FIRST DATA CORPORATION PROCESSOR DATA PROTECTION STANDARDS

1 As a world leader in electronic commerce and payment services, First Data Corporation and its subsidiaries ("First Data entity or entities"), all of which are collectively referred to in the alternative as ("First Data" or "our" or "we") provide processing solutions that help businesses and consumers engage in financial transactions nearly anywhere in the world, any time of the day, with virtually anyone in the world.

2 These Data Protection Standards express the commitment of our Executive Management and Board of Directors to data privacy and protecting all information relating to identified or identifiable natural individuals ("Data Subjects") that First Data processes (as defined below) while operating its business ("Personal Data") and in ensuring adequate protection of transfers of Personal Data between First Data entities. They emphasise and clarify the key role our employees play in providing protection for the privacy of Personal Data, and set out First Data’s overall approach to privacy and data protection.

Our Business

3 First Data operates in more than 34 countries across the United States, Latin America and Canada, Asia Pacific and the Europe, Middle East and Africa. First Data employs approximately 24,000 employees throughout these regions to provide around 60 billion payment transactions worldwide. First Data Corporation is the ultimate parent company of First Data and is headquartered in the United States.

4 First Data has nominated FDR Limited as the First Data entity within the EU to whom it delegates data protection responsibilities for the purposes of these Data Protection Standards. These responsibilities include accepting liability for breaches of these Data Protection Standards by First Data entities and / or external sub processors that are not First Data entities ("External Sub-Processors") used by First Data in processing the Personal Data outside of the EU and taking any action necessary to remedy such breaches, both as described more fully in paragraph 14 of these Data Protection Standards. First Data entities processing the Personal Data outside of the EU will be bound by these Data Protection Standards. External Sub-Processors will enter into separate arrangements with First Data to ensure the safeguarding of Personal Data in accordance with applicable law.

5 First Data has business relationships with financial institutions, credit card issuers, retail merchants, health care providers and other businesses to provide convenient and efficient payment services for tens of millions of consumers and businesses. To provide these services, First Data may process Personal Data, whether or not by automatic means, in ways such as collection, transferring, recording, organisation, storage, analysing, using, disclosing by transmission, dissemination or otherwise making available, adaptation or alteration, retrieval, consultation, alignment or combination, blocking, erasure or destruction ("process" or "processing" or "processes" or "processed"). First Data processes Personal Data in compliance with applicable data protection and privacy laws and our internal policies as amended and updated from time to time.

6 Due to the unique nature of our business, in most cases, First Data obtains Customer Information (as defined in paragraph 10 below) from our clients rather than the Data Subjects themselves. This information usually arises from a transaction initiated by a Data Subject with our client. Therefore usually First Data’s processing of Customer Information about Data Subjects is as a processor following our clients' instructions or those of other parties excluding First Data entities ("third party" or "third parties") from whom we receive information and ultimately governed by written contracts and/or applicable data protection and privacy laws. First Data's commitment to maintaining the highest standards of respect in relation to its processing of Personal Data is such that it has already applied for and been granted approval of its data protection standards in relation to the processing of Personal Data for which it is a controller and has been applying those standards so far as practicable to all Personal Data processed by First Data, including processor data. It was not possible for data processors to obtain approval of Binding Corporate Rules for Personal Data for which it was a processor at the time of its initial application and therefore First Data limited its initial application to controller data on the basis that it would apply for authorisation for its processor data as soon as that became possible. Therefore the authorisation of these Data Protection Standards in relation to Personal Data in respect of which First Data is a processor solidifies and formalises First Data’s commitment.
The Scope of These Data Protection Standards

These Data Protection Standards apply only to First Data entities which have signed a Binding Intra-Group Processor BCR Membership Agreement (the “Processor IGA”) and have a signed contract with the relevant Data Controller ensuring that the applicable First Data entity implements adequate technical and organisational security measures to safeguard the Personal Data, will only act on the instructions of the Data Controller and contains measures relating to the Data Controller’s and other third party beneficiaries’ right to enforce these Data Protection Standards (the “Services Agreement”). References to "First Data", "First Data entity or entities", "our" and "we" shall apply and refer only to such entities. A list of these entities is available from the Corporate Privacy Office whose details are set out at the end of these Data Protection Standards.

