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

These 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. They emphasise and clarify the key role our employees play in providing protection for the privacy of Personal Data, and set out First Data’s overall approach to privacy and data protection.

Our Business

First Data operates in more than 80 countries across the United States, Latin America and Canada, Asia Pacific and the Europe, Middle East and Africa. First Data employs approximately 24,500 employees throughout these regions to provide more than 60 billion payment transactions worldwide. First Data Corporation is the ultimate parent company of First Data and is headquartered in the United States.

First Data has nominated FDR Limited as the First Data entity within the EU to whom it delegates data protection responsibilities for the purposes of these Data Protection Standards. These responsibilities include accepting liability for breaches of these Data Protection Standards by First Data entities outside of the EU and taking any action necessary to remedy such breaches, both as described more fully in paragraph 14 of these Data Protection Standards.

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

Due to the unique nature of our business, in most cases, First Data obtains Customer Information (as defined in paragraph 10 below) from our clients rather than the Data Subjects themselves. This information usually arises from a transaction initiated by a Data Subject with our client. Therefore usually First Data's processing of Customer Information about Data Subjects is as a processor following our clients' instructions or those of other parties excluding First Data entities (“third party” or “third parties”) from whom we receive information and ultimately governed by written contracts and/or applicable data protection and privacy laws. Whilst authorisation for these Data Protection Standards has only been granted in relation to Personal Data for which First Data is a controller, First Data's commitment to maintaining the highest standards of respect Personal Data is such that it intends them to apply so far as practicable to all Personal Data processed by First Data, including processor data.

The Scope of These Data Protection Standards

These Data Protection Standards apply only to First Data entities which have signed a Binding Intra-Group BCR Membership Agreement and references to "First Data", "First Data entity or entities", "our" and "we" shall apply and refer only to such entities. A list of these entities are available from the Corporate Privacy Office whose details are set out at the end of these Data Protection Standards.
Data Subjects alleging breach of these Data Protection Standards shall only be entitled to enforce them as a third party beneficiary pursuant to paragraph 19 of these Data Protection Standards in respect to transfers of Personal Data made by a First Data entity located in the European Economic Area ("EEA") to a First Data entity located outside the EEA (a "Transfer").

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

**Categories of Data Subjects and Purposes of Processing and Transfers**

First Data processes and transfers Personal Data including Sensitive Personal Data relating to the following classes of Data Subject:

- Our clients and their customers in connection with the provision of services ("Customer Information");
- Individuals making payment transactions;
- Merchants accepting payments;
- Employees, former employees, dependants and beneficiaries of employees and former employees in connection with their working relationship or application for employment ("Employment Data");
- Other persons as appropriate to conduct its business such as suppliers, partners, contractors and contingent workers and prospective clients of First Data.

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

The processing and transfers undertaken by First Data in relation to the classes of Data Subject set out above includes processing for the following business purposes:

- Recruitment;
- Employee performance management and professional development;
- Payroll and administration of employee benefits;
- Research and development;
- Business development;
- Maintaining and building upon customer relationships;
- Business planning;
- Facilities management;
- Maintaining technology infrastructure and support;
- Database management;
- Training;

---

1 Due to the unique nature of First Data's business, in most cases, First Data obtains Customer Information from its clients rather than the Data Subjects themselves. This information usually arises from a transaction initiated by a Data Subject with our client. Therefore usually First Data's processing of Customer Information about Data Subjects is as a processor following our clients' instructions or those of other parties (excluding First Data entities) from whom we receive information and are ultimately governed by written contracts and/or applicable data protection and privacy laws. Authorisation for these Data Protection Standards is only granted in relation to Personal Data for which First Data is a controller. However, First Data's commitment to maintaining the highest standards of respect Personal Data is such that it intends them to apply so far as practicable to all Personal Data processed by First Data, including processor data.
• Security, data collection and processing;
• To fulfill a transaction initiated by a Data Subject;
• To fulfill a transaction with, or for, our clients for whom we are collecting, managing, using or disclosing the Personal Data;
• To agents 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;
• For identification and information verification 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 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
• Other purposes required or permitted by law or regulation.

