EFFECTIVE DATE: March 27, 2023

Global (ex EU/UK) HR Privacy Notice

This Global (ex EU/UK) HR Privacy Notice ("HR Privacy Notice") describes the practices of the Fiserv, Inc. group of companies, including Fiserv and its subsidiaries and affiliates (collectively, "Fiserv", "we", "us", or "our"), regarding Fiserv's human resources (HR) privacy practices in regions other than the European Union. A separate privacy notice applies to individuals in the European Union or the United Kingdom.

To the extent that applicable law in your jurisdiction requires your consent to our collection, use, disclosure, or other processing of your personal data as outlined in this HR Privacy Notice, you hereby provide such consent.

This HR Privacy Notice replaces any similar notices that may have previously been provided to you, but it does not form part of any employment contract or other contract for services and is not contractual. We may also provide you with more specific, "just in time", notices for some employment related data processing.

Applicability and Fiserv entity issuing this HR Privacy Notice

This Privacy Notice applies to the following categories of individuals, and the Fiserv entity issuing this Privacy Notice to such individuals and which is responsible for processing personal data is explained below:

Category of Individuals	**Which Fiserv entity is providing this HR Privacy Notice?**
Employees Former employees Interns	The Fiserv entity by which you are or were employed
Temporary staff Contractors Consultants Contingent workers	The Fiserv entity for which you perform services
Applicants for any position (whether permanent or temporary and whether as an employee, contractor, contingent worker, or otherwise)	The Fiserv entity to which you applied for a job or work
The dependents, beneficiaries, and emergency contacts of any of the foregoing	The Fiserv entity to which Fiserv personnel or staff provided your information, typically the entity that employed the personnel or staff

The data we collect about you

Personal data, or personal information, means any information that relates to an identifiable individual. It does not include data where all means of determining the individual's identity has been removed (anonymous data).

We may collect, use, store and transfer the following categories of personal data about you, where permitted by local laws:

Category of Data	Examples

Contact and identifying Information	• personal contact information:
	  ○ name
	  ○ address
	  ○ personal telephone number(s)
	  ○ personal email addresses
	• date and place of birth
	• gender
	• nationally issued identifier (such as National Insurance or Social Security Number)
	• driving license or other photo identification and photocopy
	• passport details and photocopy
	• Details of family members, such as:
	  ○ next of kin and emergency contact information
	  ○ marital status
	  ○ dependants and beneficiaries
	• photographs
	• employee ID

Financial Data	• bank account details • payroll records • tax code status information

	• credit reference certificate • payment instrument details (company credit card) • expenses, including expenses incurred on a company credit card and expenses submitted for reimbursement
Employment Records	• salary • absences (e.g. annual, parental, vacation) • pension and benefits • start date/end date • location of employment or workplace and of business travel • job titles • work history • working hours • training records • education programs • sickness records • professional memberships • compensation history • performance information (e.g., evaluations and feedback) • disciplinary, capability and grievance information • details of work travel
Candidates and New Hire Data	• professional qualifications • education and work history • language skills • copies of right to work documentation • references

	• pre-employment checks such as credit history, criminal records, education, media searches, sanction list searches, medical report or questionnaire to the extent permitted under local law • proof of address • credit reference certificate • other information included in a CV or cover letter or as part of the application process
Business Contact Details	• business telephone number(s) • business email addresses

Technical Data	• details about your own technology you use to access our systems, collected through log files, endpoint security and monitoring software, and similar means:
	  ○ Device information, such as unique device identifier, browser and operating system type and version
	  ○ IP address
	  ○ login data
	  ○ device location (where you give permission for this)

Usage Data	• information about your use of our information and communications systems • CCTV footage and other information obtained through electronic means such as electronic access records
Electronic Communications	• details about your use of Fiserv IT and communications systems, in some cases including the content of your communications • details and content of requests, concerns or complaints raised by you
Sensitive Personal Data	• in limited circumstances we may need to process personal data that may be deemed to be sensitive under local law. Where that is the case, we will only process this type of data where local laws allow. • special categories of personal data that we may collect and use include: ○ racial or ethnic origin

	○ political opinions or affiliations ○ trade union membership ○ any biometric data (where used to confirm your identity) ○ physical or mental health data ○ information relating to commission or alleged commission of criminal offenses, convictions, and any related legal actions
Other information provided by you	• You may provide us with a variety of other information in the context of an employment or similar relationship with us, including responses to internal surveys.

