Binding Intra-Group

Processor EU BCR Membership Agreement

Dated   **("Commencement Date")**

13/9/2023

Contents

Binding Intra-Group

Processor EU BCR Membership Agreement

Dated

Between

(1)   **Fiserv, Inc.** (the **Parent Company**), a corporation organised and existing under the laws of the State of Wisconsin, USA whose principal place of business is at 255 Fiserv Drive, Brookfield, WI 53045, United States of America; and

(2)   **The Members** (as defined below).

Recitals

A   The Members (as defined below) want to share Personal Data for conducting their business, management planning, security, group compliance, training and for other operational and business purposes within the Fiserv Group as further described and on the terms as set out in the BCRs and in this Agreement.

B   The main clauses of this Agreement together with the Schedules and any Declaration of Accession shall form the BCRs.

C   The Parent Company is required to nominate an entity within the EEA to whom it delegates data protection responsibilities for the purposes of the BCRs. These responsibilities include accepting liability for breaches of the BCRs outside of the EEA by Members and taking any action necessary to remedy such breaches. FDR LIMITED, LLC has been so nominated for these purposes. The Irish branch of FDR LIMITED, LLC shall be the establishment under the GDPR which accepts liability for any breaches of the BCRs by any Member not established in the EEA.

D   In order to ensure that Personal Data is accorded adequate protection in accordance with Applicable Laws, the Parent Company and each other Member wish to become bound by and become Members of the BCRs on the terms set out in this Agreement.

It is agreed:

1   Definitions and Interpretation

1.1   In and for the purposes of this Agreement, unless the context otherwise requires, the following terms shall have the following meanings:

Affiliate means any company which is a subsidiary of the Parent Company and the term **Affiliates** shall be construed accordingly.

Applicable Laws means all applicable local data protection and privacy laws and regulations including, but not limited to, the Directive and the GDPR and any legislation and/or regulation implementing or made pursuant to them.

BCRs means the EU binding corporate rules set out in the document entitled "Fiserv, Inc. Processor Data Protection Standards" which is annexed hereto in Schedule 11, as amended or varied from time to time.

Business Day means a day other than a Saturday or Sunday or day on which banks in London are permitted to be closed for the transaction of general business.

Change of Control Event means a change of control or ownership of the Parent Company or an Affiliate within the meaning of Section 416 Income and Corporation Taxes Act 1988.

Commencement Date means the date on the front page of this Agreement.

Controller Member has the meaning set out in Clause 3.4.1.

Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

Data Protection Authority means any data protection authority in the EU or EEA which has approved the BCRs.

Data Subjects has the meaning set out in the BCRs.

Directive means the Privacy and Electronic Communications Directive (Directive 2002/58/EC) as implemented in applicable EU member state law (as amended or replaced from time to time, including by any regulation on privacy and electronic communications).

EEA means the European Union member states and Norway, Iceland and Liechtenstein

Exiting Member has the meaning set out in Clause 5.1(a).

FDR LIMITED, LLC means a company incorporated and registered in the State of Delaware, United States, under No 22692-35 and registered in Ireland as a branch of an overseas company with registered address at 10 Hanover Quay, Dublin 2 with Company Number 909114 (formerly FDR Limited). References to FDR LIMITED, LLC in these BCRs shall mean as applicable, the Irish branch in respect of enforcing the BCRs in the EEA and accepting liability for any breaches of the BCRs by any Member not established in the EEA.

Fiserv Group means the Parent Company and each Affiliate.

GDPR means Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

Member has the meaning set out in Clause 2.2.

Member Commencement Date means:

(a) in respect to a Fiserv entity becoming a Member pursuant to Clause 2.2(a), the Commencement Date; and

(b) in respect to a Fiserv entity becoming a Member pursuant to Clause 2.2 (b), the date on which it has entered into a Declaration of Accession, accepted by the Parent Company in the form set out in Schedule 4.

Member Term means in respect to a particular Member, the period of time starting on the relevant Member Commencement Date and ending on the date on which this Agreement terminates in accordance with Clause 4 in respect to that Member.

Personal Data has the meaning set out in the BCRs.

processing shall have the meaning set out in Article 4 of the GDPR and **process** and **processes** shall be construed accordingly.

Processor Member has the meaning set out in Clause 3.4.1.

Regulator means th Data Protection Authority and any other regulatory body or organisation in the field of data privacy to which the Parent Company or the relevant Member is legally subject from time to time or whose consent or approval is required so that the Parent Company and/or Member may lawfully carry on its business.

Remaining Member has the meaning set out in Clause 5.3(a).

1.2 Interpretation

In this Agreement:

(a) the headings in this Agreement are for convenience only and shall not affect its interpretation;

(b) references to this Agreement mean this Binding Intra-Group Processor BCR Membership Agreement and, if the context requires, any agreement substantially in the form of this Binding Intra-Group Processor BCR Membership Agreement executed by an Affiliate before or after the Commencement Date and reference to this Agreement or any other agreement, deed or instrument is to the same as amended;

(c) reference to any gender includes the others; and words in the singular include the plural and vice versa;

(d) references to legislation include any statute, regulation or order as amended extended, re-enacted, consolidated or replaced from time to time;

(e) a company shall be deemed to be a subsidiary of another company as defined by Section 1159 of the Companies Act 2006; and

(f) the Ejusdem Generis rule does not apply to the interpretation of this Agreement. The words **include, including** and **in particular** indicate examples only. They do not limit the general nature of any preceding words. A phrase starting with the words **or other** or **otherwise** is not limited by any preceding words where a wider interpretation is possible. Where this Agreement defines a word or expression related words and expressions have a consistent meaning.

2 Undertakings to be bound by BCRs and terms of this Agreement

2.1 Each Member undertakes and agrees with each other Member that they will each from their respective Member Commencement Dates throughout their respective Member Terms:

(a) be bound by and comply with the terms of the BCRs as may be amended from time to time in accordance with Clause 8; and

(b) be bound by and comply with the other terms of this Agreement.

2.2 A **Member** shall be a Fiserv entity listed in Schedule 3 which has:

(a) executed this Agreement on or before the Commencement Date; or

(b) after the Commencement Date, executed a Declaration of Accession, with the agreement of the Parent Company in accordance with Clause 19

and

(c) not ceased to be a Member pursuant to Clause 4.

For the avoidance of doubt, the provisions of Clause 2.1 shall apply to and have effect in respect to all Members from time to time, regardless of whether they become a Member pursuant to sub-Clause 2.2(a) or sub-Clause 2.2(b), and the expression "Member" shall include all such Members from time to time. The Parent Company is also a Member.

2.3 This Agreement shall terminate in respect to any or all of the Members (as appropriate) in accordance with Clause 4.

3 Further Undertakings

3.1 Each Member agrees and undertakes during its Member Term to co-operate with each other Member during their respective Member Terms:

(a) to the extent required to enable each other to perform their obligations under the BCRs and the other terms of this Agreement; and

(b) to deal promptly and properly with all reasonable enquiries from other Members, or its data protection officer or his or her agents, about Personal Data originating from or in connection with the Member in question.

3.2 The Parent Company agrees and undertakes that it shall deal promptly and properly with all reasonable requests from any Member to procure that another Member performs its obligations under the BCRs and, where required, shall procure such performance by that Member. Each other Member shall do all things necessary to assist the Parent Company to enable it to discharge its obligations under this Clause 3.2.

3.3 The Parent Company agrees and undertakes to promptly undertake all and any actions as are required to:

(a) enable FDR LIMITED, LLC to fulfil and/or perform its obligations under the BCRs and the other terms of this Agreement; and

(b) procure that FDR LIMITED, LLC is fully indemnified by the relevant Indemnifying Member in accordance with Clause 7 of this Agreement.

3.4 Security of processing where acting as a processor

3.4.1 Each Member acknowledges that from time to time it may process Personal Data as a processor (**Processor Member**) on behalf of any and all of the other Members (the **Controller Member**) whether as a result of compliance with the BCRs or otherwise. The Member will ensure at all times that it is clearly documented where responsibility lies for the processing of such Personal Data in accordance with the GDPR.

3.4.2 Each Member agrees and acknowledges that compliance with the BCRs, particularly in relation to security measures, constitutes sufficient guarantees relating to the technical and organisational security measures governing the processing to be carried out by the Member to satisfy the requirements of the Article 32 of the GDPR.

3.4.3 The information required by Article 28(3) of the GDPR in relation to the subject-matter, duration, nature and purpose of the processing, type of Personal Data and categories of Data Subjects, is set out in the BCRs.