Nature of Data Transferred

First Data processes and transfers a broad range of Personal Data between First Data entities and to third parties (which may include our clients) as relevant to the classes and purposes identified above. The types of Personal Data include:

• Employment Data: This includes data relating to 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, employee share holdings, names, addresses, date of birth, employee performance, trade union membership and next of kin.
• Customer Information: This includes contact information of clients' employees, information relating to the client's account, clients' customers' contact details including name, address and telephone numbers and account information including other persons on the account and spend thresholds, details of clients' customers' spending and spending patterns and details of the merchants accepting payment transactions to the extent these are individuals.
• Personal Data: As well as Customer Data and Employment Data, First Data also processes contact information of the employees of its suppliers and vendors including name, email address and telephone numbers and such other personal data as may be required in order for First Data to conduct business with such suppliers and vendors.
• Anonymised/Aggregated Data: First Data may also process anonymised and/or aggregated data for the purposes set out in these Data Protection Standards.

Applicable Law and Supervising Authorities

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

2 See footnote 1.
in accordance with the Directives and all applicable data protection and privacy laws and regulations as well as with any obligations under the GBLA.

14 The policies and procedures described in these Data Protection Standards are in addition to any other remedies available under applicable data protection and privacy laws or provided under other First Data policies and procedures. FDR Limited will be responsible for and will take any action necessary to remedy any breach by any First Data entity outside the EU of the rights guaranteed in these Data Protection Standards as provided by paragraph 19. This will include any sanction imposed or other remedy available under applicable data protection and privacy laws including compensation, where legally required. FDR Limited may discharge itself from this responsibility if it is able to show that the First Data entity 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.

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

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

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

Changes to our Data Protection Standards

18 First Data may change these Data Protection Standards, additional First Data entities may sign the Binding Intra-Group BCR Membership Agreement and certain First Data entities may terminate or have their Binding Intra-Group BCR Membership Agreement terminated. The Chief Privacy Officer 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 Data Protection Standards and provide the necessary information to Data Subjects or Data Protection Authorities upon request. In addition, all changes, additions and the termination of any Binding Intra-Group BCR Membership Agreement and any substantial change to the Data Protection Standards must be subject to the approval of the Chief Privacy Officer and will be reported to each Data Protection Authority annually. Any significant changes will be reported earlier, where required. Upon approval of the Chief Privacy Officer, we will clearly indicate the date of the latest revision and communicate the Data Protection Standards to all First Data entities and post the revision on First Data's public website. No transfers will be made to a new First Data entity until that First Data entity is effectively bound by these Data Protection Standards and able to comply with them.

Compliance and Dispute Resolution

19 Under paragraph 4 of the Data Protection Standards, FDR Limited has accepted liability for breaches of these Data Protection Standards by First Data entities outside of the EU and for taking any action necessary to remedy such breaches. Data Subjects alleging breach of these Data Protection Standards against FDR Limited or the First Data entity making the Transfer (as defined in Paragraph 8) as provided in paragraphs 4 and 14 and in particular those set out in paragraphs 13, 16, 17, 19, 20 and 21 can enforce them as a third party beneficiary only if they relate to a Transfer in the following ways:
(a) We strongly encourage Data Subjects to first raise any alleged breaches through the Complaints Handling Procedure – Security and Data Privacy Hotline (copies of which can be requested via First Data’s Corporate Privacy Office), the Data Subject Complaints Policy (which appears on First Data's public website) or with the Chief Privacy Officer or Local Privacy Officer who will work with them to endeavour to resolve their concern to their satisfaction.

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

- raise the issue of breach before the competent Data Protection Authority(ies) and First Data shall cooperate as reasonably required by that Data Protection Authority; or
- bring the issue before either the courts of England and Wales or the courts of competent jurisdiction of First Data entity making the Transfer, at the Data Subject's option.

The complaints handling process under these Data Protection Standards is provided for by First Data's Privacy and Data Security Hotline. Further under First Data's Code of Conduct, there are a number of avenues under which Data Subjects can raise complaints regarding breaches of these Data Protection Standards. A decision on any complaint made will be communicated to the Data Subject within 28 days of the complaint being made in accordance with the process.

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

Communication of First Data’s Data Privacy Standards

First Data takes compliance with its data protection obligations very seriously. All First Data employees who process Personal Data will comply with these Data Protection Standards receive training on and a copy of these Data Protection Standards. First Data will also post a copy of these Data Protection Standards on its internal and public websites and will make physical copies permanently available at each of its offices and in the Corporate Privacy Office. In addition, a copy will be sent to Data Subjects on request. The Corporate Privacy Office will maintain a list of the First Data entities that are bound by these Data Protection Standards and will publish the list on First Data's public website.

