Binding Intra-Group

Processor EU BCR Membership Agreement (the **Agreement)**

Dated **(Commencement Date)**

21/07/2025

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 and 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 this Agreement.

B The main clauses of this Agreement together with the Schedules, Annexes and any Declaration of Accession and all other applicable Fiserv policies, standards and procedures relating to Fiserv privacy and data protection, data transfers and security practices (all of which are binding and listed in Annex C of Schedule 1) 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 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 To ensure that Personal Data is accorded adequate protection in accordance with Privacy 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 legislation, regulations, codes of practice, guidance and other requirements of any relevant government, governmental or regulatory agency, or other relevant body applicable in the country where the Member is operating.

BCRs means this Agreement together with the Schedules, Annexes and any Declaration of Accession and all other applicable Fiserv policies, standards and procedures relating to Fiserv privacy and data protection, data transfers and security practices (all of which are binding and listed in Annex C of Schedule 1), as amended or varied from time to time.

Business Day means a day other than a Saturday or Sunday or public holiday (as defined in the Companies Act) in Ireland on which banks are generally open for business in Dublin.

Change of Control Event shall be deemed to occur if any person (or persons connected with each other or persons acting in concert with each other) obtains control over, or increases control beyond, shares which in aggregate confer more than 50 per cent. or more of the voting rights normally exercisable at general meetings of the shareholders of the Parent Company or an Affiliate. For this purpose, "control" means the ability to direct the affairs of another whether by way of contract, ownership of shares or otherwise howsoever.

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 Subjects has the meaning set out in Schedule 1.

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

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

Fiserv Group means the Parent Company and each Affiliate.

Lead EU BCR Member means the Irish branch of FDR Limited, LLC, 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 a registered address at 10 Hanover Quay, Dublin 2 and with Company Number 909114 (formerly FDR Limited). This Member accepts responsibility for and agrees to take the necessary actions to remedy the acts of other Members outside of the EEA, and to pay compensation for any material or non-material damages resulting from a breach of the BCRs by such Members.

Member has the meaning set out in Clause 2.2.

Member Commencement Date means:

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

(b) in respect of 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 3.

Member Term means, in respect of 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 of that Member.

Personal Data has the meaning set out in Schedule 1.

Privacy Laws means 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, reenacts or consolidates any of them, and all other Applicable Laws relating to the processing of Personal Data and privacy that may exist in the EEA or any of its member states.

processing shall have the meaning set out in Schedule 1 and **process** and **processes** shall be construed accordingly.

Competent Supervisory Authority means any data protection supervisory authority in the EEA competent for the relevant Fiserv Member.

Processor Member has the meaning set out in Clause 3.4.1.

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

1.2 Interpretation

In this Agreement:

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

(b) references to this Agreement mean this Binding Intra-Group Processor EU BCR Membership Agreement (including its Schedules and Annexes) and any reference to this Agreement (or to any other agreement, deed or document referred to in this Agreement) is a reference to this Agreement or such other agreement, deed or document as varied or novated from time to time in accordance with its terms (in each case, other than in breach of the provisions of this Agreement);

(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 7 of the Companies Act 2014 and every enactment which is to be read together with that Act; 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 when a wider interpretation is possible. When this Agreement defines a word or expression, related words and expressions have a consistent meaning.

2 Undertakings to be Bound by BCRs and the 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 and 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 referred to in Schedule 2 which has:

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

(b) executed a Declaration of Accession after the Commencement Date 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 of 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 of 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 cooperate with each other Member during their respective Member Terms:

(a) to the extent required to enable each other Member 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 the Chief Data Ethics and Privacy Officer or their 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, when 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 the Lead EU BCR Member to fulfil and/or perform its obligations under the BCRs; and

(b) procure that the Lead EU BCR Member is fully indemnified by the relevant Indemnifying Member in accordance with Clause 7 of this Agreement.

3.4 Security of processing when 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 clearly documents 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 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 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 Applicable Laws for the Processor Member, provided that the Processor Member first informs the Controller Member in written form of that legal requirement before processing (unless the Applicable Laws prohibit this on important grounds of public interest);

(b) **Staff:** ensure the staff it has authorised to process 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 Personal Data (a **Sub-Processor**), except as permitted by the BCRs;

(ii) when 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 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 a **Sub-Processor Notice**) – in each case providing information regarding the Sub-Processor (in particular, its name, address and a contact person), and a description and location of the processing;

(iii) if the Controller Member has reasonable concerns that the processing of 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 written agreements with all Sub-Processors that contain obligations on such third parties that are equivalent to those set out in this Agreement – in particular, the engagement of a Sub-Processor shall be subject to the Sub-Processor providing sufficient guarantees to implement appropriate technical and organisational measures such that the processing meets the requirements of the GDPR and 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 through appropriate technical and organisational measures (insofar as this is possible) with the fulfillment of the Controller Member's obligation to respond to requests from Data Subjects to exercise their rights set out in Chapter III of the GDPR (Rights of the data subject), including their access requests;

(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 Applicable Laws for the Processor Member require the 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 the Processor Member's obligations under this Agreement; and

(ii) permit the Parent Company, the Controller Member, or a third-party auditor acting under the Controller 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 or other Privacy Laws and the Processor Member may refuse to perform such instruction until the Controller Member has amended the instruction in a manner which, in the Processor Member's opinion, would not breach the GDPR or other Privacy Laws.

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 of 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 BCR 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) through which the Members receive Personal Data that is subject to the UK GDPR or other Privacy Laws apart from the GDPR.

4.2 The Parent Company may terminate all or any part of this Agreement in respect of any or all Members (including the Parent Company) upon giving 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 of all or any Members (excluding the Parent Company) immediately upon giving 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 of all or any Members, as appropriate:

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

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

(c) upon the Parent Company ceasing to do business.

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

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

5 Consequences of Termination

5.1 Upon 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 the Parent Company's request, 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) when 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) that are needed to effect the smooth transition of Personal Data as set out in Clause 5.1(b) and, in any event, fully cooperate 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 or processes 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 the 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 Applicable Laws, and shall not affect any accrued rights or liabilities of any Member, nor the coming into force or continuance in force of any provision in this Agreement which is expressly or impliedly 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 and in respect of an Exiting Member:

(a) this Agreement shall remain in full force and effect in respect of 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 remain fully liable to each other Member for fulfilling its obligations under this Agreement and (if they apply) under Privacy Laws.

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 fully and promptly indemnify, keep indemnified and hold harmless the Lead EU BCR Member (apart from when the Lead EU BCR Member is the Indemnifying Member), and any other Member, including the Parent Company, (together, the **Indemnified Members**) on demand in respect of all liabilities, damages, costs, losses, claims, demands and proceedings whatsoever and howsoever arising, whether in contract, tort, breach of statutory duty or Applicable Law or otherwise, directly or indirectly, out of, in the course of, or in connection with any alleged or actual claims advanced against them by a Data Subject arising from a breach by the Indemnifying Member of this Agreement, the BCRs or any Privacy Law] relating to its processing of Personal Data.

7.2 The Indemnifying Member shall promptly notify the Lead EU BCR Member, 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, when the Parent Company does not elect to assume such conduct or settlement, and if requested by the Lead EU BCR Member or the relevant Indemnified Party against whom the claim or alleged claim has been advanced or is to be advanced, the Indemnifying Member 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 Member agrees that, in relation to any claim or alleged claim brought that is covered by this Clause 7, it shall fully submit to the direction of the Parent Company and fully cooperate 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 variations or 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 Chief Data Ethics and Privacy 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 of 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 of 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 purposes 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 upon giving 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’s 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 non-exclusive jurisdiction of the courts of Ireland in relation to any claim or matter arising out of or in connection with this Agreement. Data Subjects may bring a claim against any Member in connection with this Agreement in any country with jurisdiction to hear the claim.

18 Rights of Third Parties

This Agreement is not intended to, and does not, give any person who is not a party to this Agreement any rights to enforce any provisions contained in it, except any provision of this Agreement (and, in particular, section 9 of the BCRs) that expressly provides for enforcement by a third party (which shall include Data Subjects). These provisions shall be enforceable in accordance with their express terms.

19 Addition of New Members

19.1 Subject to the prior agreement of the Parent Company, which will only be provided when 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 3) 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 and complies with the BCRs.

19.2 The other Members 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 new Member, in respect of any Personal Data which they transfer to or receive from the new Member.

19.3 Schedule 2 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 EU Processor Data Protection Standards (the "EU BCRs")

PROCESSOR DATA PROTECTION STANDARDS

Effective as of _____

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, the Isle of Man, Japan, Jersey, the Faroe Islands, Guernsey, New Zealand, Israel, South Korea, Uruguay and the United Kingdom (section 3.5).

Applicable Laws means all legislation, regulations, codes of practice, guidance and other requirements of any relevant government, governmental or regulatory agency, or other relevant body applicable in the country where the Fiserv entity is operating.

Competent Supervisory Authority means, as applicable: (i) any supervisory authority in a Relevant Country competent for the Fiserv exporter(s) of the specific transfer, namely (a) the lead supervisory authority (which, in this case, is the Irish Data Protection Commission), or (b) any other supervisory authority in a Relevant Country that is "concerned" by the processing of Personal Data because a Fiserv entity is established in the country or territory where that supervisory authority is established, 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, or it has received a complaint from a Data Subject relating to the processing of Personal Data by a Fiserv entity, or (ii) when Personal Data is processed by a Fiserv Importer on behalf of a Data Controller, the Competent Supervisory Authority for the Data Controller.

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

Criminal Offence Data means Personal Data relating to criminal convictions and offences (section 4.3).

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 (section 1.2).

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

Fiserv, Fiserv entity, we or our means Fiserv, Inc. and its subsidiaries which have signed an intra-group agreement committing them to these Processor Data Protection Standards. A list of the current signatories can be found on the Fiserv Privacy Site (see sections 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) (section 7.6).

Fiserv Privacy Site means the privacy landing page on Fiserv's website, which is accessible at: www.fiserv.com/en/legal/privacy.html.

Lead EU BCR Member means the Irish branch of FDR Limited, LLC, 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 a registered address at 10 Hanover Quay, Dublin 2 and with Company Number 909114 (formerly FDR Limited). This establishment accepts responsibility for and agrees to take the necessary actions to remedy the acts of other Fiserv entities outside of the EEA and

to pay compensation for any material or non-material damages resulting from a breach of these Processor Data Protection Standards by such Fiserv entities (see sections 1.1, 2.2 and 3.1).

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

Personal Data Breach means a security incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to Personal Data (section 11.18).

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 (section 2.3).

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

Privacy Laws means 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, reenacts or consolidates any of them and all other Applicable Laws relating to the processing of Personal Data and privacy that may exist in the EEA or any of its member states (section 7.1).

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 and is available at www.fiserv.com/privacy (section 11.2).

Relevant Country means a member state of the European Union and/or the European Economic Area (section 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 (section 4.3).

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

Transfers means transfers of Personal Data (where the Privacy Laws of a Relevant Country apply (both as defined and provided for in section 3.1)) by a Fiserv entity or External Sub-Processor of that entity to another Fiserv entity acting as processor or External Sub-Processor of that entity located outside the EEA which is in a third country (other than an Adequate Third Country) (including onward Transfers to other Fiserv entities) (section 3.5).

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 to Personal Data) 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 Article 23(1) GDPR, are not in contradiction with these Processor Data Protection Standards (section 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**", "**Fiserv entity**", "**we**" or "**our**", as further defined in section 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, and with virtually anyone in the world.

1.2 These Processor Data Protection Standards (including the attached Annexes) 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 Privacy Laws of a Relevant Country apply (both as defined and provided for in section 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 than 93 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 the Lead EU BCR Member 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, as described more fully in section 7.2 of these Processor Data Protection Standards. Fiserv entities processing 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 Privacy Laws.

