DESCRIPTION OF ACCENTURE’S BINDING CORPORATE RULES

This version published June 2017
CONTENTS

1. INTRODUCTION

ANNEX 1- GLOBAL DATA PRIVACY POLICY

ANNEX 2- MEMORANDUM A: THE APPLICATION OF AND COMPLIANCE WITH DATA PRIVACY POLICY 90

ANNEX 3- MEMORANDUM B: PROCEDURES FOR RESPONDING TO INDIVIDUALS’ REQUESTS TO EXERCISE THEIR RIGHTS UNDER GLOBAL DATA PRIVACY POLICY 90

ANNEX 4 - MEMORANDUM C: COMPLAINT HANDLING PROCEDURE

ANNEX 5 – INTERCOMPANY AGREEMENT
INTRODUCTION TO ACCENTURE’S BINDING CORPORATE RULES

Accenture has implemented a set of Binding Corporate Rules (BCRs) which apply when we transfer our personal data within the Accenture global organization. These are a set of privacy rules which are binding in law and practice, and which are made up of:

a) Data Privacy Policy – a global data privacy policy that sets out the safeguards that apply across Accenture regardless of where we process your data (we call this “Policy 90”)
b) Data Privacy Procedures – such as how we should handle access requests or complaints; and
c) Intercompany Agreement – an agreement to make Policy 90 and the Data Privacy Procedures binding on all the participating Accenture group entities.

Together, these rules ensure that appropriate data privacy safeguards are in place across our organization. Our BCRs reflect the standards contained in European data privacy laws and have been approved by data privacy regulators in Europe (the European Economic Area and Switzerland).

Having BCRs means that all our group entities that sign up to them must comply with the same internal rules. It also means that your rights stay the same no matter where your data are processed by Accenture.

Accenture has a separate Client Data Protection program which governs the use of client personal data processed in our capacity as a data processor when providing services to our clients (so the BCRs do not apply to such personal data).

A full list of Accenture entities that have signed up to the BCRs is available from our Privacy Statement.

Accenture is in the process of updating our compliance program for GDPR requirements and any relevant changes to our published documents, will be reflected in due course.
ANNEX 1

GLOBAL DATA PRIVACY POLICY 90

External version

<table>
<thead>
<tr>
<th>Applies to:</th>
<th>All employees in All Career Tracks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Number:</td>
<td>0090</td>
</tr>
<tr>
<td>Policy Sponsor:</td>
<td>Legal</td>
</tr>
<tr>
<td>Effective Date of this Version:</td>
<td>21 May 2015</td>
</tr>
<tr>
<td>Supersedes the Version Dated:</td>
<td>16 September 2014</td>
</tr>
<tr>
<td>Original Effective Date:</td>
<td>1 October 2001</td>
</tr>
</tbody>
</table>

All policies/supplements are subject to local laws where the Company operates. These policies/supplements are subject to change without prior notification.
Policies Content 1

The purpose of this policy is to set out the duties of the Company and its personnel when processing personal data about individuals and to describe the rights of the individuals whose personal data is processed by the Company.

POLICY

The policy is structured as follows:

1. Scope and Application
2. The Company's duties
3. An individual's rights:
   3.1 Right of access to personal data
   3.2 Right to correct personal data
   3.3 Right to object to direct marketing
   3.4 Right to object to processing for compelling reasons
   3.5 Rights in relation to automated decision taking
4. Company compliance with this policy
5. When one Company entity processes personal data on behalf of another Company entity

1. Scope and Application

1.1 This policy regulates the way in which the Company obtains, uses, holds, transfers and otherwise processes personal data about individuals. It is also intended to ensure that personnel understand the rules on the protection of personal data and the individual's rights in relation to their personal data processed by the Company. In addition, the policy regulates the circumstances in which one Company entity processes personal data on behalf of another Company entity. This policy is without prejudice and does not override any applicable national data privacy laws and regulations in countries where the Company operates. This policy and its supporting documentation do not apply to processing of personal data on behalf of clients of the Company and other third parties during the provision of consulting, technology, outsourcing, and other services.

Certain Company entities are also subject to localized variances to this policy. Such variances are designed to regulate the processing of personal data in accordance with a country's specific local laws, where they exist. They are not intended to lower the standard set out in this policy. These localized variances, together with this policy, are intended to ensure that all personnel understand the Company's obligation to abide by the data privacy laws and regulations of all of the countries in which the Company operates. The localized variances are available as country supplements to this policy.

Guidelines are available to help personnel interpret and act in accordance with this policy. The internal global guidelines are provided in the Supporting Documentation (available upon request). Personnel should be aware, however, that localized versions of these guidelines exist for a number of countries, where localized variances to this policy exist. It is advisable therefore to contact the country's local Data Privacy Officer to ascertain if localized variances and therefore localized guidelines apply.
1.2 The Company processes personal data about individuals such as its personnel (past and present), job applicants, client contacts, supplier contacts, website users, and shareholders. The Company processes such personal data for a number of business purposes, including:

- Scheduling
- Talent Acquisition
- Employee performance management and professional development
- Payroll, fund management and accounting
- Share plan management and operations
- Business and market development
- Building and managing external relationships
- Planning and delivery of business integration capabilities
- Research and development
- Technology infrastructure and support and facilities management
- Travel management
- Knowledge management
- Other purposes required by law or regulation

2. The Company's duties

To protect personal data, the Company will observe the following guidelines:

2.1 The Company will process personal data fairly and lawfully. In particular, the Company will not process personal data unless one of the following conditions is met:

(i) the individual concerned has consented to such processing;

(ii) the Company needs to carry out such processing (1) to perform, or take steps with view to enter into, a contract with the individual concerned, (2) to comply with legal obligation of the Company or (3) to protect the vital interests of the individual concerned in a 'life or death' situation; or

(iii) the Company needs to carry out such processing to pursue the Company's legitimate interests, and those interests are not overridden because the processing prejudices the interests or fundamental rights and freedoms of the individual concerned.

2.2 When an individual gives the Company his/her personal data, the Company will provide information to the individual about the identity of the Company entity collecting/using that data and what it intends to do with the data. The Company will observe procedures so that individuals who provide their data are given certain information which shall include the name of the Company (or, if applicable, the relevant subsidiary or affiliate), the intended use of such data, and any additional information the Company deems necessary to process the data fairly and lawfully. For example, information about recipients of data, their rights under this Policy and the possibility of international transfers and/or data which is globally accessible.

The Company will make sure that information to individuals is also provided in all instances where existing personal data are going to be used in a new way, or for different purposes.
2.3 Where collecting personal data about an individual indirectly (for example, from a publicly available source), the Company will inform the individual of the identity of the Company entity that holds the data and what it intends to do with the data as soon as possible after collecting/receiving and/or deciding to retain the data.