First Data’s Privacy Principles

1. We process Personal Data fairly and lawfully

Where First Data is a data controller (as defined by the relevant legislation), it processes Personal Data fairly and lawfully, in accordance with all applicable laws and regulations and in accordance with one or more of the conditions set out in Annex A.

2. These Data Protection Standards shall constitute First Data's "Fair Processing Notice" containing the information it is required under the Directive to give to Data Subjects. Where appropriate, the information given by these Data Protection Standards shall be supplemented as required by specific Fair Processing Notice in respect to a particular piece of processing.

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

First Data collects, transfers, holds and processes Personal Data only for specified, explicit and legitimate purposes as set out in these Data Protection Standards. 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 endeavor to use only reliable and reputable sources.
3. **We limit our access to, and use of Personal Data.**

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

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

4. **We transfer Personal Data only for limited purposes.**

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;
- the transfer is based on a clear business need;
- the receiving entity has appropriate security;
- the receiving party, if a First Data entity, complies with the Data Privacy Standards for the transfer and subsequent processing; and
- in the case of all transfers to third parties (including our clients) or First Data entities who are acting as a processor there is a written contract; (a) specifying that the receiving party will follow the exporting party's instructions; (b) setting out the rights and obligations of each party including provisions relating to security and confidentiality which they must follow; and (c) where a third party entity, providing that it has adequate security measures in place.

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

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

Except as set out above and as described in the Annex to First Data's Standard Application for Approval of Binding Corporate Rules, First Data does not sell, rent, share, trade or disclose any Personal Data it keeps about a Data Subject to any other parties without the prior written consent of the Data Subject or the supplying client. In addition, First Data, by itself or via suppliers or vendors, processes Employment Data or 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 First Data's intranet or the Chief Privacy Officer.

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

First Data employs appropriate technical, organisational, administrative and physical security measures to protect Personal Data against unauthorised or unlawful processing and against accidental loss or destruction. First Data regularly reviews and, as appropriate, enhances its security systems, policies and procedures to take into account emerging threats, as well as emerging technological safeguards and precautions. First Data imposes security appropriate to the risk represented by the processing and nature of the Personal Data to be protected, with all due regard to the state of the art and cost measures.
If a security breach occurs involving unauthorised access to Personal Data on a First Data system, First Data operates a response plan which is designed to assist First Data in complying with applicable laws requiring notification of security breaches, with guidelines produced by the relevant Data Protection Authorities in relation to security breaches and with our duties under our customer contracts. As appropriate or required, First Data will also notify law enforcement authorities, financial or other regulators and/or state agencies.

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

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

6. **We provide transparency, choice and access as required by applicable data protection and privacy law.**

Where First Data is a controller (i.e. decides the purposes and means of the processing) of Personal Data, the following principles will apply.

First Data verifies Personal Data is kept up-to-date and is accurate, adequate, relevant, not excessive for the purposes for which it is processed and is kept for no longer than is necessary for the purposes for which it is being processed.

First Data makes limited use of automated decision making in the processing of Personal Data including for the purpose of determining cheque acceptance, 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, 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 Corporate Privacy Office. No evaluation or decision which significantly effects a Data Subject shall be made solely through such processing unless 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.

First Data shall consider each reasonable request of a Data Subject to the Chief Privacy Officer and/or Local Privacy Officer for access to his or her own Personal Information and will provide a copy of the Personal Data First Data processes about that Data Subject as required by applicable laws and in accordance with First Data's Data Subject Access Request 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.

Where a Data Subject considers that the processing by First Data of Personal Data about him or her is likely to cause them substantial damage or distress and that damage or distress is unwarranted then the Data Subject may request, by notice in writing, without charge, that First Data stops or does not begin processing that Personal Data. First Data shall respond within 21 days of such request stating that it has or intends to comply with the request or stating the reasons why it considers the request unjustified and what extent it has or intends to comply, if any.
7. **We recognise a Data Subject's right to object to direct marketing by First Data.**

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. Where a Data Subject wishes to object to direct marketing by First Data, he or she shall be able to communicate this via the Corporate Privacy Office or via such other method as may be identified, where applicable, in the relevant marketing communication.

