Binding Intra-Group

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

Dated **(Commencement Date)**

21/07/2025

Contents

Binding Intra-Group

Controller EU BCR Membership Agreement

Dated:

Between

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

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

Recitals

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

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.

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 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, re-enacts 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.

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 Controller 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, where 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 0; 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) has 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 his or her agents, about Personal Data originating from or in connection with the Member in question.

3.2 The Parent Company agrees and undertakes that it shall deal promptly and properly with all reasonable requests from any Member to procure that another Member performs its obligations under the BCRs and, 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.

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, the Members agree that the Binding Intra-Group Controller EU BCR Membership Agreement previously entered into between the Members is hereby terminated, or partially terminated, as of the Member Commencement Date insofar as this Agreement addresses the transfers covered by such agreements. 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 which 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; and

(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.

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 and keep indemnified and hold harmless the Lead EU BCR Member (apart from whenthe 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 andhowsoever 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 Member against whom the claim or alleged claim has been advanced or is to be advanced, the Indemnifying Member shall allow the relevant Indemnified Member 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 Member 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 ofwhom 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 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 as regards 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 any rights to enforce any provisions contained in it, except any provision of this Agreement (and in particular, Section 9 of the BCRs) which 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, Inc. EU Controller Data Protection Standards (the "EU BCRs")

EU CONTROLLER DATA PROTECTION STANDARDS

Effective as of _____

Defined Terms Used with the EU BCRs

These Controller Data Protection Standards use several 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 any supervisory authority in a Relevant Country competent for the Fiserv exporter(s) of the specific transfer(section 7.4)., namely (i) the lead Supervisory Authority (which in this case is the Irish Data Protection Commissioner) or (ii) any other supervisory authority in a Relevant Country which is "concerned" by the processing of Personal Data because (a) a Fiserv entity is established in the country or territory where that Supervisory Authority is established, (b) because Data Subjects are living in a country or territory of that Supervisory Authority and are likely to be affected by a Fiserv entity's processing of Personal Data, or (c) it has received a complaint from a Data Subject relating to the processing of Personal Data by a Fiserv entity.

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 Subjects means identified or identifiable natural person (section 1.2).

Fiserv, Fiserv entity, we or our means Fiserv, Inc. and its subsidiaries which have signed an intragroup agreement committing them to these EU Controller Data Protection Standards. A list of the current signatories can be found on the Fiserv Privacy Site (see para 1.1 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 registered address at 10 Hanover Quay, Dublin 2 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 Controller Data Protection Standards by such Fiserv entities (see section 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 11.17).

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, re-enacts 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: (a) these Controller Data Protection Standards; and (b) Fiserv's privacy notice, which is available at www.fiserv.com/privacy (section11.2).

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 (section 6.1).

Transfer means a transfer 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 to another Fiserv entity located outside the EEA which is in a country not recognised as offering adequate protection for the Personal Data pursuant to applicable Privacy Laws (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 (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 Controller Data Protection Standards. This assessment is based on the understanding that laws and practices that respect the essence of fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives in Art 23(1) GDPR, are not in contradiction with these Controller 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) 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 Controller Data Protection Standards (which include the Annexes attached hereto) express the commitment of our Executive Management and Board of Directors to data privacy and protecting all information relating to identified or identifiable natural individuals ("**Data Subjects**") that 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 Fiserv and is headquartered in the United States.

2.2 Fiserv has nominated the Lead EU BCR Member as the Fiserv establishment within the EEA to whom it delegates data protection responsibilities for the purposes of these Controller Data Protection Standards. These responsibilities include accepting liability for breaches of these Controller Data Protection Standards by Fiserv entities (as defined in section 3.1) outside of the EEA and taking any action necessary to remedy such breaches, as described more fully in section 7.2 of these Controller Data Protection Standards.

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

3 The Scope of These Controller Data Protection Standards

3.1 These Controller Data Protection Standards apply only:

3.1.1 to Fiserv entities which have signed or acceded to the Binding Intra-Group Controller EU BCR Membership Agreement in respect of these Controller Data Protection Standards and 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 Controller 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 Controller 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 Data Protection Standards and all references in these Data Protection Standards to Personal Data shall be interpreted accordingly. **Relevant Country** means a member state of the European Union and/or the European Economic Area.

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

3.3 Fiserv has been granted authorisation for: (a) these Controller Data Protection Standards, which apply only in relation to Personal Data for which Fiserv is a controller and (b) Fiserv's Processor Data Protection Standards (available on the Fiserv Privacy Site), which apply only in relation to Personal Data for which Fiserv is a processor (the "**Processor Data Protection Standards**").

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

3.5 These Controller Data Protection Standards apply to a transfer of Personal Data (where the Privacy Laws of a Relevant Country apply, both as defined and provided for in section 3.1) by one Fiserv entity to another Fiserv entity located outside the EEA that is in a country not recognised as offering adequate protection for the Personal Data, pursuant to applicable Privacy Laws (a "**Transfer**") (including onward Transfers to other Fiserv entities), where the recipient Fiserv entity is a controller of the Personal Data. 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**").

3.6 Data Subjects alleging breach of these Controller Data Protection Standards by a Fiserv Importer shall be entitled to enforce them as a third-party beneficiary, pursuant to section 9.7 of these Controller Data Protection Standards

3.7 Fiserv acknowledges that some Fiserv entities may adopt their own privacy standards, policies and procedures based on the nature of their services or clients ("**Local Policies**"). The Local Policies must be consistent with and must meet or exceed the requirements of these Controller Data Protection Standards. Where there is a conflict between the Local Policies and these Controller Data Protection Standards, the policy that is determined by the Data Protection Officer and Global Privacy Office in consultation with the General Counsel's Office (as defined below in section 7.4) to offer the highest protection will govern.