Data Subjects and Data Controllers alleging breach of these Data Protection Standards shall only be entitled to enforce them (in relation to the Data Subjects as a third party beneficiary) pursuant to paragraph 19 of these Data Protection Standards in respect to transfers of Personal Data made by a First Data entity or External Sub-Processor of that entity located in the European Economic Area (“EEA”) to a First Data entity or External Sub-Processor of that entity located outside the EEA (a "Transfer").

First Data acknowledges that some First Data entities may adopt their own privacy standards, policies and procedures based on the nature of their services or clients (“Local Policies”). The Local Policies must be consistent with and must meet or exceed the requirements of these Data Protection Standards. Where there is a conflict between the Local Policies and these Data Protection Standards, the policy that is determined by the Chief Privacy Officer in consultation with the General Counsel's Office to offer the highest protection will govern.

Categories of Data Subjects and Purposes of Processing and Transfers

Due to the unique nature of First Data's business, in most cases, First Data obtains Customer Information (defined below) from its clients rather than the Data Subjects themselves. This information usually arises from a transaction initiated by a Data Subject with our client who is usually the Data Controller in respect of the Personal Data of the Data Subject. Therefore usually First Data's processing of Customer Information about Data Subjects is as a processor following our clients' instructions or those of other parties (excluding First Data entities) from whom we receive information and are ultimately governed by written contracts and/or applicable data protection and privacy laws. In providing these services, First Data processes and transfers Personal Data including Sensitive Personal Data relating to the following classes of Data Subject:

- Our clients and their customers in connection with the provision of services ("Customer Information");
- Individuals making payment transactions;
- Merchants accepting payments;
- Other persons as appropriate to perform our clients' instructions, such as our clients' employees, suppliers, partners, contractors and contingent workers and prospective clients.

For the purposes of these Data Protection Standards, "Sensitive Personal Data" means any Personal Data about a Data Subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data about health or sex life, criminal record data, social security numbers and other national identifier numbers.

The processing and transfers undertaken by First Data in relation to the classes of Data Subject set out above includes processing for the business purposes as determined by our clients.

Nature of Data Transferred

First Data processes and transfers a broad range of Personal Data between First Data entities, External Sub-Processor of those entities and to third parties (which may include our clients) as relevant to the classes and purposes identified above. The types of Personal Data include:
- **Customer Information**: This includes contact information of clients' employees, information relating to the client's account, clients' customers' contact details including name, address and telephone numbers and account information including other persons on the account and spend thresholds, details of clients' customers' spending and spending patterns and details of the merchants accepting payment transactions to the extent these are individuals.

- **Personal Data**: As well as Customer Data, First Data also processes contact information of its clients' employees, suppliers and vendors including name, email address and telephone numbers and such other personal data as may be required in order for First Data to conduct business with such suppliers and vendors.

**Applicable Law and Supervising Authorities**

13 All First Data entities will handle Personal Data in accordance with these Data Protection Standards and all applicable local data protection and privacy laws and regulations including, but not limited to, the European Union Data Protection Directive (Directive 95/46/EC) and the Privacy in Electronic Communications Directive (Directive 2002/58/EC) (together the "Directives") and the United States Gramm-Leach-Bliley Financial Services Modernization Act (113 Stat. 1338) (the "GLBA"). Additionally, the Data Protection Standards must be interpreted in accordance with the Directives and all applicable data protection and privacy laws and regulations as well as with any obligations under the GLBA.