2.3 Fiserv has business relationships with financial institutions, corporations, credit card issuers, credit unions, acquirers, retail merchants, healthcare 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 EU 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' rights 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 Privacy Laws of a Relevant Country apply to Fiserv's processing of Personal Data, or where the Privacy Laws of a Relevant Country applied to such processing prior to the Personal Data being transferred between Fiserv entities in accordance with these Processor Data Protection Standards, or where the Services Agreement otherwise provided that these Processor Data Protection Standards should apply, and all references in these Processor 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 1.2 above) from its clients or other Fiserv entities 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 its 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 on 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"** or "**EU BCRs**").

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 transfers of Personal Data (where the Privacy Laws of a Relevant Country apply (both as defined and provided for in section 3.1)) by a Fiserv entity or External Sub-Processor of that entity to another Fiserv entity acting as processor or External Sub-Processor of that entity located outside the EEA which is in a third country (other than an Adequate Third Country) (including onward Transfers to other Fiserv entities) (a "**Transfer**").

3.6 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, the Isle of Man, Japan, Jersey, the Faroe Islands, Guernsey, New Zealand, Israel, South Korea, Uruguay and the United Kingdom (**"Adequate Third Country"**).

3.7 Data Subjects and Data Controllers alleging breach of these Processor Data Protection Standards shall only be entitled to enforce them pursuant to section 9 of these Processor Data Protection Standards.

3.8 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 described below in section 7.4) to offer the highest protection will govern.

4 Categories of Data Subjects

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 Subjects:

- other Fiserv entities as well as our 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 – for example: 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 (for example: cardholders) ("**Merchants**");
- Fiserv employees, contingent workers, consultants, prospective and former personnel and the personnel's dependents and beneficiaries ("**Personnel**");
- individuals visiting Fiserv premises, including Suppliers, auditors, prospective personnel etc. ("**Visitors**"); and
- other persons or personnel working for an organisation that provides goods or services to Fiserv ("**Suppliers**").

4.2 Fiserv processes and transfers Criminal Offence Data to its processors relating to Personnel and Suppliers.

4.3 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. "**Criminal Offence Data**" means Personal Data relating to criminal convictions and offences.

5 Sources of Personal Data, Purposes of Processing and Transfers, and Lawful Basis

5.1 When instructed by the relevant Data Controller, Fiserv collects Personal Data from several sources:

- **From 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) and 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 or other participants in a transaction chain 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 public or private databases they have access to), background checking providers 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 Subjects set out above includes processing for the business purposes as determined by the applicable Data Controller (as defined in more detail in Annex B, together with a breakdown of the purposes of Processing under these Processor Data Protection Standards).

5.3 The applicable Data Controller will determine the appropriate lawful basis for the processing of Personal Data by Fiserv entities as processors.

6 Nature of Data Transferred

6.1 Fiserv processes and transfers a broad range of Personal Data between Fiserv entities, External Sub-Processors of those entities, and 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 processed or transferred include:

- **Employment Data** – this includes information relating to a person's current, past, or prospective employment or professional experience (e.g. job history and performance evaluations), educational background, qualifications, references, training data, grievances, salary data, benefits information, absence data, background checks, survey responses, time and attendance, equal opportunities, monitoring information, as well as 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 Annex B**; and
- **Anonymised/Aggregated Data** – Personal Data obtained from Data Subjects which has been aggregated to a point where the individual is no longer able to be identified within the dataset.

7 Privacy Laws and Supervising Authorities

7.1 All Fiserv entities will handle Personal Data in accordance with these Processor Data Protection Standards and 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, reenacts or consolidates any of them, and all other Applicable Laws relating to the processing of Personal Data and privacy that may exist in the EEA or any of its members (together, the "**Privacy Laws**"). Additionally, these 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. The Lead EU BCR Member will be responsible for and will take any action necessary to remedy any breach by any Fiserv Importer or External Sub-Processor of the applicable Fiserv Importer of the rights guaranteed in these Processor Data Protection Standards, as provided by section 9. This will include any sanction imposed or other remedy available under applicable Privacy Laws, including compensation. The Lead EU BCR Member may discharge itself from this responsibility if it is able to show that the Fiserv Importer and/or the External Sub-Processor of that entity which is alleged to be in breach is not liable for the breach or that no breach took place.

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 cooperate, as reasonably required, with any Competent Supervisory Authority. "**Competent Supervisory Authority**" means, as applicable: (i) any supervisory authority in a Relevant Country competent for the Fiserv exporter(s) of the specific transfer, namely (a) the lead supervisory authority (which, in this case, is the Irish Data Protection Commission), or (b) any other supervisory authority in a Relevant Country is "concerned" by the processing of Personal Data because a Fiserv entity is established in the country or territory where that supervisory authority is established, 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, or it has received a complaint from a Data Subject relating to the processing of Personal Data by a Fiserv entity, or (ii) Personal Data are processed by a Fiserv Importer on behalf of a Data Controller, the supervisory authority for the Data Controller. Any questions about Fiserv's compliance with Privacy Laws 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 Competent Supervisory Authority, when applicable. Each Competent Supervisory Authority is authorised to audit and inspect any Fiserv entity, (including, when necessary, on-site), and advise on all matters related to these Processor Data Protection Standards. Fiserv entities must take into account any advice and consider any communication or recommendation from the Competent Supervisory Authority in relation to the interpretation and application of these Processor Data Protection Standards and comply with any formal decisions or notices issued by them in that regard, unless it conflicts with other Applicable Laws. Any disputes relating to a Competent Supervisory Authority's exercise of its powers or its supervision of compliance with these Processor Data Protection Standards will be resolved by the member state of the EU or EEA that Competent Supervisory Authority belongs to, in accordance with that member state's procedural laws. Fiserv agrees to submit itself to the jurisdiction of these courts.

