FIRST DATA CORPORATION CONTROLLER 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) 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 Controller Data Protection Standards (which include the Annexes attached hereto) 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). 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 Controller Data Protection Standards. These responsibilities include accepting liability for breaches of these Controller Data Protection Standards by First Data entities (as defined in paragraph3.1) outside of the UK and taking any action necessary to remedy such breaches, both as described more fully in paragraph 7.2 of these Controller Data Protection Standards.

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. These policies include First Data's Employee Code of Conduct, its Global Cyber Security Policy and those policies listed in Annex B.

3 The Scope of These Controller Data Protection Standards

3.1 These Controller Data Protection Standards apply only:

3.1.1 to First Data entities which have signed a Binding Intra-Group BCR Membership Agreement in respect of these Controller Data Protection Standards and 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 from the Global Privacy Office whose details are set out at the end of these Controller 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 Controller 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 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 Customer Information (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 third parties including other First Data entities from whom we receive information and are ultimately governed by written contracts and/or applicable data protection and privacy laws.

3.3 First Data has been granted authorisation for: (a) these Controller Data Protection Standards, which apply only in relation to Personal Data for which First Data is a controller; and (b) First Data's Processor Data Protection Standards (available at the following website: https://www.firstdata.com/en_us/privacy.html (the "First Data Privacy Site")), 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 Controller Data Protection Standards apply to all Personal Data transferred by one First Data entity to another First Data entity, where First Data is a controller of the Personal Data.

3.6 Data Subjects alleging breach of these Controller Data Protection Standards shall only be entitled to enforce them as a third party beneficiary pursuant to paragraph 9.1 of these Controller Data Protection Standards in respect to transfers of Personal Data made by a First Data entity located in a Relevant Country to a First Data 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 Controller Data Protection Standards. Where there is a conflict between the Local Policies and these Controller 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 paragraph7.4), to offer the highest protection will govern.

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

4.1 First Data processes and transfers Personal Data, including Special Categories of Personal Data (defined below), relating 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, including holders of payment instruments;
- Merchants accepting payments;
- Employees, contingent workers, consultants, and applicants ("**Personnel**") former Personnel, dependants and beneficiaries of Personnel and former Personnel in connection with their working relationship or application for employment or engagement ("**Employment Data**");
- Other persons as appropriate to conduct its business such as suppliers, partners, contractors and contingent workers and prospective clients of First Data and, in each case, their personnel, external advisors and agents.

4.2 For the purposes of these Controller 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.

5 Sources of Personal Data

5.1 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, First Data Personnel and business contacts, for example in completing online forms, in connection with their working relationship or application for employment, from business contacts in the course of our business. We may also collect Personal Data directly from holders of payment instruments when they engage in a transaction;
- **From our clients** - Due to the unique nature of First Data's business, in many cases, First Data obtains Personal Data from its clients, or other participants in a transaction processing chain, such as card associations and debit network operators and their members, rather than the Data Subjects themselves. This information usually arises from a transaction initiated by a Data Subject with our client;
- **From our group companies** – Personal Data may be shared between First Data entities in accordance with these Controller 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

[1] See scope of Data Protection Standards at Paragraph3.5.

information against other databases – public or private – to which they have access), fraud prevention agencies or Independent Sales Organisations (ISOs);

- **From public sources** – We may collect and check Data Subjects' information against other public databases and sources to which we have access;
- **From a Data Subject's browser** - First Data collects browser information as described in more detail in the First Data Privacy Notice available on the First Data Privacy Site; and
- **Information we create** - First Data may create and record information in relation to Data Subjects. For example, we may create employment records, details of transactions a Data Subject carries out, the services we provide to a Data Subject 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 Subjects set out above includes processing for the following business purposes:

