Remote Professionals
Data Protection Rules (DPR)

The Rules are divided into two sections:

Section A *addresses the basic principles of European data protection law REMOTE PROFESSIONALS must observe when REMOTE PROFESSIONALS processes personal data as a controller.*

Section B *deals with the practical commitments made by REMOTE PROFESSIONALS to the competent supervisory authority in connection with this Controller Policy.*

Section A

Rule 1 — Compliance with local law

Rule 1 — REMOTE PROFESSIONALS will first and foremost comply with local law where it exists.

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

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

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

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

Rule 2A — REMOTE PROFESSIONALS will explain to individuals, at the time their personal data is collected, how that data will be processed.

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

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

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

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

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

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

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

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

Or

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

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

Rule 3 — Ensuring data quality

Rule 3A — REMOTE PROFESSIONALS will keep personal data accurate and up to date.

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

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

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

Rule 3C — REMOTE PROFESSIONALS will only keep personal data which is relevant to REMOTE PROFESSIONALS.

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

Rule 4 — Taking appropriate security measures

Rule 4A — REMOTE PROFESSIONALS will always adhere to its IT Security Policies.

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

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

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

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

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

A personal data breach means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data. Where a breach is subject to European data protection law, REMOTE PROFESSIONALS will notify the supervisory authority without undue delay after becoming aware of the personal data breach.

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

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

Rule 5 — Honoring individuals' rights

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

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

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

Rule 6 — Ensuring adequate protection for international transfers

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

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

Rule 7 — Safeguarding the use of sensitive personal data

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

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

REMOTE PROFESSIONALS will:

- Avoid collection of sensitive personal data where it is not required for the purposes for which the data is collected or subsequently processed
- Limit access to sensitive personal data to appropriate persons (by either masking or making anonymous or pseudonymous the data, where appropriate) in accordance with the security standards established in REMOTE PROFESSIONALS Information Security/Privacy Policies

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

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

Rule 8 — Legitimizing direct marketing

Rule 8A — REMOTE PROFESSIONALS will allow customers to opt out of receiving marketing data.

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

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

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

Rule 9 — Automated individual decisions

Rule 9 —Individuals have the right not to be subject to a decision made solely on automated processing and to know the logic involved in such decision as well as the significance and the envisaged consequences of such processing. REMOTE PROFESSIONALS will take necessary measures to protect the legitimate interests of individuals.

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

Section B — Practical commitments

Rule 10 — Training

Rule 10 — REMOTE PROFESSIONALS will provide appropriate training to REMOTE PROFESSIONALS Personnel who have permanent or regular access to personal data, who are involved in the processing of personal data or in the development of tools used to process personal data.

REMOTE PROFESSIONALS will take reasonable and appropriate steps to communicate with REMOTE PROFESSIONALS Personnel and to provide appropriate training on the requirements of this Controller Policy.

REMOTE PROFESSIONALS Network entities to deliver as appropriate. In addition, REMOTE PROFESSIONALS Personnel within an REMOTE PROFESSIONALS Network entity should be made aware of their obligations relating to data privacy under the Global Code of Conduct.

Communication and training should cover data privacy elements such as:

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

Rule 11 — Records of processing and data protection impact assessments

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

REMOTE PROFESSIONALS Network entities keep a record of processing activities. This record will be in writing, including in Confidential electronic form, and will be made available to supervisory authorities on request.

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

Rule 12 — Assessment of compliance

Rule 12 — REMOTE PROFESSIONALS will comply with any Assessment of Compliance warranted

Rule 13 — Complaint handling

Rule 13 — REMOTE PROFESSIONALS will handle all complaints in line with internal policy

Rule 14 — Cooperation with supervisory authorities

Rule 14 — REMOTE PROFESSIONALS will always corporate with supervisory authorities

Rule 15 — Update of the rules

Rule 15 — REMOTE PROFESSIONALS will comply with the Updating Procedure set out in Privacy Policy

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

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

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

Where an REMOTE PROFESSIONALS Network entity is subject to a legal requirement that is likely to have a substantial adverse effect on the obligations in this Controller Policy, the REMOTE

PROFESSIONALS Privacy Leader will report this to the Supervisory Body. This includes any legally binding request for disclosure of personal data by a law enforcement authority or state security body.

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

REMOTE PROFESSIONALS will put such request on hold for a reasonable delay in order to notify the Supervisory Body to disclosing the data to the requesting authority. REMOTE PROFESSIONALS shall clearly inform the Supervisory Body about the request, including information about the data requested, the requesting authority and the legal basis for the disclosure.

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

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