GLOBAL PRIVACY POLICY

BINDING CORPORATE RULES FOR CONTROLLERS

CONTENTS

1. INTRODUCTION

BDO is an international network of public accounting, tax and advisory firms which perform professional services under the name of BDO. Each BDO Member Firm is a member of BDO International Limited, a UK company limited by guarantee, either as a voting or non-voting member.

Service provision within the international BDO network of independent member firms is coordinated by Brussels Worldwide Services BV ('**BWS**'), a limited liability company incorporated in Belgium with its statutory seat in Zaventem, where the BDO Global Office is located.

The BDO network is governed by the Council, the Global Board and the Executive of BDO International Limited.

The BDO network (‘**BDO**’) is committed to respect and to appropriately protect personal data it processes, including where it shares the data with others.

This BDO Global Privacy Policy (‘**Policy**’) forms part of BDO’s Standards and Policies. It establishes the approach taken by BDO to the protection and management of European Personal Data by BDO’s Member Firms when such personal data is processed in and/or transferred from the European Economic Area ('**EEA**') or Switzerland to countries outside the EEA and Switzerland (including any transfers of European Personal Data that may be made via another third country).

BDO has adopted this Policy in the form of Binding Corporate Rules for Member Firms processing European Personal Data as controllers or as a processor on behalf of another Member Firm.

For completeness, Member Firms must comply with the Binding Corporate Rules for Processors policy when processing European Personal Data as processors or sub-processors for Third Party Entities.

What European Personal Data does this Policy cover?

This Policy applies to European Personal Data processed within BDO (whether processed automatically or manually) that falls within the following categories:

- European Personal Data which relates to a Client for which a Member Firm is acting;
- European Personal Data which relates to BDO Partners and Staff (‘Employee Data’); and
- European Personal Data which relates to suppliers, sub-contractors and other third parties doing business with or interacting with BDO. This includes client counterparties and advisers.

European Personal Data is processed (and transferred) for the purposes specified below:

- In relation to **Clients** for which a Member Firm is acting, the following personal data is processed to provide **data input and analytics services, deliver services as part of a client engagement, provide marketing,** and **for management and administration** purposes: family names; given names; titles; e-mail address; physical address; phone number; images; CCTV recordings; advice, opinions, views and other comments; details of business activities; details of complaints, proceedings and incidents; details of assets, debts, income; bank records, bank statements, securities accounts, insurance policies and remuneration (including salary, benefits in kind, share options, pensions and incentive schemes); date of birth, identity documents, national insurance/social security numbers, tax reference numbers; memberships; monitored and

recorded information; and any other categories of personal data made aware in the context of providing Client services for the stated purposes.

- In relation to **Staff and Partners**, the following personal data is processed for **HR management and administration**, to provide **data input and analytics services** and for **other management and administration** purposes: family names, given names; titles; home address, e-mail address, phone number; nationality; birth date; identity documents; curriculum vitae, qualifications, education and employment history; payroll information; (profile) picture; employment type; date of hire; salary grade; passwords; business contact information; network connectivity information; expense reporting/accounting information, including credit card information; benefits data; competency assessments; dependant data; disciplinary action data; education data; emergency contact data; individual development plan; management positions; organisational data; performance data; appraisal data; security data; skills data; succession planning data; tax data; training data; CCTV recordings; access control information; images.

- In relation to **suppliers, sub-contractors and other third parties doing business with or interacting with BDO, including client counterparties and advisers**, the following personal data is processed to provide data input and analytics services and for **management and administration** purposes: name; contact information; details of services provided; identifier information; CCTV recordings; access control information; images; background check information; security vetting information.

Transfers of European Personal Data may take place from Europe to any of the Member Firms within the BDO network.

Pursuant to the Regulations of BDO International Limited, all Member Firms processing European Personal Data as controllers or as a processor on behalf of another Member Firm, along with their respective Partners and Staff, must comply with and respect this Policy (which in the case of Member Firms as processors applies to the extent that such obligations are not inconsistent with processing activities that are undertaken by Member Firms in that capacity).

All such Member Firms shall take all necessary steps to ensure compliance at all times with the provisions of this Policy by their respective Partners and Staff, by Partners and Staff of their subsidiaries and by all other persons howsoever employed, engaged or retained by the Member Firm.

This Policy is additional to, and does not replace or supersede, any specific data protection requirements or rules regarding confidentiality that might apply to a business area or function or as required by applicable law to which a Member Firm is subject.

This Policy is published on BDO's intranet and the international website accessible at https://global-www.bdo.global/en-gb/legal-privacy-cookies/bcrs which also contains more information about the structure of BDO. The list of Member Firms is provided at Appendix 7 of this Policy.

2. PURPOSE AND OBJECTIVES

2.1 Personal data and data protection law

Each day personal data is being transferred and/or processed throughout the BDO network. Personal data includes names, email addresses, photos, CVs, etc. When Member Firms process European Personal Data, they must comply with this Policy.

As this Policy only applies to European Personal Data, BDO has based this Policy on European data protection law.

2.2 BDO and European data protection law

European data protection law does not allow transfer of personal data to countries, territories or international organisations outside Europe that do not ensure an adequate level of protection for individuals' data privacy rights. As some of the countries in which Member Firms operate are not regarded by the European Commission as providing an adequate level of protection appropriate safeguards must be put in place that meet the requirements of European data protection law.

Other countries where Member Firms operate may have transfer restrictions for personal data under local law that are similar to European data protection laws. This Policy does not cover those transfers of such data.

2.3 BDO Member Firms acting as controller

Under European data protection law, when a Member Firm processes European Personal Data for its own purposes, that Member Firm is deemed to be a controller of that personal data and is therefore primarily responsible for complying with applicable data protection law.

2.4 BDO Member Firms acting as processor

Under European data protection law, when a Member Firm processes personal data in the course of providing a service to another Member Firm or to a Third Party Entity (e.g. a Client), that Member Firm is deemed to be a processor of the personal data. The controller (e.g. the Client or other Member Firm) remains primarily responsible for complying with applicable data protection law.

In practical terms this means that controllers that process European Personal Data must pass certain data protection obligations on to any processor that processes personal data in a country outside Europe on their behalf. Passing these obligations to the processor is a key requirement in order for the controller to comply with applicable data protection law, including meeting obligations relating to restrictions on data transfers outside Europe.

If a Member Firm acting as a processor fails to comply with the data protection obligations imposed on it by a controller, that controller may be in breach of applicable data protection law and in turn the Member Firm acting as processor may face a claim for breach of contract, which may result in the payment of damages or other judicial remedies. In addition, a controller that has entered into a Data Processing Agreement with a Member Firm that incorporates this Policy may enforce this Policy against any Member Firm processing European Personal Data on behalf of that controller in respect of a breach of this Policy caused by that Member Firm in the European courts, where permitted by law and subject to the terms of the Data Processing Agreement.

In such cases, if the controller can demonstrate that it has suffered damage and that it is likely that the damage has occurred because of a breach of this Policy, the burden of proof to show that a Member Firm (or any third party sub-processor located outside Europe and which is acting on behalf of a Member Firm) is not responsible for the breach, or that no such breach took place, will rest with the Member Firm transferring the

European Personal Data to the Member Firm outside Europe.