3.4.4 Each Processor Member undertakes to the Controller Member that it shall:

(a) **Instructions:** subject to Clause 3.4.5, only process the Personal Data:

(i) on the documented instructions of the Controller Member, including with regard to transfers of Personal Data to a third country or international organisation; or

(ii) as required by law applicable to the Processor Member, provided that the Processor Member first informs the Controller Member in written form of that legal requirement before processing unless that law prohibits this on important grounds of public interest;

(b) **Staff:** ensure the Processor Member staff authorised to process the Personal Data have committed themselves to obligations of confidentiality or are under an appropriate statutory obligation of confidentiality;

(c)   **Security:** take all measures required by Article 32 (Security of Processing) of the GDPR;

(d)   **Sub-processors:**

    (i)   not engage any third party to process the Personal Data (a "**Sub-Processor**"), except as permitted by the BCRs;

    (ii)   where permitted by the BCRs, inform the Controller Member of any intended changes concerning the addition or replacement of a Sub-Processor by:

        (A)   in respect of members of the Fiserv Group, publishing such changes at on Fiserv's website from time to time; or

        (B)   in respect of Sub-Processors which are not members of the Fiserv Group, providing prior written notice to the Controller Member,

    (each an "**Sub-Processor Notice**"). The Sub-Processor Notice shall include information regarding the Sub-Processor and the kind of service to be provided;

    (iii)   If the Controller Member has reasonable concerns that processing of the Personal Data by the additional or replacement Sub-Processor will not meet the requirements of the GDPR, the Controller Member shall be entitled to object to any such changes by written notice to the Processor Member within thirty (30) days of the Sub-Processor Notice, such notice to contain reasonable information to support the Controller Member's concerns;

    (iv)   enter into a written agreement with all Sub-Processors containing obligations on such third party which are equivalent to those set out in this Agreement. In particular, the engagement of an Sub-Processor is subject to the Sub-Processor providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR. The Processor Member shall remain fully liable to the Controller Member for the performance of that Sub-Processor's obligations;

(e)   **Data Subject Rights:** taking into account the nature of the processing, assist the Controller Member by appropriate technical and organisational measures, insofar as this is possible, for the fulfillment of Controller Member's obligation to respond to requests for exercising of Data Subject rights (including access requests) set out in Chapter III of the GDPR (Rights of the data subject);

(f)   **Assistance:** assist the Controller Member to comply with its obligations pursuant to Articles 32 to 36 of the GDPR, taking into account the nature of the processing and the information available to the Processor Member;

(g)   **Termination:** following termination of this Agreement, for whatever reason, delete all Personal Data and/or transfer all Personal Data to the Controller Member on request, unless the laws applicable to Processor Member require storage of the Personal Data;

(h)   **Audit:** in accordance with the BCRs:

(i)   make available to the Controller Member all information reasonably requested by the Controller Member to the extent required to demonstrate compliance with Processor Member's obligations under this Agreement; and

(ii)   permit the Parent Company, the Controller Member, or a third-party auditor acting under the Controlling Member's direction, to conduct audits, including inspections.

3.4.5   The Processor Member shall have the right to inform the Controller Member if, in the Processor Member's opinion, an instruction from the Controller Member is in violation of the GDPR and the Processor Member may refuse to perform such instruction until such time that the Controller Member has amended the instruction in a manner which, in the Processor Member's opinion, will not breach the GDPR.

4   Term and Termination

4.1   This Agreement shall commence on the Member Commencement Date and shall continue in force in relation to each Member until it is terminated in accordance with this Clause 4 in respect of that Member. This Agreement shall remain in force in respect to any Remaining Members pursuant to Clause 5.3(a). Upon termination of this Agreement in respect to all Members under this Clause 4, this Agreement shall terminate. By entering into this Agreement, Members agree that the Binding Intragroup EU Processor Membership Agreement previously entered into between some of the Members is hereby terminated, or partially terminated, as of the Member Commencement Date insofar as this Agreement addresses the transfers covered by such agreement. For the avoidance of doubt this Agreement shall not affect any data processing and data transfer agreements between the Members (or any parts thereof) whereby the Members receive Personal Data which is subject to the UK GDPR or other data protection laws aside from the GDPR.

4.2   The Parent Company may terminate all or any part of this Agreement in respect to any or all Members (including the Parent Company) on 10 Business Days' written notice to the specific Member or Members (excluding the Parent Company) at any time.

4.3   The Parent Company may terminate this Agreement in respect to all or any Members (excluding the Parent Company) immediately on written notice to the specific Member or Members if the Member or Members in question commit, or are reasonably suspected of committing, a material breach of this Agreement which is not capable of remedy or, in the case of a breach which is capable of remedy, is not remedied within 5 Business Days of service upon the Member or Members of a notice specifying the breach and requiring it to be remedied.

4.4   If there is a Change of Control Event, the Parent Company may in its discretion terminate this Agreement in respect to all Members (including the Parent Company) or just those Members (excluding the Parent Company) affected by the Change of Control Event immediately upon written notice to the relevant Member or Members, provided such notice is given within 60 days of the Parent Company becoming aware of the occurrence of the Change of Control Event.

4.5   This Agreement shall terminate immediately in any one or more of the following circumstances in respect to all or any Members as appropriate:

(a)   upon the recommendation, advice or order of any Regulator, in which event this Agreement shall terminate only in respect to the Member or Members regulated by the Regulator in question;

(b)   as required to give effect to any Applicable Laws or any other legal declaration binding upon the Parent Company; or

(c)   the Parent Company ceasing to do business.

4.6   This Agreement shall terminate automatically in respect to all or any Members (excluding the Parent Company) if the relevant Member or Members cease to be an Affiliate.

4.7   This Agreement shall terminate upon notice by a specific Member in accordance with Clause 8.3.

5   Consequences of termination

5.1   On termination of this Agreement in accordance with Clause 4 each Member in respect to which it is terminated (an **Exiting Member**) shall:

   (a)   immediately cease to be a Member, and, subject to Clause 5.1(d) and 5.2, the provisions of Clause 2.1 shall cease to apply to it;

   (b)   where the Member is not the Parent Company, upon request of the Parent Company, return to the Parent Company or relevant Affiliates, as applicable, or irrevocably destroy or delete (at the Parent Company's sole option) all Personal Data and all information, documentation and other materials relating to the Personal Data belonging to the Parent Company or any other Affiliates (other than the Member who is the Exiting Member);

   (c)   where the Member is not the Parent Company, immediately cease processing Personal Data belonging to the Members (other than the Member who is the Exiting Member), as requested by the Parent Company;

   (d)   at the request of the Parent Company, enter into such agreements (including with other Affiliates) as necessary to effect the smooth transition of Personal Data as set out in Clause 5.1(b) and in any event fully co-operate with the Parent Company and the other Affiliates as reasonably required by them; and

   (e)   return, irrevocably destroy or delete or otherwise deal with all Personal Data and all information, documentation and other materials relating to the Personal Data relating to the Controller Member in accordance with the process agreed between the Processor Member and the affected Controller Member.

   For the avoidance of doubt, nothing in this Agreement shall prevent any party from entering into such data processing and data exchange arrangements as may be necessary or legally required from time to time following termination of this Agreement.

5.2   Termination of this Agreement shall be without prejudice to any other rights or remedies a Member may be entitled to under this Agreement or at law and shall not affect any accrued rights or liabilities of any Member nor shall it affect the coming into force or the continuance in force of any provision hereof which is expressly or by implication intended to come into or continue in force on or after such termination including without limitation Clauses 1, 5.1, 5.2, 5.3, 6, 7, 13 and 17. The rights to terminate this Agreement set out in this Clause are without prejudice to any other right or remedy any Member may have under Applicable Laws.

5.3   Upon termination of this Agreement in respect to an Exiting Member:

   (a)   this Agreement shall remain in full force and effect in respect to all Members who are not Exiting Members (the **Remaining Members**); and

   (b)   subject to Clause 5.2, the Remaining Members shall cease to owe any further rights or obligations to the Exiting Member, and subject to Clauses 5.1 and 5.2, the Exiting Member shall cease to owe any further rights or obligations to the Remaining Members.

6 Liability

6.1 Each Member shall be liable for all breaches by it of the BCRs regardless of under which jurisdiction the claim is brought.

6.2 No Member excludes or limits liability to the other Members for death or personal injury arising from its negligence.

7 Indemnity

7.1 Each Member (the **Indemnifying Member**) shall be liable for and shall fully and promptly indemnify and keep indemnified and hold harmless FDR LIMITED, LLC, save where FDR LIMITED, LLC is the Indemnifying Member, and any other Member, including the Parent Company, (together, the **Indemnified Parties**) on demand in respect of all liabilities, damages, costs, losses, claims, demands and proceedings whatsoever, howsoever arising, whether in contract, tort, breach of statutory duty or Applicable Law or otherwise, directly or indirectly, out of, or in the course of or in connection with any alleged or actual claims advanced against them by a Data Subject arising from breach by the Indemnifying Member of this Agreement, the BCRs or any Applicable Law relating to its processing of Personal Data.

7.2 The Indemnifying Party shall promptly notify FDR LIMITED, LLC, the Parent Company and, if applicable, the relevant Indemnified Parties in writing if it becomes aware of any claims or alleged claims advanced or to be advanced against them or any Indemnified Parties.

7.3 Following notification in accordance with Clause 7.2, the Parent Company may at its sole option, assume conduct of and/or settle, and the Indemnifying Party shall allow the Parent Company to assume conduct of and/or settle, all negotiations and any actions resulting from any such claim or alleged claim. However, where the Parent Company does not elect to assume such conduct or settlement, and if requested by FDR LIMITED, LLC or the relevant Indemnified Party against whom the claim or alleged claim has been advanced or is to be advanced, the Indemnifying Party shall allow the relevant Indemnified Party to conduct and/or settle all negotiations and any actions resulting from any such claim or alleged claim.