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 or decisions of the Competent 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); the Lead EU BCR Member; the Local Privacy Officer and/or the Data Protection Officer, who will (in consultation with the General Counsel's Office, when necessary) responsibly decide what action to take (which may include notification to the Competent Supervisory Authority, when 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 if 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 Article 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 sets 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) the type of entities involved in the processing, (c) the economic sectors in which the transfers or sets of transfers occur, (d) the categories and formats of the Personal Data, (e) the locations of the processing (including storage), and (f) the transmission channels used; (ii) the laws and practices of the third country relevant in 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 (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 such experiences are supported by other relevant objective elements such as publicly-available or otherwise accessible and 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 (a) 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 (b) the laws and practices in the third country applicable to the processing of the Personal Data 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 the Lead EU BCR Member 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 the Lead EU BCR Member 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 a 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 section, that any proposed transfers should be suspended or prohibited as a result, the applicable Fiserv entities will be notified (and these Fiserv entities shall, in turn, 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 (upon 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 and 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 Officer if it has reason to believe that it is or has become subject to 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 the Lead EU BCR Member.

7.12 Upon verification of such notification pursuant to section 7.11, the Fiserv exporting entity along with the Lead EU BCR Member and the Local Privacy Officer and/or Data Protection Officer shall promptly identify appropriate supplementary measures to be adopted to address the situation, in consultation with the affected Data Controller (if appropriate). 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 (as well as all transfers for which the same assessment and reasoning would lead to a similar result) if (i) no appropriate supplementary measures can be ensured, (ii) if instructed by the Competent Supervisory Authority to do so, or (iii) when the Fiserv Importer is in breach of the Processor Data Protection Standards or unable to comply with them, 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 (i) these Processor Data Protection Standards cannot be complied with and compliance is not restored within 1 month of suspension, (ii) the Fiserv Importer is in substantial persistent breach of these Processor Data Protection Standards, or (iii) the Fiserv Importer fails to comply with a binding decision of a competent country or a Competent Supervisory Authority regarding its obligations under these Processor Data Protection Standards. If the transfer ends, the Fiserv Importer shall (at the

Fiserv exporting entity's choice) either securely return or destroy any Personal Data (or copies thereof) in its possession or control. If Personal Data is destroyed, the Fiserv Importer shall also confirm and certify the deletion of the Personal Data to the Fiserv exporting entity. Until the Personal Data is deleted or returned, the Fiserv Importer shall continue to ensure compliance with these Processor Data Protection Standards. If Applicable Laws prohibit the return or deletion of the transferred Personal Data, the Fiserv Importer warrants that it will continue to ensure compliance with these Processor Data Protection Standards and will only process the transferred Personal Data to the extent and for as long as required under those Applicable Laws. The Lead EU BCR Member and the Local Privacy Officer and/or Data Protection Officer 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 Transfer Impact Assessment and its results, and the decisions taken in accordance with such transfers.

Obligations in Cases 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 the Lead EU BCR Member and 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 the Lead EU BCR Member, the Local Privacy Officer and/or Data Protection Officer, and 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, details about the requests received by the Fiserv Importer (in particular, the number of requests, the types of data requested, the requesting authorities, whether requests have been challenged, and the outcomes of such challenges).

7.17 The Fiserv Importer agrees to preserve the information pursuant to sections 7.14 - 7.16 for the duration of these Processor Data Protection Standards and make it available to the Competent Supervisory Authority upon 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 the laws 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 the Lead EU BCR Member, the Local Privacy Officer and/or Data Protection Officer, and 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 the 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 reasonable 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 of Personal Data 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. Any Fiserv Importer which ceases to be bound by these Processor Data Protection Standards may keep, return, or delete the Personal Data received under these Processor Data Protection Standards at the request of the Data Controller. If the Fiserv exporter and Fiserv Importer agree that the Personal Data may be kept by the Fiserv Importer, protection shall be maintained in accordance with Chapter V GDPR. 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 Competent 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 Competent Supervisory Authority annually (via the lead supervisory authority). and any Data Controllers with whom it has a valid Services Agreement in accordance with the terms of that Services Agreement, together with a brief explanation of the reasons for the change. The Competent Supervisory Authorities will also be notified annually (even when no changes have been made) (via the lead supervisory authority). Where a change would possibly be detrimental to the level of protection offered by these Processor Data Protection Standards, or significantly affect them, Fiserv (via the Lead EU BCR Member) will communicate the update in advance to the relevant Competent Supervisory Authorities (via the lead supervisory authority). Upon approval of the Data Protection Officer, Fiserv will clearly indicate the date of the latest revision, communicate the Processor Data Protection Standards to all Fiserv entities and post the revision on Fiserv's public website without undue delay. 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.

9 Complaints Handling Procedures, Third-Party Rights and Enforcement

Complaints Handling Procedures

9.1 Data Subjects and/or Data Controllers can raise any complaints, claims or requests relating to these Processor Data Protection Standards through the Fiserv's Data Privacy Hotline (+1800-368-1000), which manages the complaints handling process or by contacting the Data Protection Officer or Local Privacy Officer (by email at dpo@fiserv.com, or by post at Janus House, Endeavour Drive, Basildon, Essex, SS14 3WF, UK). In addition, under Fiserv's Employee 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 Data Privacy Hotline. Fiserv shall inform the Data Controller of any complaint, claim or request made by a Data Subject as soon as reasonably practicable but shall not be obliged to handle or otherwise deal with such complaint, claim or request further, unless it has been agreed otherwise with the Data Controller in the Services Agreement, or unless the Data Controller has factually disappeared, ceased to exist or become insolvent and no successor has assumed the obligations of the Data Controller. Fiserv shall cooperate and assist the Data Controller in meeting its obligations under applicable Privacy Laws (as agreed between the parties in the Services Agreement).

9.2 In all cases where Fiserv handles complaints, a decision on whether any complaint made is justified or rejected will be communicated to the Data Subject or the Data Controller by the Data Privacy Hotline, the Data Protection Officer or the Local Privacy Officer (as appropriate) without undue delay and, in any event, within one 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 further months, in which case, Fiserv shall inform the Data Subject or Data Controller accordingly).