14 The policies and procedures described in these Data Protection Standards are in addition to any other remedies available under applicable data protection and privacy laws or provided under other First Data policies and procedures. FDR Limited will be responsible for and will take any action necessary to remedy any breach by any First Data entity or External Sub-Processor of the applicable First Data entity outside the EU of the rights guaranteed in these Data Protection Standards as provided by paragraph 19. This will include any sanction imposed or other remedy available under applicable data protection and privacy laws including compensation, where legally required. FDR Limited may discharge itself from this responsibility if it is able to show that the First Data entity and / or the External Sub-Processor of that entity which is alleged to be in breach is not liable for the breach or such First Data entity or the External Sub-Processor of that entity has discharged its liability for the breach.

15 Where applicable data protection and privacy laws provide less protection than those granted by these Data Protection Standards, these Data Protection Standards will apply. Where applicable data protection and privacy laws provide a higher protection, they will take precedence over these Data Protection Standards.

16 First Data shall co-operate as reasonably required with any data protection authority who has approved these Data Protection Standards ("Data Protection Authority"). Any questions about First Data’s compliance with applicable laws and regulations should be addressed to the First Data General Counsel’s Office ("General Counsel’s Office"), the First Data Chief Privacy Officer ("Chief Privacy Officer") or the relevant Local First Data Privacy Officer ("Local Privacy Officer") using the contact details set out at the end of these Data Protection Standards who will consult with the relevant Data Protection Authority, where applicable. Each Data Protection Authority is authorised to audit any First Data entity and advise on all matters related to these Data Protection Standards. First Data entities must follow any advice given by them in that regard, unless it conflicts with other local legal and/or regulatory requirements to which the relevant First Data entity is bound.

17 Where a First Data entity believes that a conflict with applicable laws prevents it from fulfilling its duties under these Data Protection Standards including following the advice of applicable Data Protection Authority, the entity will notify any affected Data Controller with whom it has a valid Services Agreement, the Local Privacy Officer and/or Chief Privacy Officer who will (in consultation with the General Counsel’s Office, the relevant Data Protection Authorities, affected First Data entities and / or the Data Controller, where necessary) responsibly decide what action to take.

**Changes to our Data Protection Standards**

18 First Data may change these Data Protection Standards, additional First Data entities may sign the Processor IGA and certain First Data entities may terminate or have their Processor IGA terminated. The Chief Privacy Officer will keep a fully updated list of First Data entities who are signatories to the Processor IGA and keep track
of and record any updates to these Data Protection Standards and provide the necessary information to Data Controllers with whom it has a valid Services Agreement, Data Subjects or Data Protection Authorities upon request. In addition, all changes, additions and the termination of any Processor IGA and any substantial change to the Data Protection Standards must be subject to the approval of the Chief Privacy Officer and will be reported to each Data Protection Authority annually and any Data Controllers with whom it has a valid Services Agreement in accordance with the terms of that Service Agreement. Any significant changes will be reported earlier, where required. Upon approval of the Chief Privacy Officer, we will clearly indicate the date of the latest revision and communicate the Data Protection Standards to all First Data entities and post the revision on First Data's public website. No transfers will be made to a new First Data entity until that First Data entity is effectively bound by these Data Protection Standards and able to comply with them.

**Compliance and Dispute Resolution**

19. Under paragraph 4 of these Data Protection Standards, FDR Limited has accepted liability for breaches of these Data Protection Standards by First Data entities outside of the EU and for taking any action necessary to remedy such breaches. First Data shall inform the Data Controller of any complaint made by a Data Subject as soon as reasonably practicable but shall not be obliged to handle or otherwise deal with such complaint further save where the Data Controller has factually disappeared, ceased to exist or become insolvent and no successor has assumed the obligations of the Data Controller. A Data Subject may only enforce these Data Protection Standards as a third party beneficiary in these limited circumstances. A Data Subject should always pursue the Data Controller in respect of any claims resulting from issues relating to the processing of its Personal Data.

