GLOBAL PRIVACY POLICY

BINDING CORPORATE RULES FOR PROCESSORS

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 processors or sub-processors.

For completeness, Member Firms must comply with the Binding Corporate Rules for Controllers policy when processing European Personal Data as controllers or as a processor on behalf of another Member Firm.

What European Personal Data does this Policy cover?

This Policy applies to European Personal Data processed within BDO (whether processed automatically or manually) by Member Firms as processors or sub-processors. Such European Personal Data falls within the following categories:

- European Personal Data which relates to a Client for which a Member Firm is acting; 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 (which includes transfers under this Policy) 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 **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 processors or sub-processors, along with their respective Partners and Staff, must comply with and respect this Policy.

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://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 processor

Under European data protection law, when a Member Firm processes European 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 the 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.

2.4 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 processed within the BDO network between Member Firms.

This Policy contains 13 Rules that identify specific obligations with which a Member Firm must comply when processing European Personal Data as a processor.

When a Member Firm acts as a processor for a Third Party Entity which is a controller, it will be up to the controller to decide whether the commitments made in this Policy provide adequate safeguards for the European Personal Data transferred. Where such controller wishes to rely upon this Policy as providing adequate safeguards, it must incorporate this Policy in any Data Processing Agreement with the Member Firm (which may be part of a wider professional services agreement). Only in cases where the Third Party Entity as controller has entered into a Data Processing Agreement incorporating this Policy with the Member Firm acting as a processor will the third party beneficiary rights set out in section 3.5 apply.

If a Third Party Entity as controller chooses not to rely upon this Policy, that controller will have the responsibility to put in place other adequate safeguards to protect European Personal Data.

2.5 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 processors or sub-processors.

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 processors or sub-processors for Clients, 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 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 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 13A.

Rule 1B – Member Firms will ensure that compliance with this Policy will not conflict with applicable local data protection laws and will co-operate with and assist the relevant controller to comply with its obligations under applicable data protection law in a reasonable time and to the extent reasonably possible.

Where Member Firms act as processors in relation to European Personal Data, they will co-operate and assist the relevant controller to comply with its obligations under European data protection law in a reasonable time and to the extent reasonably possible and as may be required under a Data Processing Agreement with a controller. Member Firms should be transparent about their security measures and use of sub-processors where required so that the controller may correctly inform individuals.

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

Rule 2A - Member Firms will assist controllers to comply with the requirement to inform individuals how their European Personal Data will be processed.

Member Firms will comply with the requirements of any Data Processing Agreement in place with a controller and provide to that controller such assistance and information as may be required under the terms of that agreement.

Rule 2B - Member Firms will only process European Personal Data in accordance with the instructions of the controller(s).

Member Firms will only process European Personal Data in compliance with the terms of the Data Processing Agreement they have entered into with the relevant controller in relation to such processing (in accordance with Article 28(3) of the GDPR), and which contains the terms required by European data protection law in so far as it relates to the engagement of a processor.

Member Firms will immediately inform the relevant controller, the Global Privacy Office and BWS if, in their opinion, an instruction infringes European data protection law, any other applicable local law or professional rules and obligations that prevents them from fulfilling, or has a substantial adverse effect on, their ability to comply with their obligations under this Policy. In addition, where a Member Firm has reason to believe that the existing or future legislation applicable to it may prevent it from fulfilling the instructions received from a relevant controller or the Member Firm's obligations under this Policy, it will promptly notify the relevant controller of this.

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.

If, for any reason, Member Firms are unable to comply with this Rule 2B or their obligations under this Policy in respect of a Data Processing Agreement they shall inform the relevant controller promptly of this fact and allow the controller to suspend the transfer of European Personal Data to them and/or terminate the Data Processing Agreement.

Member Firms will act in accordance with the instructions of the controller and return, destroy or store the European Personal Data in a secure manner or as otherwise reasonably required by the controller. In the event that applicable law, professional standards, legal process or anticipation of legal claims prevents Member Firms from returning such European Personal Data to the controller, or destroying it, Member Firms will ensure that such European Personal Data remains confidential and will not process that European Personal Data otherwise than in accordance with the instructions of the controller or as required by applicable law.

Rule 3 – Ensuring Data Quality

Rule 3 - Member Firms will assist controllers to keep European Personal Data accurate and up to date to the extent reasonably possible.

Member Firms acting as processors or sub-processors will comply with instructions and execute any necessary measures from controllers in order to update, correct, delete or anonymise European

Personal Data from the moment the identification form is not necessary anymore and inform any Member Firm to which such information has been disclosed of any deletion or anonymisation of data accordingly.

Rule 4 – Taking appropriate security measures

Rule 4A - Member Firms will adhere to their respective breach notification policies.

Member Firms 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; and
- to notify the controller without undue delay of becoming aware of the personal data breach, and to ensure that any sub-processor is subject to the same obligation under the terms of a Data Processing Agreement as required by Rule 4C.

Rule 4B - Member Firms will keep European Personal Data secure and comply with instructions from controllers in relation to security measures, breach notification requirements and the appointment of sub-processors consistent with the law applicable to the data controller.

Member Firms will put in place appropriate technical and organisational measures as agreed with the relevant controllers 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 the IT network, and against all other unlawful forms of processing, and will comply with any agreed requirements and any applicable law in relation to breach notification.

Member Firms will assist the relevant controllers in implementing appropriate technical and organisational measures to facilitate compliance with this Policy in practice (such as data protection by design and by default) so far as is reasonable taking into account the state of the art, cost of implementation, risks to data subjects, nature, scope, context and purpose of the processing.

Member Firms will comply with the requirements and instructions of the relevant controllers regarding the appointment of any sub-processors, as set out in a Data Processing Agreement and in particular will obtain prior informed specific or general written authorisation of the controller regarding the appointment of any sub-processors and where the controller has provided general written authorisation will ensure that up to date information regarding the appointment of sub-processors is available to such controllers at all times so that controllers have the opportunity to object before the data have been transferred to a new sub-processor. If a data controller objects to the appointment of a sub-processor to process its personal data, that controller will be entitled to take such steps as are consistent with the terms of its Data Processing Agreement with the Member Firm and as are referred to in Rule 2B of this Policy.

Rule 4C - Member Firms will ensure that sub-processors keep European Personal Data secure.

Member Firms using a sub-processor (either a Third Party Entity or another Member Firm) will comply with their respective due diligence processes for the selection of the sub-processor to ensure that the sub-processor has appropriate technical and organisational security measures in place to safeguard European Personal Data. Such due diligence processes may be set forth in a Data Processing Agreement. Member Firms shall impose contractual obligations in writing on the sub-processor that comply with the requirements of European data protection law (and ensure that the provisions of any applicable Data Processing Agreement are also included). Those requirements include:

a) commitments on the part of the sub-processor regarding the security of the European Personal Data, consistent with those contained in this Policy (and any applicable Data Processing Agreement);

b) that the sub-processor will act only on the Member Firm's instructions when processing the European Personal Data; and

c) that the sub-processor will comply with the obligations imposed on the Member Firm by Rule 6 of this Policy and with any relevant terms of the Data Processing Agreement the Member Firm has entered into with a controller. In particular, Member Firms shall ensure that the sub-processor provides adequate safeguards (as required under European data protection law) in respect of transfers of European Personal Data to a sub-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.

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 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 (Appendix 1).

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 or as otherwise permitted by European law.

Member Firms 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.

3.4 Section B: Practical commitments

Rule 7 – Compliance

Rule 7A - 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 exercise of such rights;
- 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 for Processors;
- 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;
- maintaining an up to date list of the sub-processors bound by this Policy; and
- liaising with the Global Privacy Office to discuss matters arising under the Policy.

Rule 7B - Member Firms processing European Personal Data will maintain a written record of their processing activities (including in electronic form) and make that record available to competent supervisory authorities on request.

The data processing records maintained by Member Firms will contain:

- the Member Firm's name and contact details;
- the name and contact details of each controller on behalf of which it is acting (and, where applicable, the controller's representative and the DPO);
- the purposes for which European Personal Data is processed;
- the categories of processing carried out on behalf of each controller;
- 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 8 – Training

Rule 8 - 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 9 – Audit

Rule 9 - Member Firms will comply with the Audit Protocol.

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

Rule 10 – Complaint handling

Rule 10 - Member Firms will comply with the Complaint Handling Procedure.

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

Rule 11 – Cooperation with Supervisory Authorities

Rule 11 - Member Firms will comply with the Co-operation Procedure.

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

Rule 12 – Update of the rules

Rule 12 - Member Firms will comply with the Updating Procedure.

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

Rule 13 – Actions where applicable local law or professional rules and obligations prevent compliance with this Policy

Rule 13A - 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 for the controller and for the Member Firm.

Member Firms will also promptly inform the controller, as provided in Rule 2B.

Rule 13B - 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 for the controller and for the Member Firm.

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

I. Where European Personal Data is processed under this Policy by a Member Firm under a Data Processing Agreement with a controller that individual will have certain third party beneficiary rights to enforce parts of this Policy in relation to that Member Firm. These rights relate to Rules 1B, 2A, 2B, 3, 4A, 4B, 4C, 5, 6, 10, 11 and 13 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) 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;

   b) to make complaints in accordance with the Complaint Handling Procedure;

   c) to bring proceedings against, or seek remedy of any breach of this Policy by, the European Member Firm acting as a data processor that has transferred the European Personal Data, or where there is no European Member Firm acting as data processor, to bring proceedings against, or seek remedy of any breach of this Policy by, BWS before the competent courts in the jurisdiction of the European country where the Member Firm or the controller is established or in the European country where the individual resides and where appropriate, to receive compensation for the entirety of any material or non-material damage suffered as a result of such breach by:

- any non-European Member Firm acting as a processor; or
- any Third Party Entity acting as a sub-processor which is established outside Europe and which is acting on behalf of a Member Firm

in accordance with the determination of the court or other competent authority; and

d) to obtain a copy of this Policy, as well as a list of Member Firms bound by this Policy.

II. Where European Personal Data is processed under this Policy by a Member Firm acting as a processor under a Data Processing Agreement with a controller and where: (i) the individual whose European Personal Data is transferred is unable to bring a claim against the controller because the controller has factually disappeared or ceased to exist in law or has become insolvent; and (ii) no successor entity has assumed the entire legal obligations of the controller by contract or by operation of law, that individual will have certain third party beneficiary rights to enforce parts of this Policy in relation to that Member Firm. These rights relate to Rules 1B, 2A, 2B, 3, 4A, 4B, 4C, 5, 6, 10, 11 and 13 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) 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;

b) to make complaints in accordance with the Complaint Handling Procedure;

c) to bring proceedings against, or seek remedy of any breach of this Policy by, the European Member Firm acting as a data processor that has transferred the European Personal Data, or where there is no European Member Firm acting as data processor, to bring proceedings against, or seek remedy of any breach of this Policy by, BWS before the competent courts in the jurisdiction of the European country where the Member Firm or the controller is established or in the European country where the individual resides and where appropriate, to receive compensation for the entirety of any material or non-material damage suffered as a result of such breach by:

- any non-European Member Firm acting as a processor; or
- any Third Party Entity acting as a sub-processor which is established outside Europe and which is acting on behalf of a Member Firm

in accordance with the determination of the court or other competent authority; and

d) 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 a Member Firm or any Third Party Entity acting as a sub-processor which is established outside Europe and which is acting on behalf of a Member Firm is liable for the breach or that such a breach took place, it will be for the Member Firm against which proceedings are issued to prove that it or any Third Party Entity acting as a sub-processor which is established outside Europe acting on its behalf is not liable for the breach, or that such breach did not occur.

The Member Firm against which proceedings are issued will ensure that any necessary action is taken to remedy any breach of this Policy by a non-European Member Firm or any sub-processor who is located outside Europe and who is processing European Personal Data on behalf of a controller.

Where a Member Firm and the client involved in the same processing are found responsible for any damage caused by such processing, individuals may be entitled to receive compensation for the entire damage directly from the Member Firm.

A Member Firm may not rely on a breach by a sub-processor of its obligations under this Policy in order to avoid liability under the terms of 3.5.

4. APPENDICES

APPENDIX 1 - INDIVIDUAL RIGHTS PROCEDURE FOR PROCESSORS

1. Individuals whose European Personal Data is processed in Europe have the right: (a) to be informed whether any European Personal Data about them is being processed (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.

2. 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 above and such rights will be dealt with in accordance with the terms of this Appendix 1.

3. When a Member Firm processes European Personal Data on behalf of a controller (e.g. a Client to whom a Member Firm provides a service) the Member Firm is deemed to be a processor of such information. 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 enable 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.

3. Controller audits

When a Member Firm processes European Personal Data in the course of providing a service to a Third Party Entity, that Member Firm is deemed to be a processor of the European Personal Data and the Third Party Entity is the controller. This relationship will be governed by a Data Processing Agreement between the Member Firm and the Third Party Entity. The Member Firms acknowledge that in such cases audits of compliance with the commitments made in this Policy may also be carried out by or on behalf of the controller in accordance with the terms of such Data Processing Agreement, and those audits may (in accordance with the terms of the Data Processing Agreement between the Member Firm and the sub-processors) also extend to any sub-processors acting on a Member Firm's behalf in respect of such processing. The scope of the audit shall be limited to the data processing facilities, data files and documentation relating to the terms of the Data Processing Agreement between that controller and the Member Firm subject to the audit adopting a risk based approach.

Upon request and to the extent that an audit relates to European Personal Data processed by a Member Firm on behalf of that controller, Member Firms will make the portion of results of such audit of compliance with this Policy that relate to the relevant controller available to that controller upon request.

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 - where a Member Firm is processing European Personal Data 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 European 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.

3.2 Complaints where the Member Firm is a processor for a Third Party Entity

i. Where a complaint arises under this Policy in respect of the processing of European Personal Data where a Member Firm is the processor in respect of that information, the Member Firm will communicate the details of the complaint to the controller promptly and will act in accordance with the terms of any Data Processing Agreement between the controller and the Member Firm.

ii. When a Third Party Entity ceases to exist

In circumstances where a controller Third Party Entity has disappeared, no longer exists or has become insolvent, individuals whose European Personal Data is processed in accordance with European data protection law and transferred between Member Firms on behalf of that controller under this Policy have the right to complain to a Member Firm and the Member Firm will deal with such complaints in accordance with section 3 of this Complaint Handling Procedure. In such cases, individuals also have the right to complain 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 or the controller is established as set out in 3.5 of this Policy, 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.

APPENDIX 4 - CO-OPERATION 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.

4.6 Privacy Champions will maintain an up to date list of the sub-processors bound by this Policy. This information will be available on request from the Global Privacy Office.

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 2B. 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 2B and 4B 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 4A 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.