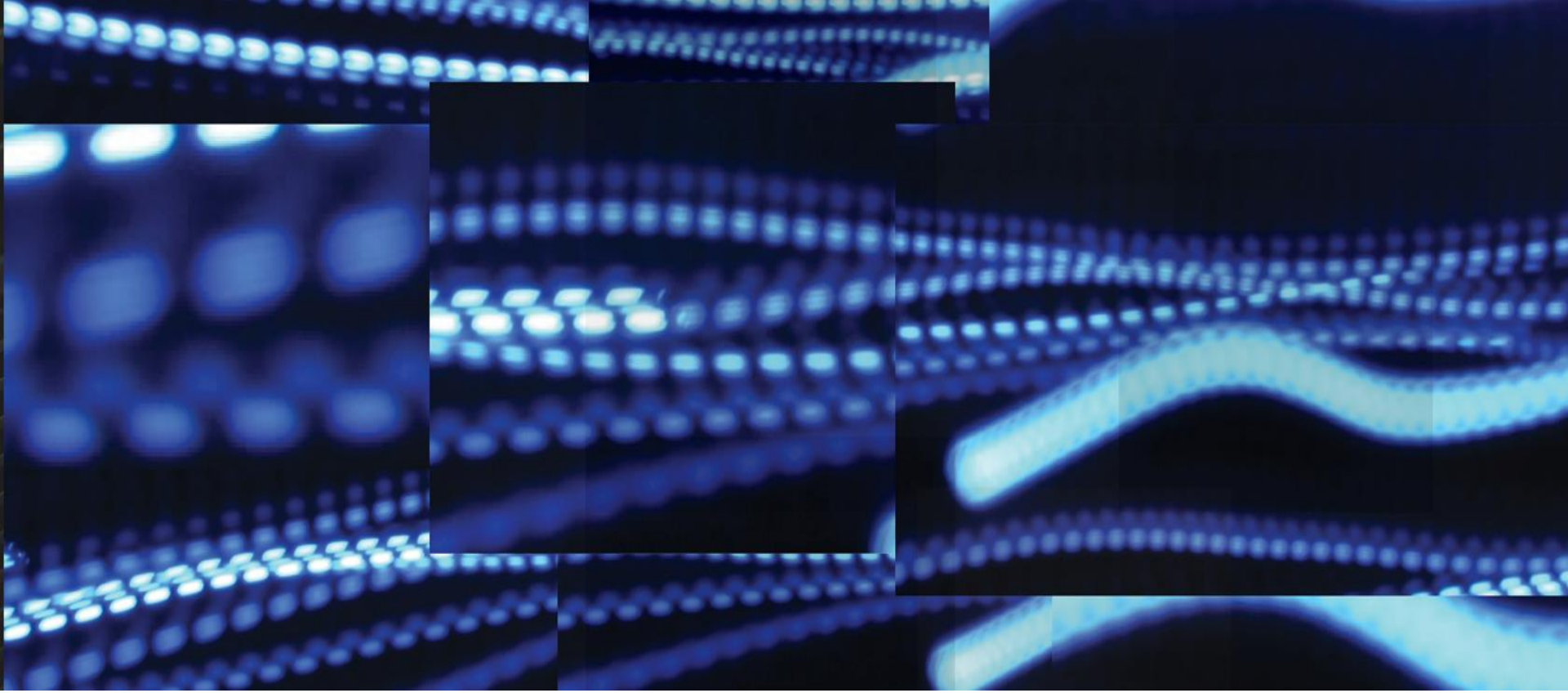


Who is who ? The roles of “data controller” and “data processor” in an IT context

Vincent Wellens – Terrence Dom – Peter Craddock

Correct personal data protection compliance in the context of IT services depends on the right qualification of all stakeholders :

single controllers

- Full GDPR compliance by each of the stakeholders

joint controllers

- Full GDPR compliance by each but tasks can be distributed
- Joint controllership agreement
- Data subjects to be informed about the key elements and can exercise their rights against each of the joint controllers !
- Impact on DPAs which must identify all joint controllers

data processor

- Only compliance with specific provisions of the GDPR aimed at processors (security measures, DPO, processing record, etc.)
- Data processing agreement (standard clauses !, audit, subcontracting …)
- Assistance requirements (general compliance, data breach, data subjects access requests …)

Qualification of stakeholders under the GDPR

Joint controllers

- **Determine jointly** the purposes (why) and the means (how)
- **EDPB** : converging decisions = complementing decisions having a tangible impact on the determination of purposes and means of the processing -> would the processing not be possible without both parties' participation (processing by each party is inseparable, i.e. inextricably linked) ?

Single controllers

- Determines alone the purposes and the means (especially « essential » means, which data, which persons, …)

Data processor

- Acting on behalf and on exclusive instruction of controller
- Decision on non-essential means possible (which software)

Qualification of stakeholders – EDPB example in an IT services context (1)

Example: standardised cloud storage service

A large cloud storage provider offers its customers the ability to store large volumes of personal data. The service is completely standardised, with customers having little or no ability to customise the service. The terms of the contract are determined and drawn up unilaterally by the cloud service provider, provided to the customer on a "take it or leave it basis". Company X decides to make use of the cloud provider to store personal data concerning its customers. Company X will still be considered a controller, given its decision to make use of this particular cloud service provider in order to process personal data for its purposes. Insofar as the cloud service provider does not process the personal data for its own purposes and stores the data solely on behalf of its customers and in accordance with instructions, the service provider will be considered as a processor.

→ if the cloud service provider does not follow the instructions any more (unless required to do so by EU or EU Member State law ≠ US law), transmitting information on the basis of a CLOUD Act request, it will become a data controller itself

Qualification of stakeholders – EDPB example in an IT services context (2)

Example: Hosting services

Employer A hires hosting service H to store encrypted data on H's servers. The hosting service H does not determine whether the data it hosts are personal data nor does it process data in any other way than storing it on its servers. As storage is one example of a personal data processing activity, the hosting service H is processing personal data on employer A's behalf and is therefore a processor. Employer A must provide the necessary instructions to H and a data processing agreement according to Article 28 must be concluded, requiring H to implement technical and organisational security measures. H must assist A in ensuring that the necessary security measures are taken and notify it in case of any personal data breach.

→ some authorities used to consider that the service provider having no access to the data was data agnostic, did from its perspective not process data and was thus not even a processor ≠ no valid argument any more but at which (IT) layer/level does the processing stop (white room rental in data center) ?

Qualification of stakeholders – EDPB example in an IT services context (3)

Example: General IT support

Company Z hires an IT service provider to perform general support on its IT systems which include a vast amount of personal data. The access to personal data is not the main object of the support service but it is inevitable that the IT service provider systematically has access to personal data when performing the service. Company Z therefore concludes that the IT service provider - being a separate company and inevitably being required to process personal data even though this is not the main objective of the service – is to be regarded as a processor. A processor agreement is therefore concluded with the IT service provider.

Example: IT-consultant fixing a software bug

Company ABC hires an IT-specialist from another company to fix a bug in a software that is being used by the company. The IT-consultant is not hired to process personal data, and Company ABC determines that any access to personal data will be purely incidental and therefore very limited in practice. ABC therefore concludes that the IT-specialist is not a processor (nor a controller in its own right) and that Company ABC will take appropriate measures according to Article 32 of the GDPR in order to prevent the IT-consultant from processing personal data in an unauthorised manner.

Qualification of stakeholders – EDPB example in an IT services context (4)

Example: Telecom operators[11]:

Providing an electronic communications service such as an electronic mail service involves processing of personal data. The provider of such services will normally be considered a controller in respect of the processing of personal data that is necessary for the operation of the service as such (e.g., traffic and billing data). If the sole purpose and role of the provider is to enable the transmission of email messages, the provider will not be considered as the controller in respect of the personal data contained in the message itself. The controller in respect of any personal data contained inside the message will normally be considered to be the person from whom the message originates, rather than the service provider offering the transmission service.

→ ePrivacy Directive = specific rules (e.g., cookies), amongst others for telecom operators (data breaches etc.), taking precedence over the GDPR

Qualification of stakeholders – EDPB example in an IT services context (5)

Example: Travel agency

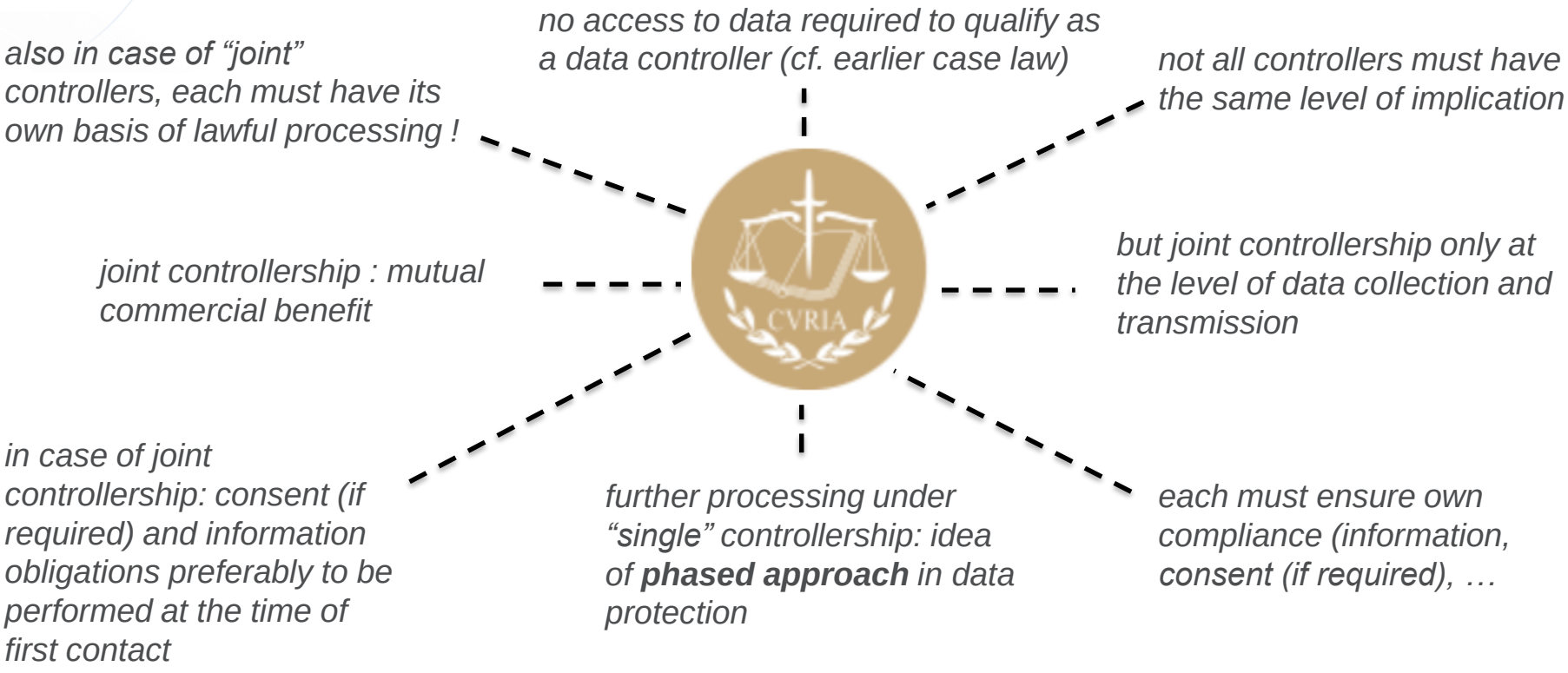
A travel agency sends personal data of its customers to the airline and a chain of hotels, with a view to making reservations for a travel package. The airline and the hotel confirm the availability of the seats and rooms requested. The travel agency issues the travel documents and vouchers for its customers. Each of the actors processes the data for carrying out their own activities and using their own means. In this case, the travel agency, the airline and the hotel are three different data controllers processing the data for their own and separate purposes and there is no joint controllership.

The travel agency, the hotel chain and the airline then decide to participate jointly in setting up an internet-based common platform for the common purpose of providing package travel deals. They agree on the essential means to be used, such as which data will be stored, how reservations will be allocated and confirmed, and who can have access to the information stored. Furthermore, they decide to share the data of their customers in order to carry out joint marketing actions. In this case, the travel agency, the airline and the hotel chain, jointly determine why and how personal data of their respective customers are processed and will therefore be joint controllers with regard to the processing operations relating to the common internet-based booking platform and the joint marketing actions. However, each of them would still retain sole control with regard to other processing activities outside the internet-based common platform.

→ identity of all joint controllers must be reflected in the DPA

Take aways from the CJEU judgment in C-40/17 Fashion ID

CJEU decision on the roles of a website operator and Facebook when embedding a Facebook “Like” social plugin:



Correct reflection of roles in different data protection compliance deliverables

Privacy notice
Consent

Controller (single or joint) ?

Processor ?

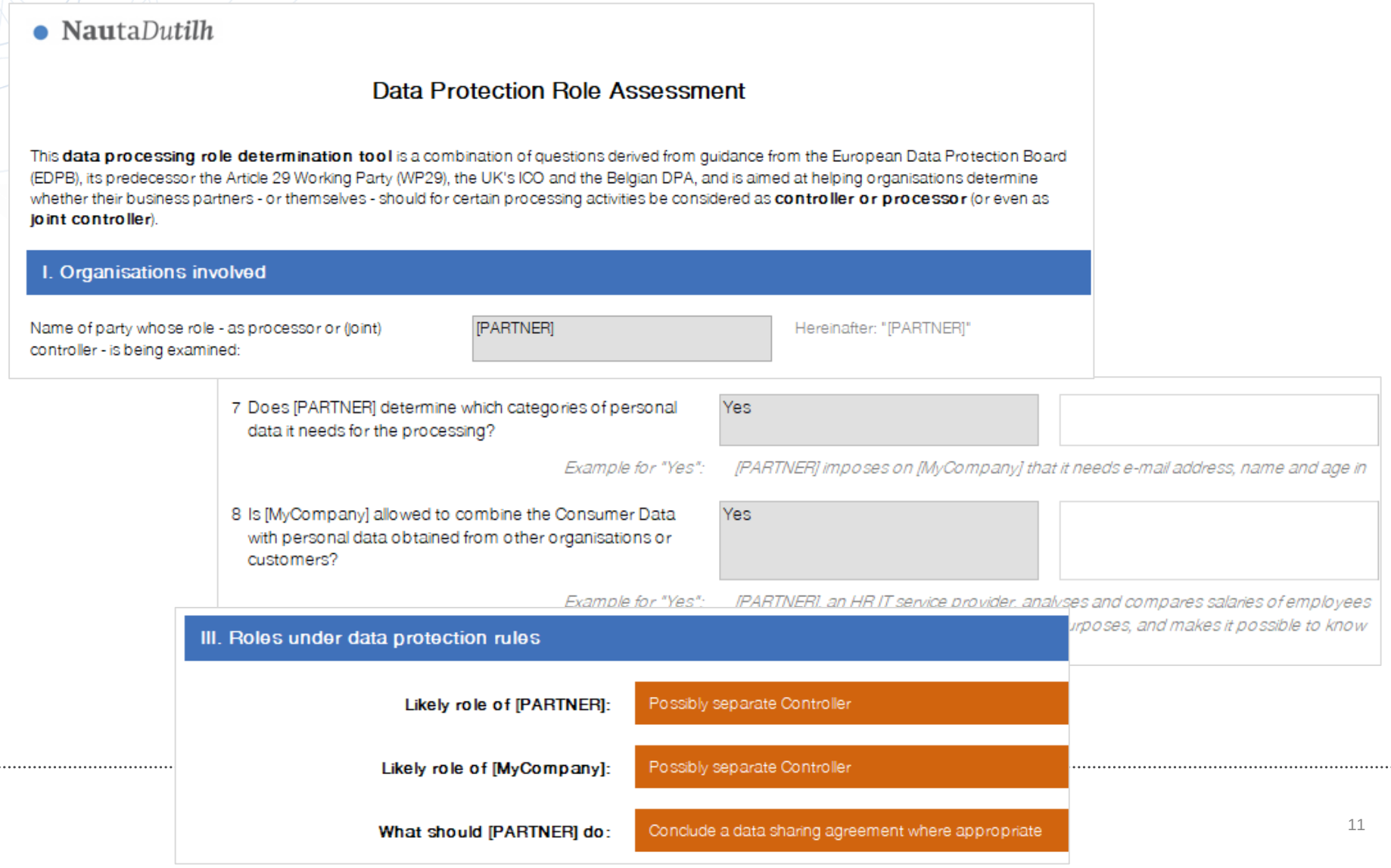
Contracts (DPA (new standard template available !)**, joint controllership…)**

Record

DPIA

BCRs (p.m.)
SCC
4 modules ! :
c-to-c
c-to-p (=DPA !)
p-to-p
p-to-c

Smart questionnaires can help



NautaDutilh

Data Protection Role Assessment

This **data processing role determination tool** is a combination of questions derived from guidance from the European Data Protection Board (EDPB), its predecessor the Article 29 Working Party (WP29), the UK's ICO and the Belgian DPA, and is aimed at helping organisations determine whether their business partners - or themselves - should for certain processing activities be considered as **controller or processor** (or even as **joint controller**).

I. Organisations involved

Name of party whose role - as processor or (joint) controller - is being examined: [PARTNER] Hereinafter: "[PARTNER]"

7 Does [PARTNER] determine which categories of personal data it needs for the processing? Yes

Example for "Yes": [PARTNER] imposes on [MyCompany] that it needs e-mail address, name and age in

8 Is [MyCompany] allowed to combine the Consumer Data with personal data obtained from other organisations or customers? Yes

Example for "Yes": [PARTNER], an HR IT service provider, analyses and compares salaries of employees urposes, and makes it possible to know

III. Roles under data protection rules

Likely role of [PARTNER]: Possibly separate Controller

Likely role of [MyCompany]: Possibly separate Controller

What should [PARTNER] do: Conclude a data sharing agreement where appropriate

Interesting sources

- GDPR
- EDPB guidelines on the notions of « controller » and « processor »
- EU Standard contractual clauses for a data processing agreement (< Art. 28 GDPR)
- EU standard contractual clauses in the context of international transfers

Contact details

Vincent Wellens
Partner, IP, Technology Law & Data Protection
T. +352 26 12 29 34
E. Vincent.Wellens@nautadutilh.com

Joris Willems
Partner, Technology Law & Data Protection
T. +31 20 71 71 670
E. Joris.Willems@nautadutilh.com

Peter Craddock
Partner, Technology Law & Data Protection
T. +32 25 66 82 46
E. Peter.Craddock@nautadutilh.com

Terrence Dom
Senior Associate, Technology Law & Data Protection
T. +31 20 71 71 473
E. Terrence.Dom@nautadutilh.com

Questions?
At your disposal!

A brief presentation of our firm

Firm profile

Number of partners, associates and other legal staff.

- An international law firm practising Dutch, Belgian, Luxembourg and Dutch Caribbean law, founded in 1724.
- One of the largest law firms in the Benelux region:
  - 388 lawyers including 72 partners, including 14 female partners.
  - 10 of our lawyers are also university professors.
- Spread across 6 offices and 5 country desks: Offices in Amsterdam, Brussels, London, Luxembourg, New York and Rotterdam.
- Our country desks focus on: Germany, France, India, China and Japan. We also monitor growth markets such as Brazil, Mexico, Indonesia, South Korea and Turkey.
- An independent firm with non-exclusive relations with the top law firms in more than 80 countries.

Office locations