal information with few exceptions.

Today's Panelists

Ahmed Baladi is a French qualified partner in the Paris office of Gibson Dunn and Co-Chair of the firm's Privacy, Cybersecurity and Consumer Protection Practice Group. His practice focuses in Data Privacy and Cybersecurity, and in Technology & Digital Transactions. Mr. Baladi has developed renowned experience in compliance and governance programs in light of the GDPR. He regularly represents clients before the French data protection authority and other national DPAs and administrative courts, and advises on data breach and national security matters.

Penny Madden is an English qualified Queen's Counsel and partner in the London office of Gibson Dunn, where she is Co-Chair of the International Arbitration Practice Group and the UK lead for the firm's Privacy, Cybersecurity and Consumer Protection Practice Group. Her recent cases include representing global corporates in relation to disputes with ICO, the Irish DPC, the Belgian DPA (BPC), and the French CNIL. Ms. Madden also regularly advises clients on compliance with GDPR.

Alexander H. Southwell is a partner in the New York office of Gibson Dunn and Co-Chair of the firm's Privacy, Cybersecurity and Consumer Protection Practice Group. Previously Mr. Southwell served as an Assistant U.S. Attorney for the Southern District of New York. He focuses on information technology-related investigations, counseling, and litigation, is recognized as a Cybersecurity and Data Privacy "Trailblazer," and is considered among the top data breach response lawyers in the U.S.

Michael Walther is a partner in the Munich office of Gibson Dunn. He advises German and international clients on European and German antitrust and competition law and on information technology related topics including cyber-security and data privacy in the context of internal investigations and compliance with GDPR.

Joseph Warin is a partner in the Washington, D.C. office of Gibson Dunn, Chair of the office's Litigation Department, and Co-Chair of the firm's White Collar Defense and Investigations Practice Group. Mr. Warin is regarded as a top lawyer globally in FCPA investigations, FCA cases, and special committee representations. He regularly handles cases involving GDPR issues in federal regulatory inquiries, criminal investigations and cross-border inquiries by international enforcers, including UK's SFO and FCA, and government regulators in Germany and elsewhere.

Our Offices

Beijing
Unit 1301, Tower 1
China Central Place
No. 81 Jianguo Road
Chaoyang District
Beijing 100025, P.R.C.
+86 10 6502 8500

Brussels
Avenue Louise 480
1050 Brussels
Belgium
+32 (0)2 554 70 00

Century City
2029 Century Park East
Los Angeles, CA 90067-3026
+1 310.552.8500

Dallas
2100 McKinney Avenue
Suite 1100
Dallas, TX 75201-6912
+1 214.698.3100

Denver
1801 California Street
Suite 4200
Denver, CO 80202-2642
+1 303.298.5700

Dubai
Building 5, Level 4
Dubai International Finance Centre
P.O. Box 506654
Dubai, United Arab Emirates
+971 (0)4 318 4600

Frankfurt
TaunusTurm
Taunustor 1
60310 Frankfurt
Germany
+49 69 247 411 500

Hong Kong
32/F Gloucester Tower, The Landmark
15 Queen's Road Central
Hong Kong
+852 2214 3700

Houston
811 Main Street
Houston, Texas 77002
+1 346.718.6600

London
Telephone House
2-4 Temple Avenue
London EC4Y 0HB
England
+44 (0) 20 7071 4000

Los Angeles
333 South Grand Avenue
Los Angeles, CA 90071-3197
+1 213.229.7000

Munich
Hofgarten Palais
Marstallstrasse 11
80539 Munich
Germany
+49 89 189 33-0

New York
200 Park Avenue
New York, NY 10166-0193
+1 212.351.4000

Orange County
3161 Michelson Drive
Irvine, CA 92612-4412
+1 949.451.3800

Palo Alto
1881 Page Mill Road
Palo Alto, CA 94304-1125
+1 650.849.5300

Paris
166, rue du faubourg Saint Honoré
75008 Paris
France
+33 (0)1 56 43 13 00

San Francisco
555 Mission Street
San Francisco, CA 94105-0921
+1 415.393.8200

São Paulo
Rua Funchal, 418, 35°andar
Sao Paulo 04551-060
Brazil
+55 (11)3521.7160

Singapore
One Raffles Quay
Level #37-01, North Tower
Singapore 048583
+65.6507.3600

Washington, D.C.
1050 Connecticut Avenue, N.W.
Washington, D.C. 20036-5306
+1 202.955.8500