Data Subjects and /or Data Controllers alleging breach of these Data Protection Standards against FDR Limited or the First Data entity or its External Sub-Processors making the Transfer (as defined in Paragraph 8) as provided in paragraphs 4 and 14 and in particular those set out in paragraphs 13, 16, 17, 19, 20 and 21 can enforce them only if they relate to a Transfer in the following ways:

(a) We strongly encourage Data Subjects and / or Data Controller to first raise any alleged breaches through the Complaints Handling Procedure – Security and Data Privacy Hotline (copies of which can be requested via First Data’s Corporate Privacy Office), using the process outlined in the First Data Corporation “Summary for Binding Corporate Rules for Data Privacy and Protection” which appears on First Data’s public website or with the Chief Privacy Officer or Local Privacy Officer who will work with them to endeavour to resolve their concern to their satisfaction.

(b) If the issue is not resolved to the Data Subject or Data Controller’s satisfaction or if the Data Subject or Data Controller prefers in the first instance without going to the Chief or Local Privacy Officer, he or she may directly:

- raise the issue of breach before the competent Data Protection Authority(ies) and First Data shall co-operate as reasonably required by that Data Protection Authority;
- bring the issue before either the courts of England and Wales, the courts of competent jurisdiction of First Data entity making the Transfer, or the Data Controller at the Data Subject's option; or
- if neither of the options above are applicable, bring the claim to the applicable court where the Data Subject is resident.

The complaints handling process under these Data Protection Standards is provided for by First Data's Privacy and Data Security Hotline. Further under First Data's Code of Conduct, there are a number of avenues under which Data Subjects can raise complaints regarding breaches of these Data Protection Standards. A decision on any complaint made will be communicated to the Data Subject within 28 days of the complaint being made in accordance with the process. First Data shall inform the Data Controller of any complaint made by a Data Subject as soon as reasonably practicable and shall co-operate with the Data Controller to assist the Data Controller to comply with its data protection obligations as agreed between the parties in the Services Agreement.

The rights contained in this paragraph are in addition to and shall not prejudice any other rights or remedies that a Data Subject may otherwise have at law including the right to compensation if appropriate.

**Communication of First Data’s Data Privacy Standards**
First Data takes compliance with its data protection obligations very seriously. All First Data employees who process Personal Data will comply with these Data Protection Standards receive training on and a copy of these Data Protection Standards and any relevant provisions of the Services Agreement. First Data will also post a copy of a summary of these Data Protection Standards on its internal and public websites. A full version can be requested from the Chief Privacy Officer and/or Local Privacy Officer and First Data will make physical copies permanently available at each of its offices and in the Corporate Privacy Office. In addition, a copy will be sent to Data Subjects on request. The Corporate Privacy Office will maintain a list of the First Data entities that are bound by these Data Protection Standards and will publish the list on First Data's public website.

First Data’s Privacy Principles

All First Data entities and employees will abide by the following principles when processing Personal Data.

1. **We process Personal Data fairly and lawfully**

   First Data processes Personal Data fairly and lawfully, in accordance with all applicable laws and regulations.

   Additionally, First Data shall upon the request of the Data Controller provide the Data Controller with such information relating to its processing and the processing of any of External Sub-Processors as may be reasonably required by the Data Controller to enable it to correctly inform its Data Subjects for the purpose of “fair processing”. These Data Protection Standards shall constitute First Data's "Fair Processing Notice" containing the information it is required under the Directive to give to Data Subjects. Where appropriate, the information given by these Data Protection Standards shall be supplemented as required by specific Fair Processing Notice in respect to a particular piece of processing.

2. **We obtain Personal Data only for carrying out lawful business activities.**

   First Data collects, transfers, holds and processes Personal Data only in accordance with the mandates it has with its clients and otherwise in accordance with its clients’ instructions.