- Recruitment;
- Personnel management and professional development;
- Payroll and administration of Personnel benefits;
- Research and development;
- Business development;
- Maintaining and building upon customer relationships;
- Business planning;
- Facilities management;
- Maintaining technology infrastructure and support;
- Database management;
- Training;
- Security, data collection and processing;
- To fulfil a transaction initiated by a Data Subject, including holders of payment instruments;
- To fulfil our contracts with our clients, including to fulfil a transaction with, or for, our clients for whom we are collecting, managing, using or disclosing the Personal Data, and where we are providing payment instrument acquiring services to a merchant;
- To agents, vendors and contractors to assist us in our business, some of which may be located outside of the collection country, including for our internal monitoring and reporting purposes, administering our business or conducting activities ancillary to the provision of services to our clients and their customers;
- As authorised by the United States Fair Credit Reporting Act ***(15 U.S.C. §1681)*** or other applicable laws;
- For fraud prevention or investigation, or other risk management purposes, including as required by First Data's policies;
- For identification and information verification purposes, including for anti-money laundering, anti-terrorism financing and sanctions monitoring purposes;
- To prospective purchasers and for protecting First Data's legal rights or assets to facilitate the acquisition or disposition of First Data businesses;
- To enforce our rights or the rights of other persons in a financial transaction;
- In response to a lawful request from a court or government agency or to otherwise comply with applicable law or compulsory process;
- On the written request of the Data Subject, where appropriate;
- To fulfil our obligations to other participants in a transaction processing chain, such as card associations and debit network operators and their members;
- In emergencies where the health or safety of a person is endangered;
- To perform or develop analytics and provide other value-added services;
- Other purposes required or permitted by law or regulation.

5.3 We collect and use Personal Data for a variety of legal reasons, including:

- **where a Data Subject has provided their consent -** For example, First Data may require a Data Subject's consent in order to process their data for electronic marketing activities under applicable laws. Where this is the case, a Data Subject can withdraw their consent at any time by contacting the organisation to whom he/she gave their consent, or a Data Subject can contact the Data Protection Officer;

- **where the processing is necessary for the performance of a contract -** For example, to allow First Data to provide a product or service to a Data Subject;
- **where First Data needs to comply with a legal obligation or it is in the public interest -** For example, First Data may need to disclose a Data Subject's Personal Data to a regulator, law enforcement agency or to a Data Subject's or First Data's representatives acting in a legal dispute or use a Data Subject's Personal Data to verify their identity, or prevent fraud; and
- **where the processing is necessary for the purposes of our legitimate interests –** First Data's legitimate interests include: (1) to provide products and services to a Data Subject or to a client of First Data; (2) to ensure a Data Subject's transaction is secure and adequately protected; and (3) the business interests described in Paragraph 5.2 above.

5.4 Where First Data requests Personal Data directly from a Data Subject, he/she does not have to provide this, but if a Data Subject decides not to provide this information, in some circumstances First Data, or our clients, may be unable to provide products or services to them. For example, we may be unable to process the Data Subject's transaction, or employ a Data Subject.

6 Nature of Data Transferred[2]

6.1 First Data processes and transfers a broad range of Personal Data between First Data entities and to 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:

- **Employment Data**: This includes data relating to recruitment, background checks, health records, benefit information, staff development records, attendance records including any days off due to illness, salary and expenses information, expatriate information, equal opportunities management, disciplinary procedures, Personnel share holdings, names, addresses, date of birth, Personnel monitoring and performance, trade union membership next of kin, the termination of the employment or service contract, call recordings of communications made by First Data's contact centre agents, Personal Data captured for access control purposes, CCTV images and bank account information.
- **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 and Employment Data, First Data also processes contact information of the personnel of its suppliers and vendors including

[2] See footnote 1.

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.

- **Anonymised/Aggregated Data:** First Data may also process anonymised and/or aggregated data for the purposes set out in these Controller Data Protection Standards.

