General Data Protection Regulation Guide

JONES DAY® | One Firm Worldwide℠

TABLE OF CONTENTS

Introduction 1

Scope 2

Legal Bases for Data Processing 3

Rights of Individuals 5

Accountability and Governance Mechanisms 7

Data Processor Obligations and Agreements 9

Data Security and Personal Data Breach Notification 11

Codes of Conduct and Certifications 12

Cross-Border Transfers of Personal Data 14

Supervision by DPAs 16

Remedies, Liabilities and Sanctions 17

Glossary 19

Contact Information 21

INTRODUCTION

In May 2016 the European Union ("EU") published the EU General Data Protection Regulation ("GDPR"). This major piece of legislation represents the most significant change in EU data protection law since 1995. It will apply in all EU Member States as of 25 May 2018.

The GDPR is a far-reaching legal instrument that will have a significant impact on all companies involved in the processing of personal data, including many outside the EU. It will increase the penalties for noncompliance, with fines of up to €20 million or 4 percent of annual worldwide turnover. In addition, supervisory authorities will have a number of broad powers.

Companies should review the GDPR and begin preparing for compliance with the new legal framework for data protection in the EU.

This guide, by providing a brief overview of the new rules imposed by this legislation and the key changes it will make, will help users prepare for the GDPR. The guide also includes a short glossary of terms used in the GDPR, and each section sets out a short to-do list for compliance. The guide will shortly be followed by further guidance, briefings and practical checklists on the GDPR.

We hope that you find this guide a useful tool. Please contact any of the lawyers listed on page 21 if you would like to receive further information.

SCOPE

ARTICLES 2 AND 3

Quick Overview

The GDPR applies to the processing of personal data that is automated or part of a filing system. The application and territorial scope of the GDPR are both broader than those of the European Data Protection Directive ("Directive").

Application

- The GDPR applies to both data controllers and data processors.
- The GDPR does not apply to a limited number of areas, such as processing for purely personal or household activity.

Territorial scope

The GDPR applies to processing:

- In the context of an establishment in the EU; and
- By a data controller or data processor *not* established in the EU of data subjects in the EU that relates to:
  - *The offering of goods or services to such data subjects*; or
  - *The monitoring of the behavior of data subjects*.

Next Steps

- ✓ Identify relevant processing of personal data.
- ✓ Confirm which establishments in the EU process personal data and where processing relates to situations in which goods or services are offered in the EU or data subjects in the EU are monitored.
- ✓ Assess whether processing is done as a controller or processor.
- ✓ Determine whether an EU representative is necessary.

LEGAL BASES FOR DATA PROCESSING

ARTICLES 6, 7 AND 8

Quick Overview

The legal bases for processing personal data under the GDPR are largely the same as those under the Directive. However, the GDPR sets new restrictions for consent, for processing based on legitimate interests and for processing for additional purposes.

Legal bases for processing personal data

The legal bases for processing personal data under the GDPR are:

- When the data subject consents; and
- When processing is necessary:
  - For the performance or negotiation of a contract with the data subject;
  - To comply with a legal obligation;
  - To protect the vital interests of the data subject or another person when the data subject is incapable of giving consent;
  - For the performance of a task carried out in the public interest or the exercise of official authority; and
  - For the purposes of legitimate interests (but subject to fundamental rights and freedoms).

New restrictions for consent, processing based on "legitimate interests", and processing for additional purposes

- For processing based on consent, the controller must be able to prove that consent has been freely given by the data subject, and the request for consent must be clearly discernible.
- The GDPR provides clarification on when "legitimate interests" can be relied upon as a basis for processing (e.g., direct marketing, preventing fraud, sharing personal data within a group of companies for internal administration, ensuring network and information security) and requires the controller to inform the data subject when it is relying on the legitimate-interests basis for processing.
- The GDPR provides a list of criteria to be considered when determining whether the processing of data for a new purpose is compatible with the original purpose for which the data was collected.

continued on page 4

Next Steps

- ✓ Assess the legal bases for current processing and check that they remain valid under the GDPR.
- ✓ Ensure that consent has been given in accordance with the new requirements and that the controller can demonstrate this.
- ✓ When relying on "legitimate interests", ensure that:
  - The balance of the interests against the data subject's rights is documented; and
  - When a controller relies on legitimate interests as the basis for processing, this fact is included in the information provided to the data subject.
- ✓ Ensure that internal governance processes document the reasons behind decisions to use data for further processing purposes.