7.4 Notwithstanding the provisions set out above, the Indemnifying Party agrees that in relation to any claim or alleged claim brought in relation to this Clause 7, it shall fully submit to the direction of the Parent Company and fully co-operate with the Parent Company and any applicable Indemnified Party in relation to the same.

8 Amendments

8.1 No variation or amendment to this Agreement, except amendments to the BCRs themselves, other than pursuant to an express provision of this Agreement, shall be effective unless and to the extent that the variation or amendment is agreed in writing by the Members.

8.2 Subject to Clause 8.3, the Parent Company shall be entitled to vary the terms of this Agreement (including, without limitation, the terms of the BCRs) with the approval of the Parent Company's Data Protection Officer. Any such changes shall be effective, in relation to the Parent Company, immediately and in relation to any other Member, immediately upon notice to the Member by the Parent Company unless otherwise specified by the Parent Company and subject to Clause 8.3.

8.3 If a Member (excluding the Parent Company) does not wish to be bound by a change notified under Clause 8.2 it shall be entitled to serve 30 calendar days written notice on the Parent Company of the same upon which this Agreement shall terminate in respect to that Member on expiry of that notice.

8.4 In the event of any conflict or inconsistency between the terms of this Agreement and the terms of any other agreement excluding the BCRs between the Members, the terms of this Agreement shall prevail. In the event of conflict between the terms of this Agreement and the BCRs, the terms of the BCRs shall prevail.

9   **Consideration**

9.1   The undertakings set out in Clause 2 are given by each Member and are in consideration of the same undertakings being given by each other Member in that Clause.

10   **Dispute Resolution**

10.1   In the event of any dispute relating to the terms of this Agreement between the Members, the dispute shall in the first instance be referred to the Data Protection Officer.

10.2   In the event that the Data Protection Officer cannot resolve the dispute to the satisfaction of the Members involved within 20 Business Days after it has been referred under Clause 10.1, the dispute shall be referred to the Fiserv Risk Committee of the board for determination.

10.3   If the dispute is not resolved to the satisfaction of the Members involved within 20 Business Days after it has been referred under Clause 10.2, the relevant Members shall be entitled to commence court proceedings in accordance with the law and jurisdiction provisions set out in Clause 17.

11   **Whole Agreement**

11.1   This Agreement, together with all schedules hereto (each of which is incorporated herein by this reference) sets out the entire agreement between the Members and supersedes any previous agreement between them in relation to the subject matter of this Agreement.

11.2   All warranties, conditions or other terms implied by statute or common law are excluded to the fullest extent permitted by law.

12   **Waiver**

No failure to exercise, nor delay or omission by any Member in exercising any right or remedy conferred under this Agreement or provided by law shall, except with the express written consent of the Member in respect to whom such right or remedy may be exercised, affect that right or remedy or operate as a waiver of it. No single or partial exercise by any Member of any right or remedy shall prevent any further exercise of that right or remedy or the exercise of any other right or remedy.

13   **Further Assurance**

Each Member shall execute and sign such documents and do all such acts and things as any other Member shall reasonably request in order to carry out the intended purpose of this Agreement or to establish, perfect, preserve or enforce that other Member's rights under this Agreement.

14   **Notices**

14.1   Any notice or other communication to be given under this Agreement shall be in writing in English and signed by or on behalf of the Member giving it or its representative (excluding the Parent Company) and, unless otherwise provided, shall be delivered by hand, sent by registered airmail, sent by reputable courier or express delivery service, or sent by facsimile to the address or facsimile transmission number of the other Member notified to the Member giving notice for this purpose (or such other address or facsimile transmission number as the receiving Member has specified to the sending Member on at least 10 Business Days' notice) or, in the case of notice by the Parent Company of changes to the terms of this Agreement (including, without limitation, the terms of the BCRs) by email, to the email address dpo@fiserv.com or other address as posted on the Parent Company Intranet site for the Data Protection Officer, as such address is amended from time to time or which is notified by the Member to the Parent Company as its contact email address. The addresses and the numbers of the Members for the purposes of this Clause 14.1 are available from the Corporate Secretary of the Parent Company upon request.

14.2   Any notice or other communication given or made under this Agreement shall, in the absence of earlier receipt, be deemed to have been received as follows:

(a)   if delivered by hand, at the time of actual delivery;

(b)   if posted by airmail, on the tenth Business Day following the day on which it was despatched by registered airmail;

(c)   if sent by facsimile transmission, with a confirmed receipt of transmission from the receiving machine, on the Business Day on which received as evidenced by such confirmed receipt;

(d)   if sent by a reputable courier or express delivery service, on the third Business Day after the Business Day of deposit with such service; or

(e)   if sent by email, on the Business Day on which it is sent, provided the sender does not receive a "bounceback" or other automated message indicating that the message could not be delivered.

15   Invalidity

If at any time any provision of this Agreement or the BCRs becomes invalid, illegal or unenforceable in any respect under the law of any jurisdiction in relation to any Member that shall, so long as the commercial purpose of this Agreement is still capable of performance, not in any way affect or impair:

(a)   the validity, legality or enforceability in that jurisdiction and in relation to that Member of any other provision of this Agreement or the BCRs; or

(b)   the validity, legality or enforceability under the law of any other jurisdiction or in relation to any other Member of that or any other provision of this Agreement or the BCRs.

16   Counterparts

The Members may execute this Agreement in any number of copies and as separate copies. Each executed copy counts as an original of this Agreement and together the executed copies form one instrument.

17   Law and Jurisdiction

This Agreement shall be governed by and construed in accordance with the laws of Ireland and the Members agree to submit to the exclusive jurisdiction of the Courts of Ireland as regards any claim or matter arising out of or in connection with this Agreement.

18   Rights of Third Parties

This Agreement is not intended to, and does not, give any person who is not a Party any rights to enforce any provisions contained in it, except the provisions of Clauses 6 and 7 shall be enforceable by any Affiliate which becomes a Member pursuant to Clause 2.2(b) and any other provision of this Agreement which expressly provides for enforcement by a third party (which shall include Data Subjects) shall be enforceable in accordance with its express terms.

19   Addition of new Members

19.1   Subject to the prior agreement of the Parent Company, which will only be provided where the Parent Company is satisfied that the new Member is capable of complying with the terms of this Agreement, a new Member may be added to this Agreement provided that it is a member of the Fiserv Group and signs a Declaration of Accession (in the form set out in Schedule 4) to

be bound by this Agreement. No transfers of Personal Data will be made to a new Member until that Member is effectively bound by this Agreement.

19.2   The other Members to this Agreement hereby authorise the Parent Company to do this at its reasonable discretion and agree to extend the commitments which they give in this Agreement to the Member, in respect of any Personal Data which they transfer to or receive from the new Member.

19.3   Schedule 3 shall be considered automatically updated upon the addition of the new Member in accordance with this Clause.

19.4   The Parent Company shall maintain an up-to-date list of the Fiserv Group companies which have entered into this Agreement, in a manner reasonably accessible to the Members (and Data Subjects).

Schedule 1: – Fiserv's Processor Data Protection Standards (the "EU BCRs")

EU PROCESSOR DATA PROTECTION STANDARDS

Effective as of _____13/9/2023_____

Defined Terms used with the EU BCRs

These Processor Data Protection Standards use a number of defined terms which are fully defined in context below. However we have repeated or simplified the most significant definitions here for ease of reference. Where appropriate these definitions are consistent with the definitions set out in the GDPR.

Adequate Third Country means any third country that is determined pursuant to applicable Privacy Laws to offer adequate protection for Personal Data. Currently this list includes Andorra, Argentina, Canada, Isle of Man, Japan, Jersey, Faroe Islands, Guernsey, New Zealand, Israel, South Korea, Uruguay and the United Kingdom (para 3.6)

controller means the natural or legal person which alone or jointly with others, determines the purposes and means of the processing of Personal Data**;**

Data Controller means a Fiserv entity or our client who is acting as the controller of Personal Data;

Data Subjects means identified or identifiable natural person (para 1.2);

External Sub-Processors means or external sub processors that are not Fiserv entities used by Fiserv in processing the Personal Data outside of the EEA (para 2.2);

Fiserv, Fiserv entity, we or our means Fiserv, Inc. and its subsidiaries which have signed an intragroup agreement committing them to these EU Processor Data Protection Standards. Fiserv, Inc. has nominated the Irish branch of FDR LIMITED, LLC as the Fiserv establishment within the EEA to whom it delegates data protection responsibilities for the purposes of these Processor Data Protection Standards. These responsibilities include accepting liability for breaches of these Processor Data Protection Standards by Fiserv entities (see para 1.1, 2.2 and 3.1);

Fiserv Importer means a Fiserv entity established in a third country outside of a Relevant Country (other than an Adequate Third Country) **(para 7.7);**

Fiserv Privacy Site means www.fiserv.com/bcr(para 3.3);