7 Applicable Law and Supervising Authorities

7.1 All First Data entities will handle Personal Data in accordance with these Controller 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 (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 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 Controller 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 outside the EU or the UK of the rights guaranteed in these Controller 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 which is alleged to be in breach is not liable for the breach or such First Data 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 Controller Data Protection Standards, these Controller Data Protection Standards will apply. Where applicable data protection and privacy laws provide a higher protection, they will take precedence over these Controller 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 First Data's General Counsel's Office ("**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 Controller 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 Controller 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 Controller Data Protection Standards including following the advice of applicable Supervisory Authority, the entity will notify 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 Controller Data Protection Standards, 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 competent Supervisory Authority 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 received to the competent Supervisory Authority annually as described in paragraph 8.1 of these Controller Data Protection Standards, to the extent permitted under applicable law; and

7.5.4 In any event, a First Data entity will not transfer Personal Data to any public authority in a manner which is massive, disproportionate and indiscriminate.

8 Changes to our Data Protection Standards

8.1 First Data may change these Controller Data Protection Standards, additional First Data entities may sign the Binding Intra-Group BCR Membership Agreement and certain First Data entities may terminate or have their Binding Intra-Group BCR Membership Agreement 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 Binding Intra-Group BCR Membership Agreement and keep track of and record any updates to these Controller Data Protection Standards and provide the necessary information to Data Subjects or Supervisory Authorities upon request. In addition, all changes, additions and the termination of any Binding Intra-Group BCR Membership Agreement and any to the Controller Data Protection Standards must be subject to the approval of the Data Protection Officer and will be reported to each Supervisory Authority annually. Any significant changes will be reported without undue delay, where required. Where an update significantly affects these Controller 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 Controller 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 Controller Data Protection Standards and able to comply with them.

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

9 Compliance and Dispute Resolution

9.1 Under paragraph 2.2 of the Controller Data Protection Standards, FDR Limited has accepted liability for breaches of these Controller Data Protection Standards by First Data entities outside of the EU and for taking any action necessary to remedy such breaches. Data Subjects alleging breach of these Controller Data Protection Standards against FDR Limited or the First Data entity making the Transfer (as defined in Paragraph 3.6) as provided in paragraphs 2.2 and 7.1 and in particular those set out in paragraphs 7.1, 7.4, 7.5, 7.6, 7.8 and

11 can enforce them as a third party beneficiary only if they relate to a Transfer in the following ways:

9.1.1 We strongly encourage Data Subjects to first raise any alleged breaches through First Data's Privacy and Data Security Hotline, the Data Subject Complaints Policy (both of which are 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.

9.1.2 If the issue is not resolved to the Data Subject's satisfaction or if the Data Subject 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(ies), 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; or
- bring the issue before either the courts of England and Wales or 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.

9.2 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 Controller 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 which may be claimed by a Data Subject is limited to that which would be due under Article 82 of the GDPR.

9.3 The complaints handling process under these Controller 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 Controller 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.

9.4 The rights contained in this section of the Controller 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 Controller Data Protection Standards, receive training on and have access to these Controller Data Protection Standards. First Data will post a copy of these Controller Data Protection Standards on its internal and public websites, including on the First Data Privacy Site. In addition, Data Subjects will be provided with the 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 Controller 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 Where First Data is a data controller (as defined by the relevant legislation), it 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 and in accordance with one or more of the conditions set out in Annex A.

11.2 First Data's "information notice" containing the information it is required to give to Data Subjects under the GDPR is set out in: (a) these Controller Data Protection Standards; and (b) First Data's privacy notice, which is available at the First Data Privacy Site (the "**Privacy Notice**"). Where appropriate, the information given by these Controller Data Protection Standards and the Privacy Notice 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, holds and processes Personal Data only for specified, explicit and legitimate purposes as set out in these Controller Data Protection Standards, the Privacy Notice and any supplementary information notice provided to a Data Subject. First Data will not process Personal Data in ways incompatible with those purposes. Where we obtain Personal Data from third parties (including our clients) and publicly available sources, we always use only reliable and reputable sources.

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 are processed, as described in Paragraph 5.2 . The purposes of retaining the data, and the specific retention periods, will be defined in First Data's applicable data retention policies and schedules, on expiry of which First Data will securely delete the relevant Personal Data. 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 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 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.

Personal Data will be accurate and, where necessary, kept up-to-date ('accuracy').

11.8 First Data verifies Personal Data is accurate and, where necessary, kept up-to-date. First Data will take every reasonable step to ensure that, in relation to the purposes for which it is processed, Personal Data that are inaccurate are erased or rectified without delay.

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 Controller Data Protection Standards in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of these Controller Data Protection Standards and protect the rights of Data Subjects.

11.10 First Data will implement appropriate technical and organisational measures for ensuring that, by default, only Personal Data which are 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. First Data will not make a Data Subject's Personal Data publically available without informing the Data Subject in advance.

We transfer Personal Data only for limited purposes.

11.11 In addition to satisfying the requirements set out in Privacy Principle 1 above, First Data will conduct intra-First Data entity transfers and transfers to third parties (which may include our clients) only when the following requirements have been met:

- all applicable legal requirements are met (including the conditions in Chapter V of the GDPR);
- the transfer is based on a clear business need;
- the receiving entity has appropriate security;
- the receiving party, if the First Data entity: (a) where acting as a controller, complies with these Data Privacy Standards; (b) where acting as a processor, complies with the Processor Data Protection Standards, for the transfer and subsequent processing; or (c) the transfer is otherwise permitted under Chapter V of the GDPR; and
- in the case of all transfers to third parties (including First Data entities) who are acting as a processor, there is a written contract including the requirements set out in Annex C.

11.12 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, where the Data Subject has given First Data permission to disclose their information to such third parties;
- third parties to whom First Data will transfer, or may transfer, its rights and duties in its agreements with Data Subjects, 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.

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

11.14 When the processing of Personal Data is outsourced by First Data to a third party, First Data will select reliable third parties.

11.15 Except as set out above and as described in the First Data Privacy Notice, 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 Data Subject or the supplying client. In addition, First Data, by itself or via suppliers or vendors, processes Personal Data as outlined in First Data's various privacy policies. For further information regarding First Data's various privacy policies, please see the list set out in Annex B and refer to the First Data Privacy Site, intranet or the Data Protection Officer or the Global Data Privacy Office.

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 agreement with First Data.

11.17 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. Each First Data entity will notify without undue delay any security incidents affecting Personal Data to FDR Limited and the Data Protection Officer, unless the security incident is unlikely to result in a risk to the rights and freedoms of the Data Subjects. First Data will notify the affected Data Subjects without undue delay where the security incident is likely to result in a high risk to the rights and freedoms of those Data Subjects. As appropriate or required, First Data will also notify law enforcement authorities, financial or other regulators (including Supervisory Authorities) and/or state agencies. Any security incidents will be documented in a security incident log (including the facts relating to the security incident, its effects and the remedial action taken) and the security incident log will be made available to the competent Supervisory Authority on request.

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

11.19 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.

11.20 Where First Data is a controller of Personal Data, a Data Subject may have rights over his/her Personal Data, including the right to:

- withdraw consent at any time, where the Data Subject has provided their consent;
- ask First Data to confirm if it is processing their Personal Data;
- ask First Data for access to their Personal Data;
- ask First Data to correct their Personal Data if it is wrong;
- ask First Data to delete their Personal Data;
- ask that First Data's systems stop using their Personal Data;
- ask First Data to restrict how it uses their Personal Data;
- ask First Data to help them to move their Personal Data to other companies by providing their Personal Data in an easily readable format to another company;
- ask First Data to stop using their Personal Data, but only in certain cases; and
- complain to the relevant Supervisory Authority, as described in paragraph 9.1.

11.21 To exercise these rights a Data Subject should contact our Data Protection Officer. These rights will only apply in certain circumstances, as they are subject to the limitations and exemptions in the GDPR and only apply to certain types of information or processing. If a Data Subject has any questions about their rights please contact the Data Protection Officer. Further information in relation to a Data Subject's rights can also be found on the First Data Privacy Site.