RIGHTS OF INDIVIDUALS

ARTICLES 12 TO 17, 19, 20 AND 21

Quick Overview

Data controllers must be more transparent with data subjects, who have increased rights to access their data and important new rights to require rectification or erasure of their personal data and to restrict further processing.

Information notices

Individuals must be given information about how their data will be processed, including details pertaining to:

- The controller's identity and contact information;
- Any data protection officer;
- The purposes and legal basis for processing;
- Any "legitimate interests" relied upon as the basis for processing;
- Any international transfers and applicable safeguards;
- The retention period or criteria for determining it;
- The right of data portability and the rights to object to processing, to require restriction and to withdraw consent to processing;
- The right to complain to a supervisory authority; and
- Any statutory or contractual requirement to provide data, as well as the consequences of not providing it.

This information must be concise, transparent and intelligible; must be in an easily accessible form; and must use clear and plain wording, particularly when addressed to children.

When data is obtained directly, the controller must explain what information is mandatory and the consequences of not providing it. When data is obtained indirectly, the controller must give the source of the information, including publicly accessible sources.

Access right

Data subjects have the right to obtain copies of their personal data, along with key details about how the data is processed. Individuals have increased rights to access their data.

- Controllers cannot charge a fee but can make a reasonable administrative charge for additional copies.

continued on page 6

- Individuals must be given details concerning international disclosures; retention periods; the rights of rectification, erasure, and restriction of processing; and the rights to object to processing and to complain to a supervisory authority.
- Controllers must disclose any third-party source of data and the significance and consequences of any processing based on automated decisions.

Data subjects' rights

Data subjects have important rights in relation to their personal data, including the following:

- The right to require rectification of personal data without undue delay and the right to have incomplete personal data completed;
- The right to erase personal data ("right to be forgotten") when processing is no longer necessary, consent is withdrawn, legitimate interests no longer apply, processing is unlawful, or erasure is required by law, and the controller must take reasonable steps to inform other controllers if it has made such data public;
- The right to prevent further processing of personal data ("restriction") when there is a dispute as to accuracy, when an objection to processing has been verified, when processing is unlawful and the data subject objects to erasure, or when the data is no longer required by the controller but the data subject requires it for the establishment, exercise or defense of a legal claim; and
- The right to require that the data provided by the data subjects for processing with their consent or under contract be provided in a commonly used and machine-readable form and transmitted to another controller ("data portability").

Controllers must notify the data recipients of any rectification, erasure and restriction unless this is impossible or involves disproportionate efforts. Also, if requested to do so, the controllers must inform the data subjects of the identity of the data recipients.

Next Steps

- ✓ Review information notices and privacy policies.
- ✓ Review data subject access procedures.
- ✓ Assess methods of complying with data portability and restriction requests.
- ✓ Consider the implications for IT systems of the right to be forgotten.
- ✓ Consider ways to automate responses to individual requests.

ACCOUNTABILITY AND GOVERNANCE MECHANISMS

ARTICLES 24, 25, 30, 32, 35, 37, 40 AND 42

Quick Overview: The New Rules

In contrast to the Directive, the GDPR requires controllers to implement programs to ensure compliance and demonstrate it to the supervisory authorities and data subjects.

Appropriate technical and organizational measures

Controllers must implement appropriate technical and organizational measures. These might include:

- Implementation of data protection policies;
- Adherence to approved codes of conduct; and
- Adherence to approved certification mechanisms.

Data protection by design and by default

Controllers must implement appropriate technical and organizational measures designed to implement data protection principles (such as pseudonymization and data minimization), both when determining the means of processing and during the processing itself. By default, only the personal data necessary for the specific purpose should be processed.

Data protection impact assessment

Before processing takes place, controllers must carry out an impact assessment of any activities posing significant risk for the rights of the data subjects (e.g., decisions based on automated processing or profiling, large-scale processing of sensitive data, and large-scale systematic monitoring of a publicly accessible area).

Appointment of a data protection officer

Controllers and processors must each appoint a data protection officer ("DPO") if their core activities require large-scale regular and systematic monitoring of data subjects or the large-scale processing of sensitive data. Public authorities or bodies also must appoint DPOs. Voluntary DPO appointment is possible, and national law may require the designation of a DPO in cases not specifically described in the GDPR.

Documentation (records of processing activities)

Controllers must maintain records of their processing activities that contain certain prescribed information (including the purposes for the processing, a description of the categories of the data subjects, the personal data and the data recipients, the technical and organizational measures implemented, and any third-country data transfers).

continued on page 8

Next Steps

- ✓ Assign responsibility and set a budget for data protection compliance, and ensure support from senior management.
- ✓ Review the existing compliance level. (This includes reviewing the existing data protection and IT security policies and identifying the relevant data-processing activities.)
- ✓ Conduct a gap analysis of data protection accountability.
- ✓ Update existing procedures to ensure compliance, and develop new procedures when necessary.
- ✓ Determine whether appointment of a DPO is mandatory; otherwise, consider voluntary appointment.

DATA PROCESSOR OBLIGATIONS AND AGREEMENTS

ARTICLES 28 TO 33 AND 37

Quick Overview: The New Rules

The GDPR specifies requirements for agreements between controllers and processors for processing personal data. These requirements are more detailed than those of the Directive.

In addition, the GDPR sets out new obligations for processors.

Requirements related to data-processing agreements for controllers and processors

- Controllers must use only processors which provide sufficient technical and organizational guarantees that the requirements of the GDPR will be met.
- The agreement between controller and processor must be in writing.
- Processing agreements must stipulate that:
  - The processor processes personal data only in accordance with the instructions of the controller;
  - The processor must ensure that its personnel are bound by a confidentiality obligation;
  - The processor must implement appropriate technical and organizational measures to ensure a level of security for the personal data which is appropriate to the risk;
  - The processor cannot subcontract the processing of personal data without the controller's prior written authorization;
  - Any agreement between a processor and a subprocessor must provide the same data protection obligations which are provided by the agreement with the controller;
  - The processor must assist the controller in ensuring compliance with security obligations, data protection impact assessment, and prior consultation with the data protection authority ("DPA") for high-risk data processing;
  - The processor must delete or return the personal data when the processing is complete; and
  - The processor must provide the controller with all information necessary to demonstrate compliance and allow for and contribute to audits.

continued on page 10

Direct obligations for processors

Except in limited cases for enterprises or organizations employing fewer than 250 persons:

- The processor must maintain a written record of all categories of processing carried out on behalf of each controller; and
- The processor must make this record available to the DPA upon request.

In addition, each processor must:

- Implement appropriate technical and organizational measures to ensure an appropriate level of security;
- Take steps to ensure that staff members with access to the personal data process it only in accordance with the controller's instructions;
- Notify the controller without undue delay after becoming aware of a personal data breach; and
- Designate a DPO in specified cases, including when: (i) processing requires regular and systematic monitoring of data subjects on a large scale, and (ii) data related to criminal convictions and offenses is being processed.

Next Steps

- ✓ Controllers must ensure that all agreements with processors comply with the GDPR.
- ✓ Processors must determine whether records related to processing for a controller have to be maintained.
- ✓ Processors must implement appropriate technical and organizational measures to ensure an appropriate level of security for the personal data and must implement a policy for reporting data breaches.
- ✓ Processors must determine whether a DPO is required.

DATA SECURITY AND PERSONAL DATA BREACH NOTIFICATION

SECTIONS 32 TO 34 AND 37

Quick Overview: The New Rules

Controllers and processors are now subject to a breach-reporting regime. When feasible, controllers must provide notice of serious breaches within 72 hours.

Data security requirements

- Controllers and processors must each apply appropriate technical and organizational security measures to guarantee an adequate level of protection for personal data.
- Where appropriate, security measures must include pseudonymization and encryption, the ability to restore personal data in a timely manner, and regular testing and assessment.
- Controllers and processors with large-scale processing or monitoring activities must appoint a DPO.

Personal data breach notification regime

Controllers and processors are now subject to a personal data breach notification regime.

- Controllers must report personal data breaches to the relevant supervisory authority without undue delay (when feasible, within 72 hours of becoming aware of the breach), unless the breach is unlikely to put the data subjects' rights and freedoms at risk.
- Controllers must notify affected data subjects of personal data breaches if the breaches pose significant risks to the data subjects' rights and freedoms.
- Processors must report personal data breaches to the controllers without undue delay in all cases.

Next Steps

- ✓ Implement procedures to identify security incidents, respond and make required notifications.
- ✓ Allocate responsibility for personal data security.
- ✓ Ensure that processors are obliged to report personal data breaches, and apply adequate security.
- ✓ Check coverage for cyber-risks.
- ✓ Evaluate security and regularly conduct tests.

CODES OF CONDUCT AND CERTIFICATIONS

ARTICLES 40 TO 43

Quick Overview: The New Rules

The GDPR provides for the approval of codes of conduct and the accreditation of certifications, seals and marks, particularly on the EU level, to help controllers and processors demonstrate compliance with the rules for data protection. Codes of conduct, while mentioned in the Directive, played a less significant role there than they do in the GDPR. Under the GDPR, certifications are regulated on a pan-European level for the first time.

Codes of conduct

- Under the GDPR, associations and other representative bodies may prepare, amend or extend a code of conduct for the purpose of specifying how the GDPR applies to certain industry sectors.
- A code of conduct must be submitted to the competent supervisory authority for approval, registration and publication.
- In cases of cross-border processing, a code of conduct must be submitted to the European Data Protection Board ("Board"), which issues an opinion. The European Commission ("Commission") can declare the code of conduct to have general validity within the EU. The Board will collate all codes of conduct in a publicly available register.
- Compliance with a code of conduct is subject to monitoring by accredited bodies. In case of infringement, the company in question may be suspended as an adherent to the code and reported to the competent supervisory authority.
- Adherence to a code of conduct enables data controllers and processors located outside the European Economic Area ("EEA") to demonstrate that they have implemented adequate safeguards in order to permit data transfers from EEA countries to countries outside the EEA.

Certification mechanisms, seals and marks

- The establishment of data protection certification mechanisms, seals and marks is encouraged for the purpose of demonstrating compliance.
- Adherence to certification mechanisms, seals and marks enables data controllers and processors located outside the EEA to demonstrate that they have implemented adequate safeguards in order to permit data transfers from EEA countries to countries outside the EEA.

- The competent supervisory authority or the Board will approve criteria for certifications. The Board may develop criteria for a common certification, i.e., the European Data Protection Seal.
- Certifications will be issued by accredited certification bodies. Accreditations for certification bodies will be issued for a maximum of five years and are subject to renewal and withdrawal when the conditions for accreditation are no longer met. Certifications will be valid for a maximum of three years and may be renewed or withdrawn when the conditions for certification are no longer met.
- The Board will maintain a publicly available register of all certification mechanisms, seals and marks.

Next Steps

✓ Identify or establish associations or representative bodies that can develop codes of conduct, particularly for cross-border data processing.

✓ Monitor the accreditation of certification bodies and consider applying for certifications.

✓ Understand certification schemes and inquire about certifications, seals and marks when selecting service providers.

CROSS-BORDER TRANSFERS OF PERSONAL DATA

ARTICLES 44 TO 50

Quick Overview: The New Rules

Like the Directive, the GDPR requires adequate justification for transfers of personal data to countries located outside the EEA. The GDPR has expanded the possible justifications for data transfers by including approved codes of conduct and certification mechanisms.

- The Commission can adopt adequacy decisions whereby specific third countries, or territories or sectors within such countries, are deemed to offer an adequate level of protection for cross-border transfers. Transfers to such countries, territories or sectors do not require any specific authorizations. The Commission's existing list of adequate third countries remains in force and includes the EU-U.S. Privacy Shield for data transfers from EEA countries to the U.S.
- Absent an adequacy decision, personal data can be transferred to third countries located outside the EEA only when appropriate safeguards are in place. Those safeguards include standard data protection clauses that can be adopted or approved by the Commission, as well as Binding Corporate Rules ("BCRs") whose required content has now been detailed in the GDPR. Other transfers subject to specific safeguards are those permitted where an approved code of conduct, an approved certification mechanism or an enforceable instrument between public authorities is in place.
- In the absence of an adequacy decision or appropriate safeguards, cross-border transfers are possible under one of the following conditions: (i) explicit consent is given by the data subject after the data subject has been informed of the possible risks of such transfers; (ii) the transfer is necessary for a contract or the implementation of pre-contractual measures between the controller and the data subject; (iii) the transfer is necessary for a contract concluded in the interest of the data subject between the controller and another legal person; (iv) the transfer is necessary for important reasons of public interest; (v) the transfer is necessary for the establishment, exercise or defense of legal claims; (vi) the transfer is necessary to protect the vital interests of the data subject or of other persons when the data subject is physically or legally incapable of giving consent; and (vii) the transfer is made from a public register.
- The GDPR also addresses third-country e-discovery situations by stating that judgments or decisions of administrative authorities of third countries requiring transfer of personal data may be recognized or enforceable only if based on an international agreement, such as a mutual legal assistance treaty between the requesting third country and the European Union or an EU Member State, without prejudice to the above grounds for transfer pursuant to the GDPR.

Next Steps

- ✓ Create data flow maps.
- ✓ Review legal justifications for all existing cross-border transfers to countries outside the EEA.
- ✓ Review the content of BCRs to ensure compliance with GDPR requirements.
- ✓ Consider new grounds for data transfers, such as codes of conduct and certifications.
- ✓ Follow legislative developments regarding adequacy decisions.

SUPERVISION BY DPAS

ARTICLES 51 TO 76

Quick Overview: The New Rules

The GDPR provides detailed and harmonized rules applicable to the organization and powers of the supervisory authorities. It also provides cooperation and consistency mechanisms to address issues related to cross-border procedures.

Data Protection Authorities

EU Member States will maintain one or more DPAs per country.

- The DPAs' independence will be strengthened by rules on the establishment of DPAs and the appointment and dismissal of their members, among other means.
- The tasks and powers of DPAs are broadened, including the power to conduct audits and access the premises of controllers and processors.
- The GDPR establishes a "one-stop shop" mechanism whereby DPAs designate a lead DPA (primarily on the basis of the main establishment of the processor) and cooperate to adopt decisions for cross-border data processing.

The European Data Protection Board

The European Data Protection Board will replace the Article 29 Working Party.

- The Board will be composed of the head of one DPA per EU Member State and the European Data Protection Supervisor ("EDPS"). It will benefit from a permanent secretariat provided by the EDPS and based in Brussels.
- The Board issues opinions and guidance and ensures consistent application of the GDPR.
- The Board has binding decision powers in case of disagreements between DPAs in the "one-stop shop" procedure (e.g., deciding which DPA should be the lead authority or determining the content of the final decision in a dispute resolution).

Next Steps

- ✓ Follow national legal developments that modify the institutional setup of DPAs.
- ✓ Understand the DPAs' expanded investigative powers for internal compliance structures.
- ✓ Determine who will be the lead supervisory authority for the company.
- ✓ Prepare for the possibility of intervening before the Board and appealing its decisions.

REMEDIES, LIABILITIES AND SANCTIONS

ARTICLES 77 TO 84

Quick Overview: The New Rules

The GDPR provides for extended remedies for data subjects and liabilities of controllers and processors, as well as for significantly increased sanctions, including fines similar to those of the antitrust regime in the EU. Unlike the Directive, the GDPR sets out in detail the conditions for imposing fines, along with their maximum amounts.

Remedies

Data subjects have the following rights against controllers and processors:

- The right to lodge complaints (via representative associations, among other means) with DPAs in the EU Member State of the data subject's residence, place of work or place of infringement, including appeals in case a DPA fails to deal with the complaint;
- The right to appeal DPAs' binding decisions before national courts; and
- The right to initiate judicial proceedings before the national courts of establishment of the controller or processor or of the data subject's residence.

Compensation and liability

Under the GDPR, the controller and the processor are obliged to fully compensate the data subject for all material and nonmaterial damage resulting from an infringement of the GDPR's provisions. This also applies if more than one controller or processor, or both a controller and a processor, share responsibility for the damage caused by the processing ("joint and several liability").

Sanctions

DPAs can impose administrative fines.

- Depending on the type of infringement, fines can be up to €20 million or, in the case of undertakings, 4 percent of annual worldwide turnover, whichever is higher.
- Fines must be determined on the basis of criteria listed in the GDPR and are subject to judicial review and due process.
- EU Member States can impose additional penalties, including criminal sanctions.

continued on page 18

Next Steps

- ✓ Consider new liabilities and penalties for compliance setup.
- ✓ Assess liability exposure under existing customer/vendor arrangements, including limitation of liability.
- ✓ Ascertain the most likely jurisdiction for proceedings.
- ✓ Follow national legislative developments creating additional penalties.

GLOSSARY

Binding Corporate Rules (BCRs)	Personal data protection policies adhered to by a controller or processor established in the territory of an EU Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings or a group of enterprises engaged in a joint economic activity. (Article 4 (20), GDPR)
Consent of the data subject	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data related to him or her. (Article 4 (11), GDPR)
Data controller	The natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of processing personal data; where the purposes and means of such processing are determined by the laws of the European Union or an EU Member State, the controller or the specific criteria for its nomination may be provided for by the laws of the European Union or the EU Member State. (Article 4 (7), GDPR)
Data processor	A natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller. (Article 4 (8), GDPR)
Data recipient	A natural or legal person, public authority, agency or other body to which the personal data is disclosed, whether a third party or not. (Article 4 (9), GDPR)
Data subject	An identified or identifiable natural person about whom personal data is being processed. (Article 4 (1), GDPR)

continued on page 20

General Data Protection Regulation (GDPR)	Regulation 2016/679/EU of 27 April 2016, repealing Directive 95/46/EC, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
Personal data	Any information related to an identified or identifiable natural person ("data subject"); an "identifiable natural person" is one who can be identified, directly or indirectly, particularly by reference to an identifier such as a name, an identification number, location data or an online identifier or by reference to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. (Article 4 (1), GDPR)
Processing	Any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, such as collection; recording; organization; structuring; storage; adaptation or alteration; retrieval; consultation; use; disclosure by transmission, dissemination, or otherwise making available; alignment or combination; restriction; erasure; or destruction. (Article 4 (2), GDPR)
Profiling	Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects of a natural person, particularly to analyze or predict aspects of that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements. (Article 4 (4), GDPR)
Third party	A natural or legal person, public authority, agency or body other than the data subject, controller or processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data. (Article 4 (10), GDPR)

CONTACTS

Dr. Undine von Diemar
Munich
+49.89.20.60.42.200
uvondiemar@jonesday.com

Jonathon Little
London
+44.20.7039.5224
jrlittle@jonesday.com

Elizabeth A. Oberle-Robertson
London
+44.20.7039.5204
erobertson@jonesday.com

Olivier Haas
Paris
+33.1.56.59.38.84
ohaas@jonesday.com

Dr. Jörg Hladjk
Brussels
+32.2.645.15.30
jhladjk@jonesday.com

Laurent De Muyter
Brussels
+32.2.645.15.13
ldemuyter@jonesday.com

POINTS OF CONTACT OUTSIDE EUROPE

Daniel J. McLoon
Los Angeles
+1.213.243.2580
djmcloon@jonesday.com

Aaron D. Charfoos
Chicago
+1.312.269.4242
acharfoos@jonesday.com

Richard J. Johnson
Dallas
+1.214.969.3788
jjohnson@jonesday.com

Guillermo E. Larrea
Mexico City
+52.55.3000.4064
glarrea@jonesday.com

Richard M. Martinez
Minneapolis
+1.612.217.8853
rmartinez@jonesday.com

Todd S. McClelland
Atlanta
+1.404.581.8326
tmcclelland@jonesday.com

Mauricio F. Paez
New York
+1.212.326.7889
mfpaez@jonesday.com

Jeff Rabkin
San Francisco
+1.415.875.5850
jrabkin@jonesday.com

Michiru Takahashi
Tokyo
+81.3.6800.1821
mtakahashi@jonesday.com


JONES DAY
One Firm Worldwide℠