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

First Data operates a comprehensive network of privacy officers around the world who are responsible for data privacy within their region including compliance with these Data Protection Standards. The Chief Privacy Officer is responsible for the network of privacy officers and the development, implementation and continuing oversight of these Data Protection Standards. The Chief Privacy Officer and the privacy officer network 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 Corporate Privacy Office works with other groups within First Data to develop additional corporate privacy policies and practices and has created the Data Security Council which aims to identify and reduce First Data's top security risks.

First Data further evidences its commitment to accountability by conducting regular internal privacy assessments as part of its comprehensive audit programme and provides mandatory training to its employees on privacy topics and issues relevant to their job type. Items identified through the audit programme are assigned to a First Data employee who is responsible for developing and executing a remediation plan and associated time frame. Upon completion, the audit team will review to determine if the item has been adequately addressed and can be closed or requires additional action. Where sought by the Data Protection Authority(ies), First Data shall supply that Data Protection Authority(ies) with a copy of the audits.

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

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

For further information relating to First Data's privacy officer network, provision of training programmes or privacy policies refer to Annex B, First Data's Intranet or contact the Chief Privacy Officer and/or Local Privacy Officer.

**Contact Information**

**Chief Privacy Officer and Corporate Privacy Office**
First Data Corporation  
6200 South Quebec Street  
Greenwood Village, CO 80111  
Telephone Phone: +1 (303) 967-5186  
Facsimile Number: +1 (303) 967-5185  
Email Address: dataprivacyoffice@firstdata.com

**General Counsel and General Counsel's Office**
First Data Corporation
6200 South Quebec Street
Greenwood Village, CO 80111
Telephone Phone: +1 (303) 967-5670
Facsimile Number: +1 (303) 967-5185

Local Privacy Officers

Privacy Officers
Janus House
Endeavour Drive
Basildon
Essex SS14 3WF
Tel: +44 (0)1268 296839 ext: 888639 or +44 (0)1268 298261
Fax: +44 (0)1268 296531
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 unambiguous consent;
- 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, other than a contractual obligation;
- The processing is necessary to protect the vital interests of the Data Subject;
- The processing is necessary for the administration of justice, exercising functions of a public nature, or conferred on a person by any enactment;
- The processing is necessary to pursue the legitimate interests of First Data or by the third party or third parties to whom the Personal Data are disclosed, save where this prejudices the fundamental rights or freedoms of the Data Subject; or
- In the case of Sensitive Personal Data, the Data Subject has given his or her explicit consent or one of the additional conditions set out below applies.

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

- The Data Subject has given his or her consent;
- The processing is necessary for the purpose of any right or obligation imposed on First Data by law in connection with employment;
- The processing is necessary to protect the vital interest of the Data Subject where the Data Subject cannot give consent or First Data cannot be reasonably expected to obtain consent or where it is necessary to prevent the vital interests of a third party and the Data Subject unreasonably withholds its consent;
- The processing is carried out in the course of its legitimate activities by any body or association which is not established or conducted for profit and exists for political, philosophical religious or trade-union purposes; is carried out with appropriate safeguards for the rights and freedoms of Data Subjects; relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes and does not involve disclosure of the Personal Data to a third party without the consent of the Data Subject;
- The information contained in the Personal Data has been made public as a result of steps deliberately taken by the Data Subject;
- The processing is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), obtaining legal advice or is otherwise necessary for the purposes of establishing, exercising or defending legal rights;
- The processing is necessary for the administration of justice, the exercise of any functions conferred on any person by or under an enactment or for the exercise of any functions of the Crown, a Minister of the Crown or a government department;
- The processing is necessary for medical purposes and is undertaken by a health professional or a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional;
- The processing is of Sensitive Personal Data consisting of information as to racial or ethnic origin, is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained and is carried out with appropriate safeguards for the rights and freedoms of Data Subjects.
**Annex B – First Data Privacy Policies**

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

<table>
<thead>
<tr>
<th>Annex B Part</th>
<th>Document name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Data Subject Access Request Policy</td>
</tr>
<tr>
<td>2</td>
<td>Complaints Handling Procedure – Security and Data Privacy Hotline</td>
</tr>
</tbody>
</table>