9.3 If the complaint is not resolved to the Data Subject or Data Controller's satisfaction, or if the Data Subject or Data Controller prefers (in the first instance) to resolve the complaint without going to the Data Protection Officer or applicable Local Privacy Officer, they may directly:

9.3.1 raise the issue of breach before a Competent Supervisory Authority, and Fiserv shall cooperate as reasonably required by that Competent Supervisory Authority; or

9.3.2 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 their habitual residence (at the Data Subject's option.

Third-Party Rights and Enforcement of These Processor Data Protection Standards

9.4 In addition to the right to complain, Fiserv recognises that the Privacy Laws also contain remedies and the right to obtain redress and (where appropriate) compensation for Data Subjects against a Fiserv entity when they fail to process a Data Subject's Personal Data in accordance with such Privacy Laws, including when a Data Subject may be represented by a not for profit body, organisation or association under applicable Privacy Laws, and that nothing in these Processor Data Protection Standards shall exclude or restrict such remedies, redress or rights to complain.

Rights That are Directly Enforceable Against a Fiserv Processor

9.5 Data Subjects can directly enforce their rights as a third-party beneficiary against Fiserv in relation to a breach by a Fiserv entity acting as a processor of the following elements of the Processor Data Protection Standards:

9.5.1 the duty to respect the instructions from the Data Controller regarding the data processing (including for data transfers to third countries) (sections 3.1.1 and 11.11);

9.5.2 the duty to implement appropriate technical and organizational security measures (section 11.16);

9.5.3 the duty to notify any Personal Data Breach to the Data Controller (section 11.18);

9.5.4 the duty to respect the conditions when engaging a sub-processor (either within or outside the Fiserv group) (sections 11.11 and 11.12);

9.5.5 the duty to cooperate with and assist the Data Controller in complying with and demonstrating compliance with the law (for instance, in answering requests from Data Subjects in relation to their rights) (sections 11.21 and 11.22);

9.5.6 the duty to provide easy access to these Processor Data Protection Standards and (in particular) easy access to the information about third-party beneficiary rights for the Data Subjects that benefit from them (section 10.1);

9.5.7 the right to complain through the Fiserv group's internal complaints mechanism (sections 9.1 - 9.3);

9.5.8 Fiserv's obligations regarding co-operation with the supervisory authority competent for the Data Controller relating to compliance obligations covered by this third party beneficiary clause (section 7.4);

9.5.9 the Data Subject's rights to judicial remedies, redress and compensation in the courts and to lodge a complaint with the Competent Supervisory Authorities, and the Lead EU BCR Member's duty to accept liability for paying compensation and to remedy any breaches of these Processor Data Protection Standards (sections 9.3, 9. 4 and 9.7);

9.5.10 Fiserv's obligations in case of Applicable Laws affecting compliance with these Processor Data Protection Standards and in respect of government access requests (sections 7.5-7.20);

9.5.11 any other provisions of applicable Privacy Laws which a Data Subject can enforce directly against a processor.

Rights which are Enforceable Against a Fiserv Processor When the Data Subject Cannot Bring a Claim Against the Data Controller

9.6 In addition, in the limited situations where: (i) the Data Controller has factually disappeared; (ii) the Data Controller has ceased to exist in law; or (iii) the Data Controller has become insolvent, unless any successor entity has assumed all legal obligations of the Data Controller by contract or by operation of law, Data Subjects shall have the right (upon request) to directly enforce against Fiserv the following elements of these Processor Data Protection Standards as third-party beneficiaries:

9.6.1 the duty to respect these Processor Data Protection Standards (section 11.25);

9.6.2 the creation of third-party beneficiary rights for Data Subjects (section 9)

9.6.3 the duty of the Lead EU BCR Member to accept liability for paying compensation and to remedy breaches of these Processor Data Protection Standards (, sections 9.7 and 9.8);

9.6.4 the right to be informed of the fact that the burden of proof lies with the Lead EU BCR Member and not with the Data Subject according to the terms of these Processor Data Protection Standards (, section 9.8);

9.6.5 the right to be provided with easy access to these Processor Data Protection Standards and, in particular, easy access to the information about third-party beneficiary rights for the Data Subject that benefits from them (section 10.1);

9.6.6 the right to complain through the Fiserv group's internal complaints mechanism (sections 9.1 - 9.3);

9.6.7 Fiserv's obligations regarding cooperation with the supervisory authority competent for the Data Controller relating to compliance obligations covered by this third party beneficiary clause (section 7.4);

9.6.8 the duty to cooperate with the Data Controller in meeting its obligations under applicable Privacy Laws (section 9);

9.6.9 Fiserv's obligations under section 11;

9.6.10 to be informed regarding Fiserv entities bound by these Processor Data Protection Standards (section 10.1); and

9.6.11 to be informed (where legally permitted) of when Applicable Laws prevent a Fiserv entity from complying with its obligations under these Processor Data Protection Standards.

9.7 As stated under section 2.2 of these Processor Data Protection Standards, the Lead EU BCR Member accepts liability for any breaches under section 9 5 or 9.6 of these Processor Data Protection Standards by a Fiserv Importer or External Sub-Processor (each a "**Breach**") as if it had arisen from its own act or omission.

9.8 If a Data Subject can demonstrate that they have suffered material or non-material damages and can establish facts which show that it is likely to have occurred because of the Breach, then it will be for the Lead EU BCR Member to prove that the Fiserv Importer or External Sub-Processor is not responsible for the Breach giving rise to the damages or that no Breach took place. Otherwise, the Lead EU BCR Member agrees to:

9.8.1 take necessary actions to remedy the Breach; and

9.8.2 compensate the Data Subject for any such damages resulting directly from the Breach,. The compensation which may be claimed by a Data Subject is limited to that which would be due under Article 82 of the GDPR.

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 (including those that have permanent or regular access to Personal Data, who are involved in the collection of Personal Data or in the development of tools used to process Personal Data) will comply with these Processor Data Protection Standards, and receive appropriate and up-to-date training on (and access to) these Processor Data Protection Standards and any relevant provisions of the Services Agreements. 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 Fiserv's 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 Privacy Laws.

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 its External Sub-Processors as may be reasonably required by the Data Controller to enable it to correctly inform its Data Subjects of this information and comply with its legal obligations in relation to this principle of "lawfulness, fairness and transparency". Fiserv's information notice containing the information it is required to give to Data Subjects under the 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 of 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 Controller's 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 section 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 Services Agreements 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). Fiserv's 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, When 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 is processed in relation to the amount of Personal Data collected, the extent of processing, the period of storage, and accessibility, and in order to assist with Data Controllers' obligations under Applicable Laws and any agreements with Data Controllers).

We Transfer Personal Data as a Processor Only for Limited Purposes ("Onward Transfers")

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

- all applicable legal requirements are met (including the conditions in Chapter V of the GDPR to ensure that the Personal Data is adequately protected);
- when 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;
- when the transfer is to an External Sub-Processor, the receiving External Sub-Processor entity has appropriate security measures in place; 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 Personal Data belonging to the Data Controller with the prior specific or general written consent of the Data Controller. The applicable Fiserv entity shall have appropriate agreements with its External Sub-Processors that: reflect the applicable provisions of these Processor Data Protection Standards and applicable Privacy Laws (in particular, those set out in Articles 28, 29, 32,45,

46, 47 or 49 of the GDPR); ensure that the External Sub-Processors 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 obligations;
- third parties, where required to protect the rights, property, or safety of Fiserv, Fiserv's clients and their customers, or others; and
- 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 Fiserv process a Data Subject's payments;
  - third-party suppliers engaged to host, manage, maintain and develop Fiserv's websites and IT systems; and
  - Fiserv's professional advisers, including its 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 Laws. When the processing of Personal Data is outsourced by Fiserv to third parties, 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 Data Subject.

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 consider emerging threats, as well as emerging technological safeguards and precautions. Fiserv imposes security measures appropriate to the risk represented by the processing and the nature of the Personal Data to be protected, with all due regard to the state of the art and cost measures for these security measures. Fiserv will ensure that any personnel who have access to Personal Data have appropriate obligations of confidentiality in their employment agreements with Fiserv.

11.17 Fiserv also enforces upon all Fiserv entities and their employees the importance of the provisions of the Services Agreements and (in particular) those measures relating to the Data

Controller's instructions with respect to the processing of Personal Data, the security of the Personal Data, and confidentiality.

11.18 If a security incident occurs that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to Personal Data ("**Personal Data Breach**") on a Fiserv system, Fiserv operates a response plan that is designed to assist Fiserv in complying with: Privacy Laws requiring notifications of Personal Data Breaches; guidelines produced by the relevant Competent Supervisory Authorities in relation to Personal Data Breaches, and Fiserv's duties under client contracts (including Services Agreements). This requires Fiserv to: (i) notify the Lead EU BCR Member and the Data Protection Officer of the Personal Data Breachwithout undue delay (who, in turn, will inform the Data Controller of the breach, in accordance with applicable Fiserv policies and its agreement with the Data Controller) unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of the Data Subjects, and (ii) keep records of Personal Data Breaches (the facts relating to the Personal Data Breach, its effects and the remedial actions taken), which will be made available to Competent Supervisory Authorities upon request. As appropriate or required, Fiserv will also notify law enforcement authorities, financial or other regulators and/or state agencies (including the Competent Supervisory Authorities).

11.19 Personal Data will not be transferred to a third country or territory which is not recognised as offering adequate protection for Personal Data, pursuant to applicable Privacy Laws, unless adequate safeguards are in place (as required by Chapter V of the GDPR) or a derogation applies (in line with Article 49 GDPR).

11.20 Special Categories of Personal Data and Criminal Offence 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 and Criminal Offence Data, when necessary. Special Categories of Personal Data and Criminal Offence Data will be disposed of under Fiserv's Global Cyber Security and Technology Management Policy, as well as the Data Classification and Handling Standard, its 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 from time to time. Fiserv requires that all Special Categories of Personal Data and Criminal Offence Data be transferred securely.

We Respect Data Subject Rights as Required by Applicable Privacy Laws

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

- The right to information.
- The right to access their Personal Data held by Fiserv;
- The right to correct their Personal Data if it is wrong (including notification obligations under Article 19 GDPR);
- The right to erase their (including notification obligations under Article 19 GDPR);
- The right to restrict how their Personal Data is being used (including notification obligations under Article 19 GDPR;
- The right to object to the processing of their Personal Data;
- The right to data portability;
- The right to automated decision making and profiling
- ; and
- The right to complain to the relevant Competent Supervisory Authorities.

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 will need 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 protection and privacy within their respective regions (including compliance with these Processor Data Protection Standards). The Data Protection Officer and Chief Data Ethics and Privacy Officer are responsible for the network of privacy officers (including the Local Privacy Officers) as well as the development, implementation and continuing oversight of these Processor Data Protection Standards. The Chief Data Ethics and Privacy Officer and the Data Protection Officer enjoy the highest management support for the fulfilling of their tasks and shall directly report to the highest management level. This includes being able to inform the highest management level if any questions or problems arise during the performance of their duties. The Global Privacy Office, and the privacy officer network (including the Data Protection Officer) run various privacy programmes, inform and advise the highest management and promote good privacy practices with respect to Personal Data throughout Fiserv through multiple means (including annual mandatory training programmes, official communications and specifically targeted training onprocedures for managing requests for access to Personal Data by public authorities). Completion of appropriate training is monitored by the Global Privacy Office. Further, the Fiserv Global Privacy Office works with other groups within Fiserv to develop additional corporate policies and practices. The Global Cyber Security Programme aims to identify and reduce Fiserv's top security risks. The Data Protection Officer shall not have any tasks that could result in conflict of interests (for instance, they shall not be in charge of carrying out data protection impact assessments nor in charge of carrying out audits of the Processor Data Protection Standards but their advice can be sought where helpful to the task).