Personal Data means any information relating to an identified or identifiable individual that Fiserv processes while operating its business (para 1.2);

process, or **processing, processes or processed** means 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 (para 2.3);

processor means the natural or legal person which processes Personal Data on behalf of the controller;

Privacy Laws means 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"**), and the Privacy and Electronic Communications Directive (Directive 2002/58/EC) and any legislation

and/or regulation implementing or made pursuant to them, or which amends, replaces, re-enacts or consolidates any of them;

Privacy Notice means the information which Fiserv is required to give to Data Subjects under the GDPR which is set out in Fiserv's privacy notice, which is available at www.fiserv.com/privacy (para 11.2);

Relevant Country means a member state of the European Union and/or the European Economic Area (para 3.1);

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 (para 4.2);

Supervisory Authority means any supervisory authority in a Relevant Country (para 7.4). The competent Supervisory Authority is (i) the lead Supervisory Authority (which in this case is the Irish Data Protection Commissioner) or (ii) any other supervisory authority in a Relevant Country which is "concerned" by the processing of Personal Data because (a) a Fiserv entity is established in the country or territory where that Supervisory Authority is established, (b) because Data Subjects are living in a country or territory of that Supervisory Authority and are likely to be affected by a Fiserv entity's processing of Personal Data, (c) it has received a complaint from a Data Subject relating to processing of Personal Data by a Fiserv entity or (d) where Personal Data are processed by a non-European Fiserv entity on behalf of a Customer, the competent supervisory authority for the customer;

third party or parties means entities which are not Fiserv entities (para 6.1);

Transfer means transfers of Personal Data made by a Fiserv entity or External Sub-Processor of that entity located in a Relevant Country to a Fiserv entity or External Sub-Processor of that entity located outside the EEA which is in a third country (other than an Adequate Third Country) (para 3.6).

Transfer Impact Assessment means an assessment to consider that the laws and practices in the third country of destination applicable to the processing of Personal Data by the Fiserv Importer or External Sub-Processor, including any requirements to disclose Personal Data or measures authorising access by public authorities do not prevent it from fulfilling its obligations under these Processor Data Protection Standards. This assessment is based on the understanding that laws and practices that respect the essence of fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives in Art 23(1) GDPR, are not in contradiction with these Processor Data Protection Standards (para 7.6).

1   Who we are

1.1   As a leading global payments and financial technology provider, Fiserv, Inc., a corporation organised and existing under the laws of the State of Wisconsin, USA whose principal place of business is at 255 Fiserv Drive, Brookfield, WI 53045, United States of America and its subsidiaries ("**Fiserv**" or "**our**" or "**we**" as further defined in paragraph 3.1.1) provide processing solutions that help businesses and consumers engage in financial transactions nearly anywhere in the world, any time of the day, with virtually anyone in the world.

1.2   These Processor Data Protection Standards (including the attached Annex) express the commitment of our Executive Management and Board of Directors to data privacy and protecting all information relating to identified or identifiable natural individuals ("**Data Subjects**") that Fiserv processes (as defined below) while operating its business ("**Personal Data**") and in ensuring adequate protection of transfers of Personal Data between Fiserv 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 Fiserv's overall approach to privacy and data protection.

2 Our Business

2.1 Fiserv operates in more than 100 countries worldwide and employs approximately 44,000 employees throughout the world to provide technology solutions and associated professional, support and maintenance services to millions of its clients, including processing more than93 billion payment transactions every year. Fiserv, Inc. is the ultimate parent company of the Fiserv Group and is headquartered in the United States.

2.2 Fiserv has nominated FDR LIMITED, LLC as the Fiserv establishment in the EEA to whom it delegates data protection responsibilities for the purposes of these Processor Data Protection Standards. These responsibilities include accepting liability for breaches of these Processor Data Protection Standards by Fiserv entities and / or external sub processors that are not Fiserv entities ("**External Sub-Processors**") used by Fiserv in processing the Personal Data outside of the EEA and taking any action necessary to remedy such breaches, both as described more fully in paragraph 7.2 of these Processor Data Protection Standards. Fiserv entities processing the Personal Data outside of the EEA will be bound by these Processor Data Protection Standards. External Sub-Processors will enter into separate arrangements with Fiserv to ensure the safeguarding of Personal Data in accordance with applicable law.

2.3 Fiserv has business relationships with financial institutions, corporations, credit card issuers, credit unions, acquirers, retail merchants, health care providers, utility companies, insurers and other businesses to provide innovative financial services and payment solutions for tens of millions of consumers and businesses. To provide these services, Fiserv processes 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**"). Fiserv processes Personal Data in compliance with applicable Privacy Laws (as defined in 7.1 below) and our internal policies as amended and updated from time to time.

3 The Scope of These Processor Data Protection Standards

3.1 These Processor Data Protection Standards apply only:

3.1.1 to Fiserv entities which have signed or acceded to the Binding Intra-Group Processor BCR Membership Agreement ("**Processor IGA**") and in respect of the processing of Personal Data in respect of which a Fiserv entity has a signed contract with the relevant Data Controller ensuring that the applicable Fiserv entity implements adequate technical and organisational security measures to safeguard the Personal Data, will only act on the instructions of the Data Controller, contains measures relating to the Data Controller's and other third party beneficiaries' right to enforce these Processor Data Protection Standards and contains all the other provisions required by Article 28 of the GDPR (the "**Services Agreement**"). Where the relevant Data Controller is also a Fiserv entity (rather than a client), the Processor IGA is the signed contract as mentioned above and contains all the provisions required by Article 28 of the GDPR, References to "**Fiserv**", "**Fiserv entity**" or "**Fiserv entities**", "**our**" and "**we**" shall apply and refer only to such entities. A list of these entities is available at the Fiserv Privacy Site or from the Global Privacy Office whose details are set out at the end of these Processor Data Protection Standards. All Fiserv entities can be contacted by email at DPO@fiserv.com,

or using the contact details set out at the end of these Processor Data Protection Standards; and

3.1.2   where the data protection laws of a Relevant Country apply to Fiserv'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 Fiserv entities in accordance with these Data Protection Standards or where the Services Agreement otherwise provided that these Processor Data Protection Standards should apply and all references in these Data Protection Standards to Personal Data shall be interpreted accordingly. **Relevant Country** means a member state of the European Union and/or the European Economic Area.

3.2   In many cases, Fiserv obtains Personal Data (as defined in paragraph 4.1 below) from our clients or other Fiserv entity acting as a controller rather than the Data Subjects themselves. Therefore Fiserv's processing of Personal Data about Data Subjects may be: (a) as a controller, for the purposes determined by Fiserv; or (b) as a processor following our clients' instructions or those of other parties (including other Fiserv entities acting as controller from whom we receive information) and which are ultimately governed by written contracts and/or applicable Privacy Laws.

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

3.4   Fiserv'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 Fiserv entities.

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

3.6   Data Subjects and Data Controllers alleging breach of these Processor Data Protection Standards shall only be entitled to enforce them (in relation to the Data Subjects as a third party beneficiary) pursuant to paragraph 9.1 of these Processor Data Protection Standards in respect to transfers of Personal Data made by a Fiservrst Data entity or External Sub-Processor of that entity located in a Relevant Country to a Fiservrst Data entity or External Sub-Processor of that entity located outside the EEA which is in a country not recognised as offering adequate protection for the Personal Data pursuant to applicable Privacy Laws (a "**Transfer**"). An adequate third country means any third country that is determined pursuant to applicable Privacy Laws to offer adequate protection for Personal Data. Currently this list includes Andorra, Argentina, Canada, Isle of Man, Japan, Jersey, Faroe Islands, Guernsey, New Zealand, Israel, South Korea, Uruguay and the United Kingdom ("**Adequate Third Country**").

3.7   Fiserv acknowledges that some Fiserv entities may adopt their own privacy standards, policies and procedures based on the nature of their services or clients ("**Local Policies**"). The Local Policies must be consistent with and must meet or exceed the requirements of these Processor Data Protection Standards. Where there is a conflict between the Local Policies and these Processor Data Protection Standards, the policy that is determined by the Data

Protection Officer and Global Privacy Office in consultation with the General Counsel's Office (as defined below in paragraph 7.4) to offer the highest protection will govern.

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

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

- Other Fiserv entities as well as Fiserv clients (and prospects) and their customers in connection with the provision of services. This includes personnel employed by the Fiserv entities, our clients and their customers (or the customers themselves to the extent they are individuals) (cardholders)). ("**Customers**");
- Individuals who interact directly with Fiserv or Fiserv products ("**Consumers**");
- Merchants accepting payments. This includes personnel employed by Merchants; proprietors when the Merchant is an individual and customers of Merchants (cardholders) ("**Merchants**");
- Fiserv employees, contingent workers, consultants, prospective and former personnel and the personnel's dependents and beneficiaries ("**Personnel**")
- Other persons or personnel working for an organisation which provides goods or services to Fiserv ("**Suppliers**").

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

---

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

5 **Sources of Personal Data**

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

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

5.2 The processing and transfers undertaken by Fiserv in relation to the classes of Data Subject set out above includes processing for the business purposes as determined by the applicable Data Controller as defined in more detail in Schedule 3 together with a breakdown of the purposes of Processing under these Processor Data Protection Standards.

5.3 We collect and use Personal Data information for a variety of legal reasons as determined by the applicable Data Controller.

6 **Nature of Data Transferred[2]**

6.1 Fiserv processes and transfers a broad range of Personal Data between Fiserv entities, External Sub-Processors of those entities and to other third parties which are not Fiserv 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 Information relating to a person's current, past, or prospective employment or professional experience (e.g., job history, performance evaluations), and educational background, qualifications, references, training data, grievances, salary data, benefits information, absence data, background check, survey responses, time and attendance, equal opportunities, monitoring information, dependent and beneficiary information
- Commercial Data: This includes account information, customer correspondence (e.g., support or requesting information), marketing preferences, transactions, spending and spending patterns, merchant data (for merchants who are individuals), products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
- Other categories of Personal Data defined in Schedule 3.
- Anonymised/Aggregated Personal data obtained from Data Subject which has been aggregated to a point where the individual is no longer able to be identified within the dataset.

---

[2] See footnote 1.

7   Applicable Law and Supervising Authorities

7.1   All Fiserv entities will handle Personal Data in accordance with these Processor Data Protection Standards and all applicable local data protection and privacy laws and regulations including, but not limited to, the European Union General Data Protection Regulation (2016/679) (the "**GDPR**"), the Privacy and Electronic Communications Directive (Directive 2002/58/EC) and any legislation and/or regulation implementing or made pursuant to them, or which amends, replaces, re-enacts or consolidates any of them) (together the "**Privacy Laws**"). Additionally, the Processor Data Protection Standards must be interpreted in accordance with the Privacy Laws.

7.2   The policies and procedures described in these Processor Data Protection Standards are in addition to any other remedies available under applicable Privacy Laws or provided under other Fiserv policies and procedures. FDR LIMITED, LLC will be responsible for and will take any action necessary to remedy any breach by any Fiserv entity or External Sub-Processor of the applicable Fiserv entity outside the EEA of the rights guaranteed in these Processor Data Protection Standards as provided by paragraph 9.1. This will include any sanction imposed or other remedy available under applicable Privacy Laws including compensation. FDR LIMITED, LLC may discharge itself from this responsibility if it is able to show that the Fiserv entity and / or the External Sub-Processor of that entity which is alleged to be in breach is not liable for the breach or such Fiserv entity or the External Sub-Processor of that entity has discharged its liability for the breach.

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

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

7.5   Where a Fiserv entity believes that a conflict with applicable laws prevents it from fulfilling its duties under these Processor Data Protection Standards including following the advice of the Supervisory Authority, the Fiserv Importer (as defined below) will notify the Fiserv entity which has a valid Services Agreement with any affected Data Controller (who in turn will notify the Data Controller), FDR Limited, LLC, the Local Privacy Officer and / or Data Protection Officer who will (in consultation with the General Counsel's Office y, where necessary) responsibly decide what action to take (which may include notification to the Supervisory Authority as appropriate).

Transfer Impact Assessments

7.6   A Fiserv entity shall only transfer Personal Data (including data in transit) to a Fiserv entity established in a third country outside of a Relevant Country (other than an Adequate Third Country) (a "**Fiserv Importer**") or an External Sub-Processor established in a third country

outside of a Relevant Country (other than an Adequate Third Country), where it has carried out a Transfer Impact Assessment with the help of the Fiserv Importer or External Sub-Processor if needed. A Transfer Impact Assessment means an assessment to consider that the laws and practices in the third country of destination applicable to the processing of Personal Data by the Fiserv Importer or External Sub-Processor, including any requirements to disclose Personal Data or measures authorising access by public authorities do not prevent it from fulfilling its obligations under these Processor Data Protection Standards. This assessment is based on the understanding that laws and practices that respect the essence of fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives in Art 23(1) GDPR, are not in contradiction with these Processor Data Protection Standards.

7.7   A Transfer Impact Assessment shall consider (i) the specific circumstances of the transfers or set of transfers and of any envisaged onward transfers within the same third country or to another third country, including (a) the purposes for which the data are transferred and processed (b)type of entities involved in the processing (c)the economic sector in which the transfer or set of transfers occur (d) categories and format of the Personal Data (e)location of the processing including storage and (f) the transmission channels used, (ii) the laws and practices of the third country relevant in the light of the specific circumstances of the transfer including those requiring the disclosure of data to public authorities or authorising access by such authorities and those providing for access to these data during transit as well as the applicable limitations and safeguards (and in particular, taking into consideration any relevant and documented practical experience with prior instances of requests for disclosure of data to public authorities or the absence of such requests provided it is supported by other relevant objective elements such as publicly available or otherwise accessible, reliable information on the existence or absence of any requests within industry) and (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Processor Data Protection Standards including measures applied during the transmission and to the processing of Personal Data in the third country and must confirm that there is no reason to believe that the laws and practices in the third country applicable to the processing of the Personal Data, including any requirements to disclose Personal Data or measures authorising access by public authorities and those providing for access to these data during transit, prevent the Fiserv Importer or External Sub-Processor from fulfilling their obligations under these Processor Data Protection Standards and provide a level of protection that is essentially equivalent to that provided by applicable Privacy Laws.

7.8   If a Transfer Impact Assessment cannot confirm the above points, the Fiserv exporting entity shall assess whether the parties to the transfer can provide further supplementary measures (such as additional contractual, technical or organisational measures) in additional to these Processor Data Protection Standards to ensure an essentially equivalent level of protection as provided by applicable Privacy Laws and shall promptly inform and involve FDR Limited, LLC and the Local Privacy Officer and/or Data Protection Officer who will (in consultation with the General Counsel's Office) decide what action to take.

7.9   Where the Fiserv entity exporting the Personal Data is not able to take any supplementary measures necessary to ensure an essentially equivalent level of protection as under applicable Privacy Laws, the Fiserv entity shall promptly inform FDR Limited, LLC and the Local Privacy Officer and/or Data Protection Officer who will (in consultation with the General Counsel's Office) decide what action to take. If, in such case, the Fiserv entity wishes to transfer Personal Data on the basis of these Processor Data Protection Standards, it should notify the competent Supervisory Authority beforehand to enable the competent Supervisory Authority to ascertain whether the proposed transfer should be suspended or prohibited in order to ensure an adequate level of protection. Where it is determined pursuant to this

paragraph that any proposed transfers should be suspended or prohibited as a result, the applicable Fiserv entities will be notified.(which in turn shall notify the relevant Data Controllers).

7.10   The Fiserv entities will document the Transfer Impact Assessment appropriately as well as any additional supplementary measures selected and implemented and will make such documentation available on request to the affected Data Controller, the competent Supervisory Authority as well as other Fiserv entities where similar transfers may be taking place.

7.11   Each Fiserv Importer agrees to notify promptly inform the Fiserv entity which has a valid Services Agreement with any affected Data Controller (who in turn will notify the applicable Data Controller), and the Local Privacy Officer and/or Data Protection Office if it has reason to believe that it is or has become subject laws or practices in the third country which would prevent it from fulfilling its obligations under these Processor Data Protection Standards or fail to provide a level of protection that is essentially equivalent to that provided by applicable Privacy Laws including following a change in the laws of the third country or a measure (such as a disclosure request). This information shall also be provided to FDR Limited LLC.

7.12   Upon verification of such notification pursuant to paragraph 7.11, the Fiserv exporting entity along with FDR Limited LLC and the Local Privacy Officer and/or Datra Protection Office shall promptly identify appropriate supplementary measures to be adopted to address the situation, if appropriate in consultation with the affected Data Controller. The same applies if the Fiserv exporting entity has reasons to believe that the Fiserv Importer can no longer fulfil its obligations under these Processor Data Protection Standards. The transfer shall be suspended if no appropriate supplementary measures can be ensured, or if instructed by the Data Controller or competent Supervisory Authority to do so as well as all transfers for which the same assessment and reasoning would lead to a similar result, until compliance is again ensured or the transfer ended. Following such a suspension, the Fiserv exporting entity has to end the transfer or set of transfers if these Processor Data Protection Standards cannot be complied with and compliance is not restored within one month of suspension. If the transfer is ended, the Fiserv Importer shall at the Fiserv exporting entity's choice either securely return or destroy any Personal Data in its possession or control. FDR Limited LLC and the Local Privacy Officer and/or Data Protection Office shall inform all other Fiserv entities of the Transfer Impact Assessment carried out and its results so that the identified supplementary measures will be applied where the same type of transfers are carried out by any other Fiserv exporting entity or where effective supplementary measures cannot be put in place, the transfers at stake are suspended or ended.

7.13   Each Fiserv exporting entity shall monitor, on an ongoing basis, and where appropriate in collaboration with the Fiserv Importer or External Sub-Processor, any legal or policy developments in the third country that could affect the initial Transer Impact Assessment and its results and the decisions taken in accordance with such transfers.