The Company will also observe procedures designed so that individuals are provided with any additional information necessary to process the data fairly and lawfully. For example, information about recipients of data, their rights under this Policy and the possibility of international transfers and/or data which is globally accessible.

This information will not be provided to the individual, where the effort involved would be disproportionate. In determining what does or does not constitute a “disproportionate effort,” the Company must balance the amount of effort required against the amount, if any, of a prejudicial effect to the individual if such information was not provided to them.

2.4 The Company does not generally seek to collect data relating to the following:

Racial or ethnic origin;

Political opinions;

Religious or other similar beliefs;

Trade union membership;

Physical or mental health;

Sexual life; and/or

Criminal record.

The Company will not collect such data unless: (i) the individual concerned agrees that the Company may do so, based on a full understanding of why the data is being collected, or ii) the Company needs to do so to meet its obligations or exercise its rights under employment law, or iii) in exceptional circumstances such as where the processing is necessary to protect the vital interests of the individual concerned, or (iv) in circumstances permitted by applicable data privacy laws.

The Company may in exceptional circumstances, rely on consent given on behalf of the individual, for example, by a company employee on behalf of a family member.

2.5 The Company will have procedures and systems to verify that:

(i) it does not collect excessive personal data

(ii) the personal data collected are adequate and relevant for the intended purposes, accurate and up to date;

(iii) it processes personal data only for the purposes specified in this policy or in information provided to the individual concerned; and

(iv) one of the conditions in section 2.1 is met if it processes personal data for new or different purposes.

2.6 The Company will maintain retention policies and procedures, so that personal data are deleted after a reasonable time, given the purposes for which the personal data are held, except where, given those purposes, another law requires the data to be kept for a certain time. When the Company no longer needs to keep personal data for the purposes for which they are held it will destroy them as soon as practicable.

2.7 (a) The Company will maintain organizational, physical and technical security arrangements in relation to all of the personal data it holds. It will ensure those arrangements are appropriate to the risks represented by the processing of, and the nature of, that personal data. Where appropriate, these arrangements will include provisions for ‘need to know’ access to personal data.
(b) The Company recognizes, in particular, that adequate security is important where it arranges for outside service providers (also known as "data processors") to process personal data on the Company's behalf. The Company will ensure that the service providers are bound by written contracts under which they agree to process such data only on the Company's instructions and to maintain appropriate security arrangements to protect such data. Where service providers are located in countries outside the EU and they have access or otherwise process personal data that originates from the Company entities in the EU, the contracts with such service providers shall include the approved EU standard clauses (controller to processor).

2.8 The Company recognizes that personal data needs to be treated with care in countries which do not have data protection laws, or whose data protection laws do not provide a level of protection corresponding to the standard within the European Union (EU). The Company will not transfer personal data to entities outside the Company in such countries for further processing (except for processing on the Company's behalf as referred to in section 2.7(b)) unless such entities agree to abide by a data privacy standard at least as high as this policy, or enter into a contractual arrangement including the approved EU standard clauses for transfers of personal data to countries outside the EU. The only exceptions are where:

(i) the transfer is necessary to 1) protect the vital interests of the individual concerned in a 'life or death' situation, or 2) enter into or perform a contract with (or for the benefit of) that individual; or

(ii) the individual has consented to the transfer.

2.9 The Company has procedures to deal with any suspected breach of data security arrangements, unauthorized access or disclosure, or loss of personal data. In particular, the Company has procedures for notifying individuals of a breach of security regarding their personal data, where such notification is legally required, or where The Company considers it appropriate. All employees are required to follow the instructions in the Security Breach Response and Notification procedures.

3. An individual's rights

3.1 Right of access

(a) On written request by an individual, and where the Company has or is given sufficient information to identify the individual making the request and decide whether the Company holds personal data about him or her, the Company will:

(i) Inform that individual whether the Company holds personal data about him or her;

(ii) Describe the personal data that it holds, the reason for holding the data and the categories of person to whom it may disclose the data; and

(iii) Provide the individual with copies of the personal data held about him or her, together with an indication of the source(s) of the data, if known.

(b) The Company will provide this information and these copies within a reasonable period after the individual's request, or within any specific period that may be required by local law in any country.

(c) The Company may, however, refuse to provide an individual with information where disclosure of that information would reveal information about another individual (in which case the Company will provide as much of the information as possible without revealing information about the other individual), unless the other individual agrees that the Company may release the information or the Company decides that it is reasonable to provide the information without the other individual's agreement.
In addition, in some countries localized country supplements may provide for other legitimate reasons for refusing an individual's request for access, in accordance with local data protection law.

3.2 Right of correction
An individual may request that the Company correct the personal data it holds about him/her. If the Company agrees that the data are incorrect, it will delete or correct the data. If it does not agree that the data are incorrect, it will, nevertheless, record in the relevant file(s) the fact that the individual considers the data to be incorrect.

3.3 Right to object to direct marketing
The Company will abide by any request from an individual not to use his/her personal data for direct marketing purposes and shall do so free of charge to the individual.

3.4 Right to object to processing for compelling reasons
Where the Company relies on the ‘balance of interests’ condition in paragraph 2.1(iii) above to justify the processing of personal data, the Company will abide by any justified request from an individual to stop that processing of his or her data if the individual objects to the processing on compelling and legitimate grounds and shall do so free of charge to the individual.

3.5 Rights in relation to automated decision taking
The Company will not generally take decisions that significantly affect an individual solely on the basis of automatic processing of data that evaluates personal aspects of the individual (such as his or her performance at work, creditworthiness, reliability or conduct). Where the Company does use such decision-making techniques in the course of entering into or performing a contract with the individual, or where such decision-making technique is authorized by law, it will ensure that suitable measures are implemented to protect the legitimate interests of the individual. Individuals have the right to receive a clear explanation of the method and criteria used in making any decision based on automated decision-making.

3.6 Rights under applicable data privacy laws
The rights in this section 3 are without prejudice to any rights an individual may have under applicable data privacy laws to make a complaint to the national data privacy supervisory authority, or to claim compensation for a breach of the applicable data privacy law.

4. Company compliance with this policy
(a) The Company will maintain internal arrangements to:
   (i) facilitate compliance with this policy, as described in Memorandum: Compliance with Policy 0090;
   (ii) allow effective exercise of individuals' rights guaranteed in the policy, as described in Memorandum: Complaint Handling Procedure; and
   (iii) consider and respond to complaints from individuals that the Company may not have complied with the policy, as described in the Memorandum: The Application of and Compliance with Global Data Privacy Policy 90 and the Complaint Handling Procedure.
(b) All individuals may rely upon these procedures and/or exercise their rights provided for in the policy by contacting their local Data Privacy Officer.
(c) If a Company entity becomes aware of the existence of any requirements under local laws that would have a substantial adverse effect on its ability to comply with this policy (or would have such an effect if the requirements
were not imposed on the Company entity by law) it will inform the Data Privacy Compliance Team and the Company entity (or entities) whose data it processes and whose data is affected by such local laws.