4 Categories of Data Subjects

4.1 Fiserv processes and transfers Personal Data, including Special Categories of Personal Data (defined below), relating to the following classes of Data Subject:

- our clients (and prospects) and their customers in connection with the provision of services, this includes personnel employed by our clients and their customers (or the customers themselves, to the extent they are individuals (for example: card holders)) ("**Customers**");
- individuals who interact directly with Fiserv or Fiserv products ("**Consumers**");
- merchants accepting payments -this includes personnel employed by merchants (when the merchant is an individual) and customers of merchants (card holders) ("**Merchants**");
- employees, contingent workers, consultants, prospective and former personnel, and dependants and beneficiaries of the personnel ("**Personnel**");
- individuals visiting Fiserv premises, including Suppliers, auditors, prospective personnel etc. ("**Visitors**"); and
- other persons or personnel working for an organisation which provides goods and services to Fiserv ("**Suppliers**").

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

4.3 For the purposes of these Controller Data Protection Standards, "**Special Categories of Personal Data**" means any Personal Data revealing race or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, and "**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 Fiserv collects Personal Data from several sources:

- **From the Data Subjects** – for example, we collect Personal Data from our actual and potential clients, Fiserv Personnel and business contacts (for example, in completing online forms, in connection with their working relationship or application for employment or from business contacts in the course of our business) and wemay also collect Personal Data directly from holders of payment instruments when they engage in a transaction;
- **From our clients** –Fiserv obtains Personal Data from its clients or other participants in a transaction processing chain (such as card associations and debit network operators and their members), rather than the Data Subjects themselves;
- **From our group companies** – Personal Data may be shared between Fiserv entities in accordance with these Controller Data Protection Standards, or otherwise when 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, fraud prevention agencies or Independent Sales Organisations (ISOs);
- **From public sources** – we may collect and check Data Subjects' information against other public databases and sources to which we have access;
- **From a Data Subject's browser or device** –we collect browser and/or device information (as described in more detail in the Fiserv Privacy Notice available on the Fiserv Privacy Site); and
- **Information we create** – we may create and record information in relation to Data Subjects. For example, we may create employment records, details of transactions a Data

Subject carries out, the services we provide to a Data Subject and their interactions with us (for example, if a Data Subject contacts us, we may keep a record of that correspondence).

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

- Merchant Acquiring and Transaction Processing Services;
- Clover Services (Marketplace Merchant Solutions Limited, trading as Clover);
- Issuing and Acquiring for Financial Institutions;
- Human Resources;
- Management Oversight;
- Product Development;
- Risk Assurance, Compliance, Legal and Audit;
- Analytics; and
- Vendor Procurement/Management.

These terms are defined in more detail in Annex E, together with a breakdown of the purposes of Processing under these Controller Data Protection Standards.

5.3 We rely on several legal bases to process Personal Data, including:

- **Where a Data Subject has provided their consent** – For example, Fiserv may require a Data Subject's consent to process their data for electronic marketing activities under applicable Privacy Laws. When this is the case, a Data Subject can withdraw their consent at any time by contacting the organisation to whom they gave their consent, or a Data Subject can contact the Data Protection Officer;
- **Where the processing is necessary for the performance of a contract** – For example, to allow Fiserv to provide a product or service to a Data Subject;
- **Where Fiserv needs to comply with a legal obligation or it is in the public interest** – For example, Fiserv may need to disclose a Data Subject's Personal Data to a regulator, law enforcement agency or to a Data Subject's or Fiserv's representatives acting in a legal dispute, or use a Data Subject's Personal Data to verify their identity, or prevent fraud; and
- **Where the processing is necessary for the purposes of our legitimate interests** – Fiserv's legitimate interests include: (1) to provide products and services to a Data Subject or to a client of Fiserv; (2) to ensure a Data Subject's transaction is secure and adequately protected; and (3) the business interests described in section 5.2 above.

  More detail on these lawful bases is set out in Annex A.

5.4 Where Fiserv requests Personal Data directly from a Data Subject, they do not have to provide this. However, if a Data Subject decides not to provide this information, in some circumstances, Fiserv or its clients may be unable to provide products or services to them. For example, Fiserv may be unable to process the Data Subject's transaction or employ a Data Subject.

6 Nature of Data Transferred

6.1 Fiserv processes and transfers a broad range of Personal Data between Fiserv entities and to 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 check, 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. requesting support or 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 and consuming histories or tendencies;
- **Other categories of Personal Data defined in Annex E;** and
- **Anonymised/Aggregated Data** –Personal Data obtained from a Data Subject 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 Controller 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 Controller Data Protection Standards must be interpreted in accordance with the Privacy Laws.

7.2 The policies and procedures described in these Controller 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 of the rights guaranteed in these Controller 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 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 Controller Data Protection Standards, these Controller Data Protection Standards will apply. Where applicable Privacy Laws provide a higher protection, they will take precedence over these Controller Data Protection Standards.

7.4 Fiserv shall cooperate as reasonably required with any supervisory authority in a Relevant Country competent for the Fiserv exporter (“Competent Supervisory Authority) and shall provide such Competent Supervisory Authority, upon reasonable request, with any information about the processing operations covered by these Controller Data Protection Standards. Any questions about Fiserv's compliance with Privacy Laws should be addressed to Fiserv's General Counsel's Office ("**General Counsel's Office**"), Data Protection Officer, Global Privacy Office, or the relevant Local Privacy Officer (using the contact details set out at the end of these Controller Data Protection Standards), who will consult with the relevant 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 Controller 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

Controller 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 dispute relating to a Competent Supervisory Authority's exercise of its powers or its supervision of compliance with these Controller 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 Controller Data Protection Standards, including following the advice or decisions of the Competent Supervisory Authority, the Fiserv Importer (as defined below) will notify the relevant Fiserv exporting entity, 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**"), when it has carried out a Transfer Impact Assessment (with the help of the Fiserv Importer, 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, including any requirements to disclose Personal Data or measures authorising access by public authorities do not prevent it from fulfilling its obligations under these Controller 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, do not contradict these Controller 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(s), (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 Controller Data Protection Standards, including measures applied during the transmission and to the processing of the Personal Data in the country of destination, 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 from fulfilling its obligations under these Controller Data Protection Standards and (b) the laws and practices in the third country applicable to the processing of 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 addition to these Controller Data Protection Standards to ensure an essentially equivalent level of protection as provided by applicable Privacy Laws, and shall promptly inform and involve 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 provided by applicable Privacy Laws, the Fiserv entity shall promptly inform 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 Controller 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.