11.24 Fiserv further evidences its commitment to accountability by conducting regular (annual) and ad-hoc internal privacy assessments (including on these Processor Data Protection Standards) as part of its comprehensive audit programme and provides mandatory training to its personnel on privacy topics (including on these Processor Data Protection Standards) and issues relevant to their job type. Fiserv shall ensure that all aspects of the Processor Data Protection Standards are monitored at appropriate regular intervals for each Fiserv entity. The audit programme is proposed to and approved by Fiserv's audit committee of the Board of Directors and the Corporate Assurance and Advisory Services department is generally responsible for conducting Fiserv's internal audits and Fiserv shall ensure that the audits address all aspects of these Processor Data Protection Standards, including (for example): applications; IT systems; databases that process Personal Data or onward transfers; decisions taken regarding mandatory requirements under national laws that conflict with these Processor Data Protection Standards; reviews of the contractual terms used for transfers outside of the Fiserv Group and if there are indications of non compliance, set out any corrective actions required to ensure verification of compliance with the Processor Data Protection Standards as well as how and when progress on corrective actions will be measured. The Personnel within the Corporate Assurance and Advisory Services department are guaranteed independence as to the performance of their duties related to these audits; On occasions, external auditors may be used to assess compliance with the Processor Data Protection Standards as part of Fiserv's bi-annual global privacy audit. All external auditors go

through Fiserv's Third Party Risk Management Programme prior to onboarding and are party to appropriate processing terms that comply with the GDPR as well as other relevant security and confidentiality provisions to the extent appropriate given the nature of the services. Items of non-compliance 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 timeframe. Upon completion, the audit team will review it to determine if the item has been adequately addressed and can be closed, or if it requires additional action, and will provide their recommendation together with a copy of the audit report to the Data Protection Officer, the Board of Directors of the relevant Fiserv entity, the Lead EU BCR Member and, when deemed appropriate by the Data Protection Officer, the Board of Directors of Fiserv, Inc. When sought by the Competent Supervisory Authority, Fiserv shall supply that Competent Supervisory Authority (including the Competent Supervisory Authority of the Data Controller) with a copy of any relevant audit content. Subject to the terms of any valid Services Agreement with the Data Controller (and only while such a 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 Competent Supervisory Authority is also authorised to audit any Fiserv entity, in accordance with section 7.4 of these Processor Data Protection Standards.

11.25 In addition, each Fiserv entity shall ensure that its personnel respect the commitments set out in these Processor Data Protection Standards and will provide appropriate means and enforcement measures to make sure those requirements are effective. This is done via the Fiserv Employee Code of Conduct, which outlines Fiserv's commitment to upholding the privacy and confidentiality of Personal Data and various other privacy-related policies. Any material violation of Privacy Laws, these Processor Data Protection Standards, the Employee 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 aware of relevant developments impacting the processing of Personal Data.

11.27 To demonstrate compliance with these Processor Data Protection Standards and applicable Privacy Laws, each Fiserv entity will maintain a record of its processing of Personal Data transferred under these Processor Data Protection Standards that contains the information set out in Annex A. This record will be maintained in writing, including in electronic form, and should be made available to Competent Supervisory Authorities (upon request).

Further information relating to Fiserv's privacy officer network, the provision of training programmes or privacy policies can be found on the Fiserv Privacy Site or by contacting the Global Privacy Office, the Data Protection Officer and/or the Local Privacy Officer.

12 Contact Information

Data Protection Officer

Email: dpo@fiserv.com

Local Privacy Officers

Email: dpo@fiserv.com

FDR LIMITED, LLC (Lead EU BCR Member)

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

Global Privacy Office

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

Annex A – Record of Processing

The records 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, the names of the Data Controllers on behalf of whom the Fiserv entity is acting, and (where applicable) the names and contact details of the Data Controller's representatives and the Data Protection Officer;
- a description of the categories of processing activities undertaken for each Data Controller;
- when applicable, details of 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 adopted; and
- where possible, a general description of the technical and organisational security measures adopted to ensure a level of security is applied to Personal Data which is appropriate to the risk involved in relation to specific processing activities.

Annex B – Processor Activities

The tables below try to give an oversight of the key purposes of processing, 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 for Processing, Categories of Data and Data Subjects below this table.

<table>
<tr><th>Business Purpose</th><th>Purposes for Processing</th><th>Categories of Data</th><th>Data Subjects</th><th>Countries of Transfer</th></tr>
<tr><td rowspan="7">Merchant Acquiring and Transaction Processing Services</td><td>Technology infrastructure and support</td><td>Identification; Special Category; Financial; Commercial; Location; Anonymised/Aggregated; Inferences; Usage</td><td rowspan="7">Customer; Merchant</td><td rowspan="3">United States; India</td></tr>
<tr><td>Transaction processing</td><td>Identification; Financial; Commercial; Location; Anonymised/Aggregated</td></tr>
<tr><td>Customer services</td><td>Identification; Special Category; Financial; Commercial; Location; Anonymised/Aggregated</td></tr>
<tr><td>Fraud prevention services</td><td>Identification; Financial; Location; Commercial; Anonymized/Aggregated; Inferences</td><td rowspan="3">United States</td></tr>
<tr><td>Support of Data Subject rights requests</td><td rowspan="2">Identification; Financial; Location; Special Category</td></tr>
<tr><td>Risk management purposes</td></tr>
<tr><td rowspan="6">Clover Services (Marketplace Merchant Solutions Limited, Trading as Clover)</td><td>Provision of business management services</td><td>Identification; Special Category; Financial; Commercial; Location; Anonymised/Aggregated; Inferences; Usage; Employment</td><td rowspan="6">Customer; Merchant</td><td rowspan="6">United States; India</td></tr>
<tr><td>Customer services</td><td>Identification; Special Category; Financial; Commercial; Location; Anonymised/Aggregated</td></tr>
<tr><td>Support of Data Subject rights requests</td><td>Identification; Financial; Location; Special Category; Employment</td></tr>
<tr><td>Risk management purposes</td><td>Identification; Financial; Location; Special Category</td></tr>
<tr><td>Technology infrastructure and support</td><td>Identification; Special Category; Financial; Commercial; Location;</td></tr>
</table>

		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 Resources	When 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:			United States; India
	Health and safety	Identification; Special Category; Criminal Offence; Location; Financial; Inferences; Usage; Employment; Anonymized/Aggregated	Personnel	
	Payroll			
	Personnel benefits			
	Personnel management			
	Training			
	Internal surveys			
	Recruitment			

	Travel and expenses reimbursement			
	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**	When 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	
	Internal compliance	Identification; Special Category; Criminal Offence; Financial; Commercial; Location; Anonymised/Aggregated; Employment; Inferences; Usage	Customer; Merchant; Personnel; Supplier; Visitor	

	Physical security	Identification; Location; Employment; Inferences; Usage	Customer; Merchant; Personnel Supplier; Visitor	
	Cyber security	Identification; Financial; Location; Employment; Inferences; Usage	Customer; Merchant; Personnel Supplier; Visitor	
	Other purposes required or permitted by law or regulation	Identification; Special Category; Criminal Offence; Financial; Commercial; Education; Location; Inferences; Anonymised/Aggregated; Employment; 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 Procurement / Management	Risk management purposes	Identification; Location; Financial; Criminal Offence	Supplier	United States

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

These descriptions are non-exhaustive and indicative only. Not all data points are used for every purpose/Data Subject.

Business Purposes	Descriptions
Analytics	Refining data to support business decisions and help Customers understand trends in their businesses.
Clover Services (Marketplace Merchant Solutions Limited, Trading as Clover)	Facilitating card transactions 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. to process transactions and provide a business management platform to support Merchants and Consumers.
Human Resources	Supporting other Fiserv entities in managing Personnel 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 transactions from Merchants to card schemes (e.g. Mastercard/Visa), both when Fiserv is a controller or a processor in respect of the services, including: providing the platform; technical support; hardware, etc. to process the transactions.
Risk Assurance, Compliance, Legal and Audit	Supporting Customers and Fiserv entities to comply with local rules and regulations on (among other things) 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 and 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 in relation to third-party vendors.

Purposes for Processing	Descriptions
Customer services	Providing various Customer support functions, including call centre services, correspondence, emails, service messages and the administration of accounts.
Database management	Supporting and setting up databases, including the querying of faults, connections to databases and access management.
Encryption	Encrypting, pseudonymising and anonymising Personal Data.
Fraud prevention services	Using various tools and methods (along with any instructions provided by internal and external Customers) to mitigate potential fraud on behalf of a controller in the EEA.
Health and safety	Supporting reasonable adjustments for sickness/disabilities and ensuring a safe workplace, both generally and in emergencies – like when the health or safety of a person is endangered (e.g. due to a Pandemic, a fire, etc.).
Internal surveys	Collecting views/opinions and information to help Fiserv entities understand Personnel, and ensure diversity and engagement within 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 evaluations, career development, disciplinaries/grievances and talent management.
Physical security	Ensuring the protection of individuals and Fiserv facilities by maintaining access management, monitoring CCTV etc.
Recruitment	Collecting and reviewing application resumes, interviews and background checks.
Regulatory requests	On behalf of Fiserv entities to support responses to lawful requests from courts or government agencies, or to otherwise comply with Applicable Laws or compulsory processes.
Risk management purposes	On behalf of Fiserv entities to support fraud prevention, anti-money laundering, anti-terrorism financing, sanctions monitoring and other similar purposes on behalf of a controller in the EEA.
Provision of business management services	Providing 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 limited to data deletion, access, correction etc. on behalf of a controller in the EEA.
Technology infrastructure and support	Supporting and hosting applications, networks, hardware, databases or other solutions that underpin the business.
Training	Providing training and monitoring training undertaken on behalf of Customers and other Fiserv entities.
Transaction analytics	Refining transaction data for usable metrics and KPIs to help Customers understand trends in their businesses.
Transaction processing	To fulfil transactions initiated by Data Subjects, or (for Merchant Services) hosting Personal Data or processing Personal Data hosted by a Merchant as part of the business application services.
Travel and expenses reimbursement	Reimbursing business costs to Personnel on behalf of Fiserv entities.

Categories of Data	**Descriptions**
Identification	Includes identifiers like a 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 or 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.
Criminal Offence	Personal Data relating to criminal convictions and offences.
Financial	Includes identifiers like a 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 data and the location transactions occurred.
Anonymized/Aggregated	Personal Data obtained from a Data Subject that has been aggregated to a point where the individual can no longer 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), educational background, qualifications, references, training data, grievances, salary data, benefits information, absence data, background checks, survey responses, time and attendance, equal opportunities, monitoring information, and 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, behaviours and attitudes.
Usage	Details about the technology used to access Fiserv's systems (e.g. IP addresses, login data, browser types and device locations). Information about the 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 Fiserv entities, Fiserv's clients and their customers (or the customers themselves, to the extent they are individuals) (e.g. 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 organisation that provides goods or services to Fiserv.
Consumers	Individuals who interact directly with Fiserv or Fiserv's products.

Annex C – Fiserv Privacy Policies

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

Annex C Part	Document name
1	Fiserv's Global Privacy Policy
2	Fiserv's Record Retention Policy
3	Fiserv's Global Cybersecurity and Technology Management Policy
4	Fiserv's Data Classification and Handling Standard
5	Fiserv's Media Handling Standard

Schedule 2 – List of Signatories

A full list of all signatories can be found on the Fiserv Privacy Site.

Schedule 3 – 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 Processor EU 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: