FIRST DATA CORPORATION PROCESSOR DATA PROTECTION STANDARDS

Effective as of 05 July 2019

1 Who we are

1.1 As a world leader in electronic commerce and payment services, First Data Corporation, a corporation organised and existing under the laws of the State of Delaware, USA whose principal place of business is at 225 Liberty Street, 29th Floor, New York, New York 10281, United States of America and its subsidiaries ("**First Data**" or "**our**" or "**we**" as further defined in paragraph 3.1.1) 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.

1.2 These Processor Data Protection Standards (including the attached Annex) 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 and where the data protection laws of a Relevant Country apply (both as defined and provided for in paragraph 3.1.1). They emphasise and clarify the key role our personnel play in providing protection for the privacy of Personal Data, and set out First Data's overall approach to privacy and data protection.

2 Our Business

2.1 First Data operates in more than 100 countries worldwide. First Data employs approximately 22,000 employees throughout the world to provide more than 93 billion payment transactions every year. First Data Corporation is the ultimate parent company of First Data and is headquartered in the United States.

2.2 First Data has nominated FDR Limited as the First Data establishment within the UK and the EU as applicable to whom it delegates data protection responsibilities for the purposes of these Processor Data Protection Standards. These responsibilities include accepting liability for breaches of these Processor 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 7.2 of these Processor Data Protection Standards. First Data entities processing the Personal Data outside of the EU will be bound by these Processor 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.

2.3 First Data has business relationships with financial institutions, credit card issuers, acquirers, 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 collecting, transferring, recording, organising, structuring, storing, analysing, using, disclosing by transmission, dissemination or otherwise making available, adapting or altering, retrieving, consulting, aligning or combining, blocking, erasing or destroying ("**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.

3 The Scope of These Processor Data Protection Standards

3.1 These Processor Data Protection Standards apply only:

3.1.1 to First Data entities which have signed a Binding Intra-Group Processor BCR Membership Agreement ("**Processor IGA**") and in respect of the processing of Personal Data in respect of which a First Data entity has 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, contains measures relating to the Data Controller's and other third party beneficiaries' right to enforce these Processor Data Protection Standards and contains all the other provisions required by Article 28 of the GDPR (the "**Services Agreement**"). References to **"First Data**", "**First Data entity**" or "**First Data entities**", "**our**" and "**we**" shall apply and refer only to such entities. A list of these entities is available at the First Data Privacy Site or form the Global Privacy Office whose details are set out at the end of these Processor Data Protection Standards. All First Data entities can be contacted by email at DPO@firstdata.com, or using the contact details set out at the end of these Processor Data Protection Standards; and

3.1.2 where the data protection laws of a Relevant Country apply to First Data's processing of Personal Data, or where the data protection laws of a Relevant Country applied to such processing prior to the Personal Data being transferred between First Data entities in accordance with these Data Protection Standards or where the Services Agreement otherwise provided that these Processor Data Protection Standards should apply and all references in these Data Protection Standards to Personal Data shall be interpreted accordingly. Relevant Countries means the Member States of the European Union and the European Economic Area (and the UK from the date at which it ceases to become a Member State of the EU).

3.2 Due to the unique nature of our business, in many cases, First Data obtains Personal Data (as defined in paragraph 4.1 below) from our clients rather than the Data Subjects themselves. This information sometimes arises from a transaction initiated by a Data Subject with our client. Therefore First Data's processing of Personal Data about Data Subjects may be: (a) as a controller, for the purposes determined by First Data; or (b) as a processor following our clients' instructions or those of other parties including other First Data entities from whom we receive information and which are ultimately governed by written contracts and/or applicable data protection and privacy laws.

3.3 First Data has been granted authorisation for: (a) its Controller Data Protection Standards (the "**Controller Data Protection Standards**"), which apply only in relation to Personal Data for which First Data is a controller (available at the following website: https://www.firstdata.com/en_us/privacy.html (the "**First Data Privacy Site**")); and (b) these processor data protection standards, which apply only in relation to Personal Data for which First Data is a processor (the **"Processor Data Protection Standards**").

3.4 First Data's commitment to maintaining the highest standards of respect for Personal Data is such that it intends to apply the appropriate Data Protection Standards to both controller and processor data processed by First Data entities.

3.5 These Processor Data Protection Standards apply to all Personal Data transferred by one First Data entity to another First Data entity where First Data is a processor of the Personal Data.

3.6 Data Subjects and Data Controllers alleging breach of these Processor Data Protection Standards shall only be entitled to enforce them (in relation to the Data Subjects as a third party beneficiary) pursuant to paragraph 9.1 of these Processor 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 a Relevant Country to a First Data entity or External Sub-Processor of that entity located outside the EEA (a "**Transfer**").

3.7 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 Processor Data Protection Standards. Where there is a conflict between the Local Policies and these Processor Data Protection Standards, the policy that is determined by the Data Protection Officer and Global Privacy Office in consultation with the General Counsel's Office (as defined below in paragraph 7.4) to offer the highest protection will govern.

4 Categories of Data Subjects and Purposes of Processing and Transfers[1]

4.1 First Data's processing and transfer of Personal Data including Special Categories of Personal Data (as defined below) for which it is a processor relates to the following classes of Data Subject:

- Our clients and their customers in connection with the provision of services ("**Customer Information**");
- Individuals initiating 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 of First Data and, in each case, their personnel.

4.2 For the purposes of these Processor Data Protection Standards, "**Special Categories of Personal Data**" means any Personal Data revealing race or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Personal Data relating to a Data Subject's criminal convictions and offences or related security measures will only be processed in accordance with applicable local laws and regulations.

[1] See scope of Data Protection Standards at Paragraph 3.5

5 Sources of Personal Data

5.1 Where instructed by the relevant Data Controller, First Data collects information from a number of sources:

- **From the Data Subjects** – for example, we collect Personal Data from our actual and potential clients and business contacts, for example in completing online forms, in connection with their working relationship, or from business contacts. We may also collect Personal Data directly from holders of payment instruments when they engage in a transaction;
- **From our clients** - First Data obtains transaction-related Personal Data from its clients to enable it to process payment transactions and provide other related services to the Data Subjects of those clients;
- **From our group companies** – Personal Data may be shared between First Data entities in accordance with these Processor Data Protection Standards, or otherwise where permitted by law;
- **From other third parties** - we may collect information about Data Subjects from third parties, such as former employers, credit reference agencies (who may check the information against other databases – public or private – to which they have access) or fraud prevention agencies;
- **From public sources** – we may collect and check Data Subjects' information against other public databases and sources to which we have access; and
- **Information we create** - we may create and record information in relation to Data Subjects. For example, we may create details of transactions a Data Subject carries out, the services we provide to Data Subjects, and their interactions with us, for example, if a Data Subject contacts us, we may keep a record of that correspondence.

5.2 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.

5.3 We collect and use Personal Data information for a variety of legal reasons as determined by our clients.

6 Nature of Data Transferred[2]

6.1 First Data processes and transfers a broad range of Personal Data between First Data entities, External Sub-Processors of those entities and to other third parties which are not First Data entities (which may include our clients) ("**third party**" or " **third parties**") as relevant to the classes and purposes identified above. The types of Personal Data include:

- **Customer Data**: This includes contact information of clients' personnel, 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' payment instruments (such as credit cards), transactions, spending and spending patterns and details of the merchants accepting payment transactions to the extent these are individuals.
- **Other Personal Data:** As well as Customer Data, when instructed by the applicable Data Controller, First Data also processes contact information of its suppliers and vendors including name, email address and telephone numbers.

7 Applicable Law and Supervising Authorities

7.1 All First Data entities will handle Personal Data in accordance with these Processor Data Protection Standards and all applicable local data protection and privacy laws and regulations including, but not limited to, the European Union General Data Protection Regulation

[2] See footnote 1.

(2016/679) (the "**GDPR**") , the UK GDPR, the UK Data Protection Act 2018 and the Privacy in Electronic Communications Directive (Directive 2002/58/EC) ("**PECR**") (until such time that it is replaced by a regulation concerning the protection of personal data in electronic communications (the "**ePrivacy Regulation**")) (together the "**Privacy Laws**") and the United States Gramm-Leach-Bliley Financial Services Modernization Act (113 Stat. 1338) (the "**GLBA**"). Additionally, the Processor Data Protection Standards must be interpreted in accordance with the Privacy Laws and all other applicable data protection and privacy laws and regulations as well as with any obligations under the GLBA.

7.2 The policies and procedures described in these Processor 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 or the UK of the rights guaranteed in these Processor Data Protection Standards as provided by paragraph 9.1. This will include any sanction imposed or other remedy available under applicable data protection and privacy laws including compensation. 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.

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

7.4 First Data shall co-operate as reasonably required with any supervisory authority in a Relevant Country (including the Information Commissioner in the UK) ("**Supervisory Authority**"). Any questions about First Data's compliance with applicable laws and regulations should be addressed to the General Counsel's Office, Data Protection Officer, Global Privacy Office or the relevant Local Privacy Officer using the contact details set out at the end of these Processor Data Protection Standards who will consult with the relevant Supervisory Authority, where applicable. Each Supervisory Authority is authorised to audit any First Data entity and advise on all matters related to these Processor 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.

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

7.5.1 Where a First Data entity believes that a conflict with applicable laws is likely to have a substantial adverse effect on the guarantees provided by these Processor Data Protection Standards, the Data Controller and the competent Supervisory Authorities will be notified, unless such notification is otherwise prohibited by applicable laws. In particular, if there is any legally binding request for disclosure of the Personal Data by a law enforcement authority or state security body, the request for disclosure shall be put on hold and the competent Supervisory Authority for the Data Controller and the competent Supervisory Authority with respect to the applicable First Data entity will be notified about the request, including information about the data requested, the

requesting body, and the legal basis for the disclosure, unless such notification is otherwise prohibited by applicable laws;

7.5.2 If the notification to the competent Supervisory Authority is prohibited by applicable laws, the First Data entity will use its best efforts to obtain a waiver of this prohibition in order to communicate as much information as it can, and as soon as possible, to Supervisory Authority;

7.5.3 If, having used its best efforts, the waiver is not granted, First Data will provide general information on the requests it receives to the competent Supervisory Authority annually as described in paragraph 8.1 of these Processor Data Protection Standards, to the extent permitted under applicable law.

8 Changes to our Data Protection Standards

8.1 First Data may change these Processor 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 Data Protection Officer with the assistance of the Global Privacy Office 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 Processor Data Protection Standards and provide the necessary information to Data Controllers with whom it has a valid Services Agreement, Data Subjects or Supervisory Authorities upon request. In addition, all changes, additions and the termination of any Processor IGA and any change to the Processor Data Protection Standards must be subject to the approval of the Data Protection Officer and will be reported to each Supervisory Authority annually and any Data Controllers with whom it has a valid Services Agreement in accordance with the terms of that Services Agreement. Any significant changes will be reported without undue delay, where required. Where an update significantly affects these Processor Data Protection Standards, or could affect the level of protection offered by them, First Data will promptly communicate the update to the relevant Supervisory Authorities. Upon approval of the Data Protection Officer, we will clearly indicate the date of the latest revision and communicate the Processor 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 Processor Data Protection Standards and able to comply with them.

8.2 If a Data Subject would like to access previous versions of these Processor Data Protection Standards, these can be requested from the Data Protection Officer.

9 Compliance and Dispute Resolution

9.1 Under paragraph 2.2 of these Processor Data Protection Standards, FDR Limited has accepted liability for breaches of these Processor 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 Processor 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.

9.2 Data Subjects and /or Data Controllers alleging breach of these Processor Data Protection Standards against FDR Limited or the First Data entity or its External Sub-Processors making the Transfer (as defined in Paragraph 3.6) as provided in paragraphs 2.2 and 7.2 and in particular those set out in paragraphs 7.1, 7.4, 7.5 and 11 can enforce them only as a third party beneficiary if they relate to a Transfer in the following ways:

9.2.1 We strongly encourage Data Subjects and / or Data Controllers to first raise any alleged breaches through the First Data's Privacy and Data Security Hotline, (which is available at the First Data Privacy Site or on 00800-368-1000) or with the Data Protection Officer or Local Privacy Officer who will work with them to endeavour to resolve their concern to their satisfaction without undue delay.

9.2.2 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 Data Protection Officer or applicable Local Privacy Officer, he or she may directly:

- raise the issue of breach before a competent Supervisory Authority including in the country of his or her habitual residence, place of work or place of the alleged infringement and First Data shall co-operate as reasonably required by that Supervisory Authority;

- bring the issue before either the courts of England and Wales, the courts of any EU member state where First Data has an establishment, or the courts of the country where the Data Subject has his or her habitual residence, at the Data Subject's option.