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 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 exporting entity and the Local Privacy Officer and/or Data Protection Office 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 Controller Data Protection Standards or fail to provide a level of protection that is essentially equivalent to that provided under 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 Office shall promptly identify appropriate supplementary measures to be adopted to address the situation. The same applies if the Fiserv exporting entity has reasons to believe that the Fiserv Importer can no longer fulfil its obligations under these Controller 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) where the Fiserv Importer is in breach of the Controller 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 Controller Data Protection Standards cannot be complied with and compliance is not restored within one month of suspension, (ii) the Fiserv Importer is in substantial or persistent breach of these Controller Data Protection Standards, or (iii) the Fiserv Importer fails to comply with a binding decision of a competent country or the Competent Supervisory Authority regarding its obligations under these Controller Data Protection Standards. If the transfer is ended, 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. The Fiserv Importer shall 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 Controller Data Protection Standards. In case of Applicable Laws that prohibit the return or deletion of the transferred Personal Data, the Fiserv Importer warrants that it will continue to

ensure compliance with these Controller Data Protection Standards and will only process the Personal Data to the extent and for as long as required under that local law.

7.13 The Lead EU BCR Member and the Local Privacy Officer and/or Data Protection Office shall inform all other Fiserv entities of the Transfer Impact Assessment carried out and its results so that the identified supplementary measures will be applied when the same type of transfers are carried out by any other Fiserv exporting entity or (when effective supplementary measures cannot be put in place) the transfers at stake are suspended or ended.

7.14 Each Fiserv exporting entity shall monitor on an ongoing basis (and, when appropriate, in collaboration with the Fiserv Importer), any legal or policy developments in the third country that could affect the initial Transfer Impact Assessment and its results, and the decisions taken accordingly in respect of such transfers.

Obligations in Case of Access by Public Authorities

7.15 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 Lead EU BCR Member and the Fiserv exporting entity, 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.

7.16 If the notification is prohibited by Applicable Laws, the Fiserv entity will use its best efforts to obtain a waiver of this prohibition in order to communicate as much information as it can, (and as soon as possible) to the relevant party. The Fiserv Importer agrees to document its best efforts in order to be able to demonstrate them on request.

7.17 When 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 exporting entity (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 outcome of such challenges).

7.18 The Fiserv Importer agrees to preserve the information pursuant to sections 7.15-7.17 for the duration of these Controller Data Protection Standards and make it available to the Competent Supervisory Authority on request, if permitted by Applicable Laws.

7.19 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.

7.20 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 exporting entity. 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.

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

8 Changes to our Data Protection Standards

8.1 Fiserv may change these Controller Data Protection Standards, additional Fiserv entities may sign the Binding Intra-Group Controller EU BCR Membership Agreement and certain Fiserv entities may terminate or have their Binding Intra-Group Controller EU BCR Membership Agreement terminated. Any Fiserv Importer which ceases to be bound by these Controller Data Protection Standards may keep, return, or delete the Personal Data received under these Controller Data Protection Standards. If the Fiserv exporter and Fiserv Importer agree that the Personal Data may be kept by 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 Binding Intra-Group Controller EU BCR Membership Agreement and keep track of and record any updates to these Controller Data Protection Standards and provide the necessary information to Data Subjects or Competent Supervisory Authorities upon request. In addition, all changes, additions and the termination of any Binding Intra-Group Controller EU BCR Membership Agreement and any changes to the Controller Data Protection Standards must be subject to the approval of the Data Protection Officer and will be reported to each Supervisory Authority annually, together with a brief explanation of the reasons for the change. The Supervisory Authority will also be notified annually (even when no changes have been made). Where a change would possibly be detrimental to the level of protection offered by these Controller 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. Upon approval of the Data Protection Officer, Fiserv will clearly indicate the date of the latest revision and communicate the Controller 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 Controller 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 have a right to complain to the Competent Supervisory Authority or to the applicable Fiserv entity if they consider that the processing of their Personal Data infringes Privacy Laws or is in breach of these Controller Data Protection Standards.

9.2 We strongly encourage Data Subjects to first raise any complaints through 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 (email: dpo@fiserv.com or post: Janus House, Endeavour Drive, Basildon, Essex, SS14 3WF, UK), who will work with them to endeavour to resolve their concern to their satisfaction without undue delay.

9.3 Further, under Fiserv's Code of Conduct, Fiserv's Personnel can raise complaints regarding breaches of these Controller Data Protection Standards by contacting the Data Protection Officer, or through the Fiserv Data Privacy Hotline.

9.4 A decision on whether any complaint made by Fiserv's Personnel or other Data Subjects is justified or rejected will be communicated to the Data Subject by the Data Privacy Hotline, the Data Protection Officer or Local Data Protection 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 accordingly.

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

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

9.5.2 bring the issue before the courts of 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 Controller Data Protection Standards

9.6 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 Controller Data Protection Standards shall exclude or restrict such remedies, redress or rights to complain.

9.7 Data Subjects can enforce their rights as a third-party beneficiary in relation to a breach by a Fiserv Importer of the following elements of these Controller Data Protection Standards:

9.7.1 the general data protection principles, lawfulness of processing, security and personal data breach notifications, restrictions on onward transfers (section 11, Annex A)

9.7.2 transparency and easy access to these Controller Data Protection Standards and, in particular, easy access to the information about their third-party beneficiary rights under these Controller Data Protection Standards (sections 9.7, 10.1 and 11.2);

9.7.3 the Data Subject's right of information, access, rectification, erasure, restriction, notification regarding rectification or erasure or restriction, objection to processing and right not to be subject to decisions based solely on automated processing, including profiling (sections 11.20 -11.24);

9.7.4 Fiserv's obligations in case of Applicable Laws affecting compliance with these Controller Data Protection Standards and in respect of government access requests (sections 7.5-7.21);

9.7.5 the Data Subject's right to complain through the Fiserv group's internal complaint process (sections 9.1-9.5);

9.7.6 Fiserv's obligations regarding cooperation with Competent Supervisory Authorities relating to compliance obligations covered by this third-party beneficiary clause (section 7.4);

9.7.7 the Data Subject's rights to judicial remedies, redress and compensation in the courts and to lodge a complaint with the Competent Supervisory Authority and the Lead EU BCR Member's duty to accept liability for paying compensation and to remedy any breaches of these Controller Data Protection Standards (sections 9.5, 9.6 and 9.8);

9.7.8 Fiserv's obligations to update the Data Subjects about any update to these Controller Data Protection Standards and of the list of BCR members (sections 8.1 and 10.1);

9.7.9 this third party beneficiary rights section (section 9.7); and/or

9.7.10 any of the provisions of applicable Privacy Laws which a Data Subject can enforce directly against a controller,

(each a "**Breach**")

9.8 As stated under section 2.2 of these Controller Data Protection Standards, the Lead EU BCR Member accepts liability for any such Breach as if it had arisen from its own act or omission.

9.9 If a Data Subject can demonstrate that they have suffered material or non-material damages and can establish facts which show it is likely that the damage occurred because of a Breach, then it will be for the Lead EU BCR Member to prove that the Fiserv Importer 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:

(i) take necessary actions to remedy the Breach; and

(ii) 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 Art 82 of the GDPR.

10 Communication of Fiserv's Data Privacy Standards

10.1 Fiserv takes compliance with its data protection obligations very seriously. All Fiserv Personnelwho 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 Controller Data Protection Standards, receive appropriate and up-to-date training on (and have access to) these Controller Data Protection Standards. Fiserv will post a copy of these Controller Data Protection Standards on its internal and public websites, including on the Fiserv Privacy Site. In addition, Data Subjects will be provided with the link to our public website upon request. The Data Protection Officer and the Global Privacy Office will maintain a list of the Fiserv entities (including contact details) that are bound by these Controller 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 Where Fiserv is a data controller (as defined by Privacy Laws), it processes Personal Data fairly, lawfully and in a transparent manner in relation to the Data Subject, in accordance with all Privacy Laws and in accordance with one or more of the lawful bases and conditions set out in Annex A.

11.2 Fiserv's "information notice" containing the information it is required to give to Data Subjects under the GDPR is set out in: (a) these Controller Data Protection Standards and (b) Fiserv's privacy notice, which is available www.fiserv.com/privacy (the "**Privacy Notice**"). Where appropriate, the information given by these Controller Data Protection Standards and the Privacy Notice shall be supplemented as required by a specific information notice in respect to a particular piece of processing.

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

11.3 Fiserv collects, transfers, holds and processes Personal Data only for specified, explicit and legitimate purposes, as set out in these Controller Data Protection Standards, the Privacy Notice and any supplementary information notice provided to a Data Subject. Fiserv will not process Personal Data in ways incompatible with those purposes. When we obtain Personal Data from third parties (including our clients) and publicly available sources, we always use only reliable and reputable sources.

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

11.4 Personal Data processed by 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 are processed, as described in section 5.2. The purposes of retaining the data, and the specific retention periods, will be defined in Fiserv's applicable data retention policies and schedules, on expiry of which Fiserv will securely delete the relevant Personal Data. Fiserv's retention periods are determined by factors such as the need to retain data to provide services to Data Subjects or our clients, the need to comply with Applicable Laws and requirements to comply with the rules provided by participants in a transaction processing chain, such as the rules provided by card associations and debit network operators and their members.

11.6 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 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 or with instructions from its clients or business partners (as applicable), in compliance with applicable Privacy Laws and in accordance with Fiserv's applicable policies (as amended from time to time). Its 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.

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

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

We implement data protection by design and default.

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

11.10 Fiserv will implement appropriate technical and organisational measures to ensure that, by default, only Personal Data which are necessary for each specific purpose of the processing are processed, in relation to the amount of Personal Data collected, the extent of processing, the period of storage and accessibility. Fiserv will not make a Data Subject's Personal Data publicly available without informing the Data Subject in advance.

We transfer Personal Data only for limited purposes (onward transfers).

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

- the transfer is based on a clear business need;
- all applicable legal requirements are met (including the conditions in Chapter V of the GDPR to ensure that the Personal Data is adequately protected); and
- in the case of all transfers or onward transfers to processors (whether Fiserv entities or third parties), there is a written contract in place that includes provisions no less protective than those set out in Annex C (which sets out the requirements in Art 28(3) GDPR, including a duty to follow the controller's instructions and implement appropriate technical and organisational measures). For the avoidance of doubt, where the processor is a Fiserv entity, its compliance with the Processor Data Protection Standards shall constitute the written agreement for these purposes.

11.12 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, where the Data Subject has given Fiserv permission to disclose their information to such third parties;
- third parties to whom Fiserv will transfer, or may transfer, its rights and duties in its agreements with Data Subjects, including if a Fiserv entity, or substantially all of its assets,

are acquired by such a 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 with in order to comply with any legal obligation;
- third parties, when required to protect the rights, property, or safety of Fiserv, our clients or their customers, or others; and
- Fiserv's vendors and agents (including their sub-contractors). In particular, Fiserv may disclose Personal Data when it uses the services of:
    - credit reference agencies;
    - fraud protection and risk management agencies;
    - identification and information verification agencies;
    - vendors and others that help us process a Data Subject's payments;
    - third party suppliers engaged to host, manage, maintain and develop our website and IT systems; and
    - our professional advisers, including lawyers and auditors.

11.13 Fiserv does not disclose Personal Data except in the circumstances set out in these Controller Data Protection Standards, or as required or otherwise permitted by Applicable Law.

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

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

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 appropriate to the risk represented by the processing and nature of the Personal Data to be protected, with all due regard to the state of the art and cost measures. Fiserv will ensure that any Personnel who have access to Personal Data have appropriate obligations of confidentiality in their agreement with Fiserv.

11.17 If a security incident occurs leading 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 which is designed to assist Fiserv in complying with Privacy Laws requiring notification of Personal Data Breaches, with guidelines produced by the relevant Competent Supervisory Authorities in relation to Personal Data Breaches and with our duties under our client contracts. This requires Fiserv to: (i) notify the Lead EU BCR Member and the Data Protection Officer of the Personal Data Breach, as well as the Fiserv entity acting as a controller if a Fiserv entity is acting as a processor, without undue delay, (ii) notify Data Subjects without undue delay of Personal Data Breaches where the breach is likely to result in a high risk to the Data Subjects, (iii) notify Personal Data Breaches to the applicable Competent Supervisory Authority without undue delay and, when feasible, not later than 72 hours after having become aware of the Personal Data Breach, unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of the Data Subjects, and (iv) keep records of Personal Data Breaches (comprising the facts relating to the Personal

Data Breach, its effects and the remedial actions taken), which will be made available to the Competent Supervisory Authority) on request. As appropriate or required, Fiserv will also notify law enforcement authorities, financial or other regulators (including Competent Supervisory Authorities) and/or state agencies.

11.18 Personal Data will not be transferred to a country or territory which is not recognised as offering adequate protection for the 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 Art 49 GDPR.

11.19 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, where necessary. Special Categories of Personal Data and Criminal Offence Data will be disposed of under Fiserv's Global Cyber Security and Technology Management Policy and the Data Classification and Handling Standard and associated Media Handling Standard, further details of which can be obtained from the Data Protection Officer, or other applicable policies as may be implemented by Fiserv. Fiserv requires that all Special Categories of Personal Data and Criminal Offence Data be transferred securely.

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

11.20 Where Fiserv is a controller of Personal Data, a Data Subject may have rights over their Personal Data. These rights include:

- **The right to information**

This right has been covered above in section 11.2 (*We process Personal Data fairly and lawfully ('lawfulness, fairness and transparency')).*

- **The right to access their Personal Data processed by Fiserv.**

A Data Subject has the right to obtain confirmation from Fiserv as to whether or not Fiserv is processing their Personal Data and if so, to access and receive a copy of their Personal Data, and the following supplementary information: a. the purpose of the processing; b. the categories of Personal Data (and any available information as to their source, where not collected directly); c. the recipients or categories of recipient of the Personal Data, including recipients located in other countries and details of the appropriate safeguards in place for the transfer of their Personal Data to other countries; d. how long the Personal Data will be retained or the retention criteria; e. any solely automated decision-making or profiling applied to the Personal Data and the significance and any envisaged consequences of such processing.

Fiserv will also make the Data Subjects aware of their rights to request rectification, erasure, restrictions on use of the Personal Data by Fiserv or the right to object and their right to lodge a complaint with a supervisory authority.

- **The right to correct their Personal Data if it is wrong;**

A Data Subject has the right to request that Fiserv rectify their Personal Data if the Personal Data is inaccurate or incomplete. Fiserv will work with the Data Subject to rectify, complete, block or erase the inaccuracy or incompleteness, should the Data Subject not have the ability to self-correct their Personal Data by signing in to a portal or similar interface. If Fiserv has disclosed the Personal Data to a recipient, it will inform the recipient of the request unless this would prove impossible or would require a disproportionate effort. A Data Subject may request

information about the recipients from Fiserv. Fiserv will keep a record that the Data Subject considers the Personal Data to be inaccurate or incomplete.

- **The right to erase their Personal Data (also known as the right to be forgotten);**

Fiserv will abide by a request from a Data Subject to erase their Personal Data under the following conditions as specified within the Privacy Laws: a) the Personal Data is no longer necessary for the purpose for which they were collected or otherwise processed; or b) a Data Subject withdraws consent and there are no other legal grounds for processing; or c) a Data Subject objects to the processing and Fiserv has no overriding legitimate interests for continuing to process their Personal Data; or d) the Personal Data is being unlawfully processed; or e) the Personal Data must be erased to comply with a legal obligation applicable to Fiserv as a controller; or f) the Personal Data is processed in relation to the offer of information society services to a child. There are circumstances when Fiserv can refuse an erasure request; these include: a) exercising the right of freedom of expression and information; b) complying with a legal obligation applicable to Fiserv as a controller or for the performance of a public interest task or exercise of official authority; c) for public health reasons or for purposes in the public interest; d) for archiving purposes in the public interest, scientific research, historical research or statistical purposes; or e) for the establishment, exercise or defence of legal claims. Fiserv will inform any recipients about the erasure request unless this would prove impossible or would require a disproportionate effort. Where Fiserv has made the data public, it will take reasonable steps, (taking into account cost and technology), to inform other recipients of the Personal Data to erase links to, copies or replication of those personal data.

- **The right to restrict how Fiserv uses their Personal Data (including notification obligations under Art 19 GDPR);**

Fiserv will agree to restrict processing of a Data Subject's Personal Data if one of the following applies: a) When a Data Subject contests the accuracy of the Personal Data, Fiserv will restrict using the Personal Data until the accuracy can be verified; b) The processing is unlawful and the Data Subject requests a restriction of use rather than erasure of their Personal Data; c) Fiserv no longer needs to process the Personal Data, but the Data Subject requires the Personal Data to establish, exercise or defend a legal claim; or d) In circumstances where a Data Subject has objected to the processing and Fiserv is considering whether Fiserv's interests override the interests of the Data Subject. If there is a restriction on processing, Fiserv has the right to store the Personal Data. Fiserv will inform any recipients of the Personal Data about the restriction unless this proves impossible or would require disproportionate effort. A Data Subject can request information about the identity of the recipients from Fiserv. If Fiserv lifts the restriction on processing, the Data Subject will be informed.

- **The right to object to Fiserv's processing of Personal Data**

A Data Subject has the right to object at any time to the processing of their Personal Data by Fiserv, including profiling which is based on legitimate interests or for the performance of any task carried out in the public interest or in the exercise of official authority vested in Fiserv.

Under certain circumstances, there may be grounds for Fiserv to continue certain types of processing where we can demonstrate that its legitimate interests override the rights of an individual or in instances where the processing is necessary for the establishment, exercise or defence of legal claims.