5. When one Company entity processes personal data on behalf of another Company entity

Where one Company entity processes personal data on behalf of another Company entity, the first such entity is referred to in this policy as the "Processor" and the second as the "Controller".

(a) The Processor will:

(i) process the personal data only on the instructions of the Controller;

(ii) implement appropriate technical and organizational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing;

(iii) make all reasonable efforts to maintain the personal data so that they are accurate and up to date at all times;

(iv) not disclose the personal data to any person except as required or permitted by law or by any agreement between the Controller and the Processor or with the Controller's written consent.

(v) provide full cooperation and assistance to the Controller in allowing the individuals to whom the personal data relate to exercise any right under this policy; and

(vi) not process the personal data except to the extent reasonably necessary to perform any agreement between the Controller and the Processor in relation to the personal data.

(b) Section 5 of this policy constitutes a written instruction from the Controller to the Processor, subject to paragraph (a), to take such steps in the processing of the Processed Data as:

(i) the Processor reasonably considers necessary or desirable for the performance of any agreement between the Controller and the Processor in relation to the personal data; and

(ii) are consistent with the Processor's obligations under any such agreement and any other applicable laws and regulations.

CONTACT INFORMATION

Questions related to this policy can be sent to the appropriate country Data Privacy Officer. Refer to the list of Local Data Privacy Officers. For global data privacy matters, please contact dataprivacy@accenture.com
ANNEX 2

MEMORANDUM A:

THE APPLICATION OF AND COMPLIANCE WITH DATA PRIVACY POLICY 90

<table>
<thead>
<tr>
<th>Author</th>
<th>DP Compliance Team</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sponsoring Organization:</td>
<td>Legal</td>
</tr>
<tr>
<td>Applies to:</td>
<td>All personnel</td>
</tr>
</tbody>
</table>

CONTENTS

1. PREAMBLE
2. INTERNAL DATA PRIVACY COMPLIANCE TEAM
3. COMPLIANCE
   3.1 Compliance with the policy
   3.2 Compliance with local data privacy laws
4. COOPERATION WITH THE NATIONAL DATA PRIVACY AUTHORITIES
5. DATA PRIVACY AUDITS
1. PREAMBLE

The purpose of this memorandum is to set out the rules and the procedures to be followed by all Accenture entities and personnel to ensure compliance with Global Data Privacy Policy 90 (the Policy).

The Policy and this memorandum do not apply to personal data processed by Accenture on behalf of and upon the instructions of clients of Accenture during the provision of consulting and outsourcing services.

2. INTERNAL DATA PRIVACY COMPLIANCE TEAM

Accenture has established a central data privacy compliance function - Data Privacy Compliance Team - directed by the Global Data Privacy Lead (Global DP Lead), and supported by Local Data Privacy Officers (Local DP Officer), for each country or geography in which Accenture has operations.

Their responsibility is to oversee and ensure compliance with the Policy and applicable data privacy laws and regulations on the global, regional and country level.

3. COMPLIANCE

3.1 Compliance with the policy

The Policy establishes uniform and global standards for an adequate level of data privacy in all countries where Accenture entities operate.

All Accenture entities must comply with the Policy. In addition, they must comply with the localized variances of the Policy - the Country Supplements - in the country where they operate, where such localized variance exists. Local Data Privacy Officers or Data Privacy Compliance Team will supply the list of all Accenture entities covered by the Policy on request.

All Accenture personnel are required to comply with the Policy (including any applicable Country Supplements) in relation to all personal data processed as part of their job.

Where Accenture deems appropriate or where required, Accenture shall take appropriate action against any individual who has breached the Policy, in accordance with the applicable national laws and regulations, including but not limited to employment laws.

Accenture makes Policy 90 available to all individuals covered by the policy and maintains an appropriate data privacy training program for its personnel.

If an Accenture entity becomes involved in a procedure involving a national data privacy supervisory authority, or a judiciary procedure on data privacy matters, the Local DP Officer shall inform the Global DP Lead or a relevant member of the Data Privacy Compliance Team.

If a local Accenture entity has reason to believe that local applicable laws prevent it from complying with Policy 90, it will inform the Global DP Lead or a relevant member of the Data Privacy Compliance Team who will take a responsible decision on what action to take and who will, in case of doubt, consult those data privacy supervisory authorities that have issued an authorization in respect of Accenture’s Binding Corporate Rules.
3.2 Compliance with local data privacy laws

In addition to complying with the Policy, each Accenture entity is responsible for taking such additional action as may be desirable or necessary to comply with the data privacy laws and regulations in the country in which it operates.

Upon the request of another Accenture entity, or any of the Accenture data privacy officers, an Accenture entity will supply a copy of such laws and regulations to the requesting party. In addition, to the extent that an Accenture entity from time to time adopts internal procedures designed to promote compliance with such local laws and regulations, it will provide the Global DP Lead with a copy of such procedures.

4. CO-OPERATION WITH NATIONAL DATA PRIVACY AUTHORITIES

Each Accenture entity will cooperate appropriately with the relevant national data privacy supervisory authority in cases of any requests for information or inspections from such an authority.

The Accenture entity will respond to any such requests within a reasonable timeframe and will endeavor to comply with any advice or decisions of such an authority in relation to the processing of personal data subject to any rights Accenture may have in applicable data privacy laws.

Any changes to Policy 90 will be made in accordance with standard Accenture internal procedures for policy approval and changes.

Accenture shall communicate material changes to Policy 90 (including the country supplements and the associated memoranda) and to the intercompany agreement (an agreement entered into between Accenture entities to give binding effect to Policy 90) to any data privacy supervisory authority that has issued an authorization in respect of Accenture’s Binding Corporate Rules once a year, except where such changes are required by applicable data protection and privacy laws court or data privacy supervisory authority’s decision.

5. DATA PRIVACY AUDITS

Accenture will carry out periodic data privacy compliance audits. These shall be conducted internally, by the DP Compliance Team and/or the internal audit function, or commissioned externally with a specialist auditing organization.

The purpose of the audits will be to assess the level of compliance with the Policy and applicable data privacy laws and regulations within an Accenture entity, or a function.

