EY
Data Protection Binding Corporate Rules Controller Policy

30 September2020

Building a better working world

Table of contents

Introduction to the Data Protection Binding Corporate Rules Controller Policy **3**

Part I: Background and actions **4**

Part II: The Rules **6**

PART III: Appendices **12**

Appendix 1 12

Data privacy roles and responsibilities 12

Appendix 2 15

Subject Access Request Procedure 15

Appendix 3 18

Assessment of Compliance Protocol 18

Appendix 4 20

Complaint Handling Procedure 20

Appendix 5 22

Cooperation Procedure 22

Appendix 6 23

Updating Procedure 23

Appendix 7 24

Privacy Training Program 24

Introduction to the Data Protection Binding Corporate Rules Controller 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, and sets 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 Controller Policy ("**Controller Policy**"). In this Controller 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 Controller 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 established in the European Union acting as controllers to EY Network entities established outside the European Union acting as controllers or 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 Controller Policy when processing[5] personal data as a controller, irrespective of the country in which they are located.

This Controller Policy contains 16 rules ("**Rules**"), which govern the processing of personal data of current, past and prospective EY Personnel, clients, suppliers, subcontractors and any other third parties ("**EY Data**").

This Controller 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.

This Controller 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 Controller 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 external clients who are bound by the Controller 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, 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 a controller (either an external client or another EY Network entity). For services where EY is acting as a processor for non-EY Network Entities, EY shall comply with the Data Protection Binding Corporate Rules Processor Policy ("**Processor Policy**") as published on ey.com/bcr. For services where an EY Network Entity acts as a controller in relation to another EY Network entity acting as controller or as 'internal processor', this Controller 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 supervisory authorities as providing an adequate level of protection for individuals' data privacy rights.

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 Controller 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.

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

Central to this BCR are 16 Rules based on, and interpreted in accordance with, relevant European data protection standards that must be followed by EY Personnel when handling personal data. All Member Firms are bound to comply with this BCR as a result of becoming a member of EYG by way of signing the joining agreement. By signing the joining agreement Member Firms are subject to: (i) comply with; and (ii) ensure other EY Network entities comply with all common standards, methodologies and policies of EY which are set out in the EYG Regulations. This Controller Policy is part of one of the common standards specifically mentioned in the EYG Regulations.

Compliance with the Controller Policy must be confirmed annually by EY Network Entities to their respective Area Privacy Leader. The Area Privacy Leader must communicate the results of the EY Network entity annual compliance confirmation to the Global Privacy Leader.

All EY Network entities who process personal data in their capacity as a controller must comply with the Rules set out in **Part II** of this Controller Policy together with the policies and procedures set out in the appendices in **Part III** of this 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 data controller and transferred to an EY Network

[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.

entity outside Europe under the Controller Policy have certain rights. These individuals may enforce the Rules set out in this Controller Policy as third party beneficiaries.

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 Controller Policy) and/or to a European supervisory authority in the jurisdiction of the EY Network entity responsible for exporting the data outside Europe.
- **Liability**: Individuals may bring proceedings to enforce compliance with this Policy 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 Controller 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 Controller Policy in accordance with the determination of a court or other competent authority.
- **Transparency**: Individuals may obtain a copy of this Controller Policy from the EY Network entity responsible for exporting the data outside Europe or any other EY Network entity by accessing the Controller 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 Controller Policy, EY has agreed that the burden of proof to show that 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 Leader[8] is the person who has overall responsibility for ensuring compliance with the Controller Policy and any other supporting policies and procedures.

Area Privacy Leaders are responsible for overseeing compliance with this Controller 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 Controller Policy, your rights under this Controller Policy or any other data privacy issues you may contact the EY Global Privacy Leader 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 Leader

Email: global.data.protection@ey.com

Address: Office of the General Counsel (GCO), 6 More London Place, London, SE1 2DA

The Global Privacy Leader is responsible for ensuring that changes to this Controller 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.

[8] At present EY's Global Lead Counsel Privacy and Security serves as the Global Privacy Leader as referenced in the BCRs.

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 controller.

Section B deals with the practical commitments made by EY to the competent supervisory authority (the "Autoriteit Persoonsgegevens" in the Netherlands) in connection with this Controller Policy.

Section A

Rule 1 – Compliance with local law

Rule 1 – 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 controller 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 Controller Policy.

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

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

Rule 2A – EY will *explain to individuals*, at the time their personal data is collected, how that data will be processed.

EY will ensure that individuals are told in a clear and comprehensive way (usually by means of a fair processing statement) about the uses and disclosures made of their data (including the secondary uses and disclosures of the data), the recipients or categories of recipients of the personal data and the identity of the data controller when such data is obtained by EY from the individual, or, if not practicable to do so at the point of collection, as soon as possible after that.

Where EY obtains an individual's personal data from a source other than that individual, EY will provide this information to the individual when their personal data is first recorded or, if it is to be disclosed to a third party, no later than the time when the data is first disclosed.

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 defence, for the prevention or detection of crime, taxation purposes, legal proceedings or where otherwise permitted by law.

Rule 2B – EY will only process personal data for those purposes which are *known to the individual* or which are *within their expectations* and are *relevant to EY.*

This rule means that EY will identify and make known the purposes for which personal data will be used (including the secondary uses and disclosures of the data) when such data is obtained or, if not practicable to do so at the point of collection, as soon as possible after that, unless there is a legitimate basis for not doing so as described in Rule 2A.

Rule 2C – EY may only process personal data collected in Europe for a different or new purpose if EY has a legitimate basis for doing so, consistent with the applicable law of the European country in which the personal data was collected.

If EY collects personal data for a specific purpose (as communicated to the individual via the relevant fair processing statement) and subsequently EY wishes to process the data for a different or new purpose, the relevant individuals will be made aware of such a change unless:

- It is within their expectations and they can express their concerns

Or

- There is a legitimate basis for not doing so, as described in Rule 2A above

In certain cases, for example, where the processing is of sensitive personal data, or EY is not satisfied that the processing is within the reasonable expectation of an individual, the individual's consent to the new uses or disclosures may be necessary.

Rule 3 — Ensuring data quality

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

In order to ensure that the personal data held by EY is accurate and up to date, EY actively encourages individuals to inform EY when their personal data changes.

Rule 3B — EY will only keep personal data in a form which permits identification for *as long as is necessary*.

Personal data will always be retained and/or deleted to the extent required by law, regulation and professional standards and in line with the applicable EY global service line and any local retention policies applying to that EY Network entity. The EY Network entity will dispose of personal data only in a secure manner in accordance with EY global security policies.

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 properly to 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*.

EY will comply with the requirements contained in EY global security policies as revised and updated from time to time together with any other security procedures relevant to a business area or function.

The technical and organizational security measures as implemented by EY will be designed to implement data protection principles and to facilitate compliance with data protection by design and by default.

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 (e.g., a payroll provider), 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 proportionate technical and organizational security measures to safeguard the personal data.

Rule 4C — EY will notify any personal data breach in accordance with and to the extent required by applicable law.

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 supervisory authority without undue delay after becoming aware of the personal data breach.

Rule 4D — Where an EY Network entity *processes personal data as a service provider,* that EY Network entity will adhere to Rule 4A and act only on the instructions of the data controller on whose behalf the processing is carried out.

Where a service provider is an EY Network entity processing personal data on behalf of another EY Network entity as a data controller, the service provider must act only on the instructions of the data controller on whose behalf the processing is carried out and ensure that it has in place proportionate technical and organizational security measures to safeguard the personal data.

Rule 5 — Honoring individuals' rights

Rule 5A — EY will adhere to the *Individual's Rights Request Procedure* and will respond to any queries or requests made by individuals in connection with their personal data in accordance with applicable law.

Individuals may ask EY (by making a written request to EY) to provide them with access to, and a copy of, any personal data EY holds about them (including both electronic and paper records). EY will follow the steps set out in the Individual's Rights Request Procedure (see Appendix 2) when dealing with.

Rule 5B — EY will deal with requests to rectify, restrict the processing of personal data, receive data in a machine-readable format or to object to the processing of personal data in accordance with the *Individual's Rights Request Procedure*.

Rule 6 — Ensuring adequate protection for international transfers

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

In principle, international transfers of personal data to third parties outside EY are not allowed without appropriate steps being taken, such as signing up to contractual clauses, which will protect the personal data being transferred.

Rule 7 — Safeguarding the use of sensitive personal data

Rule 7A — EY will only process sensitive personal data if it is *absolutely necessary* to use it.

"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, 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:

- 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

Rule 7B — EY will only process sensitive personal data where the individual's *explicit consent* has been obtained unless EY has a legitimate basis for doing so consistent with the requirements of applicable data protection laws in accordance with Rule 1.

In principle, individuals must give their explicit consent to the processing of their sensitive personal data by EY unless EY has a legitimate basis for doing so. Consent to process sensitive personal data by EY must be specific, informed, unambiguous and freely given.

Rule 8 — Legitimizing direct marketing

Rule 8A — EY will allow customers to *opt out* of receiving marketing data.

Individuals have the right to object to the use of their personal data for direct marketing purposes and EY will honor all such opt-out requests.

Rule 8B — EY will *suppress* from marketing initiatives the personal data of individuals who have opted out of receiving marketing data.

EY will take all necessary steps to prevent the sending of marketing materials to individuals who have opted out.

Rule 9 — Automated individual decisions

Rule 9 —Individuals have the right not to be subject to a decision made 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 take 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 individual's 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 undertake any reasonably necessary measures to comply with its duty to inform individuals.

Section B — Practical commitments

Rule 10 — Training

Rule 10 — 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 Controller Policy in accordance with the Privacy Training Program set out in Appendix 7. The Global Privacy Leader will provide foundational training materials in this regard for EY Network entities to deliver as appropriate. In addition, EY Personnel within an EY Network entity should be made aware of their obligations relating to data privacy under the Global Code of Conduct.

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
- Consultation and resources.

Rule 11 — Records of processing and data protection impact assessments

Rule 11 — EY will keep a record of categories of processing activities carried out. Processing activities likely to result in a high risk to the rights and freedoms of natural persons will be subject to a data protection impact assessment.

EY Network entities keep a record of processing activities. This record will be in writing, including in

electronic form, and will be made available to supervisory authorities on request.

Processing operations that are likely to result in a high risk to the rights and freedoms of natural persons will be subject to a data protection impact assessment. Where such data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the EY Network entity to mitigate the risk, the supervisory authority, prior to processing, will be consulted.

Rule 12 – Assessment of compliance

Rule 12 – EY will comply with the *Assessment of Compliance Protocol* set out in *Appendix 3*.

Rule 13 – Complaint handling

Rule 13 – EY will comply with the *Complaint Handling Procedure* set out in *Appendix 4*.

Rule 14 – Cooperation with supervisory authorities

Rule 14 – EY will comply with the *Cooperation Procedure* set out in *Appendix 5*.

Rule 15 – Update of the rules

Rule 15 – EY will comply with the *Updating Procedure* set out in *Appendix 6*.

Rule 16 – Actions in case of national legislation preventing respect for the Controller Policy

Rule 16A – EY will ensure that where it has reason to believe that existing or future *legislation applicable to it prevents it from fulfilling its obligations under the Controller Policy* or such legislation has a *substantial effect on its ability to comply with the Controller Policy*, EY will promptly inform the Global Privacy Leader unless otherwise prohibited by a law enforcement authority.

Rule 16B – EY will ensure that where there is a conflict between the national law and this Controller Policy, the Global Privacy Leader will take a responsible decision on the action to take and will consult the supervisory authority with competent jurisdiction in case of doubt.

Where an EY Network entity is subject to a legal requirement that is likely to have a substantial adverse effect on the obligations in this Controller Policy, the EY Global Privacy Leader will report this to the Autoriteit Persoonsgegevens. This includes any legally binding request for disclosure of personal data by a law enforcement authority or state security body.

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 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 Autoriteit Persoonsgegevens to disclosing the data to the requesting authority. EY shall clearly inform the Autoriteit Persoonsgegevens 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 Autoriteit Persoonsgegevens 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 Autoriteit Persoonsgegevens (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.

Transfers of personal data by an EY Network entity to any public authority will never be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

PART III: Appendices

Appendix 1

Data protection roles and responsibilities

Data Protection Network

1. EY Global Privacy Leader

1.1 The EY Global Privacy Leader 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's global systems with applicable data protection rules including the Processor Policy and this Controller Policy (analysis of systems, definition of actions, ongoing compliance)
- Coordinating a community of EY Area Privacy Leaders (see below) for the purpose of competency building, collaboration on implementation of and revisions as necessary to the global privacy program (including the Controller Policy and Processor 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 Leaders, overseeing the compliance of EY Network entities with the global privacy program (including the Processor Policy and this Controller Policy)
- With the assistance of the Area Privacy Leaders, developing and providing communications and uniform training material and support
- With the assistance of the Area Privacy Leaders, providing guidance to EY Network entities in implementing and modifying local data privacy policies and compliance programs

2. Area Privacy Leaders

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

- Providing assistance to Regional Privacy Leaders and Local Privacy Leaders to identify local business, and legal and regulatory risks surrounding data privacy issues
- Providing assistance to Regional Privacy Leaders and Local Privacy Leaders 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 Processor Policy and this Controller 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 Leader 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 Controller Policy)
- Confirming to the EY Global Privacy Leader, EY Network entity compliance with the global privacy program and, in particular, the Controller Policy
- Collaborating relevant Talent, Risk Management, General Counsel and IT teams, service lines and other functions on data privacy matters
- Periodically monitoring the effectiveness of the Area Privacy functions

3. Regional / Local Privacy Leaders

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

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

Data Protection Officers

1.1 EY Network entities that are subject to the EU General Data Protection Regulation ("GDPR") shall designate a Data Protection Officer ("DPO") where they have determined that 1) its core activities consist of processing operations which require regular and systematic monitoring of individuals on a large scale; or 2) the core activities consist of processing on a large scale of sensitive personal data (Rule 7A) and personal data relating to criminal convictions and offences.

1.2 Various EY Network entities may appoint one DPO, for example a DPO acting on behalf of all EY Network entities in one Region.

1.3 The DPO may be the same person as the Regional or Local Privacy Leader but the role may also be undertaken by a separate individual.

1.4 Where a DPO is acting on behalf of multiple EY Network entities, such EY Network entity will appoint a Local Privacy Leader who will assist the DPO in the exercise of its responsibilities. The DPO may delegate its responsibilities to the Local Privacy Leader who may perform these responsibilities under supervision and on behalf of the DPO.

1.5 A DPO will have the following responsibilities:

- Informing and advising the EY Network entity and EY Personnel with respect to obligations under the GDPR and other EU data protection provisions;
- Monitoring the EY Network Entity's compliance with the GDPR and other EU data protection provisions, the regulations of Ernst & Young Global Limited insofar as they relate to the protection of personal data and any other applicable policies in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of EY Personnel and conducting and/or arranging for internal audits as appropriate;
- When requested, advising on data protection impact assessments;
- Working and cooperating with the EY Network Entity's designated representative where applicable and serving as the contact point for the representative on issues relating to the processing of personal data;

- Being available to respond to inquiries from individuals relating to data protection practices and data subjects' rights, including withdrawal of consent, the right to be forgotten, and related rights;
- Assisting in the developing and monitoring of local procedures for personal data breach handling, and being available as a first point of contact to assist with responding to any breaches of personal data, including assessing whether the data breach must be notified to supervisory authorities and/or individuals;
- Keeping up-to-date the EY Network Entity's record of processing;
- Keeping up-to-date its in-depth knowledge of the GDPR, including GDPR guidance issued by supervisory authorities and relevant legal decisions that may impact the EY Network Entity's processing of personal data;
- Providing an annual report for the EY Network Entity's leadership (as applicable).

1.6 The DPO may fulfill other tasks and duties, provided such tasks and duties do not result in a conflict of interests.

1.7 EY will publish the contact details of EY Network Entities' DPOs on EY's website ey.com.

Appendix 2

Individual's Rights 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 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 Individual's Rights Request Procedure (referred to as "**valid request**"). A subject access request is subject to European data protection law where the EY Network entity 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 Individual's Rights Request Procedure, the local data protection law will prevail.

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

1.3.1 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

1.3.2 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

1.3.3 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

1.4 The request must be made in writing[9], 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.

1.5 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.

1.6 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 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 Personnel receives a request from an individual for access to his or her personal data, they must pass the communication to the Local Privacy Leader and DPO (where applicable) upon receipt indicating the date on which the request was received

[9] 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.

together with any other information that may assist the Local Privacy Leader and DPO (where applicable) to deal with the request.

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

2.2 Initial steps

2.2.1 The Local Privacy Leader and DPO (where applicable) 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 Leader and DPO (where applicable) 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. 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

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

2.4 The Search and the response

2.4.1 The Local Privacy Leader and DPO (where applicable) will arrange a search of all relevant electronic and paper filing systems.

2.4.2 The Local Privacy Leader and DPO (where applicable) may refer any complex cases to the Area Privacy Leader or ultimately to the Global Privacy Leader 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 Leader or DPO (where applicable) 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 Leader or DPO (where applicable), 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 1.3 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 Leader or DPO (where applicable). 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 Leader or DPO (where applicable) to the Area Privacy Leader and ultimately to the Global Privacy Leader 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 Leader or DPO (where applicable).

2.6 All queries relating to this procedure are to be addressed to the Local Privacy Leader or DPO (where applicable).

Appendix 3

Assessment of Compliance Protocol

1. Background

1.1 The purpose of this Controller Policy is to safeguard personal data transferred between the EY Network entities. This Controller Policy requires approval from the supervisory authorities in the European Member States from which the personal data is transferred. One of the requirements of the supervisory authorities is that EY assesses compliance with this Controller Policy and satisfies certain conditions in so doing, and this document describes how EY deals with such requirements.

1.2 One of the roles of the EY Global Privacy Leader and also the Area Privacy Leader is to provide guidance about the processing of personal data subject to this Controller 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 Controller Policy as required by the supervisory authorities, this is only one way in which EY ensures that the provisions of the Controller Policy are observed and corrective actions 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 Controller Policy and will ensure that such assessments address all aspects of this Controller Policy. 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 the EY Global Privacy Leader who will ensure that any actions identified to implement the Controller Policy take place correctly. The Global Privacy Leader will ensure that any reports indicating unsatisfactory compliance in relation to this Controller Policy will be brought to the attention of the Global General Counsel who attends the meetings of the Global Executive.

2.2 Timing

2.2.1 Review of compliance with the global privacy program, including this Controller Policy will take place on a regular basis at the instigation of Risk Management. 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 Controller Policy will be undertaken by Risk Management and responsibility for compliance with this Controller Policy on a day-to-day basis will be undertaken by the EY Global Privacy Leader and the Area Privacy Leader.

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 provide copies of the results of any assessment of compliance with the Controller Policy to the competent European supervisory authority.

2.4.2 EY will also provide a copy of the results of any assessment of compliance to the EY Global Privacy Leader who will be responsible for liaising with the European supervisory authorities for this purpose. In addition, EY has agreed that in accordance with the provisions of clause

5 of the Cooperation Procedure,[10] supervisory authorities may assess compliance by EY with this Controller Policy. The EY Global Privacy Leader will also be responsible for liaising with the European supervisory authorities for this purpose.

[10]Clause 5 states: Where any EY Network entity is located within the jurisdiction of a supervisory authority based in Europe, EY agrees that that supervisory 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 Controller Policy safeguards personal data transferred between EY Network entities where such entity acts as a controller. The content of this Controller Policy is determined by the supervisory 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 the Controller 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 Leader at 6 More London Place, London, SE1 2DA or via email at global.data.protection@ey.com.

3. Who handles complaints?

3.1 The local GCO or Regional or Local Privacy Leader will handle all complaints arising under the Controller Policy in conjunction with executive leadership and the Global Privacy Leader 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 Leader will acknowledge receipt of a complaint to the individual concerned within five working days, 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 Leader 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/Local Privacy Leader, the complainant notifies the local GCO or Regional or Local Privacy Leader accordingly. The matter will then be referred to the Region or Area GCO contact or ultimately to the Global Privacy Leader 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 Leader will respond to the complainant within one month of the referral. As part of the review the Region, Area GCO contact or Global Privacy Leader 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 Leader 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, Area GCO contact or Global Privacy Leader will arrange for any necessary steps to be taken as a consequence.

6. Right to complain to a European supervisory 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 supervisory 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 Controller Policy has been resolved by EY.

Appendix 5

Cooperation Procedure

1. This Cooperation Procedure sets out the way in which EY will co-operate with the European supervisory authorities in relation to this Controller Policy.
2. Where required, EY will make the necessary personnel available for dialogue with a European supervisory authority in relation to this Controller Policy.
3. EY will actively review and consider:
   - Any decisions made by relevant European supervisory authorities on any data protection law issues that may affect the Controller Policy
   - The views of the Article 29 Working Party (or European data protection board) as outlined in its published guidance on Binding Corporate Rules for Controllers
4. EY will provide upon request copies of the results of any assessment of compliance of this Controller Policy to a European supervisory 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 supervisory authority based in Europe, that supervisory authority may audit that EY Network entity for the purpose of reviewing compliance with this Controller 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 Controller Policy, 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 supervisory authority where a right to appeal is not exercised on any issues related to the interpretation and application of this Controller Policy.

Appendix 6

Updating Procedure

1. Background

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

2. Material changes

2.1 EY will communicate in advance any material changes to this Controller Policy to the Autoriteit Persoonsgegevens and any other relevant European supervisory authorities as soon as reasonably practicable.

3. Administrative changes

3.1 EY will communicate changes to this Controller 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 Autoriteit Persoonsgegevens and other relevant supervisory authorities at least once a year. EY will also provide a brief explanation of the reasons for any notified changes to this Controller Policy.

4. Communicating changes to the Controller Policy

4.1 EY will communicate all changes to this Controller Policy, whether administrative or material in nature, to the EY Network entities bound by this Controller Policy, and material changes to the data subjects who benefit from this Controller 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 Autoriteit Persoonsgegevens 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 Autoriteit Persoonsgegevens and any other relevant European supervisory authorities when required.

5. Logging changes to the Controller Policy

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

5.2 The Global Privacy Leader will maintain an up-to-date list of the EY Network entities this Controller Policy is applicable to. EY will ensure that all new EY Network entities are bound by this Controller Policy before a transfer of personal data to them takes place.

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 The EY Global Privacy Leader 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 Controller 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 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.

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. 010398-18Gbl
BCR no. 2862
ED None

ey.com