- **The right to data portability**

A Data Subject has the right to request portability of Personal Data which they provided to Fiserv, if: a) the processing is based on the Data Subject's consent or for the performance of a

contract, and b) the processing is automated. This right only applies to Personal Data a Data Subject has provided to Fiserv. If the Personal Data includes Personal Data about other individuals, Fiserv will take steps to ensure providing the information would not affect the rights and freedoms of other individuals. Fiserv will: a) provide the Personal Data free of charge and in a structured, commonly used and machine-readable format, and b) transfer the Personal Data directly to another controller at the request of the Data Subject, where technically feasible.

-
- **The right in relation to automated decision making and profiling**

A Data Subject has the right not to be subjected to solely automated decisions which produce legal effects or otherwise similarly significantly affect them. A Data Subject has the right to ask for a review of the decision, offer their opinion and challenge the decision. The right does not apply, where the decision is a) made with the explicit consent of a Data Subject; b) for the purposes of a contract; or c) authorized by law. Where consent or contracts are relied upon, there must be suitable safeguards such as human intervention to review the decision in order to protect the Data Subject. There are further restrictions on making solely automated decisions using special category personal data. Fiserv will comply with the relevant requirements when making automated decisions and will institute any additional safeguards to protect Data Subject rights where required to do so. See further information on automated processing in Section 11.22.

11.21 A Data Subject can exercise these rights by contacting the Global Privacy Office using the following link. These rights will only apply in certain circumstances, as they are subject to the limitations and exemptions in the GDPR and only apply to certain types of information or processing. If a Data Subject has any questions about their rights, please contact the Data Protection Officer by emailing *dpo@fiserv.com* . Further information in relation to a Data Subject's rights can also be found on the .

11.22 Fiserv makes use of automated decision-making (including profiling) in the processing of Personal Data, including for the purpose of: determining cheque acceptance; identification and information verification (including for anti-money laundering, anti-terrorism financing and sanctions monitoring purposes); in deciding whether to underwrite a merchant (for automatic approval only, when relevant criteria are not met by a merchant, the decision whether to decline will be referred to an individual); certain job applications (to determine whether the applicant meets minimum criteria); commemorating length of employee service; to monitor and identify potential fraudulent transactions; to notify Fiserv's clients of possible fraudulent transactions; certain credit card applications (with the criteria being set by Fiserv's clients) and where job applicants do not agree to Fiserv's privacy statement and/or a background check, but agreement is necessary to consider the application. Further details of these are available upon request from the Data Protection Officer or the Global Privacy Office. No evaluation or decision which produces legal effects concerning them or (similarly) significantly affecting them shall be made solely through such processing, unless the evaluation or decision:

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

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

Fiserv's Data Protection Officer and/or Local Privacy Officer shall process each Data Subject's request for exercising their rights in respect of Personal Data as required by Privacy Laws and in accordance with Fiserv's Global Privacy Policy. If a Data Subject asserts the Personal Data kept about them is incorrect, we will work with the Data Subject to rectify, block or erase the inaccuracy, should the Data Subject not have the ability to self-correct their Personal Data by signing in to a portal or similar interface. Fiserv shall also communicate any rectification or erasure of Personal Data or restriction of processing to each recipient to whom the Personal Data has been disclosed, unless this proves impossible or involves disproportionate effort.

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

11.23 When Fiserv uses Personal Data for its own direct marketing, it must do so in accordance with applicable Privacy Laws and any further guidance produced by the relevant Competent Supervisory Authority. A Data Subject has the right to object to direct marketing by Fiserv at any time. To exercise this right, they shall be able to communicate this via the Global Privacy Office or via such other method as may be identified, when applicable, in the relevant marketing communication.

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

11.24 Each Fiserv entity will be responsible for, and able to demonstrate compliance with, these Controller Data Protection Standards. Fiserv's Global Privacy Office operates a comprehensive network of privacy officers around the world who are responsible for data privacy within their region, including compliance with these Controller 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 and the development, implementation and continuing oversight of these Controller Data Protection Standards. The Global Privacy Office and the privacy officer network, including the Data Protection Officer and the Local Privacy Officers, run various privacy programmes, promote good privacy practices with respect to Personal Data throughout Fiserv through multiple means, including annual mandatory training programmes, official communications and specifically targeted training (e.g. on procedures 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.

11.25 Fiserv further evidences its commitment to accountability by conducting regular (annual) and ad-hoc internal privacy assessments (including on these Controller Data Protection Standards) as part of its comprehensive audit programme and provides mandatory training to its Personnel on privacy topics (including on these Controller Data Protection Standards) and issues relevant to their job type. 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 Controller 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 Controller 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 Controller Data Protection Standards and 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 Controller 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 time frame. 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 and to the Board of Directors of the relevant Fiserv entity and 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 with a copy of any relevant audit content.

11.26 In addition, each Fiserv entity shall ensure that its Personnel respect the commitments set out in these Controller Data Protection Standards and will provide appropriate means and enforcement measures to make sure those requirements are effective. This is done via the Fiserv Code of Conduct, which sets forth our commitment to uphold the privacy and confidentiality of Personal Data and various other privacy-related policies. Any material violation of Privacy Laws, these Controller Data Protection Standards, the Code of Conduct or relevant corporate policies by a member of Fiserv's Personnel may result in disciplinary action, up to and including dismissal.

11.27 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.

11.28 To demonstrate compliance with these Controller Data Protection Standards and applicable Privacy Laws, Fiserv will maintain a record of its processing of Personal Data transferred under these Controller Data Protection Standards containing the information set out in Annex D when processing as a controller. This record will be maintained in writing, including in electronic form, and should be made available to a Competent Supervisory Authority upon request.

11.29 Fiserv will perform a data protection impact assessment in respect of any processing operations on Personal Data transferred under these Controller Data Protection Standards that are likely to result in a high risk to the rights and freedoms of Data Subjects. When a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by Fiserv to mitigate the risk, Fiserv will consult the Competent Supervisory Authority before processing.