2.5 BDO's solution

BDO wants to ensure that the processing of European Personal Data within the BDO network is secure and complies with applicable laws. The purpose of this Policy, therefore, is to set out a framework based on European data protection law that provides an overall adequate level of protection for European Personal Data transferred within the BDO network between Member Firms.

This Policy contains 16 Rules that identify specific obligations with which a Member Firm must comply when processing European Personal Data as a controller or as a processor on behalf of another Member Firm.

2.6 Further information

If you have any questions regarding this Policy, your rights under this Policy or any other data protection issues, you can contact BDO's Global Privacy Office (who will either deal with the matter or forward it to the appropriate person within BDO) at the following address:

Email: privacy@bdo.global

3. POLICY

3.1 Introduction

Clause 3 of this Policy is divided into three sections:

I. **Section A** addresses the basic principles that Member Firms must observe when processing European Personal Data as controllers or as processors on behalf of another Member Firm.

II. **Section B** deals with Member Firms' practical commitments to the European supervisory authorities in relation to European Personal Data.

III. **Section C** describes the third party beneficiary rights that are granted by Member Firms under this Policy to individuals in respect of European Personal Data.

3.2 Definitions

BDO is the brand name for the BDO Network and for each of the BDO Member Firms.

BDO Network means the network (not being a separate legal entity) comprising the Member Firms.

Client means an individual or Third Party Entity for which a Member Firm provides a service.

controller means the entity which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processing Agreement means a contract or any other type of legal instrument containing data processing terms and conditions, whether as part of a contract for professional services or otherwise.

Employee Data means personal data processed by BDO which relates to Partners and Staff.

Europe means, for the purpose of this Policy, the EEA and Switzerland.

Exporting Entity means a European Member Firm exporting European Personal Data to a Member Firm outside Europe.

European data protection law means the European (EU) Regulation 2016/679 (the General Data Protection Regulation or 'GDPR') and any data protection law of a European Member State and Switzerland including local law implementing or interpreting the requirements of the GDPR, as amended from time to time.

European Personal Data means personal data that is subject to European data protection law (as defined above).

Global Privacy Policy or Policy means this policy as adopted by the Executive of BDO International Limited (with the approval of the Global Board) setting out rules for the processing of European Personal Data by the Member Firms in their capacity as controllers or as a processor on behalf of another Member Firm, as amended or updated from time to time.

Global Privacy Office means the department that has overall responsibility for this Policy and that reports via the Global Head of Risk, Quality and Governance to the Global Board of BDO.

Importing Entity means a Member Firm outside Europe receiving European Personal Data.

Individual means a natural person whose European Personal Data is subject to this Policy.

Privacy Champion means the person who is responsible for day to day compliance issues within his/her area of responsibility and who is responsible for reporting major privacy issues involving European Personal Data to the Global Privacy Office. He/she also oversees training on this Policy within his/her Member Firm.

Member Firms means the independent firms which are admitted from time to time as member firms of the BDO Network pursuant to the Articles and Regulation 6 and have not ceased to be member firms. “Member Firms” includes Voting Members and Non-Voting Members or any of them. For the purpose of this Policy, the term “Member Firms” includes BDO International Limited together with any other central entities of BDO that provide services to the BDO Network, including BWS.

Partners are individuals who are current, past or prospective partners of BDO.

processor means the entity which processes European Personal Data on behalf of the controller.

processing of European Personal Data shall have the meaning given in the GDPR.

Special Category Data means European Personal Data relating to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life, sexual orientation, genetic or biometric data for the purposes of uniquely identifying a person.

Personal data, means any information relating to an identified or identifiable natural person ('**data subject**'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Staff means full or part-time current, past or prospective employees, individual contractors, secondees, interns and work experience students.

Third Party Entity means an entity which is not a Member Firm.

3.3 Section A: Basic principles

Rule 1 – Lawfulness and fairness

Rule 1A – Member Firms will first and foremost comply with any applicable local law.

Member Firms, when they are a controller or a processor of European Personal Data, must always comply with any applicable local law relating to European Personal Data and must ensure that European Personal Data is processed in accordance with applicable local law.

Where there is no applicable local law or the law does not meet the standards set out by the Rules in this Policy, Member Firms shall process European Personal Data in accordance with the Rules in this Policy. Where applicable local law requires a higher level of protection for European Personal Data than is provided for in this Policy, the higher level of protection will take precedence over this Policy and should be applied to the processing of European Personal Data.

Where applicable local law prevents Member Firms from fulfilling, or has a substantial adverse effect on their ability to comply with, their obligations under this Policy, Member Firms will follow the process set out in Rule 16A.

Rule 1B – Member Firms will ensure that their processing of European Personal Data is fair and lawful and that a legal basis exists for processing European Personal Data.

Member Firms when they are a controller of European Personal Data will ensure that their processing of European Personal Data is fair and lawful, and that a legal basis for processing European Personal Data exists where required. Taking into account any specific provisions of a particular European or Member State law, Member Firms will only process European Personal Data where:

- the individual has given consent to the processing of his or her European Personal Data and that consent meets the required standards under European data protection law;
- it is necessary for the performance of a contract to which the individual is a party, or in order to take steps at the request of the individual before entering into a contract;
- it is necessary for compliance with a legal obligation to which the Member Firm is subject where that legal obligation derives from European law or the law of a European Member State;
- it is necessary in order to protect the vital interests of the individual or of another individual;
- it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in a Member Firm where that processing is set out either under European law or the law of a European Member State to which the Member Firm is subject; or
- it is necessary for the purposes of the legitimate interests pursued by a Member Firm or by a third party, except where those interests are overridden by the interests or fundamental rights and freedoms of the individual.

Where the processing of European Personal Data relates to criminal convictions and offences or related security measures, Member Firms will not carry out such processing otherwise than under the control of official authority or when the processing is authorised by European or Member State law that provides appropriate safeguards for the rights and freedoms of individuals.

Rule 1C – Member Firms will assess the impact of any new processing activities that involve European Personal Data that are likely to result in a high risk to the rights and freedoms of individuals.

Member Firms when they are a controller of European Personal Data will assess the necessity and proportionality of new processing activities that involve European Personal Data, including the risks to individuals, when, such processing activities are likely to result in a high risk to the rights and freedoms of individuals in accordance with their privacy impact assessment policies, as amended and updated from time to time and their obligations in relation to such processing activities under this Policy including, where the assessment indicates that such processing would result in a high risk to individuals in the absence of measures taken to mitigate the risk, to consult the competent supervisory authority prior to commencing such processing.

Member Firms will put in place appropriate safeguards and technical and organisational mechanisms in order to protect European Personal Data and the corresponding rights of individuals when implementing and using new processing activities.

Rule 2 – Ensuring transparency and using European Personal Data for a known purpose only

Rule 2A – Member Firms will inform individuals, at the time such individuals' European Personal Data is collected, how that data will be processed.

Member Firms when they are a controller of European Personal Data will ensure that individuals are informed in a clear and comprehensive manner how their European Personal Data will be processed. Specifically, Member Firms must notify such individuals of the following:

- the identity and contact details of the controller and the contact details of the DPO (if there is one);
- individuals' rights in relation to European Personal Data to: access, rectify, erase, restrict, object to the processing of European Personal Data, to data portability; where processing is based on consent, the right to withdraw consent; and to complain to a supervisory authority;
- the purpose and legal basis for processing, including an explanation about any processing based on the legitimate interests legal basis;
- the safeguards in place to protect European Personal Data when it is transferred internationally (which in the case of transfers based on this Policy, must include reference to this Policy, and how to access it);
- the length of time for which European Personal Data will be retained, or the criteria applied to calculate this;

- whether the provision of the information is a statutory or contractual requirement, or a requirement necessary to enter into contract, as well as whether the data subject is obliged to provide the personal data and the consequences of the failure to provide European Personal Data in such circumstances;

- the recipients or categories of recipients of European Personal Data and the source and categories of information received from third parties; and

- where applicable, the processing of European Personal Data for automated decision-making (including profiling) and, at least where required by European Data Protection Law, meaningful information about the logic involved, as well as the significance and the envisaged consequences of the processing.

The requirements of the law in the country where the European Personal Data is collected may determine that further or different information must be provided to individuals in addition to that stated above.

Such information will be made available when European Personal Data is obtained by Member Firms or within a timeframe otherwise permitted under European data protection law.

If European Personal Data is obtained from a source other than from the individual, Member Firms will provide the relevant individual with the information:

- within a reasonable period after obtaining the European Personal Data, but at the latest within one month, having regard to the specific circumstances in which such European Personal Data is processed;

- at the time of the first communication to that individual; or

- if such European Personal Data is to be disclosed to a third party, before it is first disclosed.

Member Firms will follow this Rule 2A unless not providing information is specifically permitted by European data protection law.

Rule 2B – Member Firms will only process European Personal Data for specified, explicit and legitimate purposes.

Member Firms when they are a controller of European Personal Data shall process European Personal Data only for specified, explicit and legitimate purposes. If Member Firms wish to process European Personal Data for a different or new purpose other than those which have been notified to individuals, it will not further process that European Personal Data in a way incompatible with the purpose for which it was collected.

In certain cases, for example, the individual's consent to the processing may be necessary unless the processing is based on European law which constitutes a necessary and proportionate measure in a democratic society to safeguard important objectives of general public interest.

Where Member Firms intend to further process European Personal Data for a purpose other than that for which the European Personal Data were collected, Member Firms shall provide individuals prior to that further processing with information on those other purposes and with any relevant information as referred to in Rule 2A above.

Rule 3 – Ensuring Data Quality

Rule 3A – Member Firms will keep European Personal Data accurate and retain it only for as long as is necessary for the purposes for which it is collected and processed.

In order to ensure that European Personal Data held by BDO is accurate and up to date, Member Firms when they are a controller of European Personal Data shall actively encourage individuals to inform Member Firms when such European Personal Data changes. Having regard to the purposes for which European Personal Data is processed, Member Firms will take every reasonable step to ensure that European Personal Data that is inaccurate is erased or rectified without undue delay.

Member Firms will comply with their respective local data retention policies and procedures as revised and updated from time to time.

Rule 3B – Member Firms will only process European Personal Data which is adequate, relevant and limited to what is necessary for the purposes for which it is processed.

Member Firms when they are a controller of European Personal Data will process the minimum amount of European Personal Data that is required in order to properly fulfil the purpose or purposes for which the Member Firms are processing the European Personal Data.

Rule 4 – Taking appropriate security measures

Rule 4A – Member Firms will keep European Personal Data secure.

Member Firms when they are a controller or a processor of European Personal Data will implement appropriate technical and organisational measures to protect European Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where processing involves transmission of European Personal Data over an IT network, and against all other unlawful forms of processing; the Member Firms will comply with their respective IT security policies as revised and updated from time to time.

Rule 4B – Member Firms will adhere to their respective breach notification policies.

Member Firms when they are a controller or a processor of European Personal Data will adhere to their respective breach notification policies (as revised and updated from time to time) which set out the processes that Member Firms must follow, in accordance with European data protection law:

- to notify the Global Privacy Office and BWS without undue delay in the event of a personal data breach;
- to document the facts relating to the personal data breach, its effects and the remedial action taken) and provide such information to a supervisory authority on request;

- where the Member Firm is a processor on behalf of a Member Firm to notify the controller without undue delay of becoming aware of the personal data breach;

- where the Member Firm is a controller, where required, notify the competent supervisory authority of a data breach involving European Personal Data where such breach is likely to result in a risk to the rights and freedoms of individuals; and

- where the Member Firm is a controller, where required, notify individuals of a data breach involving European Personal Data when such breach is likely to result in a risk to the individuals' rights and freedoms unless notification is not required because the conditions set out in European Data Protection Law are met.

Rule 4C – Member Firms will ensure that Third Party Entities or other Member Firms acting as service providers keep European Personal Data secure.

Member Firms using a processor when they are a controller or a processor of European Personal Data will comply with their respective due diligence processes for the selection of the processor to ensure that the processor has appropriate technical and organisational security measures in place to safeguard European Personal Data. Member Firms shall impose contractual obligations in writing on the processor that comply with the requirements of European data protection law (i.e. in line with Article 28 GDPR) in the form of a Data Processing Agreement.

The requirements for inclusion in a Data Processing Agreement are:

a) details of the subject- matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller;

b) commitments on the part of the processor:
    - that the processor will act only on the Member Firm's instructions when processing the European Personal Data including with regard to transfers of such personal data to a third country or an international organisation, unless required to do so by European Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits such information on important grounds of public interest;

    - to ensure that persons authorised to process European Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

    - to take all measures regarding the security of the European Personal Data, consistent with those contained in this Policy;

    - not to engage another processor without the prior specific or general written authorisation of the Member Firm, and in the case of general written authorisation, the processor shall inform the Member Firm of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes;

    - where the processor engages another processor for carrying out specific processing activities on behalf of the Member Firm, to include the same data protection obligations as are set out in the Data Processing Agreement with the processor in a contract or other legal act under European Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR. Where the other

processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the Member Firm for the performance of that other processor's obligations;

- taking into account the nature of the processing, to assist the Member Firm by appropriate technical and organisational measures, insofar as this is possible, to fulfil its obligations under Rule 5;

- taking into account the nature of the processing and the information available to the processor to assist the Member Firm in ensuring compliance with the obligations on the Member Firm under Rules 1C, 4A and 4B;

- at the choice of the Member Firm, to delete or return to the Member Firm all European Personal Data after the end of the provision of the services provided under the Data Processing Agreement, and to delete existing copies unless European Union or Member State law requires storage of such personal data; and

- to make available to the Member Firm all information necessary to demonstrate compliance with the obligations imposed upon the processor under the Data Processing Agreement, and allow for, and contribute to, audits, including inspections, conducted by the Member Firm, or another auditor mandated by the Member Firm.

c) that the processor will comply with the obligations imposed on the Member Firm by Rule 6 of this Policy (and where the Member Firm is a processor, with any relevant terms of the Data Processing Agreement the Member Firm has entered into with that controller). In particular, Member Firms shall ensure that the processor provides adequate safeguards (as required under European data protection law) in respect of transfers of European Personal Data to a processor established in a country outside Europe that European supervisory authorities do not consider ensures an adequate level of protection for individuals' data privacy rights.

Where one Member Firm is processing European Personal Data as a processor on behalf of another Member Firm the Data Processing Agreement may take the form of the Processing Schedule set out in Appendix 6. Member Firms providing a service to another Member Firm as a processor on the basis of the Processing Schedule must:

- comply with the obligations set out in Part 2 of the Processing Schedule in relation to such processing;

- act only on the instructions of the controller Member Firm;

- implement appropriate technical and organisational measures to protect personal data; and

- comply with their respective IT security policies as revised and updated from time to time.

Rule 5 – Honouring individuals' rights

Rule 5 – Member Firms will honour individuals' rights in respect of their European Personal Data.

On request, individuals whose European Personal Data is processed under this Policy are entitled to exercise their right to:

- access their European Personal Data;

- request rectification, completion, erasure, or restriction, as appropriate of their European Personal Data;

- exercise their right to data portability in relation to their European Personal Data; and/or
- object to the processing of their European Personal Data, including processing for direct marketing purposes and to profiling to the extent that it is related to such marketing.

Member Firms, when they are a controller of European Personal Data, will deal with queries or requests made by individuals in connection with their European Personal Data in accordance with the Individual Rights Procedure (Appendix 1) and Member Firms acting as processors will act in accordance with the lawful instructions of the controller and will undertake any reasonably necessary measures to enable that controller to comply with its duty to respect the rights of individuals in respect of European Personal Data. In such cases Member Firms will follow the steps set out in the Individual Rights Procedure in so far as it relates to processors.

Rule 6 – Ensuring adequate protection for transfers and onward transfers

Rule 6 – Member Firms will only transfer European Personal Data outside Europe to a controller or a processor Third Party Entity if adequate protection is ensured.

Transfers and onward transfers of European Personal Data to a Third Party Entity outside Europe are not allowed unless adequate protection of the European Personal Data is ensured as provided for under Chapter V of the GDPR, such as by signing up to appropriate Standard Contractual Clauses or by way of a derogation such as obtaining the explicit consent of individuals. This obligation applies to Member Firms whether they are a controller or a processor of European Personal Data. However, Member Firms acting as processors will only transfer European Personal Data outside Europe to a Third Party Entity outside Europe in accordance with the instructions of the controller as set out in a Data Processing Agreement that meets the requirements of European data protection law.

Rule 7 – Safeguarding the processing of Special Category Data

Rule 7A – Member Firms will only process Special Category Data if it is absolutely necessary.

Member Firms when they are a controller of European Personal Data will assess whether Special Category Data is required for the proposed processing and whether the proposed processing is absolutely necessary in the context of the Member Firm's business.

Rule 7B – Member Firms will only process Special Category Data where the individual's explicit consent has been obtained or the processing is otherwise permitted by European or Member State law.

Individuals must expressly agree to a Member Firm processing their Special Category Data as a controller of such data unless European or Member State law provides that the prohibition to processing special category data may not be lifted by an individual. This permission for the Member Firm to process Special Category Data must be genuine and freely given. Otherwise, processing of Special Category Data is only permitted on certain grounds with the following being most relevant to processing undertaken by Member Firms:

- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of Member Firms or of the individual in the field of employment and social security and social protection law in so far as it is authorised by European or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and interests of individuals;

- processing is necessary in order to protect the vital interests of an individual where that individual is physically or legally incapable of giving consent;

- processing relates to European Personal Data that are manifestly made public by the individual;

- processing is necessary for the establishment, exercise or defence of legal claims, or whenever courts are acting in a judicial capacity;

- processing is necessary for reasons of substantial public interest on the basis of European or Member State law provided that it is proportionate to the aim pursued, respects the essence of data protection, and provides for suitable and specific measures to safeguard the fundamental rights and interests of the individual;

- processing is necessary for the purposes of preventive or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of European or Member State law provided that the processing is undertaken by or under the responsibility of a professional subject to duties of confidentiality under European or Member State law or by rules established by national competent bodies; or

- processing is necessary for reasons of public health which provides for suitable and specific measures to safeguard the rights and freedoms of individuals, in particular duties of professional confidentiality.

Rule 8 – Legitimising direct marketing

Rule 8 - Member Firms must offer individuals the right to opt out of receiving marketing information.

All individuals have the right to object, free of charge, to the processing of their European Personal Data for direct marketing purposes (including the processing of such data for profiling to the extent that it is related to such marketing). Member Firms processing European Personal Data as a controller will honour all such opt out requests.

Rule 9 – Automated individual decisions

Rule 9 - Member Firms will respect the rights of individuals not to be subject to a decision made solely as a result of processing European Personal Data by automated means (including profiling) that has a legal or similarly significant effect on them. The exception to this is when the processing is permitted under European law and Member Firms have put in place measures to safeguard the legitimate interests of individuals.

European data protection law requires that a controller may not make an evaluation of, or decision about, an individual that significantly affects him or her based solely on the automated processing of that individual's European Personal Data, except where:

- the processing is authorised under European law;
- the decision is necessary for entering into a contract between the individual and the Member Firm; or
- the individual has given explicit consent.

Where an exception applies, Member Firms processing European Personal Data as a controller will put in place measures to protect the rights and freedoms and legitimate interests of individuals.

3.4 Section B: Practical commitments – applicable to Member Firms processing European Personal Data as a controller or as a processor

Rule 10 – Compliance

Rule 10A - Member Firms will be responsible for and will be able to demonstrate compliance with this Policy and will have appropriate staff and support to implement and oversee compliance with this Policy throughout the business.

Overall responsibility to monitor compliance with this Policy rests with the Global Privacy Office. The Global Privacy Office is ultimately accountable to the Global Board by virtue of the fact that the Global Privacy Office staff report to the Global Head of Risk, Quality and Governance, who is a member of the Global Leadership Team and Secretary of the Board. The Global Privacy Office's tasks include:

- responding to Member Firm queries relating to matters arising under this Policy;
- deciding what action to take where notified by Member Firms of an inability to comply with the Policy (and notifying the competent supervisory authority of the same);
- providing the competent supervisory authority with general information about any legally binding requests for disclosure of European Personal Data by a law enforcement agency or state security body;
- assisting Member Firms to deal with complex individual rights requests and queries relating to the Individual Rights Procedure;
- providing an annual summary of the Audit results to the Executive of BDO;
- communicating changes to the Policy to the competent supervisory authorities; and
- liaising with the Privacy Champions to discuss matters arising under the Policy.

Each Member Firm has a Privacy Champion to implement and oversee compliance with this Policy within the Member Firm on a day to day basis. Privacy Champions outside Europe may be appointed on a regional basis to manage compliance within a geographical region. The Privacy Champion's tasks include:

- overseeing training within the Member Firm;
- responding to individual rights requests in accordance with the Individual Rights Procedure;
- liaising with European supervisory authorities to provide copies of the results of any Audit;

- handling complaints arising under the Policy in respect of the processing of European Personal Data; and
- liaising with the Global Privacy Office to discuss matters arising under the Policy.

Rule 10B – Member Firms processing European Personal Data will maintain a written record (including in electronic form) of their processing activities and make that record available to competent supervisory authorities on request.

The data processing records maintained by Member Firms contain:

- the Member Firm's name and contact details;
- the purposes for which European Personal Data is processed;
- a description of the categories of data subjects and the European Personal Data being processed;
- the categories of recipients to whom European Personal Data has been or will be disclosed;
- details of the third country or countries to which European Personal Data is transferred;
- where possible, the period for which European Personal Data will be retained; and
- where possible, a general description of the technical and organisational security measures used to protect European Personal Data.

Rule 10C – Member Firms will implement appropriate technical and organisational measures to enable and facilitate compliance with this Policy in practice.

Taking into account the state of the art and cost of implementation and the scope, nature, context and purposes of the processing, Member Firms will implement appropriate technical and organisational measures which meet the principles of data protection by design and by default as required by European data protection law.

Rule 11 – Training

Rule 11 – Member Firms will provide appropriate training to Partners and Staff who have permanent or regular access to European Personal Data and/or who are involved in the processing of such personal data or in the development of tools used to process such personal data.

Member Firms will provide appropriate training to Partners and Staff, Partners and Staff of their subsidiaries, and to all other persons howsoever employed, engaged or retained by them, who have permanent or regular access to European Personal Data and/or who are involved in the processing of such European Personal Data or in the development of tools used to process such personal data.

Rule 12 – Audit

Rule 12 - Member Firms will comply with the Audit Protocol.

Member Firms will ensure compliance with the Audit Protocol (Appendix 2).

Rule 13 – Complaint handling

Rule 13 - Member Firms will comply with the Complaint Handling Procedure.

Member Firms will ensure compliance with the Complaint Handling Procedure (Appendix 3).

Rule 14 – Cooperation with Supervisory Authorities

Rule 14 - Member Firms will comply with the Co-operation Procedure.

Member Firms will ensure compliance with the Co-operation Procedure (Appendix 4).

Rule 15 – Update of the rules

Rule 15 - Member Firms will comply with the Updating Procedure.

Member Firms will ensure compliance with the Updating Procedure (Appendix 5).

Rule 16 – Actions where applicable local law or professional rules and obligations prevent compliance with this Policy

Rule 16A - Member Firms will promptly inform the Global Privacy Office when they believe applicable local law or professional rules and obligations prevent them from fulfilling, or have a substantial adverse effect on, their ability to comply with their obligations under this Policy.

Member Firms will promptly inform (unless otherwise prohibited by law) the Global Privacy Office and BWS of such inability to comply with this Policy. The Global Privacy Office will make a decision on what action to take and will notify the competent supervisory authority.

In cases where the Member Firm is a processor, that Member Firm will also promptly inform the controller, as provided in Rule 4B.

Rule 16B - Member Firms located outside Europe will ensure that when they receive from a law enforcement authority or state security body a legally binding request for disclosure of European Personal Data, they will, unless prevented from doing so by the requesting authority, put the request on hold and promptly notify the controller and the competent supervisory authority.

When Member Firms located outside Europe receive a legally binding request for disclosure of European Personal Data under this Policy and they are prohibited by a law enforcement authority or state security body from putting the request on hold and/or from notifying the relevant supervisory authorities, they will:

- use their best efforts to obtain a waiver of this prohibition in order to communicate as much information as they can and as soon as possible to the relevant supervisory authorities to include information about the data requested, the requesting body and the legal basis for disclosure; and

- demonstrate to the relevant supervisory authorities the steps they have followed to deal with the request in accordance with this Policy.

It is important that the Global Privacy Office is promptly made aware of such requests in order to allow it to provide to the competent supervisory authority, on an annual basis, general information about the nature and number of such requests received by Member Firms. Member Firms will ensure that any transfers they make to a law enforcement authority or state security body are not massive, disproportionate or indiscriminate in a manner that would go beyond what is necessary in a democratic society.

3.5 Section C: Third party beneficiary rights for European Personal Data under this Policy

European data protection law requires that individuals whose European Personal Data is processed in Europe by an Exporting Entity and transferred to an Importing Entity must be able to benefit from certain rights to enforce parts of this Policy. These rights relate to Rules 1A, 1B, 2A, 2B, 3A, 3B, 4A, 4B, 4C, 5, 6, 7, 8, 9, 10C, 13, 14, 16A and 16B as well as these liability and jurisdiction provisions and Member Firms' commitment to provide easy access to this Policy. This Policy ensures that such individuals are able to enforce such rights as follows:

a) **Complaints:** such individuals may make complaints to the Exporting Entity in accordance with the Complaints Handling Procedure and/or to a European supervisory authority in the jurisdiction of the individual's place of work, habitual residence, or in the place of the alleged infringement.

b) **Proceedings:** those individuals may also bring proceedings against the Exporting Entity that transferred European Personal Data to enforce compliance by the Exporting Entity with this Policy before the competent courts in the European country where the Exporting Entity is established or in the European country where the individual resides.

c) **Liability:** these individuals may in addition seek appropriate redress from the Exporting Entity (before the competent courts as described in (b) above), which agrees to take the necessary action to remedy any breach of this Policy by any Importing Entity and, where appropriate, receive compensation from the Exporting Entity for any material or non-material damage suffered as a result of a breach this Policy by a Member Firm in accordance with the determination of a court or other competent authority.

d) These individuals also have the right to obtain a copy of this Policy, as well as a list of Member Firms bound by this Policy.

In the event of a claim being made in which an individual has suffered material or non-material damage and where that individual can demonstrate that it is likely that such damage has occurred because of a breach of this Policy, the burden of proof will be reversed so that, rather than it being the responsibility of the individual making a claim to show that an Importing Entity is responsible for the breach or that such a breach took place, it will be for the Exporting Entity to prove that the Importing Entity is not responsible for the breach, or that such a breach has not occurred.

4. APPENDICES

APPENDIX 1 - INDIVIDUAL RIGHTS PROCEDURE FOR CONTROLLERS

When a Member Firm acts as a controller of European Personal Data

1. Introduction

1.1 When a Member Firm processes European Personal Data for its own purposes, the Member Firm is deemed to be a controller of that European Personal Data and is therefore primarily responsible for meeting the requirements of European data protection law.

1.2 Individuals whose European Personal Data is processed in Europe have the right: (a) to be informed by a Member Firm whether any European Personal Data about them is being processed by the Member Firm (the right of subject access); and (b) to rectify, erase, restrict, or complete their European Personal Data, to data portability, and/or to object to the processing of their European Personal Data. The privacy notice provided by Member Firms to explain how they will process European Personal Data sets out how these rights may be exercised.

1.3 In addition, when European Personal Data subject to this Policy is transferred to another Member Firm outside Europe, such European Personal Data will continue to benefit from the rights referred to in 1.2 above and such rights will be dealt with in accordance with the terms of this Individual Rights Procedure ("**Procedure**").

1.4 This Procedure explains how Member Firms deal with requests relating to European Personal Data which fall into the categories in sections 1.2 and 1.3 above (each referred to as "**Valid Request**" in this Procedure).

Where applicable European data protection law differs from this Procedure, the applicable European data protection law will prevail.

2. Individuals' rights

2.1 Subject to applicable European data protection law, an individual making a Valid Request to a controller Member Firm is entitled to be informed whether the Member Firm is processing European Personal Data about that individual together with:

i. the purposes for which the European Personal Data is being processed;

ii. the categories of European Personal Data processed;

iii. the recipients or classes of recipient to whom such European Personal Data is, or may be, disclosed by the Member Firm, in particular recipients outside Europe or international organisations;

iv. where possible, the envisaged period for which the European Personal Data will be stored, or the criteria used to determine that period;

v. the right to lodge a complaint with a supervisory authority;

vi. the source of the European Personal Data not collected from the individual;

vii. the logic involved in, and significance and consequences of any processing undertaken by automatic means, including profiling (at least where required by European Data Protection Law);

viii. where European Personal Data is transferred to a third country, details of the safeguards in place relating to the transfer;

ix. communication in intelligible form of the European Personal Data held by the Member Firm. If the request is made by email, the information shall be provided by email, unless the individual making the request indicates otherwise;

x. the rights to require rectification, erasure, restriction, portability or completion of their European Personal Data; and/or

xi. the right to object to the processing of their European Personal Data.

2.2 The request may be made in writing, which can include email. A request may be made orally, in which case the request must be recorded and a copy provided to the individual making the request before dealing with it.

2.3 Member Firms must deal with a Valid Request within one month of its receipt. This period may be extended by two further months where necessary, taking into account the complexity and number of requests. If the Member Firm does not intend to act on the request, or wishes to extend the response time, this must be notified to the person making the request within one month of the date of the request, together with reasons for not taking action or for the extension, as appropriate, together with the right to complain to a supervisory authority.

2.4 Subject to applicable European data protection law, when the request does not relate to Employee Data, Member Firms are only obliged to comply with a Valid Request if the individual making the request supplies the Member Firm with such information which the Member Firm may reasonably require to confirm the identity of the individual making the request.

3. Process

3.1 If a Member Firm receives any request from an individual for his or her European Personal Data or information relating thereto, this must be passed to the relevant European Privacy Champion immediately upon receipt indicating the date on which the request was received together with any other information which may assist that Privacy Champion to deal with the request. If for any reasons it is not possible to transfer the request, the relevant local Privacy Champion will deal with the request.

3.2 Unless applicable European data protection law dictates otherwise, the request does not have to be in an official form or mention data protection law to qualify as a Valid Request.

3.3 Initial steps

i. The Privacy Champion will make an initial assessment of the request to decide whether it is a Valid Request and whether confirmation of the individual's identity, or any further information, is required. The initial assessment will include consideration as to whether the request is manifestly unfounded or excessive and, if so, whether the Member Firm will refuse to act on the request or charge a reasonable fee for dealing with it.

ii. The Privacy Champion will then contact the individual in writing to confirm receipt of the Valid Request, seek confirmation of identity or further information, if required, or decline the request if one of the exemptions applies, or the request is manifestly unfounded or unreasonable.

4. Declining a valid request

4.1 Subject to applicable European data protection law, a Valid Request may be refused on the following grounds:

i. Where the subject access request is made to a European Member Firm and relates to the processing of European Personal Data by that Member Firm, if the refusal to provide the information is consistent with the data protection law within the jurisdiction in which that Member Firm is located; or

ii. Where the subject access request is made to a non-European Member Firm for European Personal Data, if the relevant Privacy Champion in Europe is unable to deal with the request in accordance with clause 3.1, the relevant non-European Privacy Champion will only withhold information that is the subject of the request if the grounds for withholding such information are consistent with the data protection law within the jurisdiction from which the information was transferred.

5. Search and the response

5.1 The Privacy Champion will arrange a search of all relevant electronic and paper filing systems.

5.2 The Privacy Champion may refer any complex cases to the Global Privacy Office for advice, particularly where the response to the request (that is, European Personal Data and information relating thereto) may or is likely to include information or European Personal Data relating to third parties, or where the release of European Personal Data may prejudice commercial confidentiality or legal proceedings.

5.3 The information requested will be collated by the Privacy Champion into a readily understandable and where applicable machine readable format (internal codes or identification numbers used at BDO that correspond to European Personal Data shall be translated before being disclosed). A covering letter will be prepared by the Privacy Champion which includes the information required to be provided in response to a subject access request.

5.4 Where the provision of the information in permanent form is required under applicable European data protection law but is not possible or would involve disproportionate effort, there is no obligation to provide a permanent copy of the information if this is permitted under applicable European data protection law. The other information referred to in section 2 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.

5.5 If a Valid Request is received from an individual to delete, rectify, restrict, complete, erase, object to the processing of, or request data portability of his or her European Personal Data where the Member Firm is the controller for that personal data, such a request must be considered and dealt with as appropriate by the Privacy Champion in accordance with applicable European law.

5.6 If a request is received advising of a change or inaccuracy in an individual's European Personal Data where the Member Firm is the controller for that personal data, such information must be rectified or updated accordingly without undue delay if the Member Firm is satisfied that there is a legitimate basis for doing so.

5.7 When a Member Firm makes any changes to European Personal Data pursuant to 5.5 and 5.6 above, or responds to a request for data portability, it will notify any other Member Firm or any Third Party Entity that is actively engaged in processing that European Personal Data so that it can also update the relevant personal data.

5.8 If the individual requests a Member Firm as a controller to cease processing that individual's European Personal Data because the rights and freedoms of the individual are prejudiced by virtue of such processing, or on the basis of other compelling legitimate grounds, the matter will be referred to the Privacy Champion to assess. Where the Member Firm is able to demonstrate compelling legitimate grounds which override the interests, rights and freedoms of the individual, or for the establishment, exercise or defence of legal claims or the processing undertaken by the Member Firm is required by law, the Member Firm must notify the individual within one month of the date of the request, setting out reasons for not taking action, together with the right to complain to a supervisory authority. Where the objection is justified, the processing must cease.

5.9 All queries relating to this Procedure are to be addressed to the Privacy Champion or to the Global Privacy Office.

When a Member Firm acts as a processor

6. Requests made to BDO where a Member Firm is a processor of the European Personal Data

6.1 When a Member Firm processes European Personal Data on behalf of a controller (e.g. another Member Firm to whom a Member Firm provides a service) the Member Firm is deemed to be a processor of such information and the controller will be primarily responsible for meeting the legal requirements of the subject access request. The data processing Member Firm must act in accordance with the instructions of the controller in respect of such requests. This means that if any Member Firm receives a request from an individual exercising his or her rights under European data protection law in its capacity as a processor, that Member Firm must transfer such request promptly to the relevant controller and not respond to the request unless authorized to do so by the controller (such as pursuant to a Data Processing Agreement).

APPENDIX 2 - AUDIT PROTOCOL

1. Approach to BDO Network audit

This Audit Protocol describes the formal assessment process adopted by the BDO Network to ensure compliance by Member Firms with this Policy as required by the supervisory authorities.

1.1 Overview of audit

i. The BDO Global Risk, Quality & Governance Department ('RQG') will oversee the compliance by Member Firms with this Policy and will ensure that such audits address all aspects of this Policy adopting a risk based approach.

ii. The audit process within BDO is made up of the elements described in 1.2 below.

1.2 Audit process, timing and scope

Audit of this Policy comprises the following elements (together referred to as the 'Audit Process') and ensures that all aspects of the Policy are reviewed on a continuous basis, and at least once every three years, as described below:

i. The Accreditation process ('Accreditation')

This is a self-assessment process that Member Firms are required to adhere to which takes place on a continuous basis, and at least once every three years. Member Firms must submit evidence to demonstrate that they comply with prescribed Accreditation criteria, and one area of compliance addresses information security and privacy. Instances of non-compliance are referred to the Compliance Counsel (which comprises members of the RQG) which is responsible, on behalf of the Executive, for recommending appropriate sanctions to be imposed on the Member Firm in the event of non-compliance.

ii. Dedicated assessments of compliance

Additional compliance monitoring assessments or campaigns run in tandem to Accreditation. These targeted assessments are carried out in respect of all Member Firms to ensure compliance with the Standards and Policies of BDO, including all aspects of the Global Privacy Policy. This includes completion of a pre-assessment questionnaire the responses to which form the basis of targeted assessments based on privacy controls established by the Global Privacy Office. The targeted assessments are carried out on a continuous basis, and at least once every three years. Any Member Firm that does not achieve full implementation of the controls must submit a remediation plan linked to a number of action points that enables the progress of completion of the action points.

1.3 Auditors

The Audit of this Policy will be undertaken by the RQG as described above.

1.4 Report

i. RQG will make the results of the Audits available to the Global Privacy Office in so far as they relate to this Policy. The Global Privacy Office will provide an annual summary of the Audit results to the Executive of BDO;

ii. RQG will bring any issues or instances of non-compliance to the attention of the Managing Partner of the relevant Member Firm and to the Global Privacy Office. It is the responsibility of the individual Member Firms to ensure that any corrective actions to ensure compliance take place within a reasonable timescale. In the event

that such corrective actions do not take place, the Global Privacy Office will report the matter to the CEO and Regional CEOs of BDO.

2. Supervisory Authority audits

i. Upon request the relevant Member Firm will provide copies of the results of any Audit to any European supervisory authority who will upon receiving the Audit results be reminded of their duty of professional secrecy under Article 54(2) of the GDPR.

ii. The Privacy Champions in EU countries will be responsible for liaising with the European supervisory authorities for the purpose of providing the information described above.

iii. In addition all Member Firms agree to be audited by European supervisory authorities in accordance with the applicable audit procedures of such European supervisory authorities.

APPENDIX 3 - COMPLAINT HANDLING PROCEDURE

1. Introduction

The purpose of this Complaint Handling Procedure is to explain how complaints brought by an individual whose European Personal Data is processed by a Member Firm under this Policy are dealt with.

2. How individuals can bring complaints

All complaints made under this Policy - whether a Member Firm is processing European Personal Data on its own behalf or on behalf of a controller - can be brought in writing (which includes email) to the relevant Privacy Champion. To contact a Member Firm please visit www.bdo.global which contains a link to the websites of all Member Firms. Details of the Privacy Champion will be found via the link to the Legal and Privacy page. Individuals may also either email privacy@bdo.global or write to the Global Privacy Office at Brussels Worldwide Services BV, Brussels Airport, The Corporate Village, Elsinore Building, Leonardo Da Vincilaan 9 – 5/F, 1930 Zaventem, Belgium if they cannot locate the relevant information.

3. Who handles complaints?

3.1 Complaint Handling Process

i. The relevant Privacy Champion will handle all complaints arising under this Policy in respect of the processing of European Personal Data. The Privacy Champion will liaise with relevant business units to investigate the complaint and will coordinate a response.

ii. What is the response time?

The Privacy Champion will acknowledge to the individual concerned receipt of his or her complaint within 10 working days, and will investigate and provide a substantive response to the individual within one month. If, due to the complexity of the complaint, a substantive response cannot be given within this period, the relevant Privacy Champion will advise the complainant of the reason for the delay within one month of receipt of the complaint, and provide a reasonable estimate for the timescale (not exceeding two further months) within which a response will be provided.

iii. When a complainant disputes a finding

If the complainant disputes the response of the relevant Privacy Champion or any aspect of a finding, and notifies the Member Firm accordingly, the matter will be referred to the Managing Partner of the Member Firm (or any other Partner as designated by the Member Firm) who will review the case and advise the complainant of his/her decision either to accept the original response or finding, to reopen the matter, or to substitute a new response or finding. The Managing Partner of the Member Firm may consult the Global Privacy Office about the complaint and consider the response of the Privacy Champion. The Managing Partner of the Member Firm will respond to the complainant within one month of the referral. If, due to the complexity of the complaint, a substantive response cannot be given within this period, the Managing Partner of the Member Firm will advise the complainant of the reason for the delay within one month of receipt of the referral, and provide a reasonable estimate for the timescale (not exceeding two further months) within which a response will be provided. If the complaint is upheld, the Managing Partner of the Member Firm (in cooperation with the Global Privacy Office) will arrange for any necessary steps to be taken as a consequence.

iv. Individuals whose personal data is processed in accordance with European data protection law also have the right to make a complaint to a European supervisory authority in the country of the individual's place of work, habitual residence, or in the place of the alleged infringement, and/or to lodge a claim with a court of competent jurisdiction which means in a court in the European country where the Member Firm is established or in the European country where the individual resides and this will apply whether or not they have first made a complaint to the Member Firm.

v. In relation to claims against a Member Firm referred to in paragraph (d), if the matter relates to European Personal Data which has been exported to a Member Firm outside Europe and an individual wants to make a claim against BDO, the claim may be made against the European Member Firm responsible for exporting the European Personal Data as set out in 3.5 of this Policy.

APPENDIX 4 – CO-OPERATING PROCEDURE

1. Introduction

This Co-operation Procedure sets out the way in which Member Firms will co-operate with the European supervisory authorities in relation to this Policy.

2. Co-operation Procedure

2.1 Where required, the European Member Firms will make the necessary personnel available for dialogue with a European supervisory authority in relation to this Policy.

2.2 The relevant European Member Firms will actively review and consider:

i. any decisions made by relevant European supervisory authorities on any data protection law issues that may affect this Policy; and

ii. the views of the European Data Protection Board (formerly the Article 29 Working Party) as outlined in its published guidance on Binding Corporate Rules for controllers and Binding Corporate Rules for processors.

2.3 Upon request, the BDO Global Privacy Office will provide copies of the results of any audit of this Policy pursuant to Appendix 2 to a relevant European supervisory authority who will upon receiving the Audit results be reminded of their duty of professional secrecy under Article 54(2) of the GDPR.

2.4 Member Firms agree that supervisory authorities based in Europe may carry out a data protection audit of that Member Firm in accordance with the applicable law of the European country from which the data is transferred.

2.5 Where any Member Firm is located within the jurisdiction of a supervisory authority based in Europe, Member Firms acknowledge that any European supervisory authority may audit that Member Firm for the purpose of reviewing compliance with this Policy, in accordance with the applicable law of the country in which the Member Firm is located.

2.6 All Member Firms agree to be audited by European supervisory authorities in accordance with the applicable audit procedures of such European supervisory authorities.

2.7 Each Member Firm agrees to take into account the advice, and comply with the formal decisions, of, a competent supervisory authority relating to the interpretation and application of this Policy, without prejudice to any right to appeal such formal decisions.

APPENDIX 5 - UPDATING PROCEDURE

1. Introduction

This Updating Procedure sets out the way in which the BDO Network will communicate changes to this Policy to the European supervisory authorities and individuals whose European Personal Data is processed under this Policy.

2. Material changes to this Policy

2.1 The Global Privacy Office will communicate any material changes to this Policy without undue delay to the Belgian DPA and via the Belgian DPA to other supervisory authorities concerned.

2.2 Where a change to this Policy materially affects the conditions under which a Member Firm processes European Personal Data on behalf of a controller under the terms of its Data Processing Agreement, the Member Firm will communicate such information to any affected controller. If such change is contrary to any term of the Data Processing Agreement between the Member Firm and the controller, the Member Firm will communicate the proposed change before it is implemented, and with sufficient notice to enable affected clients to object. The controller may then suspend the transfer of such European Personal Data to the Member Firm and/or terminate the relevant contract, in accordance with the terms of its Data Processing Agreement with the Member Firm.

3. Administrative changes to this Policy

The Global Privacy Office will communicate to the Belgian DPA and via the Belgian DPA to other supervisory authorities concerned at least once a year changes to this Policy. Examples of such changes that may arise include those that are administrative in nature (including changes in the list of Member Firms); have occurred as a result of a change of applicable European data protection law; or resulting from any legislative, court or supervisory authority measure. The Global Privacy Office will also provide a brief explanation to the Belgian DPA and to any other relevant supervisory authorities of the reasons for any notified changes to this Policy. Where Member Firms act as a processor, Member Firms shall provide such information to controllers on whose behalf the Member Firms process European Personal Data.

4. Communicating and logging changes to this Policy

4.1 This Policy contains a change log which sets out the date of revisions to this Policy and the details of any revisions made.

4.2 The Global Privacy Office will communicate all changes to this Policy, whether administrative or material in nature, to the Member Firms without undue delay and publish an updated version of this Policy on the website [www.bdo.global] and on BDO's intranet.

4.3 Member Firms acting as controllers shall systematically inform individuals about the relevant changes using generally accepted communication tools (*e.g.* via the internet or a newsletter).

4.4 Member Firms acting as processors will communicate all changes to this Policy, whether administrative or material in nature, to controllers on whose behalf the Member Firm processes European Personal Data using generally accepted communication tools (*e.g.* via the internet or an email).

4.5 The Global Privacy Office will maintain an up to date list of the changes made to this Policy and a list of Member Firms bound by this Policy and will provide the necessary information to individuals or supervisory authorities upon request.

5. New Member Firms

When joining the BDO Network, following an assessment of the prospective Member Firm's ability to meet the required standards, including standards related to data protection and privacy, and agreeing to be bound by the Regulations of BDO International Limited, a Member Firm automatically agrees to abide by this Policy and therefore to comply with and respect this Policy when processing European Personal Data and European Member Firms will not make any transfers of European Personal Data to a new Member Firm located outside Europe until the new Member Firm is effectively bound by the Regulations and can deliver compliance with this Policy.

APPENDIX 6 - PROCESSING SCHEDULE

The Controller (as defined in Part 1 to this Processing Schedule ("Part 1")) wishes to appoint the Processor (also as defined in Part 1) to process certain Personal Information on its behalf in accordance with Rule 4C. The Controller and the Processor have elected to complete this Processing Schedule as the means by which to satisfy the requirements of the GDPR.

This Processing Schedule is to be read and interpreted in conjunction with this Policy.

Part 1: Processing Instructions

1.1. Name of Member Firm as controller: ……..……(the "Controller")

1.2. Name of Member Firm as processor: ……..……(the "Processor")

1.3. Purpose of the processing carried out by the Processor: …….....

1.4. The European Personal Data processed will include the following categories of personal data:

i. [list each category of European Personal Data that will be processed, e.g. names, email addresses, financial information]

1.5. The data subjects to whom the European Personal Data relates are:

i. [list each category of data subjects, e.g. staff]

1.6. The activities to be carried out by the Processor on behalf of the Controller will consist of:

i. [describe services carried out by the Processor on the Controller's behalf in detail]

1.7. Duration of processing carried out by the Processor: …….....

Part 2: Processor's Obligations

2. The Processor shall:

2.1 ensure that employees and contractors authorised to process the European Personal Data described in Part 1 (the "Data") have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

2.2 inform the Controller: i) if it is legally required to process the Data otherwise than as instructed by the Controller before such processing occurs, unless the law requiring such processing prohibits the Processor from notifying the Controller, in which case it will notify the Controller as soon as that law permits it to do so; and ii) about any instruction from the Controller which, in the Processor's opinion, infringes applicable data protection law;

2.3 not subcontract any processing of the Data or otherwise disclose the Data to any third party except as authorised by the Controller in writing. Where sub-contracting is permitted the Processor will: (a) ensure that it has a written contract (the "Processing Subcontract") in place with the relevant subcontractor which imposes on the subcontractor the same obligations in respect of processing of the Data as are imposed on the Processor under Rule 4B and 4C and this Part 2 to the Processing Schedule ("Part 2"); (b) ensure that there are sufficient guarantees in place to ensure the Processing Subcontract meets the requirements of Article 28 of the GDPR; (c) remain fully liable to the Controller for its obligations under Rule 4C and

this Part 2; and (d) ensure that Rule 6 of this Policy is complied with in the event that Data is subject to a trans-border transfer to a sub-contractor; and

2.4 provide such co-operation and assistance as the Controller reasonably considers to be necessary to enable the Controller to: (a) verify Processor's compliance with the obligations of a processor under this Policy and this Processing Schedule; (b) carry out prior assessments of processing activities which are likely to result in a high risk to the rights and freedoms of individuals and any related consultations with competent supervisory authorities; (c) fulfil its obligations in respect of any request by an individual to exercise their rights under this Policy, including by notifying the Controller without undue delay of any such request; and (d) investigate, mitigate and notify in accordance with Rule 4B of this Policy any Data Protection Breach involving the Data, including by notifying the Controller without undue delay of any such Data Protection Breach.

APPENDIX 7 – LIST OF MEMBER FIRMS

A list of Member Firms is published on BDO's international website, accessible at https://global-www.bdo.global/en-gb/legal-privacy-cookies/firm-list.