11.22 First Data makes use of automated decision making, including profiling, in the processing of Personal Data including for the purpose of determining cheque acceptance, for identification and information verification purposes (including for anti-money laundering, anti-terrorism financing and sanctions monitoring purposes), deciding whether to underwrite a merchant (automatic approval only, where relevant criteria is not met by a merchant the decision

whether to decline will be referred to an individual), certain job applicants (to determine whether the applicant meets a minimum criteria), commemorating length of employee service, to monitor and identify potential fraudulent transactions, notify First Data's clients of possible fraudulent transactions, certain credit card applications (criteria is set by First Data's clients) and where job applicants do not agree to First Data's privacy statement and/or a background check but agreement is necessary to consider the application. Further details of these are available upon request from the Data Protection Officer or the Global Privacy Office. No evaluation or decision which produces legal effects concerning him or her or similarly significantly affects him or her shall be made solely through such processing unless the evaluation or decision:

11.22.1 is necessary for entering into, or performance of, a contract between the Data Subject and First Data, or is based on the Data Subject's explicit consent, and First Data has ensured that adequate safeguards are in place to protect the legitimate interests of the Data Subject. Such safeguards include where the processing taking place as a result of entering into or performing a contract at the request of the Data Subject, the right for the Data Subject to put his or her comments to First Data regarding the decision and the right to have that decision considered by a human; or

11.22.2 is authorised by law to which First Data is subject and which also lays down suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests.

11.23 First Data's Data Protection Officer and/or Local Privacy Officer shall process each Data Subject's reasonable request for exercising his or her rights in respect of Personal Data as required by applicable laws and in accordance with First Data's Data Subject Rights Policy. If a Data Subject asserts the Personal Data kept about him or her is incorrect, we will work with the Data Subject to rectify, block or erase the inaccuracy, should the Data Subject not have the ability to self-correct their Personal Data by signing in to a portal or similar interface.

We recognise a Data Subject's right to object to direct marketing by First Data.

11.24 Where First Data uses Personal Data for its own direct marketing, it must do so in accordance with applicable data protection and privacy laws and any further guidance produced by the relevant regulating authority. A Data Subject has the right to object to direct marketing by First Data at any time. To exercise this right, he or she shall be able to communicate this via the Global Privacy Office or via such other method as may be identified, where applicable, in the relevant marketing communication.

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

11.25 Each First Data entity will be responsible for, and able to demonstrate compliance with, these Controller 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 Controller 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 Controller Data Protection Standards. The Global Privacy Office and the privacy officer network, including the Data Protection Officer and the Local Privacy Officers, 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.

11.26 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 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) with a copy of the audits.

11.27 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 Controller Data Protection Standards, the Code of Conduct or relevant corporate policies by a member of First Data Personnel may result in disciplinary action, up to and including dismissal.

11.28 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.

11.29 First Data will maintain a record of its processing of Personal Data in accordance with these Controller Data Protection Standards containing the information set out in Annex D where processing as a controller. This record will be maintained in writing, including in electronic form, and should be made available to the Supervisory Authority on request.

11.30 First Data will perform a data protection impact assessment in respect of any processing operations that are likely to result in a high risk to the rights and freedoms of Data Subjects. Where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by First Data to mitigate the risk, First Data will consult the competent Supervisory Authority, prior to processing.

For further information relating to First Data's privacy officer network, provision of training programmes or privacy policies refer to Annex B, the First Data Privacy Site, First Data's Intranet or contact the Global Privacy Office, 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
Tel: +1 800 735-3362

Global Privacy Office

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

Annex A – Conditions Required to Be Met by First Data Prior to the Processing of Personal Data

At least one of the following conditions must be met prior to the processing of Personal Data by First Data:

- The Data Subject gives his or her consent to the processing of his or her Personal Data for one or more specific purposes. Where processing is based on consent, First Data will be able to demonstrate that the Data Subject has consented to processing of his or her Personal Data and the consent meets the requirements set out in Articles 7 and 8 of the GDPR;
- The processing is necessary for the performance of a contract to which the Data Subject is a party or for taking steps at the request of the Data Subject prior to entering into a contract;
- The processing is necessary for compliance with First Data's legal obligations;
- The processing is necessary to protect the vital interests of the Data Subject or of another natural person;
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in First Data; or
- The processing is necessary to pursue the legitimate interests of First Data or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Data, in particular where the Data Subject is a child.