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

12 Contact Information

Data Protection Officer

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

Local Privacy Officers

Email: dpo@fiserv.com

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 – Conditions Required to Be Met by Fiserv Prior to the Processing of Personal Data

At least one of the following conditions must be met before the processing of Personal Data by Fiserv:

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

At least one of the following conditions must be met before the processing of Special Categories of Personal Data by Fiserv:

- the Data Subject has given their explicit consent to the processing of the Personal Data for one or more specified purposes, except when Union or EU/EEA member states' laws provide that the prohibition on processing Special Categories of Personal Data may not be lifted by the Data Subject;
- the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of Fiserv or of the Data Subject in the field of employment and social security and social protection law insofar as it is authorised by Union or EU/EEA member states' laws, or a collective agreement pursuant to those member states' laws providing for appropriate safeguards for the fundamental rights and the interests of the Data Subject;
- the processing is necessary to protect the vital interests of the Data Subject or another natural person when the Data Subject is physically or legally incapable of giving consent;
- the processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on the condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the Personal Data are not disclosed outside that body without the consent of the Data Subjects;
- the processing relates to Personal Data which are manifestly made public by the Data Subject;
- the processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- the processing is necessary for reasons of substantial public interest, on the basis of Union or EU/EEA member states' laws which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject;
- the processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the Personnel, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or EU/EEA member states' laws, or pursuant to contract with a health professional and subject to the professional being subject to the obligation of professional secrecy in accordance with Art 9(3) of the GDPR;
- the processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of

quality and safety of healthcare and medicinal products or medical devices, on the basis of Union or EU/EEA member states' laws which provide for suitable and specific measures to safeguard the rights and freedoms of the Data Subject, in particular professional secrecy; or

- the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in accordance with Art 89(1) of the GDPR based on Union or EU/EEA member states' laws, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the Data Subject.

Criminal Offence Data shall only be processed by Fiserv to the extent such processing is authorised by Union or EU/EEA member states' laws providing for appropriate safeguards for the rights and freedoms of Data Subjects.

Annex B – Fiserv Privacy Policies

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

Annex B 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

Annex C – Mandatory Contractual Terms for Processors

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

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

Annex D – Record of Processing

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

- the name and contact details of the relevant Fiserv entity and, where applicable, the joint controller, and the Data Protection Officer;
- the purposes of the processing;
- a description of the categories of Data Subjects and of the categories of Personal Data;
- the categories of recipients to whom the Personal Data have been or will be disclosed, including recipients in third countries or international organisations;
- where applicable, transfers of Personal Data to a third country or an international organisation, including the identification of that third country or international organisation and, when relevant, the suitable safeguards;
- when possible, the envisaged time limits for erasure of the different categories of Personal Data; and
- when possible, a general description of the technical and organisational security measures to ensure a level of security is applied to the Personal Data which is appropriate to the risk.

Annex E – Controller Activities

Introduction

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

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

Business Purposes	Purposes for Processing	Categories of Data	Data Subjects	Countries of Transfer
Merchant Acquiring and Transaction Processing Services	Building and maintaining customer relationships, including marketing	Identification, Location, Financial, Commercial, Inferences, Anonymised/Aggregated	Customer; Merchant	United States
	Fraud prevention services	Identification, Financial, Location, Anonymized/Aggregated, Inferences, Usage		
	To fulfil our contracts with our clients	Identification, Financial, Location, Special Category		
	Support of Data Subject Rights Requests			
	Risk management purposes			
Clover Services (Marketplace Merchant Solutions Limited, trading as Clover)	Building and maintaining consumer relationships, including providing receipts and enabling marketing	Identification, Financial, Location, Special Category, Commercial, Inferences, Usage, Anonymised/Aggregated	Consumer; Merchant	United States
	Fraud prevention services			
	To fulfil our contracts with our clients			
	Support of Data Subject Rights Requests			
Issuing and Acquiring for Financial Institutions	Building and maintaining customer relationships, including marketing	Identification, Location, Financial, Commercial, Inferences, Anonymised/Aggregated	Customer; Merchant	United States
	Risk management purposes	Identification, Financial, Location, Special Category		
	To fulfil our contracts with our clients	Identification, Special Category, Financial, Location		
Human Resources	Health and safety	Identification, Special Category, Location, Employment	Personnel	United States All Fiserv entities in third
	Payroll	Identification, Financial, Location, Employment		

	Personnel benefits			countries may access corporate directory information about EU Personnel
	Personnel management	Identification, Financial, Location, Employment, Special Category, Criminal Offence, Usage		
	Training	Identification, Location, Employment		
	Internal surveys			
	Recruitment	Identification, Special Category, Criminal Offence, Financial, Location, Employment		
	Travel and expenses reimbursement	Identification, Financial, Location, Employment		
	Support of Data Subject Rights Requests	Identification, Special Category, Location, Financial, Inferences, Usage, Employment, Anonymized/ Aggregated		
	Monitoring Fiserv systems	Identification, Location, Usage		
Management Oversight	Business development	Identification, Financial, Location, Employment, Commercial	Personnel; Customer; Merchant	United States
	Business planning			
	Mergers and disposition	Identification, Financial, Location, Commercial		
	Facilities management	Identification, Special Category, Location, Anonymized/Aggregated, Employment, Usage	Customer; Merchant; Personnel; Visitors; Suppliers	
Product Development	Research and development	Identification, Financial, Location, Commercial, Anonymized/Aggregated	Customer; Merchant	United States
Risk Assurance, Compliance, Legal and Audit	Risk management purposes	Identification, Financial, Location, Employment, Commercial, Usage	Personnel; Customer; Merchant	United States
	Regulatory requests	Identification, Special Category, Financial, Location, Employment, Commercial, Usage		
	Internal compliance	Identification, Special Category, Criminal Offence, Financial, Commercial, Location, Anonymized/Aggregated, Employment, Inferences, Usage		
	Physical security	Identification, Location, Employment, Inferences, Usage	Personnel; Customer; Merchant; Supplier; Visitor	