During the audit, each Accenture entity shall cooperate with the auditor(s) and shall disclose to the auditors any and all information or documents as may be required for the accomplishment of the auditors’ objectives, subject to compliance with any local laws and regulations.

The results of the audit shall be reported to the DP Compliance Team, the relevant local DP officer and the other relevant Accenture functional and geographic leadership and shall be made available to any data privacy supervisory authority that has issued an authorization in respect of Accenture’s Binding Corporate Rules upon their reasonable request.

The Global DP Lead, Local DP Officer and any other member of the DP Compliance Team shall action any findings of the audit report, in co-operation with other Accenture leadership identified in the audit report.
Where the audit report reveals a non-compliance with the Policy, or with the applicable data privacy laws and regulations, the DP Compliance Team shall propose solutions and determine a time period to implement corrective measures.
ANNEX 3

MEMORANDUM B:

PROCEDURES FOR RESPONDING TO INDIVIDUALS’ REQUESTS TO EXERCISE THEIR RIGHTS UNDER GLOBAL DATA PRIVACY POLICY

CONTENTS

1. PREAMBLE

2. THE RIGHTS OF ACCESS, RECTIFICATION AND OBJECTION
   2.1 Nature of the rights
   2.2 Who can make a request?

3. PROCEDURE FOR RESPONDING TO REQUESTS FROM INDIVIDUALS

4. EXERCISE OF THE RIGHT OF ACCESS
   4.1 Response time
   4.2 Processing requests

5. EXERCISE OF THE RIGHT OF RECTIFICATION

6. EXERCISE OF THE RIGHT TO OBJECT
   6.1 Right to object to direct marketing
   6.2 Right to object on compelling and legitimate grounds
1. PREAMBLE

The purpose of this memorandum is to set out the procedures which apply whenever an individual exercises any of the rights given in the Global Data Privacy Policy 90 (the Policy) and the applicable data privacy laws and regulations, in particular the right of access; the right of rectification (correction); and, the right to object.

The Policy and this memorandum do not apply to personal data processed by Accenture on behalf of and upon the instructions of clients of Accenture during the provision of consulting and outsourcing services.

2. THE RIGHTS OF ACCESS, RECTIFICATION AND OBJECTION

2.1 Nature of the rights

The Policy and the applicable data privacy legislation and regulations provide that any individual has a right to access personal information Accenture processes about her/him. If Accenture processes such information, the individual may request a copy of such information.

The individual may also request the rectification of such information if it is found to be incomplete and/or inaccurate.

Individuals also have the right to object to the processing of their personal data by Accenture. When such data are processed for direct marketing purposes, the objection can be made upon request and free of charge. When such data are processed for other purposes, the individual has the right, in accordance with the Policy and applicable data privacy laws and regulations, to object to such processing on the basis of compelling legitimate reasons.

Any individual is allowed to exercise the above rights and Accenture will consider, respond and process such requests in a considerate and prompt manner.

2.2 Who can make a request?

Requests may be made by any individual, within or outside Accenture, such as current and former personnel, job applicants, client contacts, supplier and vendor contacts and website users. The individual can only make a request in respect of data relating to him/her: it is strictly a personal right.

3. PROCEDURE FOR RESPONDING TO REQUESTS FROM INDIVIDUALS

The Local Data Privacy Officer (Local DP Officer) is responsible for considering, responding to, and processing all requests by individuals in their jurisdiction to exercise the rights of access, rectification and objection. If appropriate, the Local DP Officer will be assisted by the relevant local Legal & Commercial contact and any functional data privacy representatives, in countries where such representatives have been appointed or a representative of the relevant department or function. In the absence of a Local DP Officer, a relevant Legal & Commercial contact should process these requests.
The Global Data Privacy Lead (Global DP Lead) and a relevant member of the Data Privacy Compliance Team will be involved at the discretion of the Local DP Officer, and/or in any case involving any global databases and procedures.

The Local DP Officer will consider, respond to and process all requests within the timeframe required by applicable data privacy legislation and regulations.

If a person other than the Local DP Officer receives a request from any individual wishing to exercise his/her rights, s/he must immediately forward it to the Local DP Officer.

The Local DP Officer will open a case-file (electronic or manual) for each request from an individual seeking to exercise his/her rights under the Policy or applicable data privacy legislation and regulations. The file will contain all the relevant documentation, including any correspondence, both internal and with the individual. The Local DP Officer will maintain the file in accordance with Accenture’s document retention policy in case the individual makes a subsequent request, or complains to the national data privacy supervisory authority.

The Local DP Officer will keep a log of the numbers and the types of requests by individuals seeking to exercise their data privacy rights. The Local DP Officer will provide this information to the Global DP Lead on an annual basis.

4. EXERCISE OF THE RIGHT OF ACCESS

An individual making a request for access is not required to justify the request.

The individual concerned has a right to request the following:

- to know whether Accenture processes personal data concerning him/her,
- the purposes for which such data are processed,
- the categories of data undergoing processing,
- the recipients or categories of recipients of such data,
- any information available as to the origin of such data,
- a copy of the actual data processed about him/her.

If such processing may result in automated decisions, the request for access may also cover the logic involved in such automatic processing of data concerning the individual.

4.1 Response time

The Local DP Officer will respond to a request for access within a reasonable period following the receipt of such request, or within any specific period that may be set by any applicable data privacy laws and regulations.

4.2 Processing requests

The Local DP Officer, together with the persons identified in Section 3 above, will consider, respond to, and process a request from an individual to access their personal data as follows:

4.2.1 The Local DP Officer will ask the individual making a request to prove his/her identity, for example, by providing a copy of his/her personnel number, ID or any other satisfactory document to verify the individual’s identity.
4.2.2 The Local DP Officer may request the individual concerned to supply any additional information as may be necessary or desirable to better define his/her request, or to help Accenture locate the relevant data, in particular where the requested data relates to Accenture’s electronic mail systems.

4.2.3 The Local DP Officer will assess if the request falls within the scope of any exemptions from the right of access provided for by the applicable data privacy laws and regulations, or other applicable country laws.

If this is the case, the Local DP Officer will fully document any decision to withhold the data on the basis of an exemption provided in the applicable data privacy laws, or other applicable country laws. This will form part of the access request case-file, as described in Section 3 above.

4.2.4 The Local DP Officer will contact the relevant Accenture departments and functions likely to process personal data concerning the individual. Such departments and functions will co-operate with the Local DP Officer and supply any necessary information and data as the Local DP Officer deems appropriate.

4.2.5 Once the Local DP Officer has obtained all the information needed, the Local DP Officer will ensure that the disclosure of those data would not infringe the data privacy rights of another individual.

Where the information to be provided as a result of an access request contains data about another individual, the Local DP Officer will provide the requested information only if:

- it is possible to delete or conceal the data identifying the other individual, or
- the other individual has consented to such a disclosure, or
- in cases where consent has not been sought or has proven impossible to obtain, and where it is impossible to delete or conceal the data identifying the other individual, the Local DP Officer determines that under the circumstances of that particular case it is appropriate and reasonable to provide the data.

4.2.6 Where the requested data could not be provided to the individual due to the above considerations, or any other valid considerations under applicable data privacy laws and regulations, the Local DP Officer will inform the individual that Accenture is unable to respond to his/her request and specify the reasons for such decision.

The Local DP Officer will fully document any considerations and decisions in this respect and include it in the case-file described in Section 3 above.

4.2.7 The data to be provided to the individual must be presented in an intelligible form. Any codes used must be clearly explained and the data translated in a language comprehensible to the individual concerned.

4.2.8 The requested data will be provided to the individual concerned in a written form or, where agreed, the individual will be given the opportunity of viewing the requested data.

5. EXERCISE OF THE RIGHT OF RECTIFICATION

Any individual may, either as a result of an access request, or at any time, request that the personal data processed about her/him by Accenture be corrected whenever s/he considers such data to be inaccurate or incomplete.

On receipt of such a request, the Local DP Officer should verify that, taking into consideration the information communicated by the individual concerned, the data processed are actually inaccurate or incomplete. The individual making such request must provide appropriate documentation to the satisfaction of the Local DP Officer to substantiate the correction.
If the verification process shows that the data are actually inaccurate or incomplete, the Local DP Officer will instruct the relevant department or function to correct or complete the data. If the verification process shows the data in question to be accurate, the Local DP Officer shall make a note of the findings and communicate this to the individual.

When the information has been rectified, the department or function will send a copy of the rectified data to the Local DP Officer who, in turn, will forward this to the individual concerned to confirm that his/her request has been considered, and where appropriate, processed.

Where it is determined that incorrect and/or incomplete information was communicated to other Accenture and/or third party entities, the Local DP Officer will instruct the department or function concerned to communicate the rectified data to those entities, unless such operation is impossible or involves a disproportionate effort.

6. EXERCISE OF THE RIGHT TO OBJECT

6.1 RIGHT TO OBJECT TO DIRECT MARKETING

Any individual has the right to object at any time to receiving any promotional and marketing materials by post, telephone, fax, email or any other form of communication from Accenture. The individual also has a right to object to Accenture using his/her data for any direct marketing purposes.

Upon receipt of such an objection, the Local DP Officer will ask the departments or functions concerned to record such an objection on the relevant system, and cease using the individual’s data for direct marketing purposes.

This right may be exercised at any time notwithstanding any previously given consents (either opt-in, or opt-out) for direct marketing, which may have been obtained from individuals in the past.

6.2 RIGHT TO OBJECT ON COMPELLING AND LEGITIMATE GROUNDS

Accenture must abide by any justified request from an individual to stop the processing of his or her data, if the individual objects to the processing on compelling and legitimate grounds specific to that individual and where Accenture finds the request to be legitimate and appropriate.
ANNEX 4

MEMORANDUM C:

COMPLAINT HANDLING PROCEDURE

<table>
<thead>
<tr>
<th>Author</th>
<th>DP Compliance Team</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sponsoring</td>
<td>Legal</td>
</tr>
<tr>
<td>Organization</td>
<td></td>
</tr>
<tr>
<td>Applies to:</td>
<td>All personnel</td>
</tr>
</tbody>
</table>

CONTENTS

1. PREAMBLE
2. DATA PRIVACY COMPLIANCE FUNCTION
3. COMPLAINT PROCEDURE
   3.1 Submitting a complaint
   3.2 Persons involved
4. THE INQUIRY
5. INQUIRY FOLLOW-UP
   5.1 Drafting of a report
   5.2 The result of the complaint
1. PREAMBLE

The purpose of this memorandum is to set out the rules and the procedures to be followed by all Accenture entities and personnel to respond to any complaint arising out of the application of the Policy 90 or of the applicable data privacy laws or regulations.

These internal complaint and dispute resolution procedures are without prejudice to recourse to national courts, or the national data privacy supervisory authority, or such governmental, self-regulatory and/or other body as Accenture may designate to investigate or hear complaints, disputes or claims relating to the subject matter of the Policy.

The Policy and this memorandum do not apply to personal data processed by Accenture on behalf of and upon the instructions of clients of Accenture during the provision of consulting and outsourcing services.

2. INTERNAL DATA PRIVACY COMPLIANCE TEAM

Accenture has established a central data privacy compliance function directed by the Global Data Privacy Lead (Global DP Lead), and supported by Local Data Privacy Officers (Local DP Officer), for each country in which Accenture has an office.

Their responsibility is to oversee and ensure compliance with the Policy and applicable data privacy laws and regulations on the global, regional and country level.

3. COMPLAINT PROCEDURE

3.1 Submitting a complaint

Any individual whose personal data is processed and controlled by Accenture for Accenture’s own use and purposes, such as current and former personnel, job applicants, client contacts, supplier contacts, website users, may submit a complaint to the Local DP Officer in the following situations:

- If s/he considers to have suffered from a breach of the rules set out in the Policy or the applicable data privacy laws and regulations, or
- If s/he considers that there is a non-compliance with the Policy or the applicable data privacy laws and regulations.

The complaint must be submitted to the Local DP Officer in writing or personally by appointment. In the absence of a Local DP Officer, the complaint should be submitted to the relevant Legal & Commercial contact. An individual can also submit a complaint directly to the Global DP Lead or the relevant member of the Data Privacy Compliance Team.

Nobody in Accenture shall suffer any prejudice or undergo any sanction for having submitted a data privacy related complaint.

Any such complaint is without prejudice to the exercise of the rights of individuals, such as the right of access, rectification and objection, given in the Policy and applicable national data privacy laws and regulations.
3.2 Persons involved

Any complaints received by any Accenture department or function will be promptly passed to the relevant Local DP Officer, who will act upon it in a timely manner.

The Local DP Officer will conduct an inquiry, with the involvement and assistance of the relevant local contact in Accenture’s Legal & Commercial group.

Where the complaint implicates or is directed at an individual from another Accenture entity, the Local DP Officer will contact the Local DP Officer of the entity concerned and they will conduct an inquiry together.

The relevant member of the Data Privacy Compliance Team and/or Global DP Lead will assist in the inquiry in the following circumstances:

- if the complaint concerns any of Accenture global systems, global processes and global processing operations,
- if the alleged breach has been committed by an Accenture entity, other than the one where the individual’s data originated from or are located in, or
- if there is a disagreement between two Local DP Officers involved in the inquiry in the situation described above.