3. **We limit our access to, and use of Personal Data.**

   First Data limits access to Personal Data to those employees who need access to this data to fulfil their responsibilities. All employees with access to Personal Data are forbidden from accessing or using this data for personal reasons or for any purposes other than fulfilling their First Data responsibilities. We require our External Sub-Processors, contractors, agents and suppliers to adopt a similar approach to Personal Data they access in connection with providing services to First Data.

   First Data processes Personal Data in accordance with its written agreements including the Service Agreement or with instructions from our clients or business partners (as applicable), in compliance with applicable data protection and privacy laws and in accordance with First Data's applicable policies as amended from time to time. Our use of Personal Data received from vendors or other third parties, such as credit bureaus, is governed by written agreements and by applicable data protection and privacy laws that specify permissible uses and restrict disclosures of the information.

4. **We transfer Personal Data as a processor only for limited purposes.**

   First Data will conduct intra-First Data entity transfers and transfers to third parties on the instructions of our clients and upon such other terms as we may agree with them and only when the following requirements have been met:

   - all applicable legal requirements are met;
where the transfer is to an External Sub-Processor, the transfer is as permitted by the agreements with our client or upon the instructions of our client;

where the transfer is to an External Sub-Processor, the receiving External Sub-Processor entity has appropriate security; and

the receiving party, if a First Data entity, complies with the Data Privacy Standards for the transfer and subsequent processing.

First Data entities may only appoint External Sub-Processors to process the Personal Data belonging to the Data Controller with the prior written consent of the Data Controller. The applicable First Data entity has appropriate agreements with its External Sub-Processors that reflect the applicable provisions of these Data Protection Standards and informs the Data Controller of the use of any External Sub-Processors with sufficient time for the Data Controller to object to the use of that particular External Sub-Processor.

First Data does not disclose Personal Data except in the circumstances set out in these Data Protection Standards or as required or otherwise permitted by applicable law.

Except as set out above and in accordance with First Data’s Data Controller Binding Corporate Rules, First Data does not sell, rent, share, trade or disclose any Personal Data it keeps about a Data Subject to any other parties without the prior written consent of the supplying client.

5. **We use appropriate security safeguards.**

First Data employs appropriate technical, organisational, administrative and physical security measures to protect Personal Data against unauthorised or unlawful processing and against accidental loss or destruction. First Data regularly reviews and, as appropriate, enhances its security systems, policies and procedures to take into account emerging threats, as well as emerging technological safeguards and precautions. First Data imposes security appropriate to the risk represented by the processing and nature of the Personal Data to be protected, with all due regard to the state of the art and cost measures.

First Data also enforces via the mechanism described in paragraph 21, section 8 upon all First Data entities and their employees the importance of the provisions of the Services Agreement and, in particular, those measures relating to instructions of the Data Controller with respect to the processing of Personal Data, the security of the Personal Data and confidentiality.

If a security breach occurs involving unauthorised access to Personal Data on a First Data system, First Data operates a response plan which is designed to assist First Data in complying with applicable laws requiring notification of security breaches, with guidelines produced by the relevant Data Protection Authorities in relation to security breaches and with our duties under our customer contracts including any Service Agreement. As appropriate or required, First Data will also notify law enforcement authorities, financial or other regulators and/or state agencies.

Personal Data will not be transferred to a country or territory which has inadequate data protection laws, unless adequate safeguards are in place.

Sensitive Personal Data will only be processed in accordance with applicable data protection and privacy laws and regulations including but not limited to the Directives. This may include the use of enhanced safeguards in relation to such Sensitive Personal Data, where necessary. Sensitive Personal Data will be disposed of under First Data's Information Security Policy and the Confidential Document Disposal Policy, further details of which can be obtained from the Chief Privacy Officer, or other applicable policies as may be implemented by First Data. First Data requires that all Sensitive Personal Data be transferred securely.

6. **We provide transparency, choice and access as required by applicable data protection and privacy law.**
Upon the request of the Data Controller, First Data will assist, to the extent instructed by the Data Controller, with verifying whether its Personal Data is up-to-date and is accurate, adequate, relevant, not excessive for the purposes for which it is processed and is kept for no longer than is necessary for the purposes for which it is being processed.