9.3 Subject to paragraph 3.6, any Data Subject who has suffered damage (whether material or non material) as a result of an infringement of the rights expressly granted to Data Subjects under these Processor Data Protection Standards will have the right to receive compensation from First Data for the damage suffered First Data shall have the burden of proving that it is not in any way responsible for the event giving rise to the damage. The compensation claimed by a Data Subject is limited to that which would be due under Article 82 of the GDPR.

9.4 The complaints handling process under these Processor Data Protection Standards is provided for by First Data's Privacy and Data Security Hotline. Further, under First Data's Code of Conduct, First Data's personnel can raise complaints regarding breaches of these Processor Data Protection Standards by contacting the Data Protection Officer or through the First Data's Privacy and Data Security Hotline. A decision on any complaint made (whether made by First Data's Personnel or other Data Subjects) will be communicated to the Data Subject within one (1) month of the complaint being made, save that taking into account the complexity and number of complaints a response may be extended by up to two (2) further months and First Data shall inform the Data Subject accordingly. First Data shall inform the Data Controller of any complaint made by a Data Subject without undue delay 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.

9.5 The rights contained in this section of these Processor Data Protection Standards 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.

10 Communication of First Data's Data Privacy Standards

10.1 First Data takes compliance with its data protection obligations very seriously. All First Data personnel who process Personal Data will comply with these Processor Data Protection

Standards, and receive training on and access to these Processor Data Protection Standards and any relevant provisions of the Services Agreement. First Data will post a copy of these Processor Data Protection Standards on its internal and public websites, including on the First Data Privacy Site. In addition, Data Subjects will be provided with a link to our public website upon request. The Data Protection Officer and the Global Privacy Office will maintain a list of the First Data entities (including contact details) that are bound by these Processor Data Protection Standards and will publish the list on the First Data Privacy Site.

11 First Data's Privacy Principles

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

We process Personal Data fairly and lawfully ('lawfulness, fairness and transparency')

11.1 First Data processes Personal Data fairly and lawfully and in a transparent manner in relation to the Data Subject, in accordance with all applicable laws and regulations.

11.2 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 complying with its legal obligations relating to this principle of 'lawfulness, fairness and transparency'. First Data's information notice containing the information it is required to give to Data Subjects under GDPR is set out in: (a) these Processor Data Protection Standards; and (b) First Data's privacy policy, which is available at the First Data Privacy Site (the "**Privacy Policy**"). Where appropriate, the information given by these Processor Data Protection Standards and the Privacy Policy shall be supplemented as required by a specific information notice in respect to a particular piece of processing.

We obtain Personal Data only for carrying out lawful business activities ('purpose limitation').

11.3 First Data collects, transfers (including transfers outside the EEA), holds and processes Personal Data only in accordance with the mandates it has with its clients and otherwise in accordance with its clients' instructions.

We limit our access to, and use of Personal Data ('data minimisation') and we do not store Personal Data longer than necessary ('storage limitation').

11.4 Personal Data processed by First Data will be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

11.5 First Data will keep Personal Data in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is processed, as described in Paragraph 5.2. The purposes of retaining the data, and the specific retention periods, will be as instructed by the relevant Data Controller or, in the absence of any such instructions, in accordance with First Data's applicable data retention policies on expiry of which First Data will securely delete the relevant Personal Data or return such Personal Data to the applicable client, as agreed with that client. First Data's retention periods are determined by factors such as the need to retain data to provide services to Data Subjects or our clients, the need to comply with applicable laws and requirements to comply with the rules

provided by participants in a transaction processing chain, such as the rules provided by card associations and debit network operators and their members.

11.6 First Data limits access to Personal Data to those personnel who need access to this data to fulfil their responsibilities. All personnel 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.

11.7 First Data processes Personal Data in accordance with its written agreements including the Services 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.

We keep Personal Data accurate and, where necessary, up-to-date ('accuracy')

11.8 First Data will execute necessary measures upon the request of the Data Controller to ensure Personal Data is kept up-to-date and is accurate. First Data will take every reasonable step to ensure that, in relation to the purposes for which it is processed and in accordance with the request from the Data Controller, Personal Data that is inaccurate is erased or rectified without delay and will inform any other First Data entities to whom it has disclosed such Personal Data of such erasure or rectification, if applicable.

We implement data protection by design and default.

11.9 Where appropriate, First Data will implement appropriate technical and organisational measures, such as pseudonymisation and data minimisation, which are designed to implement, and to facilitate compliance with, these Processor Data Protection Standards in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of these Processor Data Protection Standards and to protect the rights of Data Subjects, taking into account the nature of the processing and the information available to it.

11.10 First Data will implement appropriate technical and organisational measures for ensuring that, by default, only Personal Data which is necessary for each specific purpose of the processing are processed, in relation to the amount of Personal Data collected, the extent of processing, the period of storage and accessibility in order to assist with its client's obligations under applicable law and any agreements with that client.

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

11.11 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 (including the conditions in Chapter V of the GDPR);
- 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.

11.12 First Data entities may only appoint External Sub-Processors to process the Personal Data belonging to the Data Controller with the prior specific or general 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 Processor 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.

11.13 Where the conditions above are met, the recipients of Data Subjects Personal Data may include:

- First Data entities;
- First Data's clients;
- other participants in a transaction processing chain, such as merchants, issuers of payment instruments, providers of payment instrument acquiring services, card associations and debit network operators and their members;
- third parties, upon the request of the Data Controller,
- third parties to whom First Data will transfer, or may transfer, its rights and duties in its agreements with Data Controllers, including if a First Data entity, or substantially all of its assets, are acquired by such third party, in which case Personal Data held by it will be one of the transferred assets;
- third parties to whom First Data is under a duty to disclose or share Personal Data in order to comply with any legal obligation;
- third parties, where required to protect the rights, property, or safety of First Data, our clients, or their customers or others;
- First Data's vendors and agents (including their sub-contractors). In particular, First Data may disclose Personal Data where it uses the services of:
  - credit reference agencies;
  - fraud protection and risk management agencies;
  - identification and information verification agencies;
  - vendors and others that help us process a Data Subject's payments;
  - third party suppliers engaged to host, manage, maintain and develop our website and IT systems; and
  - our professional advisers, including lawyers and auditors.

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

11.15 Except as set out above and in accordance with the Controller Data Protection Standards, 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.

We use appropriate security safeguards ('integrity and confidentiality').

11.16 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 will ensure that any personnel who has access to Personal Data has appropriate obligations of confidentiality in their employment agreement with First Data.

11.17 First Data also enforces via the mechanism described in paragraph 31, section 9 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.

11.18 If a security incident 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 incidents, with guidelines produced by the relevant Supervisory Authorities in relation to security incidents and with our duties under our client contracts including any Services Agreement. Each First Data entity will notify without undue delay any security incidents affecting Personal Data to FDR Limited and the Data Protection Officer who will inform the Data Controller of such breach in accordance with the applicable First Data policies and its agreement with the Data Controller, unless the security incident is unlikely to result in a risk to the rights and freedoms of the Data Subjects. As appropriate or required, First Data will also notify law enforcement authorities, financial or other regulators and/or state agencies (including the Supervisory Authorities). Any security incidents will be documented in a security incident log (including the facts relating to the security data breach, its effects and the remedial action taken) and the security incident log will be made available to the competent Supervisory Authority on request.

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

11.20 Special Categories of Personal Data will only be processed in accordance with applicable data protection and privacy laws and regulations including but not limited to the GDPR. This may include the use of enhanced safeguards in relation to such Special Categories of Personal Data, where necessary. Special Categories of Personal Data will be disposed of under First Data's Global Cyber Security Policy and the Data Classification and Handling Standard and associated Media Handling Standard, further details of which can be obtained from the Data Protection Officer, or other applicable policies as may be implemented by First Data. First Data requires that all Special Categories of Personal Data be transferred securely.

We respect Data Subject rights as required by applicable data protection and privacy law.

11.21 To the extent instructed by the Data Controller, First Data will assist the Data Controller, so far as is possible, with responding to requests by Data Subjects relating to the following:

- confirmation of First Data's processing of the Personal Data of the Data Subject.
- access to Personal Data of the Data Subject held by First Data.
- correction of Personal Data of the Data Subject held by First Data.
- deletion of Personal Data of the Data Subject held by First Data.
- requests that First Data's systems stop using Personal Data of the Data Subject.
- restrictions being placed on how First Data uses the Personal Data of the Data Subject.
- requests to move the Personal Data of the Data Subject held by First Data to other companies in an easily readable format.
- complaints to the relevant Supervisory Authority.

11.22 First Data shall pass each request of a Data Subject to exercise any of the rights above to the Data Controller and will work with the applicable Data Controller (including the provision of

useful information applicable to the right exercised) to help the Data Controller comply with its duty to respect the rights of Data Subjects in accordance with the GDPR.

We recognise the importance of data privacy and hold ourselves accountable to our Data Protection Standards ('accountability').

11.23 Each First Data entity will be responsible for, and able to demonstrate compliance with, these Processor Data Protection Standards. First Data's Global Privacy Office operates a comprehensive network of privacy officers around the world who are responsible for data privacy within their region including compliance with these Processor Data Protection Standards. The Data Protection Officer and Chief Privacy Officer are responsible for the network of privacy officers, including the Local Privacy Officers, and the development, implementation and continuing oversight of these Processor Data Protection Standards. The Global Privacy Office, and the privacy officer network including the Data Protection Officer run various 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 Global Privacy Office works with other groups within First Data to develop additional corporate policies and practices. The Global Cyber Security Program aims to identify and reduce First Data's top security risks.

11.24 First Data further evidences its commitment to accountability by conducting regular internal privacy assessments as part of its comprehensive audit programme and provides mandatory training to its personnel on privacy topics and issues relevant to their job type. Items identified through the audit programme are assigned to a member of First Data's personnel 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 and will provide their recommendation to the Data Protection Officer and to the Board of Directors of the relevant First Data entity and, where deemed appropriate by the Data Protection Officer, First Data Corporation. Where sought by the Supervisory Authority (ies), First Data shall supply that Supervisory Authority(ies) (including the competent Supervisory 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 Services Agreement is in force, the Data Controller or an independent third party auditor may audit the applicable First Data entity for compliance with these Processor Data Protection Standards and its obligations as a Data Processor set out in the GDPR, where legally permissible. Each Supervisory Authority is also authorised to audit any First Data entity in accordance with paragraph 21 of these Processor Data Protection Standards.

11.25 In addition, First Data's personnel 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 various other privacy related policies. Any material violation of applicable laws, these Processor Data Protection Standards, the Code of Conduct or relevant corporate policies by First Data's personnel may result in disciplinary action, up to and including dismissal.

11.26 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.

11.27 Each First Data entity will maintain a record of its processing of Personal Data in accordance with these Processor Data Protection Standards containing the information set out in Annex A. This record will be maintained in writing, including in electronic form, and should be made available to the Supervisory Authority on request.

For further information relating to First Data's privacy officer network or provision of training programmes please see the First Data Privacy Site or contact the Global Privacy Office, the Data Protection Officer and/or Local Privacy Officer.

12 Contact Information

Data Protection Officer

Janus House
Endeavour Drive
Basildon
Essex SS14 3WF
Tel: +44 (0)1268 820532
Email: dpo@firstdata.com

Local Privacy Officers

Email: dpo@firstdata.com

Contact information for First Data's offices can be found here.

FDR Limited

FDR Limited
Janus House
Endeavour Drive
Basildon
Essex SS14 3WF
Tel: +44 (0)1268 820532

General Counsel's Office

29th Floor
225 Liberty Street
New York, NY 10281
Telephone: +1 800 735-3362

Global Privacy Office

Email: dataprotection@firstdata.com
Privacy Hotline: +1 800-368-1000

Annex A – Record of Processing

The record of processing maintained by each First Data entity shall contain the following information to the extent the entity processes Personal Data:

- the name and contact details of the relevant First Data entity and the name of the Data Controllers on behalf of which the First Data entity is acting, where applicable, the name of the Data Controller's representative, and the Data Protection Officer;
- a description of the categories of processing undertaken for each Data Controller;
- where applicable, transfers of Personal Data to a third country or an international organisation, including the identification of that third country or international organisation and, where relevant, the suitable safeguards;
- where possible, a general description of the technical and organisational security measures to ensure a level of security is applied to the Personal Data which is appropriate to the risk.