We may also collect, create, use and share data on an aggregated basis such as statistical or demographic data.

How is your personal data collected?

We collect personal information about individuals in the following ways:

- information provided by you
- information obtained from third parties (where permitted under local laws), such as:
  - former employers
  - employment agencies
  - personal references
  - credit reference agencies
  - other background check agencies
  - international sanctions lists from governments and monitoring agencies
  - insurance agencies
  - social security funds
  - third party service providers (such as payroll providers, medical providers, leasing companies, telecom operators, other)
  - public records sources
- information provided by recruiters or individuals who refer an individual for a job
- information provided from your managers and peers
- information provided to us by public authorities, courts or tribunals
- information provided to us by our personnel regarding dependents and beneficiaries
- data created or observed by us in the course of job-related activities during your employment/engagement with us.

If you fail to provide certain information when requested, we may not be able to hire you, perform all our legal or contractual obligations or carry out all activities regarding your employment or engagement such as payroll, benefits, tax and insurance and to ensure health and safety. It is important that the personal information that we hold about you is accurate and up-to-date. You should keep us informed if your personal information changes and wherever possible update your records on the self-service systems available to you.

How we use your personal data

We may use your personal data for the following purposes:

- **Human resources management**

  We use personal data for purposes of human resources management, including recruitment, establishment, maintenance and termination of employment relationship, career development, training, education, talent management, performance management, appraisals and disciplinary and grievance management, management forecasts and planning changes in our group structure, and providing information and references to potential or actual future employers.

- **Conducting employment-related checks**

  We use personal data to conduct employment-related checks, such as background checks, credit checks, anti-fraud checks, checks to prevent fraud and money laundering, and drug tests, in all cases to the extent permitted under applicable local law.

- **Staff administration and operational purposes**

  We use personal data for staff administration and operational purposes, such as managing absences, pay, benefits, compensation, stock administration, business travel, maintaining employee directories, and administering corporate expenses and reimbursements (including reviewing details of transactions made using corporate credit cards, corporate travel, and expenses submitted for reimbursement.

- **IT administration and security**

  We use personal data to administer and provide security for our IT assets, for instance controlling and enabling access to our systems and resources, managing authorization controls and user access, ensuring the security of our systems and resources, maintaining internal networks and IT systems, providing IT support, IT security monitoring, and incident response).

- **Physical security management**

  We use personal data to administer to manage physical security, including controlling and enabling access to our premises and physical assets.

- **Maintaining business records**

  We use personal data in connection with maintaining business records, including by storing staff communications, records, and work product, including as necessary or appropriate to operate Fiserv's business.

- **Monitoring**

  We use personal data in connection with our monitoring activities, such as where we monitor for compliance with Fiserv policies provided to you and to take action against staff who breach these policies, including through monitoring of IT and telephony usage and communications, checking which apps and files you use and which websites you visit and checking email addresses to which emails are sent and the content of the email (as permitted by local law), as well as how long you spend on different tasks online and monitoring of the physical premises (e.g., via CCTV or badge access data) solely to the extent permitted by applicable law, for purposes including to ensure that Fiserv systems and premises are used primarily for business purposes, have sufficient capacity for the needs of the business and are protected against cybersecurity threats such as malware and to efficiently manage our staff and their working time to ensure adherence to attendance rules and to facilitate performance improvement. The BUDDY portal lets you see information on how efficiently you are working. Reports from BUDDY about how you work are also shared with managers.

- **Automated Decisions**

  We will collect personal data (whether provided by you or collected by us from third parties) prior to your employment or engagement with us and as part of our continuing checks throughout your employment or engagement. We only do this where it is required by contract or law for the purposes of sanctions screening, anti-money laundering checks, background checks and assessment of your skill set for certain positions. No automated decision is made about your employment or engagement with us, as each decision is made with human involvement. For example, you will be automatically screened against international sanctions lists, and if you are identified as a listed in one of these lists, one of our representatives will check the accuracy of the automatic search and make the decision manually as to whether your application is able to proceed. Checking methods are regularly tested to make sure that they remain fair, effective and unbiased.

- **Emergency management**

  We use personal data in managing and responding to emergencies, including by contacting emergency contacts, family members, dependents, or other individuals in the event of an emergency.

- **Complying with our legal obligations or where necessary for exercising, establishing or defending legal claims**

  We use personal data to comply with our legal obligations and to exercise, establish, or defend legal claims. This may include the disclosure of your personal data to third parties in connection with proceedings or investigations anywhere in the world, such to public authorities, law enforcement agencies, regulators and third party litigants.

- **When changing our business structure**

  We may use personal data when changing our business structure, such as in the event of a business sale or corporate restructuring, where we may disclose your personal data to any potential acquirer of, or investor in, any part of our business (and to their legal advisors and consultants) for the purpose of that acquisition or investment. If required by applicable laws, we will obtain your express consent prior to disclosing your personal data to any such third party.

- **Carrying out obligations under client contracts**

  We may use personal data to comply with our contractual obligations with our customers. This may involve co-listening, recording of telecommunications between contact center agents and clients' customers, providing recordings to clients and/or client's customers.

- **Surveys and marketing activities**

  We may use personal data in connection with carrying out employee surveys, developing and carrying out marketing activities for products and services of the company (including introducing client referral programs), subject to our obtaining your consent where we are required to do so by applicable laws.

How long will you use my personal data?

We will use your personal data for as long as necessary based on why we collected it and what we use it for. This may include our need to satisfy a legal, regulatory, accounting, or reporting requirement.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure of your

personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

You can contact us for details of the retention periods applicable to your personal data. In general terms, we will retain your personal data for the duration of the recruitment process and/or your contract with us, and as long as necessary to comply with our legal, regulatory, accounting, and reporting requirements and to defend against legal claims. There are also certain types of information which are required to be retained for a certain period by law.

When personal data is no longer needed, we will destroy or remove information that makes the data personally identifiable in accordance with applicable law and our data retention policies.

Who we share your personal data with

We may share your personal data with other Fiserv group companies and any of the following for purposes consistent with this Privacy Notice, to the extent permitted by law:

- any third party where we are required by law to do so (such as tax authorities and similar government authorities);
- credit reference agencies;
- fraud protection and risk management agencies;
- identification and information verification agencies;
- third party vendors engaged to host, manage, maintain and develop our IT systems;
- our professional advisers, including lawyers and auditors;
- any third party that you have given us permission to use including healthcare providers;
- vendors we use to supply services in connection with the management or administration of staff, payroll, benefits, or otherwise in connection with our engagement with you;
- clients and their customers with respect to recorded telecommunications;
- potential buyers, transferees or merger partner or seller and their advisers in connection with an actual or potential transfer or merger of part or all of Fiserv's business or assets, or any associated rights or interests, or to acquire a business or enter into a merger with it (subject to our obtaining your consent where we are required to do so by applicable laws).

Your rights and choices

- **Accessing, correcting, or deleting your information**

  In some jurisdictions, applicable law may provide certain rights to individuals regarding their personal data, such as:

- **Access**. You may ask us if we are holding or processing your personal data and, if so, for a copy of the personal data we hold about you.
- **Correction**. If any personal data we hold about you is incomplete or inaccurate, you can request that we correct it, though we may need to verify the accuracy of the new data you provide to us.
- **Erasure**. You may ask us to delete or remove personal data where permitted.
- **Restriction**. You may ask us to suspend our use of your personal data in certain scenarios provided by law.

Where applicable law provides these (or other) rights, you may contact us at *DataPrivacyOffice@fiserv.com* or as otherwise specified *below* to exercise your legal rights. We may not be required to honor your request in all circumstances, and we will provide you with an explanation if we do not grant your request.

- **Complaints**

If you have a complaint about our handling of your personal data, you may contact our data protection officer / privacy officer at *DataPrivacyOffice@fiserv.com* or as otherwise specified below. We request that a complaint be made in writing. Please provide details about your concern or complaint so that our data protection officer can investigate it. We will take appropriate action in response to your complaint, which may include conducting internal discussions with relevant business representatives. We may contact you for additional details or clarification about your concern or complaint. We will contact you to inform you of our response to your complaint. You also may have a right to file a complaint with a national or local regulatory agency.

International transfers

Fiserv is headquartered in the United States, and it maintains offices and has service providers in other countries, such as:

- **The Americas**: Argentina, Belize, Bolivia, Brazil, Canada, Caribbean, Chile, Colombia, Costa Rica, Dominican Republic, El Salvador, Guatemala, Honduras, Mexico, Nicaragua, Panama, Paraguay, Peru, Puerto Rico, Uruguay, and the United States.
- **Europe**: Austria, Bosnia and Herzegovina, Bulgaria, Croatia, Czech Republic, Finland, France, FYROM, Germany, Greece, Hungary, Ireland, Italy, Netherlands, Norway, Poland, Portugal, Romania, Russia, Serbia, Slovakia, Spain, Switzerland, and the UK
- **Middle East & Africa**: Bahrain, Egypt, Kuwait, Qatar, Saudi Arabia, South Africa, and the UAE

- **Asia Pacific**: Australia, China, Hong Kong & Macau, India, Malaysia, New Zealand, Singapore, and South Korea.

Your personal data may be transferred to the United States or other locations outside of your state, province, country or other governmental jurisdiction where we or our service providers maintain offices and where privacy laws may not be as protective as those in your jurisdiction. If we make such a transfer, we will do so in compliance with the relevant law and we will require that the recipients of your personal data provide data security and protection in accordance with applicable law.

Security measures

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

Contact information

If you have any questions, concerns, or complaints about this Privacy Notice or our privacy practices, or to request access to your personal data, you may contact our Data Protection Officer at ***DataPrivacyOffice@fiserv.com***.

We also maintain a Data Privacy Hotline, which is available 24 hours per day from the United States, at +1 800-368-1000. The Hotline is the most appropriate contact for an urgent concern, such as regarding a potential breach regarding your personal data. We will work together with the local Privacy Officer to resolve your concerns.

Changes to this Privacy Notice

We may change this policy at any time and will notify you of any material changes to it by posting information about the change on the employee intranet or by other reasonable means before they take effect.

ADDENDUM

Privacy Notice for California Employees

California law requires that we provide you this notice about the collection and use of your personal information. We encourage you to read it carefully.

Effective Date: January 1, 2023

Introduction

This notice ("**Notice**") describes the categories of personal information that Fiserv, Inc. ("**Company**", "**we**", "**us**" and "**our**") collects about our employees who are California residents, and the purposes for which we use that information.

For purposes of this Notice, "**personal information**" has the meaning given in the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act (the "**CCPA**") but excludes information exempted from the CCPA's scope.

This Notice does not create or form part of any employment contract.

If you have questions about this Notice, please contact DataPrivacyOffice@fiserv.com.

The information below summarizes our collection, use and sharing of Personal Information during the last 12 months.

Information we collect about employees

Categories of personal information

For a description of data collected, see The data we collect about you above.

In certain cases we may ask you for additional information for purposes of monitoring equal opportunity and/or complying with applicable laws. We may also inquire about criminal records. We will do so only where permitted by applicable law.

Sources of personal information

For a description of sources of personal information, see How is your personal data collected above.

How we use personal information of employees

Purposes for which we use personal information

For a description of data used, see How we use your personal data above.

Sharing personal information

For a description of sharing of data, see Who we share your personal data with above.

Your California privacy rights

If you are a California resident, you have the rights listed below. However, these rights are not absolute, and we may decline your request as permitted by the CPRA.

- ***Information.*** *You can request the following information about how we have collected and used your Personal Information for the applicable period of time.*
- ***Access.*** *You can request a copy of the Personal Information that we maintain about you.*
- ***Correction.*** *You can ask us to correct inaccurate Personal Information that we maintain about you.*
- ***Deletion.*** *You can ask us to delete the Personal Information that we maintain about you.*
- ***Nondiscrimination.*** *You are entitled to exercise the rights described above free from discrimination. This means that we will not penalize you for exercising your rights by taking actions such as by denying you goods or services, increasing the price/rate of goods or services, decreasing the service quality, or suggesting that we may penalize you as described above for exercising your rights.*

How to exercise your rights

If you are a California resident, you may exercise your access, correction, and deletion rights as follows:

- *Visiting* www.fiserv.com/privacyrequests
- *Calling 1-888-999-1114*
- *Identify verification. The CCPA requires us to verify the identity of the individual submitting the request before providing a substantive response to the request. A request must be provided with sufficient detail to allow* us to understand, evaluate and respond. The requester must provide sufficient information to allow us to reasonably verify that the individual is the person about whom we collected information. A request may also be made on behalf of your child under 13.