First Data shall pass each request of a Data Subject for access to his or her own Personal Information to the Data Controller and will work with the applicable Data Controller to provide a copy of the Personal Data First Data processes about that Data Subject as required by applicable laws and if so requested by the Data Controller. If a Data Subject asserts the Personal Data kept about him or her is incorrect, we will work with the Data Controller to rectify, block or erase the inaccuracy.

7. We recognise the importance of data privacy and hold ourselves accountable to our Data Protection Standards.

First Data operates a comprehensive network of privacy officers around the world who are responsible for data privacy within their region including compliance with these Data Protection Standards. The Chief Privacy Officer is responsible for the network of privacy officers and the development, implementation and continuing oversight of these Data Protection Standards. The Chief Privacy Officer, in coordination with the Senior Vice President, Internal Audit collaborates to establish an appropriate audit schedule for the First Data’s compliance and privacy programs including the BCR programme, which is then presented for approval to the Audit Committee of First Data’s Board of Directors as part of its annual overall Internal Audit review. The Chief Privacy Officer and the privacy officer network run various other privacy programmes, promote good privacy practices with respect to Personal Data throughout First Data through multiple means including annual training programmes, official communications and specifically targeted training. Further, the First Data Corporate Privacy Office works with other groups within First Data to develop additional corporate privacy policies and practices and has created the Data Security Council which aims to identify and reduce First Data's top security risks.

First Data further evidences its commitment to accountability by conducting regular internal privacy assessments including in relation to the principles set out in these Data Protection Standards as part of its comprehensive audit programme and provides mandatory training to its employees on privacy topics and issues relevant to their job type. Items identified through the audit programme are assigned to a First Data employee who is responsible for developing and executing a remediation plan and associated time frame. Upon completion, the audit team will review to determine if the item has been adequately addressed and can be closed or requires additional action. Where sought by the Data Protection Authority(ies), First Data shall supply that Data Protection Authority(ies) (including the competent Data Protection Authority of the Data Controller) with a copy of the audits. Subject to the terms of any valid Services Agreement with the Data Controller and only while such Service Agreement is in force, the Data Controller or an independent third party auditor may audit the applicable First Data entity for compliance with these Data Protection Standards, where legally permissible. Each Data Protection Authority is also authorised to audit any First Data entity in accordance with paragraph 16 of these Data Protection Standards.

In addition, First Data's employees are required to comply with the First Data Code of Conduct, which sets forth our commitment to uphold the privacy and confidentiality of Personal Data and Employment Data and various other privacy related policies. Any material violation of applicable laws, these Data Protection Standards, the Code of Conduct or relevant corporate policies by a First Data employee may result in disciplinary action, up to and including dismissal.

Finally, First Data participates actively in relevant privacy discussions, debates and works with other companies, organisations, consumer and advocacy groups and government agencies to ensure that First Data is apprised of relevant developments impacting the processing of Personal Data.

For further information relating to First Data's privacy officer network or provision of training programmes please see First Data's website or contact the Chief Privacy Officer and/or Local Privacy Officer.
Contact Information

Chief Privacy Officer and Corporate Privacy Office
First Data Corporation
6902 Pine St
PS-30
Omaha, NE 68106
Telephone Phone: +1 (402) 222-0050
          +1 (888) 337-0434 (toll free US)
Facsimile Number: +1 (402) 916-6100
Email Address: dataprivacyoffice@firstdata.com

General Counsel and General Counsel’s Office
First Data Corporation
5775 DTC Blvd.
Mail Stop 100 North
Greenwood Village, CO 80111
Telephone Phone: +1 404 890-2000

Local Privacy Officers

Privacy Officers
Janus House
Endeavour Drive
Basildon
Essex SS14 3WF
Tel: +44 (0)1268 296839
Fax: +44 (0)1268 296967