If the complaint concerns a member of the DP Compliance Team (including the Global DP Lead, other members of the Data Privacy Compliance Team and Local DP Officers), the complaint will be dealt with by the relevant Legal & Commercial Lead or ultimately the Accenture General Counsel and Compliance Officer.

4. THE INQUIRY

The procedure set out below is without prejudice to any provisions and requirements of applicable national laws and regulations, including but not limited to labor laws, which must be complied with.

The Local DP Officer will acknowledge receipt of the complaint in writing and, where applicable, may request in such acknowledgement additional information or documents from the person bringing the complaint.

If the complaint is against or is directed at one or more specific individual(s) identified or identifiable or, if in the course of the inquiry, the Local DP Officer discovers that an individual may be responsible for the breach of the Policy, the Local DP Officer will notify such individual(s) in writing of the following:

- that s/he is implicated in a data privacy complaint procedure, and
- that, in the course of the inquiry, the Local DP Officer may collect personal data concerning him/her from third parties.

This notification will contain a copy of this memorandum. This notification will not be necessary where providing such notification to the individual would prejudice the conduct and the outcome of the inquiry.

The Local DP Officer may ask, verbally or in writing, for such explanations or documents as s/he may deem adequate to determine the facts.

The individual at whom the complaint or inquiry is directed has the right to respond and present his/her point of view to the Local DP Officer. The Local DP Officer will notify the individual of this right from the outset or as soon as it is appropriate.
5. INQUIRY FOLLOW-UP

A. DRAFTING OF A REPORT

At the end of the inquiry, the Local DP Officer will produce a report, with the involvement of the persons described in Section 4.2 above. The Local DP Officer will send the report to:

a) the person bringing the complaint,
b) each of the individuals involved in the complaint or inquiry,
c) the relevant person in the Human Resources Department, or to the hierarchical superior of each individual implicated by the complaint or inquiry,
d) the head of the department concerned, in cases where the inquiry reveals any non-compliance in the procedures implemented within the department,
e) the Global Data Privacy Lead and relevant members of the Data Privacy Compliance Team,
f) the Geographic Legal Lead,
g) the Managing Director of the Accenture entity concerned, the relevant Geographic Services Lead and Accenture General Counsel (Corporate Compliance Officer) if the report states that an offence has been committed or that Accenture’s liability is at risk, or if the report recommends a more serious modification of the internal procedures applied for the processing of personal data.

The recipients of the report have a right to communicate their observations.

B. THE RESULT OF THE COMPLAINT

Where the complaint is justified, Accenture shall use reasonable efforts to rectify and remedy the situation which gave rise to the complaint, in accordance with the Policy and applicable data privacy laws and regulations.

In addition, where required, Accenture shall take appropriate action against any individual who has breached the Policy, in accordance with the provisions and requirements of applicable national laws and regulations, including but not limited to employment laws.

If the complaint handling process does not achieve the desired results for the individual who has made the complaint and such individual has the rights under the Data Protection Intercompany Agreement, Accenture shall inform the individual about their rights under the Agreement.
ANNEX 5

INTERCOMPANY AGREEMENT

"Note – this is a sample copy. A list of entities that have signed this agreement can be found at https://www.accenture.com/us-en/legal-countries-incorporation."

ACCENTURE (UK) LIMITED

AND

XXXXXXXX

DATA PROTECTION INTERCOMPANY AGREEMENT
### CONTENTS

<table>
<thead>
<tr>
<th>CLAUSE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Definitions</td>
<td>1</td>
</tr>
<tr>
<td>2. Authorization and Performance by Subsidiaries</td>
<td>4</td>
</tr>
<tr>
<td>3. Compliance with Policy 90</td>
<td>4</td>
</tr>
<tr>
<td>4. Third Party Beneficiary Rights</td>
<td>5</td>
</tr>
<tr>
<td>5. Indemnity</td>
<td>6</td>
</tr>
<tr>
<td>6. Term and Termination</td>
<td>6</td>
</tr>
<tr>
<td>7. English Language</td>
<td>7</td>
</tr>
<tr>
<td>8. Severability</td>
<td>7</td>
</tr>
<tr>
<td>9. Entire Agreement</td>
<td>7</td>
</tr>
<tr>
<td>10. Notice</td>
<td>7</td>
</tr>
<tr>
<td>11. No Partnership, Agency, Etc.</td>
<td>7</td>
</tr>
<tr>
<td>12. Governing Law and Jurisdiction</td>
<td>7</td>
</tr>
<tr>
<td>13. Counterparts</td>
<td>7</td>
</tr>
<tr>
<td>Schedule 1 DATA IMPORTERS</td>
<td>9</td>
</tr>
<tr>
<td>Schedule 2 ACCENTURE DATA PRIVACY POLICY 90</td>
<td>10</td>
</tr>
</tbody>
</table>
DATA PROTECTION INTERCOMPANY AGREEMENT

THIS AGREEMENT is made on the date(s) set forth below

BETWEEN AND AMONG:

ACCENTURE (UK) LIMITED, a company incorporated in England under company number 4757301, whose registered address is at 30 Fenchurch Street, London EC3M 3BD (hereinafter the “Data Privacy Administrator”) on its behalf and on behalf of each other Data Importer; and

XXXXXXXX, a company incorporated in XXXXXXX under company number XXXX, whose registered address is XXXXXXXXX.

WHEREAS:

2. The parties are members of the Accenture Organization (as defined below).

3. The Accenture Organization engages in a coordinated consulting, technology and outsourcing business serving clients that operate on a global basis utilizing state of the art know-how and technology.

4. In the course of its consulting, technology and outsourcing business, the Accenture Organization engages in activities that involve international transfers of personal data (as defined below) among the parties.

5. The laws of certain jurisdictions restrict international transfers of personal data except where there are adequate safeguards in place to protect the transferred personal data (subject, in some cases, to approval of those safeguards by a national data protection authority).

6. The parties wish to put this Agreement (and the other agreements contemplated herein) in place so as to adduce adequate safeguards to protect personal data transferred among them, and the parties have agreed to do so on the terms and conditions set out below and in the other agreements contemplated herein.

THEREFORE IT IS AGREED as follows:

2. DEFINITIONS

2.1. In this Agreement, "Commission", "controller", "data subject", "personal data", "processing" and "processor" have the respective meanings given to them in the Directive.