- Authorized agents. California residents can empower an "authorized agent" to submit requests on their behalf. We will require the authorized agent to have a written authorization confirming that authority.

Sale or Sharing of Personal Information for cross-context behavioral advertising

We have not sold or shared, as those terms are defined in the CCPA, your Personal Information in the past 12 months.

Other information about this Notice

Third parties

This Notice does not address, and we are not responsible for, the practices of any third parties, which have their own rules for how they collect and use your personal information. Our links to third party websites or services are not endorsements.

Changes to this Notice

We reserve the right to change this Notice at any time. The "Effective Date" heading at the top of this Notice indicates when it was last revised. Any changes will become effective when we post the revised notice on our intranet.

Your obligations

It is your responsibility to ensure that information you submit does not violate any third party's rights.

You should keep your personal information on file with the Company up to date and inform us of any significant changes to it.

Privacy Notice for California Contractors and Candidates

California law requires that we provide you this notice about the collection and use of your personal information. We encourage you to read it carefully.

Effective Date: January 1, 2023

Introduction

This notice ("**Notice**") describes the categories of personal information that Fiserv, Inc. ("**Company**", "**we**", "**us**" and "**our**") collects about our contractors and candidates who are California residents, and the purposes for which we use that information.

For purposes of this Notice, "**personal information**" has the meaning given in the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act (the "**CCPA**") but excludes information exempted from the CCPA's scope.

This Notice does not create or form part of any employment contract.

If you have questions about this Notice, please contact DataPrivacyOffice@fiserv.com.

The information below summarizes our collection, use and sharing of Personal Information during the last 12 months.

Information we collect, use and share

The information collected, sources of information, how we use and share the information, would be limited, as appropriate, of the descriptions provided in the above sections:

- The data we collect about you
- How is your personal data collected
- How we use your personal data
- Who we share your personal data with

Your California privacy rights

If you are a California resident, you have the rights listed below. However, these rights are not absolute, and we may decline your request as permitted by the CPRA.

- ***Information.*** *You can request the following information about how we have collected and used your Personal Information for the applicable period of time:*
- ***Access.*** *You can request a copy of the Personal Information that we maintain about you.*
- ***Correction.*** *You can ask us to correct inaccurate Personal Information that we maintain about you.*
- ***Deletion.*** *You can ask us to delete the Personal Information that we maintain about you.*
- ***Nondiscrimination.*** *You are entitled to exercise the rights described above free from discrimination. This means that we will not penalize you for exercising your rights by taking actions such as by denying you goods or services, increasing the price/rate of goods or services, decreasing the service quality, or suggesting that we may penalize you as described above for exercising your rights.*

How to exercise your rights

If you are a California resident, you may exercise your access, correction, and deletion rights as follows:

- Visiting *www.fiserv.com/privacyrequests*
- Calling 1-888-999-1114
- Identify verification. The CCPA requires us to verify the identity of the individual submitting the request before providing a substantive response to the request. A request must be provided with sufficient detail to allow us to understand, evaluate and respond. The requester must provide sufficient information to allow us to reasonably verify that the individual is the person about whom we collected information. A request may also be made on behalf of your child under 13.
- Authorized agents. California residents can empower an "authorized agent" to submit requests on their behalf. We will require the authorized agent to have a written authorization confirming that authority.

Sale or Sharing of Personal Information for cross-context behavioral advertising

We have not sold or shared, as those terms are defined in the CCPA, your Personal Information in the past 12 months.

Other information about this Notice

Third parties

This Notice does not address, and we are not responsible for, the practices of any third parties, which have their own rules for how they collect and use your personal information. Our links to third party websites or services are not endorsements.

Changes to this Notice

We reserve the right to change this Notice at any time. The “Effective Date” heading at the top of this Notice indicates when it was last revised. Any changes will become effective when we post the revised notice on our intranet.

Your obligations

It is your responsibility to ensure that information you submit does not violate any third party’s rights.

You should keep your personal information on file with the Company up to date and inform us of any significant changes to it.