Obligations in case of access by public authorities

7.14   If a Fiserv Importer becomes aware of any direct access to Personal Data by public authorities or if there is any legally binding request for disclosure of the Personal Data from a public authority (e.g by a law enforcement authority or state security body), it agrees to notify FDR Limited, LLC, the Fiserv entity which has the valid Services Agreement with any affected Data Controller (which in turn shall notify the Data Controller) including information about the data requested, the requesting body, and the legal basis for the disclosure and the response provided, unless such notification is otherwise prohibited by applicable laws;

7.15   If the notification is prohibited by applicable laws, the Fiserv Importer 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 the relevant party. The Fiserv Importer agrees to document its best efforts in order to be able to demonstrate them on request;

7.16   Where permitted by applicable laws, the Fiserv Importer agrees to provide FDR Limited, LLC, the Local Privacy Officer and / or Data Protection Officer, the Fiserv entity which has a valid Services Agreement with any affected Data Controller (who in turn will notify the Data Controller) at regular intervals and with as much relevant information as possible of the requests received by the Fiserv Importer (in particular, number of requests, type of data requested, requesting authorities, whether requests have been challenged and the outcome of such challenges).

7.17   The Fiserv Importer agrees to preserve the information pursuant to paragraph 7.14 – 7.16 for the duration of these Processor Data Protection Standards and make it available to the competent Supervisory Authority on request, if permitted by applicable laws.

7.18   The Fiserv Importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under of the country of destination, applicable obligations under international law and principles of international comity. The Fiserv Importer shall, under the same conditions, pursue the possibility of appeal. When challenging a request, the Fiserv Importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the Personal Data requested until required to do so under the applicable procedural rules.

7.19   The Fiserv Importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to FDR Limited, LLC, the Local Privacy Officer and/or Data Protection Officer, the Fiserv entity which has a valid Services Agreement with any affected Data Controller (who shall in turn make available to the Data Controller). It shall also make it available to relevant competent Supervisory Authority on request. The Fiserv Importer agrees to provide only information that is strictly necessary when responding to a request for disclosure, based on a reasonably interpretation of the request.

7.20   In any event, Fiserv entities must not provide Personal Data to public authorities in a way which would involve massive, disproportionate and indiscriminate transfers that go beyond what is necessary in a democratic society.

8   Changes to our Data Protection Standards

8.1   Fiserv may change these Processor Data Protection Standards, additional Fiserv entities may sign the Processor IGA and certain Fiserv entities may terminate or have their Processor IGA terminated. The Data Protection Officer with the assistance of the Global Privacy Office will keep a fully updated list of Fiserv entities who are signatories to the Processor IGA and keep track of and record any updates to these Processor Data Protection Standards and provide the necessary information to Data Controllers with whom it has a valid Services Agreement, Data Subjects or Supervisory Authorities upon request. In addition, all changes, additions and the termination of any Processor IGA and any change to the Processor Data Protection Standards must be subject to the approval of the Data Protection Officer and will be reported to each Supervisory Authority annually and any Data Controllers with whom it has a valid

Services Agreement in accordance with the terms of that Services Agreement. Any significant changes will be reported without undue delay, where required. Where an update significantly affects these Processor Data Protection Standards, or could affect the level of protection offered by them, Fiserv will promptly communicate the update to the relevant Supervisory Authorities. Upon approval of the Data Protection Officer, we will clearly indicate the date of the latest revision and communicate the Processor Data Protection Standards to all Fiserv entities and post the revision on Fiserv's public website. No transfers will be made to a new Fiserv entity until that Fiserv entity is effectively bound by these Processor Data Protection Standards and able to comply with them.

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

9   **Compliance and Dispute Resolution**

9.1   Under paragraph 2.2 of these Processor Data Protection Standards, FDR LIMITED, LLC has accepted liability for breaches of these Processor Data Protection Standards by Fiserv entities outside of the EEA, and for taking any action necessary to remedy such breaches. Fiserv shall inform the Data Controller of any complaint made by a Data Subject as soon as reasonably practicable but shall not be obliged to handle or otherwise deal with such complaint further save where the Data Controller has factually disappeared, ceased to exist or become insolvent and no successor has assumed the obligations of the Data Controller. A Data Subject may only enforce these Processor Data Protection Standards as a third party beneficiary in these limited circumstances. A Data Subject should always pursue the Data Controller in respect of any claims resulting from issues relating to the processing of its Personal Data.

9.2   Data Subjects and/or Data Controllers alleging breach of these Processor Data Protection Standards against FDR LIMITED, LLC or the Fiserv entity or its External Sub-Processors making the Transfer (as defined in Paragraph 3.6) as provided in paragraphs 2.2 and 7.2 and in particular those set out in paragraphs 7.1, 7.4, 7.5, 7.6, 7.8 and 11 can enforce them only as a third party beneficiary if they relate to a Transfer in the following ways:

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

9.2.2   If the issue is not resolved to the Data Subject or Data Controller's satisfaction <u>or</u> if the Data Subject or Data Controller prefers in the first instance without going to the Data Protection Officer or applicable Local Privacy Officer, he or she may directly:

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

- bring the issue before the courts in the EEA where Fiserv has an establishment, or the courts of the country where the Data Subject has his or her habitual residence, at the Data Subject's option.

9.3   Subject to paragraph 3.6, any Data Subject who has suffered damage (whether material or non-material) as a result of an infringement of the rights expressly granted to Data Subjects

under these Processor Data Protection Standards will have the right to receive compensation from Fiserv for the damage suffered. Fiserv shall have the burden of proving that it is not in any way responsible for the event giving rise to the damage. The compensation claimed by a Data Subject is limited to that which would be due under Article 82 of the GDPR.

9.4   The complaints handling process under these Processor Data Protection Standards is provided for by Fiserv's Security Hotline. Further, under Fiserv's Code of Conduct, Fiserv's personnel can raise complaints regarding breaches of these Processor Data Protection Standards by contacting the Data Protection Officer or through the Fiserv Security Hotline. A decision on any complaint made (whether made by Fiserv'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 Fiserv shall inform the Data Subject accordingly. Fiserv shall inform the Data Controller of any complaint made by a Data Subject without undue delay and shall co-operate with the Data Controller to assist the Data Controller to comply with its data protection obligations as agreed between the parties in the Services Agreement.

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

10   Communication of Fiserv's Processor Data Protection Standards

10.1   Fiserv takes compliance with its data protection obligations very seriously. All Fiserv personnel who process Personal Data will comply with these Processor Data Protection Standards, and receive training on and access to these Processor Data Protection Standards and any relevant provisions of the Services Agreement. Fiserv will post a copy of these Processor Data Protection Standards on its internal and public websites, including on the Fiserv Privacy Site. In addition, Data Subjects will be provided with a link to our public website upon request. The Data Protection Officer and the Global Privacy Office will maintain a list of the Fiserv entities (including contact details) that are bound by these Processor Data Protection Standards and will publish the list on the Fiserv Privacy Site.

11   Fiserv's Privacy Principles

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

11.2   Additionally, Fiserv shall upon the request of the Data Controller provide the Data Controller with such information relating to its processing and the processing of any of External Sub-Processors as may be reasonably required by the Data Controller to enable it to correctly inform its Data Subjects for the purpose of complying with its legal obligations relating to this principle of 'lawfulness, fairness and transparency'. Fiserv's information notice containing the information it is required to give to Data Subjects under GDPR is set out in: (a) these Processor Data Protection Standards; and (b) Fiserv's Privacy Notice, which is available at www.fiserv.com/privacy. Where appropriate, the information given by these Processor 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   Fiserv collects, transfers (including transfers outside the EEA), holds and processes Personal Data only in accordance with the mandates it has with the applicable Data Controller and otherwise in accordance with the Data Controllers' instructions.

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

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

11.5   Fiserv will keep Personal Data in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is processed, as described in Paragraph 5.2. The purposes of retaining the data, and the specific retention periods, will be as instructed by the relevant Data Controller or, in the absence of any such instructions, in accordance with Fiserv's applicable data retention policies on expiry of which Fiserv will securely delete the relevant Personal Data or return such Personal Data to the applicable Data Controller, as agreed with that Data Controller. Fiserv's retention periods are determined by factors such as the need to retain data to provide services to Data Subjects or the Data Controller, 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   Fiserv 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 Fiserv responsibilities. We require our External Sub-Processors, contractors, agents and suppliers to adopt a similar approach to Personal Data they access in connection with providing services to Fiserv.

11.7   Fiserv processes Personal Data in accordance with its written agreements including the Services Agreement or with instructions from the Data Controller (as applicable), in compliance with applicable Privacy Laws and in accordance with Fiserv'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 Privacy Laws that specify permissible uses and restrict disclosures of the information.

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

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

We implement data protection by design and default.

11.9   Where appropriate, Fiserv will implement appropriate technical and organisational measures, such as pseudonymisation and data minimisation, which are designed to implement, and to facilitate compliance with, these Processor Data Protection Standards in an effective manner

and to integrate the necessary safeguards into the processing in order to meet the requirements of these Processor Data Protection Standards and to protect the rights of Data Subjects, taking into account the nature of the processing and the information available to it.