2.2. In this Agreement unless the context otherwise requires:

"Accenture PLC " means Accenture PLC, a Company incorporated in 1 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland with company number 98-0627530;

"Accenture Organization" means Accenture PLC (and its successor), Accenture SCA (and its successors) and their Subsidiaries;

"Accenture SCA" means Accenture SCA, a Luxembourg partnership limited by shares;

"Company" means the terms set out in this document (including its schedules) as amended from time to time;

"Agreement" means anybody corporate or partnership or unincorporated association carrying on any trade, business or any other activity, with or without a view to profit;

“Data Exporter” means XXXXXXX;

“Data Importer” means each of the persons set out in Schedule 1 (including the Data Privacy Administrator), as amended from time to time pursuant to this Agreement;
"Directive" means Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

"Effective Date" means:

a) in relation to the Data Privacy Administrator and the Data Exporter, the date of this Agreement; and

b) in relation to each other Data Importer, the later of the date of this Agreement and the date on which that Data Importer enters into an agreement (as "Data Exporter") with the Data Privacy Administrator containing terms and conditions substantially similar to this Agreement;

"Entity" means any Company within the Accenture Organization;

"Exporting Country" means, in the case of a claim by a data subject that he or she is entitled to enforce this Agreement as a third-party beneficiary under clause 4, the country from which the transfer of personal data concerning such data subject giving rise to the claim was made;

"Memoranda" means:

a) the following memoranda set out in schedule 2:

   i) Memorandum A: The Application of and Compliance with Accenture Data Privacy Policy 90;

   ii) Memorandum B: The Procedures for Responding to Individuals’ Requests to Exercise Their Rights under Global Data Privacy Policy 90; and

   iii) Memorandum C: The Complaints Handling Procedure; and

b) the other policies and/or documents referenced (but not incorporated by such reference) as part of the policy identified in paragraph (a) of the definition of "Policy 90", together with all amendments, supplements, translations and restatements of the foregoing from time to time;

"Original Data Exporter" means, in respect of any personal data that are subject to a Restricted Transfer, the Entity that was (or whose Subsidiary was), before the Restricted Transfer, the first Entity to obtain those personal data in a Protective Jurisdiction;

"Policy 90" means:

a) the policy set out in schedule 2, comprising Accenture Global Policy Number 90 entitled “Data Privacy”, together with all amendments, supplements, translations and restatements of the foregoing from time to time; and

b) the Memoranda;

"Protective Jurisdictions" means the member states of the European Economic Area and the other jurisdictions which have been found by the Commission under paragraph 6 of article 25 of the Directive to ensure an adequate level of protection, within the meaning of paragraph 2 of that article, for the protection of the private lives and basic freedoms and rights of individuals;

"Restricted Transfer" means a transfer of personal data which would, but for this Agreement, have been prohibited by restrictions on international transfer of personal data in the data protection law of a member state of the European Economic Area or another jurisdiction whose data protection laws impose such restrictions; and

"Subsidiary" means, in relation to a Company, any other Company:
a) which the first Company controls, where control means the ability whether directly or indirectly to direct the affairs of another by means of ownership, contract or otherwise; or

b) in which the first Company has the right under the constitution of that Company or by reason of the operation of an agreement among the members of that Company to direct the overall policy of that undertaking or to alter the terms of its constitution.

1.3 In this Agreement:

1.3.1 a reference to an Entity obtaining personal data is to be construed as including a reference to that Entity generating or otherwise acquiring those personal data (and "obtain" shall be construed accordingly); and

1.3.2 a reference to an Entity obtaining or transferring personal data is to be construed as including a reference to a processor obtaining or transferring those personal data on behalf of that Entity (and "obtain" and "transfer" shall be construed accordingly).

AUTHORIZATION AND PERFORMANCE BY SUBSIDIARIES

1 By execution of this Agreement, the Data Exporter authorizes the Data Privacy Administrator to:

2.1.1. enter into, and amend, from time to time, agreements containing terms and conditions substantially similar to this Agreement with other Entities (as "Data Exporters") on its behalf (as a "Data Importer") for the purpose of adducing adequate safeguards to protect personal data transferred by those other Entities to it (and agrees to be bound by such agreements as though it were a signatory thereto as a "Data Importer"); and

2.1.2. from time to time amend Schedule 1 to reflect all Entities that, as of the date of such amendment, have entered into, and remain subject to, an agreement with the Data Privacy Administrator containing terms and conditions substantially similar to this Agreement (and the Data Privacy Administrator shall determine, at its sole and absolute discretion, whether any agreement is deemed to contain terms and conditions similar to this Agreement for the purposes of this clause 2.1.2).

2.2. For the purposes of clause 2.1.2, the Data Exporter:

2.2.1. offers to enter into this Agreement with any Entity whose details are added to Schedule 1 in an amended copy provided to the Data Exporter by the Data Privacy Administrator from time to time;

2.2.2. authorizes the Data Privacy Administrator to receive such amended copies on its behalf; and

2.2.3. authorizes the Data Privacy Administrator to delegate to other Entities the authority granted hereunder.

2.3 The authorizations and offer set out in clauses 2.1 and 2.2 shall be irrevocable for the term of this Agreement.

2.4 Each Data Importer shall cause its Subsidiaries to adhere to this Agreement as though each such Subsidiary were a "Data Importer" party to this Agreement. If such Subsidiary (i) fails to comply with any performance obligation under this Agreement applicable to a "Data Importer" that is actionable under this Agreement and (ii) fails to permit the Data Exporter to seek recourse against it as a "Data Importer" party, then the Data Exporter shall have the right to seek recourse against the Data Importer for such failure.
COMPLIANCE WITH POLICY 90

1 Each Data Importer undertakes and warrants to the Data Exporter that:

3.1.1 it will comply with Policy 90 where it (or a processor on its behalf) processes personal data as a controller; and

3.1.2 it will comply with part 5 of Policy 90 where it processes personal data as a processor on behalf of the Data Exporter.

3.2 Each party undertakes and warrants to the other parties, that it will make a copy of this Agreement available to any data subject upon request.

4. THIRD PARTY BENEFICIARY RIGHTS

4.1 Subject to this clause 4, a person who is not a party to this Agreement has no right to enforce any term of this Agreement.

4.2 Subject to clauses 4.3, 4.5 and 4.6, any data subject as a third-party beneficiary:

4.2.1 can enforce:

a) any breach of clause 3.1 in relation to the processing of personal data concerning such data subject, or any breach of clause 3.2, by the Data Importer or its Subsidiary; and

b) any breach of clause 3.2 by the Data Exporter or its Subsidiary, against the Data Exporter; and

4.2.2 will, if it enforces any such breach against the Data Exporter under clause 4.2.1, be entitled to the remedies available under applicable law in respect of that breach, including rights to be paid compensation and/or obligations of the Data Exporter to take or procure remedial action.

4.3 A data subject is not entitled to enforce a breach of clause 3.1 against the Data Exporter unless:

4.3.1 the relevant personal data have been subject to a Restricted Transfer made by any Entity;

4.3.2 the Data Exporter was the Original Data Exporter in respect of those personal data; and

4.3.3 the Data Importer's or its Subsidiary's processing in breach of clause 3.1 takes place outside the Protective Jurisdictions.

4.4 If there is a dispute between a data subject and the Data Exporter in relation to an alleged breach of clause 3.1 or 3.2, and provided that the Data Exporter has been informed of the nature of the alleged breach, with sufficient information reasonably to enable it to consider the allegation, the burden of proof shall be on the Data Exporter to demonstrate that the alleged breach did not occur or that the Data Exporter is not responsible for that breach under this Agreement (including the third party beneficiary provisions of clause 4).

4.5 Clause 4.2 does not create third-party beneficiary rights in respect of breaches of clause 3.1 consisting solely of failures to comply with the Memoranda.

4.6 The parties to this Agreement do not require the consent of any data subject to rescind or vary this Agreement at any time.

5. INDEMNITY

5.1 Each Data Importer shall indemnify the Data Exporter and keep it indemnified against each loss, liability and cost incurred by the Data Exporter as a result of or in relation to a claim brought by a data subject against the Data Exporter under clause 4.2 alleging a breach of clause 3.1 or 3.2 by that Data Importer or its Subsidiary, including
each loss, liability and cost incurred as a result of defending or settling that claim, except to the extent that the loss, liability or cost arises as a result of a breach by the Data Exporter of clause 5.2.

5.2 In respect of any claim to which clause 5.1 applies, the Data Exporter shall:

1.1 promptly notify the relevant Data Importer of the claim (stating in reasonable detail the nature of the matter and, if practicable, the amount claimed);

1.2 in connection with proceedings related to the claim (other than against the Data Importer), use advisers chosen by the Data Importer and, if the Data Importer requests, allow the Data Importer the exclusive conduct of the proceedings;

1.3 give the Data Importer and its advisors reasonable assistance and information in relation to the claim; and

1.4 not admit liability in respect of or settle the claim without first obtaining the Data Importer’s written consent (not to be unreasonably withheld or delayed).

5.3 To the extent that Data Importer indemnifies Data Exporter:

(a) Any applicable taxes due to the indemnity will be billed as a separate item or line item. Data Importer shall pay any applicable transaction taxes that arise from the payment of indemnity. This excludes any taxes based solely on Data Exporters income or property. If Data Importer is required to withhold or deduct any taxes from indemnity payment, Data Importer shall not be required to “gross up” the amount of such payment and shall pay the total amount reflected on the invoice less the applicable withholding taxes. Data Importer and Data Exporter shall cooperate in good faith to minimize taxes to the extent legally permissible. Both Data Importer and Data Exporter shall provide and make available to the other any resale certificates, treaty certification or other exemption information reasonably requested.

6. TERM AND TERMINATION

6.1 This Agreement shall come into force, to the extent that it relates to the rights and obligations of each party, on the applicable Effective Date.

6.2 Any party (other than the Data Privacy Administrator) may terminate this Agreement at any time to the extent that it relates to that party’s rights and obligations under this Agreement by written notice to the Data Privacy Administrator. The Data Privacy Administrator shall promptly notify each other party of receipt of any such notice. Each party irrevocably authorizes the Data Privacy Administrator to receive such notifications on its behalf.

6.3 If this Agreement terminates to the extent that it relates to the rights and obligations of a particular Data Importer, the rights and obligations of that Data Importer under this Agreement, and the related rights of any third-party beneficiaries under clause 4, shall survive such termination to the extent that they relate to processing of personal data transferred to that Data Importer by the Data Exporter before such termination takes effect (and, to that extent, shall continue in full force and effect indefinitely).

6.4 The rights and obligations of each party under clause 3.2, and the related rights of any third-party beneficiaries, shall survive termination of this Agreement.

7. ENGLISH LANGUAGE

The English language version of this Agreement is the official and controlling text for all purposes.

8. SEVERABILITY

If any provision of this Agreement is determined to be partially void or unenforceable by any court or body of competent jurisdiction or by virtue of any legislation to which it is subject or by virtue of any other reason
whatsoever, it shall be void or unenforceable to that extent only and no further and the validity and enforceability of any of the other provisions herein shall not be affected thereby.

9. ENTIRE AGREEMENT

This Agreement and any documents referred to in this Agreement contain the entire agreement between and among the Data Exporter and the Data Importers (or any one of them) with respect to the subject matter hereof and supersede all previous agreements and understandings between them in relation to the same subject matter.

10. NOTICE

Notices shall be in writing (in English) and may be served by mail, e-mail with confirmation of delivery or facsimile with confirmation of delivery to the address of the party to be served stated in the signature page or last known to the party serving the notice and shall be deemed to have arrived if sent by post within three (3) days of posting and if sent by e-mail or facsimile at the time of transmission thereof. Each party irrevocably authorizes the Data Privacy Administrator to receive such notifications on its behalf, and the Data Privacy Administrator shall promptly notify each other relevant party of receipt of any such notice concerning such party.

11. NO PARTNERSHIP, AGENCY, ETC.

Subject to the authority granted to the Data Privacy Administrator under this Agreement, nothing in this Agreement (nor in the other agreements contemplated herein) shall create, or be deemed to create, a partnership or joint venture nor establish an agency relationship between the parties hereto.

12. GOVERNING LAW AND JURISDICTION

12.1 This Agreement shall be governed and construed in accordance with the laws of England, without regard to its conflict of law provisions.

12.2 If an individual claims to be entitled to enforce this Agreement against the Data Exporter as a third-party beneficiary under clause 4, the courts of the Exporting Country shall have exclusive jurisdiction to resolve any disputes arising as a result of or in connection with that claim.

13. COUNTERPARTS

This Agreement may be executed in one or more counterparts by the parties.

IN WITNESS WHEREOF, the parties have executed this Agreement on the date noted below, effective as of ___ __________, 20__.
ACCENTURE (UK) LIMITED

By:  
Its:  
Date:  
Address:  

30 Fenchurch Street,  
London  
EC3M 3BD

By:  
Its: Director  
Date:  
Address:  

XXXXXXXXX
**SCHEDULE 1**

**DATA IMPORTERS**

List of entities that agree to be bound by the terms of this agreement and that have authorised the data privacy administrator to enter into agreements similar to this agreement on their behalf with other entities within the Accenture organization.

This schedule may be amended pursuant to this agreement.

<table>
<thead>
<tr>
<th>Name</th>
<th>Country of Organization</th>
</tr>
</thead>
</table>


SCHEDULE 2

ACCENTURE DATA PRIVACY POLICY 90