At least one of the following conditions must be met prior to the processing of Special Categories of Personal Data by First Data:

- The Data Subject has given his or her explicit consent to the processing of the Personal Data for one or more specified purposes, except where Union or Member State law provide that the prohibition on processing Special Categories of Personal Data may not be lifted by the Data Subject;
- The processing is necessary for the purposes of carrying out the obligations and exercising specific rights of First Data or of the Data Subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the Data Subject;
- The processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent;
- The processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the Personal Data are not disclosed outside that body without the consent of the Data Subjects;
- The processing relates to Personal Data which are manifestly made public by the Data Subject;
- The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- The processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject;
- The processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the Personnel, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a

health professional and subject to the professional being subject to the obligation of professional secrecy in accordance with Article 9(3) of the GDPR;

- The processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the Data Subject, in particular professional secrecy; or
- The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the GDPR based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject.

Annex B – First Data Privacy Policies

Copies of the policies set out below are available on request from the Global Privacy Office.

Annex B Part	Document name
1	Data Subject Rights Policy
2	First Data's Privacy and Data Security Hotline

Annex C – Mandatory Contractual Terms for Processors

The following conditions will be included in contracts with third parties, including First Data entities, acting as a processor:

- The contract shall set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and First Data's obligations and rights as data controller;
- The processor shall only process the Personal Data on the documented instructions of First Data, including with regard to international transfers of Personal Data, unless the processor is required to do so by UK, Union or Member State law in which case the processor shall inform First Data of that legal requirement before processing the Personal Data, unless that law prohibits such disclosure on important grounds of public interest;
- Persons authorised to process the Personal Data must have committed themselves to confidentiality or be under an appropriate statutory obligation of confidentiality;
- The processor shall take all measures, including technical and organisational measures, in relation to security of data under Article 32 of the GDPR;
- The processor shall respect the conditions for engaging another processor;
- Taking into account the nature of the processing, the processor shall assist First Data by appropriate technical and organisational measures, insofar as possible, for First Data to fulfil their obligations to respond to requests for the exercise of data subject's rights laid down in Chapter III of the GDPR;
- The processor shall assist First Data in ensuring compliance with the obligations set out in Article 32 to 36 of the GDPR, taking into account the nature of processing and the information available to the processor;
- The processor shall, at the choice of First Data, delete or return all the Personal Data to First Data after the end of the provision of services relating to processing, and deletes existing copies unless UK, Union or Member State law requires storage of the Personal Data;
- The processor shall make available to First Data all information necessary to demonstrate compliance with these obligations and allow for and contribute to audits, including inspections conducted by First Data or another auditor mandated by First Data;
- The processor shall immediately inform First Data if, in its opinion, an instruction infringes the GDPR or other UK, Union or Member State data protection law;
- The processor shall not engage another processor (a sub-processor) without First Data's prior or general written authorisation; if First Data provides a general written authorisation the processor shall inform First Data of any intended changes concerning the addition or replacement of other processors, allowing First Data the opportunity to object; and
- If the processor engages a sub-processor, the same data protection obligations set out in the contract with First Data shall be included in the processor's contract with the sub-processor, in particular providing sufficient guarantees to implement the appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR. If a sub-processor fails to fulfil its obligations the initial processor shall remain fully liable to First Data for the performance of the sub-processor's obligations.

Annex D – 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 as controller or processor:

- the name and contact details of the relevant First Data Entity and, where applicable, the joint controller, and the Data Protection Officer;
- the purposes of the processing;
- a description of the categories of Data Subjects and of the categories of Personal Data;
- the categories of recipients to whom the Personal Data have been or will be disclosed including recipients in third countries or international organisations;
- 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, the envisaged time limits for erasure of the different categories of Personal Data; and
- 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.