	Cyber security	Identification, Financial, Location, Employment, Inferences, Usage		
	Other purposes required or permitted by law or regulation	Identification, Special Category, Criminal Offence, Financial, Commercial, Education, Location, Inferences Anonymized/Aggregated, Employment, Usage		
Analytics	Personnel management	Identification, Location, Anonymized/Aggregated, Inferences, Usage, Employment	Personnel	United States
	Providing analytics on products to customers	Identification, Location, Anonymized/Aggregated, Inferences, Usage, Employment, Commercial, Financial	Customer; Merchant; Consumer	
	Improvement to process, product and services	Identification, Financial, Location, Inferences, Commercial, Anonymized/Aggregated	Customer; Merchant; Consumer	
	Provision of KPIs to stakeholders			
Vendor Procurement/ Management	Creating and maintaining vendor relationships	Identification, Location, Financial, Criminal Offence	Supplier	United States
	Risk management purposes			

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

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

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

Purposes for Processing	Descriptions
Building and maintaining customer relationships, including marketing	Building and personalising customer relationships, including onboarding, loyalty programs, retention, audit support and marketing.
Business development	Pursuing strategic opportunities, cultivating partnerships or other commercial relationships, identifying new markets for products or services.
Business planning	Processing multiple points of data to understand resource allocation, expansion into new markets, financial planning for projects, process improvement and innovation.
Creating and maintaining vendor relationships	Engaging with vendors for activities such as account management, onboarding, debt collection and dispute management.
Cyber security	The processing of personal data for data loss prevention and protecting, detecting and mitigating other cyber security risks and threats.
Facilities management	Organization and management of onsite personnel supporting Fiserv offices, including the provision of equipment, operation of access controls, CCTV and site security.
Fraud prevention services	Using various tools and methods to mitigate potential fraud when the Fiserv entity outside the EEA is a controller in respect of this activity.
Health and safety	Supporting reasonable adjustments for sickness/disabilities, ensuring a safe workplace and in emergencies when the health or safety of a person is endangered (e.g. Pandemic, fire, etc.).

Improvement to process, product, and services	Using multiple data elements to assess performance of products and services within markets and identify trends and further opportunities for improvements
Internal compliance	Ensuring compliance with Applicable Laws, policies and company procedures, including whistleblowing, internal IT security and internal investigations and processing to protect our rights, privacy, safety or property and to protect, deter or investigate against fraudulent, harmful, unauthorised or illegal activities.
Internal surveys	Collecting views/opinions and information to understand our Personnel and to ensure diversity and engagement in the business.
Mergers and disposition	Sharing information to prospective purchasers and sellers to facilitate the acquisition or disposition of Fiserv businesses.
Monitoring Fiserv systems	To ensure use of Fiserv infrastructure is primarily for business purposes and in line with Fiserv policies, to ensure we have sufficient technology capacity for the needs of the business, to see if staff are working in an efficient manner, and to ensure we are protected against cyber security threats, such as malware.
Other purposes required or permitted by law or regulation	Other use cases which may be reviewed and approved by appropriate leadership at Fiserv from time to time (e.g. financial regulators may require the disclosure of certain personal data during an audit or request for information).
Payroll	Determining compensation payable to Personnel.
Personnel benefits	Healthcare, Insurance, Time Away (including parental leave), Retirement, Learning & Development, Financial Benefits, Discounts & Savings and Other Benefits.
Personnel management	Performance evaluation, career development, disciplinary/grievances and talent management.
Physical security	Ensuring protection of Fiserv individuals and facilities by maintaining access management, monitoring CCTV etc.
Provision of KPIs to stakeholders	Collection, processing and analysis of various data elements to understand performance of applications, products and services to enable stakeholders to make informed business decisions.
Providing analytics on products to customers	Providing information to customers to help them understand business trends, their competitiveness and their end-customers when a Fiserv entity outside the EEA is a controller in respect of this activity.
Recruitment	Collection and review of application resumes, interviews and background checks.
Regulatory requests	In response to a lawful request from a court or government agency or to otherwise comply with Applicable Laws or compulsory processes.
Research and development	Understanding opportunities for products and services, along with the innovation and improvement of new and existing products.
Risk management purposes	For the purposes of fraud prevention, anti-money laundering, anti-terrorism financing, sanctions monitoring, due diligence and background checks of suppliers or other similar purposes when the Fiserv entity outside the EEA is a controller in respect of this activity.
Support of Data Subject Rights Requests	Receipt of and response to data requests received from Data Subjects when the Fiserv entity outside the EEA is a controller.
To fulfil our contracts with our clients	Fiserv will perform activities which include (but are not limited to): account management, onboarding, debt collection and dispute management.
Training	Monitoring of mandatory training and performance of training taken.
Transaction processing	To fulfil a transaction initiated by a Data Subject.
Travel and expenses reimbursement	Taking decisions in relation to reimbursement of business costs to Personnel.

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, 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 number, credit history and other financial information.
Commercial	Includes account information, customer correspondence (e.g. requesting support or 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 and the location transactions occurred.
Anonymized/Aggregated	Personal data obtained from a Data Subject which has been aggregated to a point where the individual is no longer able to be identified within the dataset.
Employment	Information relating to a person's current, past, or prospective employment or professional experience (e.g. job history, performance evaluations), educational background, qualifications, references, training data, grievances, salary data, benefits information, absence data, background checks, survey responses, time and attendance, equal opportunities, monitoring information, dependent and beneficiary information.
Inferences	Inferences drawn from any personal data collected to create a profile about a Data Subject reflecting the Data Subject's spending patterns, preferences, characteristics, predispositions, behaviours and attitudes.
Usage	Details about technology used to access Fiserv's systems (e.g. IP address, login data, browser type and device location). 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	Fiserv clients (and prospects) and their customers in connection with the provision of services. This includes personnel employed by our clients and their customers (or the customers themselves, to the extent they are individuals) (cardholders).
Merchant	Merchants accepting payments. This includes personnel employed by Merchants, proprietors when the Merchant is an individual and customers of Merchants (cardholders).
Personnel	Includes Fiserv employees, contingent workers, consultants, prospective and former personnel and the personnel's dependents and beneficiaries.
Suppliers	Person or personnel working for an organization which provides goods or services to Fiserv.
Visitors	An individual who is visiting Fiserv's premises, including Suppliers, auditors, prospective personnel etc.
Consumers	Individuals who interact directly with Fiserv or Fiserv's products.

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 Controller 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: