EY
Data Protection Binding Corporate Rules Processor Policy

24 April 2018

Building a better working world

Contents

Introduction to the Data Protection Binding Corporate Rules Processor Policy

EY has established a foundation for the privacy of all personal data, which is processed worldwide in its global personal data privacy program ("**global privacy program**"). The global privacy program comprises a series of policies and procedures, which set out the principles to be applied to the processing of personal data within EY.

One of the policies forming part of the global privacy program is this Data Protection Binding Corporate Rules Processor Policy ("**Processor Policy**"). In this Processor Policy, we use "**EY**" to refer to the global organization of independent member firms ("**EY Member Firm**")[1] and other entities in the EY organization ("**EY Network entity**"),[2] which are bound to comply with the requirements of Ernst & Young Global Limited ("**EYG**"). EYG is the central governance entity of the EY organization and coordinates EY Network entities and the cooperation among them.

This Processor Policy has been created to establish EY's approach to compliance with European[3] data protection law and specifically to transfers of personal data between EY Network entities where such EY Network entities are acting as processors.

All EY Network entities[4] and their partners, directors, employees, new hires, individual contractors and temporary staff ("**EY Personnel**") must comply with, and respect, this Processor Policy when processing[5] personal data as a processor, irrespective of the country in which they are located.

EY will process personal data under this Processor Policy on behalf of the following controllers:

- External clients ("**Clients**")
- Other EY Network entities, when acting as a controller

Hereinafter, they will be collectively referred to as "**Controllers.**"

The Processor Policy contains 14 rules ("**Rules**") that govern the processing of personal data of current, past and prospective EY Personnel, clients, suppliers, subcontractors and any other third parties ("**EY Data**").

This Processor Policy applies to all EY Data wherever it is processed as part of the regular business activities of EY. Transfers of personal data take place between EY Network entities during the normal course of business and such data may be stored in centralized databases accessible by EY Network entities from anywhere in the world. Each EY Network entity and its EY Personnel shall respect the instructions regarding the data processing and the security and confidentiality measures as provided in the contract or other binding document that such EY Network entity enters into with the Controller.

This Processor Policy is accessible on EY's website at ey.com/bcr.

---

[1] EY Member Firm means any corporation, partnership or other entity or organization that is admitted from time to time as members of Ernst & Young Global Limited pursuant to the regulations of Ernst & Young Global Limited.

[2] EY Network entity means any one of the network of entities comprising Ernst & Young Global Limited, EYGN Limited, EYGM Limited, EYGS LLP, EYGI B.V., EY Global Finance, Inc. and their members. It also means any entity controlled by any such entity, under common control with any such entity, or controlling such entity or any corporation, partnership, or other business organization that is a member firm or a subsidiary of the entity, or which is directly or indirectly a majority owned or controlled subsidiary of the entity, together with any partner, director, employee or agent of any such entity. For the purposes of this definition, "control" means (a) ownership, either directly or indirectly, of equity securities entitling either such entity to exercise in the aggregate of at least 50% of the voting power of such entity in question; or (b) possession, either directly or indirectly, of the power to direct or cause the direction of the management and policies of such entity in question, whether through ownership of securities, by contract or otherwise.

[3] For the purpose of this Processor Policy, reference to Europe means the European Economic Area (EEA) and Switzerland and European should be construed accordingly.

[4] The list of the EY Network entities providing services to Clients who are bound by the Processor Policy is accessible on EY's website at ey.com/uk/en/home/legal via "View a list of EY member firms and affiliates".

[5] "Processing" in European data protection law means any set of operations performed upon personal data, whether or not by automatic means. This is interpreted widely to include collecting, storing, organizing, destroying, amending, consulting, destroying and disclosure of the personal data.

Part I: Background and actions

What is data protection law?

Data protection law gives people the right to control how their "**personal data**"[6] is used. When EY processes EY Data, this is covered and regulated by data protection law.

Data protection law distinguishes between the concepts of "**controller**" and "**processor**". The controller determines, alone or jointly with others, the purposes and the means of the processing of personal data. The processor, on the other hand, processes personal data on behalf of the controller.

For the majority of professional services, EY is acting as a controller, processing personal data in accordance with its own strict professional obligations. For a limited type of professional services, EY will be acting as a processor under the detailed instructions of the Controller (either a Client or another EY Network entity). For services where EY is acting as a controller, EY shall comply with the Data Protection Binding Corporate Rules Controller Policy ("**Controller Policy**") as published on ey.com/bcr. For services where EY acts as a processor, this Processor Policy applies.

How does data protection law affect EY internationally?

European data protection law does not allow the transfer of personal data to countries outside Europe that do not ensure an adequate level of data protection[7]. Some of the countries in which EY operates are not regarded by European data protection authorities as providing an adequate level of protection for individuals' data privacy rights.

When EY acts as a processor, the Controller retains the responsibility to comply with European data protection law. Controllers in Europe will pass certain data protection obligations on to EY in the contracts or other binding documents EY has with them. Consequently, if EY fails to comply with the terms of a contract or other binding document it enters into with a Controller, the Controller may be in breach of applicable data protection law and EY may face a claim for breach of contract, which may result in the payment of compensation or other judicial remedies.

In such cases, if a Controller demonstrates that it has suffered damage, and that it is likely that the damage has occurred due to a breach of the Processor Policy by an EY Network entity outside Europe (or a third party sub-processor established outside Europe), that Controller is entitled to enforce the Processor Policy against EY and, in such cases, the obligation will be on the EY Network entity accepting liability (namely the EY Network entity that is a party to the contract or other binding document with the Controller) to demonstrate that the EY Network entity outside Europe (or the third party sub-processor established outside Europe) is not responsible for the breach, or that no such breach took place.

What is EY doing about it?

EY must take proper steps to ensure that it processes personal data on an international basis in a safe and lawful manner. This Processor Policy sets out a framework to satisfy the standards contained in European data protection law and, in particular, to provide an adequate level of protection for all personal data processed in Europe and transferred to EY Network entities outside Europe, where the personal data is collected by a Client or an EY Network entity in Europe as a Controller.

Although the legal obligations under European law apply only to personal data processed in Europe, EY will apply this Processor Policy globally whenever it acts as a processor, and in **all cases** where EY processes EY Data both manually and by automatic means.

EY will apply the Rules contained in this Processor Policy whenever it acts as a processor on behalf of a Client or whenever it provides a service to another EY Network entity. Where the Controller relies upon this Processor Policy as providing adequate safeguards, an obligation to comply with this Processor Policy will be included in the contract or other binding document EY has with the Controller and a copy of this Processor Policy will be incorporated into such contracts or other binding documents or referenced with a

[6] Personal data means any information relating to an identified or identifiable natural person in line with the definition in the EU Data Protection Regulation 2016/679.
[7] Several exceptions to this rule can be applicable.

possibility of electronic access. If the Controller chooses not to rely upon this Processor Policy, that Controller is responsible for putting in place another adequate safeguard to protect the personal data.

All EY Network entities who process personal data to provide services to a Client, or who provide a service to another EY Network entity, in their capacity as a processor, must comply with the Rules set out in **Part II** of this Processor Policy together with the policies and procedures set out in the appendices in **Part III** of this Processor Policy.

For the avoidance of doubt:

- Where EY acts as a controller, EY shall comply with the Controller Policy as published on ey.com/bcr. EY Network entities may act as both a controller and a processor and must therefore comply with both the Processor Policy and the Controller Policy.
- For some internal administrative processes and for compliance with regulatory requirements, EY will always act as a controller in its own right (e.g., compliance with regulatory requirements, to check conflicts, for quality, risk management or financial accounting purposes and for the provision of internal administrative or IT support services). For such processes, EY shall comply with the Controller Policy.

What does this mean in practice for personal data processed in the EEA?

Under European data protection law, individuals both within and outside Europe whose personal data is processed in Europe by an EY Network entity acting as a processor and transferred to an EY Network entity outside Europe under the Processor Policy have certain rights. These individuals may enforce the Rules set out in this Processor Policy as third-party beneficiaries where they are not able to bring a claim against the Controller in respect of a breach of any of the commitments in this Processor Policy by an EY Network entity (or by a sub-processor) acting as a processor (for example in case the Controller has factually disappeared or ceased to exist in law or has become insolvent, unless any successor entity has assumed the entire legal obligations of the Controller by contract or by operation of law).

In such cases, these individuals' rights are as follows:

- **Complaints**: Individuals may complain to an EY Network entity established in Europe in accordance with the Complaint Handling Procedure (as set out in Appendix 4 of this Processor Policy) and to a European data protection authority in the jurisdiction of the EY Network entity responsible for exporting the data outside Europe.
- **Liability**: Individuals may bring proceedings against the EY Network entity responsible for exporting the data outside Europe:
  - In the courts of the country where the EY Network entity responsible for exporting the data is established
  - In the jurisdiction from which the personal data was transferred

    Or
  - In the courts of the jurisdiction of the EEA Member State where the individual resides
- **Compensation**: Individuals may seek appropriate redress from the EY Network entity established in Europe and responsible for exporting the data (including the remedy of any breach of this Processor Policy by an EY Network entity outside Europe) and where appropriate, receive compensation from the EY Network entity established in Europe and responsible for exporting the data for any damage suffered as a result of a breach of this Processor Policy by:
  - An EY Network entity established outside Europe

    Or
  - Any third-party processor that is established outside Europe and is acting on behalf of an EY Network entity inside Europe or outside Europe, in accordance with the determination of the court or other competent authority
- **Transparency**: Individuals may obtain a copy of this Processor Policy from the EY Network entity responsible for exporting the data outside Europe or any other EY Network entity by accessing the Processor Policy on EY's website: ey.com/bcr.

In the event of a claim being made in which an individual has suffered damage, where that individual can demonstrate that it is likely that the damage has occurred because of a breach of the Processor Policy, EY has agreed that the burden of proof to show that (i) an EY Network entity outside Europe or (ii) any third-party sub-processor who is established outside Europe and who is acting on behalf of an EY Network entity outside Europe is not responsible for the breach, or that no such breach took place, will rest with the EY Network entity responsible for exporting the personal data to the EY Network entity outside Europe.

Data protection roles and responsibilities

The EY Global Privacy Officer is the person who has overall responsibility for compliance with the Processor Policy and any other supporting policies and procedures.

Area Privacy Officers are responsible for overseeing compliance with this Processor Policy by the EY Network entities within their area on a day-to-day basis.

A description of the roles and responsibilities of the EY global privacy team is set out in Appendix 1.

Further information

If you have any questions regarding the provisions of this Processor Policy, your rights under this Processor Policy or any other data privacy issues, you may contact the EY Global Privacy Officer who will either deal with the matter or forward it to the appropriate person or department within EY at the following address:

EY Global Privacy Officer
Andrew Heaton
Email: global.data.protection@ey.com
Address: Office of the General Counsel (GCO), 6 More London Place, London, SE1 2DA.

The Global Privacy Officer is responsible for ensuring that changes to this Processor Policy are notified to the EY Network entities and to individuals whose personal data is processed by EY via the EY website at ey.com/bcr.

Part II: The Rules

The Rules are divided into two sections. Section A addresses the basic principles of European data protection law EY must observe when EY processes personal data as a processor.

Section B deals with the practical commitments made by EY to the European data protection authorities in connection with this Processor Policy.

Section A

Rule 1 — Compliance with local law

Rule 1A — EY will first and foremost comply with local law where it exists.

EY will comply with any applicable legislation relating to personal data and will ensure that, where personal data is processed as a processor, this is done in accordance with applicable local law.

Where local legislation relating to personal data requires a higher level of protection for personal data, such legislation will take precedence over this Processor Policy.

Where there is no law or the law does not meet the standards set out by the Rules in this Processor Policy, EY's position will be to process personal data adhering to the Rules in this Processor Policy.

Rule 1B — EY will cooperate and assist a Controller to comply with its obligations under local law in a reasonable time and to the extent reasonably possible.

EY will, within a reasonable time and to the extent reasonably possible, as required under the contract or other binding document it has entered into with a Controller, assist such Controller to comply with its obligations under applicable data protection law.

Rule 2 — Ensuring transparency and using personal data for a known purpose only

Rule 2A — EY will assist a Controller to comply with the requirements to *explain to individuals* how their data will be used and to be transparent about data processing activities.

The Controller has a duty to explain to individuals how their personal data will be processed (for example, by providing a privacy notice or privacy statement). EY will assist a Controller, insofar as this is possible, to comply with this requirement.

EY will follow this Rule 2A unless there is a legitimate basis for not doing so, for example, where it is necessary to safeguard national security or defense, for the prevention or detection of crime, legal proceedings or where otherwise permitted by law.

Rule 2B — EY will only obtain and use personal data on behalf of and in accordance with the instructions of the Controller.

EY will only process personal data on behalf of and in compliance with the (lawful) instructions of a Controller, as specified in the contract or other binding document it has with such Controller. Where the Controller relies upon this Processor Policy as providing adequate safeguards, an obligation to comply with this Processor Policy will be included in the contract or other binding document and a copy of this Processor Policy will be incorporated into such contract or other binding document or referenced with a possibility of electronic access.

If EY is unable to comply with this Rule or its obligations under this Processor Policy, EY will inform the Controller promptly of this fact. The Controller may then take appropriate action (such as suspending the transfer of personal data and terminating the contract or other binding document it has with EY).

Rule 3 — Ensuring data quality

Rule 3A — EY will assist the Controller to keep personal data *accurate* and *up to date*.

EY will act upon the instructions of the Controller in order to help and assist such Controller to comply with its obligations to keep personal data accurate and up to date. EY shall execute any necessary measures when asked by the Controller in order to have the personal data updated or corrected.

When required to do so on instruction from a Controller, as required under the terms of the contract or other binding document with that Controller, EY will delete, anonymize, update or correct personal data.

EY will notify other EY Network entities or any third-party sub-processors to whom the personal data has been disclosed accordingly so that they can also update their records.

Rule 3B — EY will only keep personal data for *as long as is necessary*.

Personal data will always be retained and/or deleted or anonymized to the extent required by law, regulation and professional standards, under the instructions of the Controller (provided such instructions do not conflict with such law, regulation and professional standards) and in line with the applicable EY service lines and any local retention policies applying to an EY Network entity. EY will dispose of personal data only in a secure manner in accordance with EY global security policies.

On the termination of the provision of professional services to a Controller, EY will — at the choice and at the request of the Controller — return all the personal data transferred and the copies thereof to the Controller or destroy all the personal data (except for backup copies) and certify to the Controller that it has done so. If applicable legislation or professional regulations prevent EY from returning or destroying the personal data to a Controller, EY will ensure that such personal data remains confidential.

Rule 3C — EY will only keep personal data which is *relevant* to EY.

EY will identify the minimum amount of personal data that is required in order to properly fulfil its purpose. EY will only process personal data that is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Rule 4 — Taking appropriate security measures

Rule 4A — EY will always adhere to its *IT Security Policies* and the information security measures as specified in the contract or other binding document with a Controller.

EY will comply with the requirements contained in EY global security policies as revised and updated from time to time together with any other information security procedures relevant to a business area or function, as well as with information security measures specified in a contract or other binding document it enters into with a Controller.

Rule 4B — EY will ensure that providers of services to EY also adopt appropriate and equivalent security measures.

European law expressly requires that where a provider of a service to EY has access to EY Data, strict contractual obligations, evidenced in writing and dealing with the security of that data, are imposed to ensure that such service providers act only on EY's instructions when using that data and that they have in place appropriate technical and organizational security measures to safeguard the personal data.

Rule 4C — EY will notify a Controller of any personal data breach in relation to personal data processed on behalf of the Controller in accordance with and to the extent required by applicable law and in accordance with the terms of the contract or other binding document with that Controller.

EY will notify a Controller of any personal data breach in relation to personal data processed on behalf of that Controller in accordance with and to the extent required by applicable law and the terms of the contract or other binding document with that Controller. A personal data breach means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or

access to, personal data. Where a breach is subject to European data protection law, EY will notify the Controller without undue delay after becoming aware of a personal data breach.

Rule 4D — EY will ensure that sub-processors undertake to comply with provisions that are consistent with the terms in its contract or other binding document with a Controller and this Processor Policy, specifically with regard to the adopting of security measures.

EY may only appoint sub-processors who provide appropriate and equivalent technical and organizational security measures that are applicable to their use of the personal data to which such sub-processor will have access in accordance with the terms of the contract or other binding document EY has with the Controller.

To comply with this Rule, where a sub-processor has access to EY Data, EY will impose strict contractual obligations, in writing, on the sub-processor regarding (i) the security of such data, consistent with those contained in this Processor Policy and with the terms of the contract or other binding document EY has with the Controller, (ii) the sub-processor's obligation to act only on EY's instructions when using EY Data and (iii) such obligations as may be necessary to ensure that the commitments on the part of the sub-processor reflect those made by EY in this Processor Policy.

Rule 4E — EY will comply with the requirements of a Controller regarding the appointment of any sub-processor.

EY will inform the Controller where processing, undertaken on its behalf in the context of providing services, will be conducted by a sub-processor and will comply with the particular requirements of a Controller with regard to the appointment of sub-processors as set out under the terms of the contract or other binding document with that Controller. EY will ensure that up-to-date information regarding its appointment of sub-processors is available to the Controller at all times so that its general consent is obtained. If, on reviewing this information, a Controller objects to the appointment of a sub-processor to process personal data on behalf of EY, that Controller will be entitled to take such steps as are consistent with the terms of the contract or other binding document it has with EY.

Rule 5 — Honoring individuals' rights

Rule 5A — EY will assist the Controller to comply with the rights of individuals to be informed whether any personal data about them is being processed.

EY will act in accordance with the instructions of the Controller and undertake any reasonably necessary measures to enable the Controller to comply with its duty to respect the rights of individuals.

Rule 5B — EY will handle requests from individuals to access, rectify and delete their personal data and to *cease the processing* of their personal data in accordance with the instructions of the Controller and — where applicable — with the *Subject Access Request Procedure*.

Individuals have the right to access their personal data, including to rectify or delete their personal data where it is inaccurate or incomplete and, in certain circumstances, to object to the processing of their personal data.

EY will act in accordance with the terms of the contract or other binding document it has with the Controller and undertake any reasonably necessary measures to enable the Controller to comply with its duty to respect the rights of individuals. If an EY Network entity receives a subject access request, it will manage such request in accordance with the contract or other binding document it has with the Controller, which may include transferring the request to the relevant Controller and not responding to such request. Where EY is authorized to do so or is required by law, EY will adhere to the *Subject Access Request Procedure* (as set out in Appendix 2).

Rule 6 — Ensuring adequate protection for international transfers

Rule 6 — EY will *not* transfer personal data to external third parties *outside* Europe *without ensuring adequate protection* for the data.

In principle, international transfers of personal data to third parties outside Europe are not allowed without appropriate steps being taken by EY, such as contractual clauses, in order to protect the personal data that is being transferred.

Rule 7 — Safeguarding the use of sensitive personal data

Rule 7A — EY will only process sensitive personal data as instructed by a Controller and only if such processing is *absolutely necessary*.

"**Sensitive personal data**" is data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, and data concerning a natural person's sex life or sexual orientation. Legal restrictions may also apply to criminal convictions, social security files, government identification numbers or financial account numbers under applicable laws. Sensitive personal data needs to be handled with additional care, in order to respect local customs and applicable local laws. In particular, EY will:

- Only process sensitive personal data under the instructions of the Controller
- Avoid collection of sensitive personal data where it is not required for the purposes for which the data is collected or subsequently processed
- Limit access to sensitive personal data to appropriate persons (by either masking or making anonymous or pseudonymous the data, where appropriate) in accordance with the security standards established in EY Global Information Security Policies and the instructions of the Controller

Rule 7B — EY will only process sensitive personal data where the Controller has obtained the individual's *explicit consent* unless the Controller has a legitimate basis for doing so consistent with the requirements of applicable data protection laws.

In principle, individuals must give their explicit consent to the processing of their sensitive personal data. This consent must be obtained by the Controller, unless the Controller has a legitimate basis for processing sensitive data. Consent to process sensitive personal data must be specific, informed, unambiguous and freely given. The responsibility to obtain the consent of the individuals is on the Controller.

Rule 8 — Automated individual decisions

Rule 8 — Individuals have the right not to be subject to a decision based solely on automated processing and to know the logic involved in such decision as well as the significance and the envisaged consequences of such processing. EY will assist Controllers in taking necessary measures to protect the legitimate interests of individuals.

Under European data protection law, no decision which produces legal effects concerning an individual or significantly affects that individual can be based solely on the automated processing of that individuals' personal data (including profiling), unless such decision is: (i) necessary for entering into, or performance of, a contract between the individual and the data controller; (ii) authorized by law; or (iii) based on the individual's explicit consent. EY will act in accordance with the instructions of the Controller and undertake any reasonably necessary measures to enable the Controller to comply with its duty to inform individuals.

Section B — Practical Commitments

Rule 9 — Training

Rule 9 — EY will provide appropriate *training* to EY Personnel who have *permanent or regular access* to personal data, who are involved in the processing *of personal data* or in the *development of tools* used to process personal data.

EY will take reasonable and appropriate steps to communicate with EY Personnel and to provide appropriate training on the requirements of this Processor Policy in accordance with the Privacy Training Program set out in Appendix 7.

Rule 10 — Assessment of compliance

Rule 10A — EY will comply with the *Assessment of Compliance Protocol* set out in *Appendix 3*.

Rule 10B — EY will — at the request of a Client acting as a Controller — allow its data processing facilities to be audited in relation to the processing activities of the Controller.

EY will allow its data processing facilities to be audited at the request of a Client. Such audit may consist of:

- The provision by EY of written information (including, without limitation, questionnaires, related independent SOC2 audit reports or reports of a similar nature and information security policies) that may include information relating to sub-processors

  Or
- Interviews with EY's IT personnel

Such audit may be carried out by the Client or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, provided such members are not working for direct competitors of EY.

For the avoidance of doubt, no access to any part of IT systems or infrastructure will be permitted due to strict confidentiality obligations towards Clients.

Rule 11 — Complaint handling

Rule 11 — EY will comply with the *Complaint Handling Procedure* set out in *Appendix 4*.

Rule 12 — Cooperation with data protection authorities

Rule 12 — EY will comply with the *Cooperation Procedure* set out in *Appendix 5*.

Rule 13 — Update of the rules

Rule 13 — EY will comply with the *Updating Procedure* set out in *Appendix 6*.

Rule 14 — Actions in case of national legislation preventing respect for the Processor Policy

Rule 14A — EY will ensure that where it believes that existing or future legislation applicable to it may prevent it from fulfilling the instructions received from the Controller, or its obligations under the Processor Policy, or its obligations under the contract or other binding document with the Controller, EY will promptly inform the Controller, the Global Privacy Officer and the data protection authority competent for the Controller unless otherwise prohibited.

Where EY has reasons to believe that the existing or future legislation applicable to it may prevent it from fulfilling the instructions received from the Controller, or its obligations under this Processor Policy or the obligations under the contract or other binding document it has with the Controller, it will promptly notify this to:

- The Controller, who is entitled to suspend the data transfer and terminate the contract or other binding document with EY
- EY's Global Privacy Officer
- The data protection authority competent for the Controller

Rule 14B — EY will ensure that where it receives a *legally binding request for disclosure* **of personal data, which is subject to this Processor Policy, EY will:**

- **Notify the** *Controller promptly unless prohibited from doing so by a law enforcement authority*
- **Put the request on hold and notify the lead data protection authority for this Processor Policy and the appropriate data protection authority competent for the Controller unless prohibited from doing so by a law enforcement authority or agency**
- **Comply with the Law Enforcement Data Access Procedure set out in Appendix 8**

EY will assess each data access request by any law enforcement authority or state security body (the "**requesting authority**") on a case-by-case basis. EY will use its best efforts to inform the requesting authority about EY's obligations under European data protection law and to obtain the right to waive this prohibition.

EY will put such request on hold for a reasonable delay in order to notify the data protection authority competent for the Controller and the lead data protection authority for this Processor Policy prior to disclosing the data to the requesting authority. EY shall clearly inform the competent data protection authorities about the request, including information about the data requested, the requesting authority and the legal basis for the disclosure.

If, despite having used best efforts, EY is not in a position to notify the competent data protection authorities and to put the request on hold, in such case, EY will provide on an annual basis general information about the requests it has received to the competent data protection authorities (e.g., number of applications for disclosure, type of data requested and requesting authority if possible), to the extent it has been authorized by the said requesting authority to disclose such information to third parties.

PART III: Appendices

Appendix 1

Data privacy roles and responsibilities

1. EY Global Privacy Officer

1.1 The EY Global Privacy Officer is responsible for:

- Advising the Global General Counsel, Risk Management Executive Committee and other EYG leaders on data privacy matters
- Recommending modifications to the global privacy program, as regulations and the business environment evolve, and to other EY policies, practices or agreements relating to data privacy for Risk Management Executive Committee approval
- Maintaining the compliance of EY global systems with applicable data protection rules, including the Controller Policy and this Processor Policy (analysis of systems, definition of actions and ongoing compliance)
- Coordinating a community of EY Area Privacy Officers (see below) for the purpose of competency building, collaboration on implementation of and revisions as necessary to the global privacy program (including the Processor Policy and Controller Policy), sharing of leading practices, monitoring of relevant applicable regulations, and consistency of communications between EY Network entities and their respective local regulators with the global privacy program
- Collaborating with EY Talent, Risk Management, General Counsel, and Global IT teams, service lines and other relevant functions on data privacy matters
- With the assistance of the Area Privacy Officers, overseeing the compliance of EY Network entities with the global privacy program (including the Controller Policy and this Processor Policy)
- With the assistance of the Area Privacy Officers, developing and providing communications and uniform training material and support
- With the assistance of the Area Privacy Officers, providing guidance to EY Network entities in implementing and modifying local data privacy policies and compliance programs.

2. Area Privacy Officers

2.1 EY Area Privacy Officers work with the EY Global Privacy Officer to evaluate and develop global policy and processes. The Area Privacy Officers will coordinate the implementation of the Processor Policy locally. In particular, they are responsible for the following within their respective Areas:

- Providing assistance to Regional Privacy Officers and Local Privacy Officers to identify local business, and legal and regulatory risks surrounding data privacy issues
- Providing assistance to Regional Privacy Officers and Local Privacy Officers on local privacy matters, including developing local data privacy policies, as necessary
- Developing and implementing consistent solutions on a global or area basis to mitigate data privacy risks
- Coordinating the development and implementation of a data privacy program in their area that complies with the global privacy program (including the Controller Policy and this Processor Policy)
- Advising the General Counsel's Office and relevant executive and country management on data privacy issues

- Escalating within the General Counsel's Office and relevant executive, Regional and country management any significant compliance issues and plans for their resolution, as well as implications of local data privacy regulations
- Advising the EY Global Privacy Officer of any local data privacy regulations in their Area that may have international or cross-border implications, which are not adequately addressed by the global privacy program (which includes the Processor Policy)
- Confirming to the EY Global Privacy Officer, EY Network entity compliance with the global privacy program and, in particular, the Processor Policy
- Collaborating with relevant Talent, Risk Management, General Counsel and IT teams, service lines, and other relevant functions on data privacy matters
- Periodically monitoring the effectiveness of the Area Privacy functions

3. Regional / Local Privacy Officers

3.1 EY may appoint Regional / Local Privacy Officers to assist with the coordination and implementation of Global standards locally.

3.2 The Regional / Local Privacy Officer remains knowledgeable about the relevant country, region and state laws, governmental regulations, professional practice obligations, and regulatory guidance, which relate to data privacy compliance and are applicable to the EY Network entities of the Region.

3.3 The Regional / Local Privacy Officer handles subject access requests and complaints under the Processor Policy and may refer such request or complaint to the Area Privacy Officer or the Global Privacy Officer as needed.

Appendix 2

Subject Access Request Procedure

1. Subject Access Request Procedure

1.1 European data protection law gives individuals whose personal data is processed the right to be informed whether any personal data about them is being processed by an organization. This is known as the right of subject access.

1.2 When EY processes personal data on behalf of a Controller, EY is considered to be a processor of the data and the Controller will be primarily responsible for meeting the legal requirements as a controller. If an EY Network entity receives a subject access request, the EY Network entity will manage such request in accordance with the contract or other binding document it has with the Controller. This may include transferring the request to the Controller and not responding to such request. Where EY is authorized to do so or is required by law, EY will adhere to the terms of this Subject Access Request Procedure.

1.3 Where a subject access request is subject to European data protection law, such a request will be dealt with by EY in accordance with this Subject Access Request Procedure (referred to as "**valid request**" in this procedure). A subject access request is subject to European data protection law where the EY Network entity or the Controller is established in the EU or where the processing activities are related to the offering of goods or services to individuals in the EU or to the monitoring of their behavior as far as their behavior takes place within the EU. Where applicable local data protection law differs from any aspect of this Subject Access Request Procedure, the local data protection law will prevail.

1.4 An individual making a valid request to an EY Network entity is entitled to:

1.4.1 Be informed whether the EY Network entity holds and is processing personal data about that individual and, where that is the case, access such personal data

1.4.2 Be given a description of the personal data; the purposes for which they are being held and processed; the recipients or classes of recipient to whom the personal data is, or may be, disclosed by the EY Network entity (in particular recipients in third countries); the envisaged period for which the personal data is stored or — if this is not possible — the criteria used to determine that period; the existence of the right to request from the Controller rectification or erasure of personal data or restriction of processing; the right to lodge a complaint with a supervisory authority and — where personal data are not collected from the individual — any available information as to their resource

1.4.3 Receive — free of charge — a copy of the personal data undergoing processing; for any further copies requested by the individual, a reasonable fee based on administrative costs may be charged

1.5 The request must be made in writing[8], which can include email. Where the individual makes the request by electronic means, the personal data shall be provided in a commonly-used electronic form, unless otherwise requested by the individual.

1.6 The EY Network entity must respond to a valid request without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of requests. The individual will be informed of any such extension within one month of receipt of the request, together with the reasons for the delay.

1.7 The EY Network entity is not obliged to comply with a subject access request unless the EY Network entity is supplied with such information which it may reasonably require in order to

[8] Unless the local data protection law provides that an oral request may be made, in which case EY will document the request and provide a copy to the individual making the request before dealing with it

confirm the identity of the individual making the request and to locate the information which that person seeks.

2. Procedure

2.1 Receipt of a subject access request

2.1.1 If any member of EY's Personnel receives a request from an individual for access to his or her personal data, they must first pass the communication to the Controller. If the EY Network entity is authorized to deal with such request directly or is required by law, they must then pass the communication to the Local Privacy Officer indicating the date on which the request was received together with any other information that may assist the Local Privacy Officer to deal with the request.

2.1.2 The request does not have to be official or mentioned as data protection law to qualify as a subject access request.

2.2 Initial steps

2.2.1 The Local Privacy Officer will make an initial assessment of the request to decide whether it is a valid request and whether confirmation of identity, or any further information, is required.

2.2.2 The Local Privacy Officer will then contact the individual in writing to confirm receipt of the subject access request, seek confirmation of identity or further information, if required, or decline the request if one of the exemptions to subject access applies.

2.3 Exemptions to subject access

2.3.1 A valid request may be refused on the following grounds:

a. Where the Controller instructs the EY Network entity not to deal with such request directly

b. If the refusal to provide the information is consistent with the data protection law within the jurisdiction in which that EY Network entity is located

Or

c. Where the subject access is not subject to European data protection law

2.4 The Search and the response

2.4.1 The Local Privacy Officer will arrange a search of all relevant electronic and paper-filing systems.

2.4.2 The Local Privacy Officer may refer any complex cases to the Area Privacy Officer or ultimately to the Global Privacy Officer for advice, particularly where the request includes information relating to third parties or where the release of personal data may prejudice commercial confidentiality or legal proceedings.

2.4.3 The information requested will be collated by the Local Privacy Officer into a readily understandable format (internal codes or identification numbers used at EY that correspond to personal data shall be translated before being disclosed). A covering letter will be prepared by the Local Privacy Officer, which includes information required to be provided in response to a subject access request.

2.4.4 Where the provision of the information in permanent form is not possible or would involve disproportionate effort, there is no obligation to provide a permanent copy of the information. The other information referred to in 1.4 above must still be provided. In such circumstances, the individual may be offered the opportunity to have access to the information by inspection or to receive the information in another form.

2.5 Requests for erasure, amendment, cessation of processing or to port information

2.5.1 If a request is received for the deletion of that individual's personal data, such a request must be considered and dealt with as appropriate by the Local Privacy Officer. If a request is received advising of a change in that individual's personal data, such information must

be rectified or updated accordingly if the EY Network entity is satisfied that there is a legitimate basis for doing so.

2.5.2 If the request is to cease processing that individual's personal data because the rights and freedoms of the individual are prejudiced by virtue of such processing by the EY Network entity, or on the basis of other compelling legitimate grounds, the matter will be referred by the Local Privacy Officer to the Area Privacy Officer and ultimately to the Global Privacy Officer to assess. Where the processing undertaken by the EY Network entity is required by law, the request will not be regarded as valid.

2.5.3 If a request is to receive personal data in a structured, commonly used and machine-readable format and to have that data transmitted to another controller, such a request must be considered and dealt with as appropriate by the Local Privacy Officer.

2.6 All queries relating to this procedure are to be addressed to the Local Privacy Officer.

Appendix 3

Assessment of Compliance Protocol

1. Background

1.1 The purpose of this Processor Policy is to safeguard personal data transferred between the EY Network entities where EY acts as a processor. This Processor Policy requires approval from the data protection authorities in the European member states from which the personal data is transferred. One of the requirements of the data protection authorities is that EY assesses compliance with this Processor Policy and satisfies certain conditions in so doing, and this Appendix describes how EY deals with such requirements.

1.2 One of the roles of the EY Global Privacy Officer and also the Area Privacy Officer is to provide guidance about the processing of personal data subject to this Processor Policy and to assess the processing of personal data by the EY Network entities for potential privacy-related risks. The processing of personal data with the potential for a significant privacy impact is, therefore, subject to detailed review and evaluation on an ongoing basis. Accordingly, although this Appendix describes the formal assessment process adopted by EY to ensure compliance with this Processor Policy as required by the data protection authorities, this is only one way in which EY ensures that the provisions of the Processor Policy are observed and corrective actions are taken as required.

2. Approach

2.1 Scope of assessment

2.1.1 The EY Global Risk Management function ("Risk Management") will be responsible for carrying out assessments of compliance with this Processor Policy and will ensure that such assessments address all aspects of this Processor Policy (including methods of ensuring that corrective actions will take place). The assessments will comprise a review of the performance of particular functions within the business and also an assessment of the EY Network entity adopting a risk-based approach. Risk Management will be responsible for ensuring that the results of the assessment are brought to the attention of EY's Global Privacy Officer who will ensure that any actions identified to implement this Processor Policy take place correctly. The Global Privacy Officer will ensure that any reports indicating unsatisfactory compliance in relation to the Processor Policy will be brought to the attention of the Global General Counsel who attends the meetings of the Global Executive.

2.1.2 EY Clients (or auditors acting on their behalf) may assess compliance with the commitments made in this Processor Policy in accordance with the terms of the relevant Client's contract with an EY Network entity. The assessment of compliance may consist of:

- The provision by EY of written information (including, without limitation, questionnaires, related independent SOC2 audit reports or reports of a similar nature and information security policies) that may include information relating to sub-processors

  Or

- Interviews with EY's IT personnel

2.1.3 EY will not provide a Client with access to any part of IT systems or infrastructure which process personal data of other Clients.

2.2 Timing

2.2.1 Review of compliance with the global privacy program, including the Processor Policy, will take place on a regular basis at the instigation of Risk Management and as required by the terms of the relevant Client's contract with EY. The scope of the compliance assessment

will be decided by EY's independent Global Internal Audit team with input from the Global General Counsel's Office.

2.3 Auditors

2.3.1 Review of compliance with this Processor Policy will be undertaken by Risk Management and responsibility for compliance with this Processor Policy on a day-to-day basis will be undertaken by EY's Global Privacy Officer and the Area Privacy Officers.

2.3.2 In the event that a Client exercises its right to assess EY for compliance with this Processor Policy, such assessment may be undertaken by that Client, or by independent and suitably experienced auditors selected by that Client, as required and defined by the terms of the relevant Client's contract with an EY Network entity.

2.4 Report

2.4.1 Upon request and subject to applicable law and respect for the confidentiality and trade secrets of the information provided, EY will:

a. Provide copies of the results of any assessment of compliance with the Processor Policy to the competent European data protection authority

b. Provide a copy of the results to the Client, to the extent that an assessment relates to personal data EY processes on behalf of that Client

2.4.2 EY will also provide a copy of the results of any assessment of compliance to EY's Global Privacy Officer who will be responsible for liaising with the European data protection authorities for this purpose. In addition, EY has agreed that in accordance with the provisions of clause 5 of the Cooperation Procedure,[9] data protection authorities may assess compliance by EY with this Processor Policy. EY's Global Privacy Officer will also be responsible for liaising with the European data protection authorities for this purpose.

[9]Clause 5 states: Where any EY Network entity is located within the jurisdiction of a data protection authority based in Europe, EY agrees that that data protection authority may audit that EY Network entity for the purpose of reviewing compliance with the BCR, in accordance with the applicable law of the country in which the EY Network entity is located, or, in the case of an EY Network entity located outside Europe, in accordance with the applicable law of the European country from which the personal data is transferred under the BCR, on giving reasonable prior notice and during business hours, with full respect to the confidentiality of the information obtained and to the trade secrets of EY.

Appendix 4

Complaint Handling Procedure

1. Background

1.1 This Processor Policy safeguards personal data transferred between EY Network entities where such entity acts as a processor. The content of this Processor Policy is determined by the data protection authorities in the European member states from which the personal data is transferred and one of their requirements is that EY must have a Complaint Handling Procedure in place. The purpose of this procedure is to explain how complaints brought by an individual whose personal data is processed by EY under this Processor Policy are dealt with.

2. How individuals can bring complaints

2.1 Individuals can bring complaints in writing by contacting the General Counsel's Office ("GCO") or the Global Privacy Officer, 6 More London Place, London, SE1 2DA, or via email at global.data.protection@ey.com.

2.2 Where a complaint relates to the processing of personal data by EY acting as a processor, EY will communicate the details of the complaint to the Controller promptly and will act in accordance with the terms of the contract or other binding document between the Controller and EY. If the Controller requires EY to deal with the complaint, the below mentioned steps will be applicable.

2.3 In circumstances where a Controller has disappeared, no longer exists or has become insolvent, individuals whose personal data is processed by EY on behalf of that Controller have the right to complain to the EY Network entity that is processing the data. EY will deal with such complaints in accordance with the below mentioned steps.

3. Who handles complaints?

3.1 The local GCO or Regional or Local Privacy Officer will handle all complaints arising under the Processor Policy in conjunction with executive leadership and the Global Privacy Officer, and will liaise with colleagues from relevant business and support units as appropriate to deal with complaints.

4. What is the response time?

4.1 The local GCO or Regional or Local Privacy Officer will acknowledge receipt of a complaint to the individual concerned within five working days (after having received confirmation from the Controller that it requires EY to deal with the complaint), investigating and making a substantive response within one month. If, due to the complexity of the complaint, a substantive response cannot be given within this period, the local GCO or Regional or Local Privacy Officer will advise the complainant accordingly and provide a reasonable estimate for the timescale within which a response will be provided, which will not exceed six months from the date the complaint was brought.

4.2 The response will indicate whether the complaint is considered justified or whether it is rejected, as well as the consequences of such response.

5. When a complainant disputes a finding

5.1 If the complainant disputes the response (or any aspect of a finding) of the local GCO or Regional or Local Privacy Officer, the complainant notifies the local GCO or Regional or Local Privacy Officer accordingly. The matter will then be referred to the Region or Area GCO contact or ultimately to the Global Privacy Officer as appropriate who will review the case and advise the complainant of his or her decision either to accept the original finding or to substitute a new finding. The Region, Area GCO contact or Global Privacy Officer will respond to the complainant within one month of the referral. As part of the review, the Region or Area GCO contact or Global Privacy Officer may arrange to meet the parties in an attempt to resolve the complaint. If, due to the complexity of the complaint, a substantive response cannot be given within this period, the Region, Area GCO contact or Global Privacy Officer will advise the complainant accordingly and

provide a reasonable estimate for the timescale within which a response will be provided, which will not exceed three months from the date the complaint was referred.

5.2 If the complaint is upheld, the EY Region or Area GCO contact or Global Privacy Officer will arrange for any necessary steps to be taken as a consequence.

6. Right to complain to a European data protection authority and to lodge an application with a court of competent jurisdiction

6.1 In addition to the right to bring a claim to EY in accordance with this Complaint Handling Procedure, individuals whose personal data is processed in accordance with European data protection law have the right to complain to a European data protection authority and to lodge an application with a court of competent jurisdiction. This also applies if the individual is not satisfied with the way in which the complaint relating to this Processor Policy has been resolved by EY.

Appendix 5

Cooperation Procedure

1. This Cooperation Procedure sets out the way in which EY will cooperate with the European data protection authorities in relation to this Processor Policy.
2. Where required, EY will make the necessary personnel available for dialogue with a European data protection authority in relation to this Processor Policy.
3. EY will actively review and consider:
   - Any decisions made by relevant European data protection authorities on any data protection law issues that may affect the Processor Policy
   - The views of the Article 29 Working Party as outlined in its published guidance on Binding Corporate Rules for Processors
4. EY will provide upon request copies of the results of any assessment of compliance of the Processor Policy to a European data protection authority of competent jurisdiction subject to applicable law and respect for the confidentiality and trade secrets of the information provided.
5. EY agrees that:
   - Where any EY Network entity is located within the jurisdiction of a data protection authority based in Europe, that data protection authority may audit that EY Network entity for the purpose of reviewing compliance with this Processor Policy, in accordance with the applicable law of the country in which the EY Network entity is located, or, in the case of an EY Network entity located outside Europe, in accordance with the applicable law of the European country from which the personal data is transferred under this Processor Policy.
   - Where any EY Network entity is processing personal data on behalf of a Controller located within the jurisdiction of a data protection authority based in Europe, that data protection authority may audit that EY Network entity for the purpose of reviewing compliance with this Processor Policy, in accordance with the applicable law of the country in which the Controller is located on giving reasonable prior notice and during business hours, with full respect to the confidentiality of the information obtained and to the trade secrets of EY.
6. EY agrees to abide by a formal decision of the applicable data protection authority where a right to appeal is not exercised on any issues related to the interpretation and application of this Processor Policy.

Appendix 6

Updating Procedure

1. Background

1.1 This Updating Procedure sets out the way in which EY will communicate changes to this Processor Policy to the European data protection authorities, Controllers, data subjects and to the EY Network entities bound by this Processor Policy.

2. Material changes

2.1 EY will communicate in advance any material changes to this Processor Policy to the Information Commissioner's Office ("ICO") and any other relevant European data protection authorities as soon as reasonably practicable.

2.2 Where a change to this Processor Policy materially affects the conditions under which EY processes personal data on behalf of a Controller under the terms of the contract or other binding document EY has with that Controller, EY will communicate the proposed change to the Controller before it is implemented, and with sufficient notice to enable the affected Controller to object. The Controller may then suspend the transfer of personal data to EY and terminate its relationship with EY, in accordance with the terms of its contract or other binding document with EY.

3. Administrative changes

3.1 EY will communicate changes to this Processor Policy, which are administrative in nature (including changes in the list of EY Network entities) or which have occurred as a result of a change of applicable data protection law in any European country, through any legislative, court or supervisory authority measure, to the ICO and other relevant data protection authorities at least once a year. EY will also provide a brief explanation of the reasons for any notified changes to this Processor Policy.

4. Communicating changes to the Processor Policy

4.1 EY will communicate all changes to this Processor Policy, whether administrative or material in nature, to the EY Network entities bound by this Processor Policy, and material changes to the Controller and data subjects who benefit from this Processor Policy.

4.2 Communication internally will be via the EY internal communications process which comes from the EY Global Leader, Risk Management and the EY Global Vice Chair and General Counsel, cascading down to the Area Privacy Officers, Regional Privacy Officers and General Counsel's Offices, and Local Privacy Officers and Local General Counsel's Offices. Such communication includes publication on EY's intranet and on EY's external site: ey.com/bcr.

4.3 EY will communicate to the ICO any substantial changes to the list of EY Network entities once a year. Otherwise, EY will communicate an up-to-date list of entities to the ICO and any other relevant European data protection authorities when required.

5. Logging changes to the Processor Policy

5.1 This Processor Policy contains a change log which sets out the date on which this Processor Policy is revised and the details of any revisions that have been made.

5.2 The Global Privacy Officer will maintain an up-to-date list of the EY Network entities this Processor Policy is applicable to. EY will ensure that all new EY Network entities are bound by this Processor Policy before a transfer of personal data to them takes place. Each EY Network entity will maintain an up-to-date list of all sub-processors it has appointed to process personal data on behalf of a Controller.

Appendix 7

Privacy Training Program

1. Background

1.1 EY trains EY Personnel on the basic principles of data protection, confidentiality and information security awareness. Training and awareness will be provided through posting messages and videos on EY's intranet and daily news articles, as well as by making available web-based training courses.

1.2 EY Personnel who have permanent or regular access to personal data, and who are involved in the processing of personal data or in the development of tools to process personal data receive additional, tailored training on the Policies and specific data protection issues relevant to their role. This web-based training is further described below.

2. Responsibility for the privacy training program

2.1 EY's Global Privacy Officer has overall responsibility for privacy training at EY, with input from colleagues from other functional areas, including Information Security, Talent and other departments, as appropriate. They will review training from time to time to ensure it addresses all relevant aspects of the Processor Policy and that it is appropriate for individuals who have permanent or regular access to personal data, and who are involved in the processing of personal data or in the development of tools to process personal data.

2.2 Communication and training should cover data privacy elements such as:

- Basic principles
- Importance of data privacy
- Definitions
- Personal and sensitive personal data
- Data privacy considerations with respect to information security

3. About the training courses

3.1 EY has developed a global Web-Based Learning (WBL) that is available for all EY Personnel. The course is designed to be both informative and user-friendly, generating interest in the topics covered. At the end of the WBL, EY Personnel must correctly answer a series of multiple choice questions for the course to be deemed complete.

3.2 The WBL starts with asking a member of EY Personnel what his or her area of work (marketing, human resources, information technology or other) is and whether he or she manages other members of EY Personnel. Depending on the choices being made, the WBL will provide relevant information.

3.3 EY management supports the completion of the WBL and is responsible for ensuring that individuals within the organization are given appropriate time to complete the course. Local management determines which members of EY Personnel in their respective country will be mandated to complete the WBL. Compliance will be monitored. New hires are required to complete the training as part of their induction program.

4. Awareness

4.1 EY will regularly provide reinforcement content to EY Personnel reminding them of their responsibilities regarding data protection, confidentiality and information security awareness. Such content will be provided through posting messages and videos on EY's intranet, posters in EY network entities' offices and daily news emails provided to all EY Personnel.

Appendix 8

Law Enforcement Data Access Procedure

1. Background

1.1 This Law Enforcement Data Access Procedure sets out EY's policy for responding to a request received from a law enforcement or other government authority (together the "**Requesting Authority**") to disclose personal data processed by EY on behalf of a Controller (hereafter "**Data Production Request**"). Where EY receives a Data Production Request, it will handle that Data Protection Request in accordance with this Procedure. If applicable data protection law(s) require a higher standard of protection for personal data than is required by this Procedure, EY will comply with the relevant requirements of applicable data protection law(s).

2. General principle on Data Production Requests

2.1 As a general principle, EY does not disclose personal data in response to a Data Production Request unless either:

- It is under a compelling legal obligation to make such disclosure

  Or

- Taking into account the circumstances and the privacy rights of any affected individuals, there is an imminent risk of serious harm that merits disclosure in any event

2.2 Even where disclosure is required, EY's policy is that the Controller should have the opportunity to protect the personal data requested because it has the greatest interest in opposing, or is in the better position to comply with, a Data Production Request.

2.3 For that reason, unless it is legally compelled to do so or there is an imminent risk of serious harm, EY will first consult with the competent data protection authorities and provide the Controller with details of the Data Production Request. EY will cooperate with the competent data protection authorities and the Controller to address the Data Production Request.

3. Data Production Request Review

3.1 If EY receives a Data Production Request, the recipient of the request must pass it to EY's Regional or Local Privacy Officer and Regional or Local General Counsel immediately upon receipt, indicating the date on which it was received together with any other information which may assist EY's Regional or Local Privacy Officer and Regional or Local General Counsel to deal with the request.

3.2 The request does not have to be made in writing, made under a Court order, or mention data protection law to qualify as a Data Production Request.

3.3 EY's Regional or Local Privacy Officer and Regional or Local General Counsel will carefully review each and every Data Production Request individually and on a case-by-case basis, and will deal with the request to determine the nature, urgency, scope and validity of the Data Production Request under applicable laws and to identify whether action may be needed to challenge the Data Production Request.

4. Notice of a Data Production Request

4.1 After assessing the nature, urgency, scope and validity of the Data Protection Request, EY will notify and provide the Controller with the details of the Data Production Request prior to disclosing any personal data, unless legally prohibited or where the imminent risk of serious harm prohibits prior notification.

4.2 EY will also put the request on hold in order to notify and consult with the competent data protection authorities, unless legally prohibited or where the imminent risk of serious harm prohibits prior notification.

4.3 Where EY is prohibited from notifying the competent data protection authorities and suspending the request, EY will use its best efforts (taking into account the nature, urgency, scope and validity of the request) to inform the Requesting Authority about its obligations under applicable data protection law(s) and to obtain the right to waive this prohibition. Such efforts may include asking the Requesting Authority to put the request on hold so that EY can consult with its competent data protection authorities and may also, in appropriate circumstances, include seeking a court order to this effect. EY will maintain a written record of the efforts it takes.

5. Transparency reports

5.1 In cases where EY is prohibited from notifying the competent data protection authorities about a Data Production Request, it commits to providing the competent data protection authorities with a confidential annual report (i.e., "Transparency Report"), which reflects to the extent permitted by applicable laws, the number and type of Data Production Requests it has received for the preceding year and the Requesting Authorities who made those requests.

6. Queries

6.1 All queries relating to this Procedure are to be addressed to EY's Global Privacy Officer at global.data.protection@ey.com.

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

EYG no. 02376-183GBL
ED None

ey.com