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

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

11.11   Fiserv will conduct intra-Fiserv entity transfers and transfers to third parties on the instructions of the applicable Data Controller (including with regard to transfers of Personal Data to third countries) and upon such other terms as we may agree with them and only when the following requirements have been met:

- all applicable legal requirements are met (including the conditions in Chapter V of the GDPR);
- where the transfer is to an External Sub-Processor, the transfer is as permitted by the agreements with the applicable Data Controller or upon the instructions of the Data Controller;
- where the transfer is to an External Sub-Processor, the receiving External Sub-Processor entity has appropriate security; and
- the receiving party, if a Fiserv entity, complies with the Processor Data Protection Standards for the transfer and subsequent processing.

11.12   Fiserv entities may only appoint External Sub-Processors to process the Personal Data belonging to the Data Controller with the prior specific or general written consent of the Data Controller. The applicable Fiserv entity has appropriate agreements with its External Sub-Processors that reflect the applicable provisions of these Processor Data Protection Standards and applicable Privacy Laws (and in particular as set out in Articles 28, 29, 32,45, 46, 47 or 49 of the GDPR) and which ensures that the External Sub-Processor will respect substantially the same obligations as are imposed on the Fiserv entity under the Services Agreement and informs the Data Controller of the use of any External Sub-Processors with sufficient time for the Data Controller to object to the use of that particular External Sub-Processor.

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

- Fiserv entities;
- Fiserv's clients;
- other participants in a transaction processing chain, such as merchants, issuers of payment instruments, providers of payment instrument acquiring services, card associations and debit network operators and their members;
- third parties, upon the request of the Data Controller,
- third parties to whom Fiserv will transfer, or may transfer, its rights and duties in its agreements with Data Controllers, including if a Fiserv 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 Fiserv 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 Fiserv, our clients, or their customers or others;

- Fiserv's vendors and agents (including their sub-contractors). In particular, Fiserv may disclose Personal Data where it uses the services of:
    - credit reference agencies;
    - fraud protection and risk management agencies;
    - identification and information verification agencies;
    - vendors and others that help us process a Data Subject's payments;
    - third party suppliers engaged to host, manage, maintain and develop our website and IT systems; and
    - our professional advisers, including lawyers and auditors.

11.14   Fiserv does not disclose Personal Data except in the circumstances set out in these Processor Data Protection Standards or as required or otherwise permitted by applicable law. When the processing of Personal Data is outsourced by Fiserv to a third party, Fiserv will select reliable third parties.

11.15   Except as set out above and in accordance with the Controller Data Protection Standards, Fiserv does not sell, rent, share, trade or disclose any Personal Data it keeps about a Data Subject to any other parties without the prior written consent of the supplying client.

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

11.16   Fiserv employs appropriate technical, organisational, administrative and physical security measures to protect Personal Data against unauthorised or unlawful processing and against accidental loss or destruction. Fiserv 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. Fiserv 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. Fiserv will ensure that any personnel who has access to Personal Data has appropriate obligations of confidentiality in their employment agreement with Fiserv.

11.17   Fiserv also enforces upon all Fiserv entities and their employees the importance of the provisions of the Services Agreement and, in particular, those measures relating to instructions of the Data Controller with respect to the processing of Personal Data, the security of the Personal Data and confidentiality.

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

11.19   Personal Data will not be transferred to a third country or territory which has inadequate data protection laws, unless appropriate safeguards or derogations are provided according to applicable Privacy Laws.

11.20   Special Categories of Personal Data will only be processed in accordance with applicable Privacy Laws. 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 Fiserv'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 Fiserv. Fiserv requires that all Special Categories of Personal Data be transferred securely.

We respect Data Subject rights as required by applicable Privacy Law.

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

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

11.22   Fiserv shall pass each request of a Data Subject to exercise any of the rights above to the Data Controller and will work with the applicable Data Controller (including the provision of useful information applicable to the right exercised) to help the Data Controller comply with its duty to respect the rights of Data Subjects in accordance with the GDPR.

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

11.23   Each Fiserv entity will be responsible for, and able to demonstrate compliance with, these Processor Data Protection Standards. Fiserv's Global Privacy Office operates a comprehensive network of privacy officers around the world who are responsible for data privacy within their region including compliance with these Processor Data Protection Standards. The Data Protection Officer and Chief Privacy Officer are responsible for the network of privacy officers, including the Local Privacy Officers, and the development, implementation and continuing oversight of these Processor Data Protection Standards. The Global Privacy Office, and the privacy officer network including the Data Protection Officer run various privacy programmes, promote good privacy practices with respect to Personal Data throughout Fiserv through multiple means including annual training programmes, official communications and specifically targeted training. Further, the Fiserv Global Privacy Office works with other groups within Fiserv to develop additional corporate policies and practices. The Global Cyber Security Program aims to identify and reduce Fiserv's top security risks.

11.24   Fiserv 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 Fiserv's personnel who is responsible for developing and executing a remediation plan and associated time frame. Upon completion, the audit team will review to determine if the item has been adequately addressed and can be closed or requires additional action and will provide their recommendation to the Data Protection Officer and to the Board of Directors of the relevant Fiserv entity and, where deemed appropriate by the Data Protection Officer, Fiserv, Inc.. Where sought by the Supervisory Authority (ies), Fiserv shall supply that Supervisory Authority (ies) (including the competent Supervisory Authority of the Data Controller) with a copy of the audits. Subject to the terms of any valid Services Agreement with the Data Controller and only while such Services Agreement is in force, the Data Controller or an independent third party auditor may audit the applicable Fiserv entity for compliance with these Processor Data Protection Standards and its obligations as a Data Processor set out in the GDPR, where legally permissible. Each Supervisory Authority is also authorised to audit any Fiserv entity in accordance with paragraph 7.4 of these Processor Data Protection Standards.

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

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

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

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

12   **Contact Information**

Data Protection Officer

Unit 9
Richview Office Park
Clonskeagh Road
Clonskeagh
Dublin 14
Ireland
Email: dpo@fiserv.com

Local Privacy Officers

Email: dpo@fiserv.com

Contact information for Fiserv's offices can be found here
FDR LIMITED, LLC

FDR LIMITED, LLC
Unit 9
Richview Office Park
Clonskeagh Road
Clonskeagh
Dublin 14
Ireland

General Counsel's Office

Global Privacy Office

Email: dpo@fiserv.com
Security Hotline: +1 800-368-1000

Annex A – Record of Processing

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

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

Schedule 2 – Processor Activities

Introduction

The tables below endeavour to give an oversight of the key purposes of processing and the data transfers that these BCRs are designed to cover, and the principal countries outside of the EEA that receive the data.

The processing and transfers undertaken by Fiserv in relation to the Data Subjects set out below includes processing activity undertaken when acting as a processor.

There are further descriptions of Business Purpose, Purposes of Processing, Categories of Data and Data Subjects below this table.

Business Purpose	Purposes for Processing	Categories of Data	Data Subjects	Countries of transfer
Merchant Acquiring and Transaction Processing Services	Technology infrastructure and support	Identification; Special Category; Financial; Commercial; Location; Anonymised/Aggregated; Inferences; Usage	Customer; Merchant	United States; India
	Transaction processing	Identification; Financial; Commercial; Location; Anonymised/Aggregated		
	Customer services	Identification; Special Category; Financial; Commercial; Location; Anonymised/Aggregated		
	Fraud prevention services	Identification, Financial, Location, Commercial; Anonymized/ Aggregated, Inferences		United States
	Support of Data Subject Rights Requests	Identification, Financial, Location, Special Category		
	Risk management purposes			
Clover Services (Marketplace Merchant Solutions Limited, trading as Clover)	Provision of business management services	Identification; Special Category; Financial; Commercial; Location; Anonymised/Aggregated; Inferences, Usage; Employment	Customer; Merchant	United States; India
	Customer services	Identification; Special Category; Financial; Commercial; Location; Anonymised/Aggregated		
	Support of Data Subject Rights Requests	Identification, Financial, Location, Special Category, Employment		
	Risk management purposes	Identification, Financial, Location, Special Category		
	Technology infrastructure and support	Identification; Special Category; Financial; Commercial; Location; Anonymised/Aggregated Inferences, Usage		

Issuing and Acquiring for Financial Institutions	Technology infrastructure and support	Identification; Special Category; Financial; Commercial; Location; Anonymised/Aggregated Inferences, Usage	Customer; Merchant	United States; India
	Transaction processing	Identification; Financial; Commercial; Location; Anonymised/Aggregated		
	Customer services	Identification; Special Category; Financial; Commercial; Location; Anonymised/Aggregated		
	Fraud prevention services	Identification, Financial, Location, Commercial; Anonymized/ Aggregated, Inferences		
	Support of Data Subject Rights Requests	Identification, Financial, Location, Special Category		United States; India
	Risk management purposes	Identification; Financial; Commercial; Location; Anonymised/Aggregated		
Human Resource	Where Fiserv entities outside the UK / EEA host personal data used for the purposes listed below, and carry out processing in support of these activities on behalf of Fiserv entities in the EEA: Health and Safety, Payroll, Personnel Benefits, Personnel management, Training, Internal Surveys, Recruitment, Travel and expenses reimbursement	Identification, Special Category, Location, Financial, Inferences, Usage, Employment, Anonymized/ Aggregated	Personnel;	India; United States
	Support of Data Subject Rights Requests			
	Monitoring Fiserv Systems	Identification, Location, Usage		
	Supplying Equipment	Identification, Location, Special Category		
Technical Support	Technology infrastructure and support	Identification; Special Category; Financial; Commercial; Location; Anonymised/Aggregated Inferences, Usage	Customer; Merchant; Personnel;	United States; India
	Database management	Identification; Financial; Location; Anonymised/ Aggregated		

	Encryption	Identification, Financial, Location, Commercial		
	Customer services	Identification; Financial; Commercial; Location; Anonymised/Aggregated		
Risk Assurance, Compliance, Legal and Audit	Where Fiserv entities outside the UK / EEA host personal data used for the purposes listed below, and carry out processing in support of these activities on behalf of Fiserv entities in the EEA:			
	Risk management purposes	Identification, Financial, Location, Employment, Commercial, Usage	Customer; Merchant	United States
	Regulatory requests	Identification, Special Category, Financial, Location, Employment, Commercial, Usage	Customer; Merchant; Personnel	
	Physical Security	Identification, Location, Employment, Inferences, Usage	Customer; Merchant; Personnel Supplier; Visitor	
Analytics	Database management	Identification; Financial; Location; Anonymised/ Aggregated	Customer; Merchant	United States; India
	Transaction analytics	Identification; Financial; Commercial; Location; Anonymised/Aggregated		
	Customer services	Identification; Special Category; Financial; Commercial; Location; Anonymised/Aggregated		
	Training	Identification, Location, Employment	Personnel	United States
	Internal surveys			
Vendor Management	Risk management purposes	Identification, Location, Financial	Supplier	United States

Descriptions of Business Purposes, Purposes of Processing, Categories of Data and Data Subjects

These descriptions are non-exhaustive and indicative only, and not all data points are used for every purpose / data subject.

Business Purposes	Descriptions
Analytics	Refining data to support business decisions and help our customers understand trends in their businesses
Clover Services (Marketplace Merchant Solutions Limited, trading as Clover)	Facilitating card transaction from merchants to card schemes (e.g., Mastercard/Visa) where Fiserv is a controller in respect of the service(s): including providing the platform, technical support, hardware, etc. in order to process the transaction and providing a business management platform to support merchants and consumers.
Human Resources	Supporting other Fiserv entities management of Personnel both employed directly and indirectly within Fiserv
Issuing and Acquiring for Financial Institutions	Facilitating card transactions and providing acquiring as a service on behalf of issuing banks and other financial institutions
Merchant Acquiring and Transaction Processing Services	Facilitating card transaction from merchants to card schemes (e.g., Mastercard/Visa), both where Fiserv is a controller or a processor in respect of the services: including providing the platform, technical support, hardware, etc. in order to process the transaction
Risk Assurance, Compliance, Legal and Audit	Supporting Customers and Fiserv entities to comply with local rules and regulations which may include anti money laundering, fraud, privacy, competition, regulatory or legal investigations, litigation and contract management. Fiserv will also support client audits which include reviewing processes to ensure all departments are following documenting policies, procedures, and controls
Technical Support	Providing technical support on application, hardware, network and database management
Vendor Procurement / Management	Supporting other Fiserv entities for risk management purposes of third-party vendors.

Purposes for Processing	Descriptions
Customer Services	Providing various customer support functions including call centre services, correspondence, email and service messages and administration of accounts
Database management	Support and set up of database including querying of faults, connections to database and access management
Encryption	Providing encryption, pseudonymization and anonymization on personal data
Fraud prevention services	Using various tools and methods, along with any instructions provided by customers (both internal and external) to mitigate potential fraud on behalf of a controller in the EEA
Health and Safety	Supporting reasonable adjustment for sickness/ disabilities, ensuring a safe workplace and in emergencies where the health or safety of a person is endangered (e.g., Pandemic, fire, etc.)
Internal surveys	Collecting views/opinions and information to help Fiserv entities understand Personnel and to ensure diversity and engagement into the business
Payroll	Determining compensation payable to Personnel
Personnel benefits	Healthcare, Insurance, Time Away (including parental leave), Retirement, Learning & Development, Financial Benefits, Discounts & Savings and Other Benefits
Personnel management	Performance evaluation, career development, disciplinary/grievances and talent management

Physical Security	Ensuring protection of individuals and Fiserv facilities by maintaining access management, monitoring CCTV etc.
Recruitment	Collection and review of application resumes, interview and background checks
Regulatory requests	On behalf of Fiserv entities to support response to a lawful request from a court or government agency or to otherwise comply with applicable law or compulsory process
Risk management purposes	On behalf of Fiserv entities to support fraud prevention, anti-money laundering, anti-terrorism financing, sanctions monitoring or other similar purposes on behalf of a controller in the EEA
Provision of business management services	Provision of business management services to merchants and transferring data to third party apps used by merchants
Support of Data Subject Rights Requests	Per Customer instruction supporting actions required to fulfil data subject rights requests, including but not exclusive of data deletion, access, correction on behalf of a controller in the EEA
Technology infrastructure and support	Support and hosting of application, network, hardware, database or other solution that underpins the business
Training	On behalf of Customers and other Fiserv entities, provision and performance monitoring of training of training taken
Transaction Analytics	Refining transaction data to usable metrics and KPIs to help our customers understand trends in their businesses.
Transaction processing	To fulfil a transaction initiated by a Data Subject or for Merchant Services, hosting and carrying out processing on personal data hosted by a merchant as part of the business application services.
Travel and expenses reimbursement	Reimbursement of business costs to Personnel on behalf of Fiserv entities

Categories of Data	Descriptions
Identification	Real name, alias, postal address, unique personal identifier, customer number, email address, account name, other similar identifiers, phone number, employee ID, job title, login details, passport, visa, work permit, photos, date of birth, nationality
Special Category	Includes race or ethnic origin, political opinions, religious or philosophical beliefs, 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.
Financial	Bank account number, debit or credit card numbers, credit history and other financial information.
Commercial	Includes account information, customer correspondence (e.g., support or requesting information), marketing preferences, transactions, spending and spending patterns, merchant data (for merchants who are individuals), products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
Location	Addresses both personal and business, along with geolocation, location transactions occurred.
Anonymized/Aggregated	Personal data obtained from Data Subject which has been aggregated to a point where the individual is no longer able to be identified within the dataset

Employment	Information relating to a person's current, past, or prospective employment or professional experience (e.g., job history, performance evaluations), and educational background, qualifications, references, training data, grievances, salary data, benefits information, absence data, background check, survey responses, time and attendance, equal opportunities, monitoring information, dependent and beneficiary information
Inferences	Inferences drawn from any personal data collected to create a profile about a Data Subject reflecting the Data Subject's spending patterns, preferences, characteristics, predispositions, behaviour and attitudes
Usage	Details about technology used to access Fiserv systems e.g., IP address, login data, browser type, device location. Information about use of information and communications systems, interactions with Fiserv products and services, CCTV footage and other information obtained through electronic means such as electronic access records and badge data.

Data Subjects	Descriptions
Customer	Other Fiserv entities as well as Fiserv clients (and prospects) and their customers in connection with the provision of services. This includes personnel employed by the Fiserv entities, our clients and their customers (or the customers themselves to the extent they are individuals) (cardholders).
Merchant	Merchants accepting payments. This includes personnel employed by Merchants; proprietors when the Merchant is an individual and customers of Merchants (cardholders)
Personnel	Includes Fiserv employees, contingent workers, consultants, prospective and former personnel and the personnel's dependents and beneficiaries
Suppliers	Person or personnel working for an organization which provides goods or services to Fiserv
Consumers	Individuals who interact directly with Fiserv or Fiserv products.

Schedule 3 - List of Signatories

A full list of all signatories can be found at: www.fiserv.com/en/legal/privacy.html.

Schedule 4 – Form of Declaration of Accession

This Declaration of Accession is made effective as of [DATE] (the "**Accession Date**") by [NEW FISERV ENTITY] (the "**New Member**") with regard to Fiserv's EU Processor Binding Corporate Rules Membership Agreement dated [DATE], including any amendments thereto, and made between certain members of the Fiserv Group (the "**Agreement**").

1.   The New Member hereby confirms it has been provided with a full copy of the Agreement including its Schedules, all as amended from time to time.

2.   The New Member hereby agrees to be party to the Agreement, be bound by its provisions and comply with them as a Member with effect as from the Accession Date, subject to this Declaration of Accession being accepted by Fiserv Inc pursuant to Clause 19 of the Agreement.

3.   In case of any dispute out of or in connection with the Agreement (including this Declaration of Accession), the New Member in any case hereby agrees to be bound by Clause 10 of the Agreement for the resolution of such disputes.

Date:_____

By and on behalf of [•]:

Name:

Position:

The accession of the New Member to the Agreement is hereby accepted by Fiserv Inc, causing the New Member to be a Member to the Agreement as of the Accession Date:

Date:_____

By and on behalf of Fiserv Inc:

Name:

Position: