LAST UPDATED: 4th November 2022

Please contact us if you need a copy of this notice as of a particular date.

HR Privacy Notice

At Fiserv, Inc., the privacy and security of your data is of the utmost importance. We have implemented global policies and procedures to ensure that we take all appropriate steps to protect your data in everything we do.

This privacy notice relates to you if you are any of the following in relation to Fiserv where you are located in the EU or employed or engaged by a Fiserv company, which is in the EU:

- an employee;
- an applicant for any position (whether permanent or temporary and whether as an employee, contractor or contingent worker);
- a former employee;
- a contractor;
- a contingent worker;
- the dependent or beneficiary of any employee or former employee.

This notice will inform you about how we protect your personal data and tell you about your rights and how the law protects you. It overrides any similar notices previously 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.

We may change this policy at any time and will notify you of any significant changes to it before they take effect.

1. Important information and who we are

Controller

Fiserv is made up of different legal entities. This privacy notice is issued on behalf of the Fiserv group of companies so when we mention "Fiserv", "we", "us" or "our" in this privacy notice, we are referring to the relevant company in the Fiserv group responsible for handling your data. The member of the Fiserv group that is the controller of your data is the one with which you, your company or agency, or the person to whom you are a dependent or beneficiary has or had a contract.

We have appointed a data protection officer (DPO) who is responsible for overseeing questions in relation to this privacy notice. If you have any questions about this privacy notice, including any requests to exercise your legal rights, please contact the DPO using the details set out below.

Contact details

Our full details are:

Data Protection Officer, Fiserv

Email address: ***dpo@fiserv.com***

Postal address: Janus House

Endeavour Drive

Basildon

Essex

SS14 3WF

You have the right to make a complaint at any time to a data protection authority (for more information go to *https://edpb.europa.eu/about-edpb/board/members_en* and *https://ico.org.uk/global/contact-us/*.

Fiserv's Privacy Principles

All members of the Fiserv group are committed to the following privacy principles:

A. *We process Personal Data fairly and lawfully*

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

C. *We limit our access to, and use of Personal Data and we do not store Personal Data longer than necessary*

D. *Personal Data will be accurate and, where necessary, kept up-to-date*

E. *We implement data protection by design and default*

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

G. *We use appropriate security safeguards*

H. *We respect Data Subject rights as required by applicable data protection and privacy law*

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

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

2. 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	Description

Contact and identifying Information	• personal contact information:
	  ○ name, including any previous name;
	  ○ address;
	  ○ personal telephone number(s);
	  ○ personal email addresses;
	• date of birth
	• gender
	• nationality
	• nationally issued identifier (such as National Insurance or Social Security Number)
	• next of kin and emergency contact information
	• marital status and dependants
	• photographs

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

	• credit reference certificate • payment instrument details (company credit card) • T&E expenses
Employment Records	• Salary • leaves of absence (e.g. annual, parental) • 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 • disciplinary, capability and grievance information
Candidates and New Hire Data	• copy of driving licence, passport or other photographic ID • 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:
	  ○ IP address
	  ○ login data
	  ○ browser type
	  ○ 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 and in some cases content of business related telecommunications and emails • details and in some cases content of requests, concerns or complaints raised by you. For example if you raise a complaint to the Complaints Handling Hotline (for more information see **Complaints Handling Procedures** below)

Special Categories of Personal Data	• in limited circumstances we may need to process special categories of personal data. 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)
	  ○ health data

	○ information relating to criminal convictions

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

3. How is your personal data collected?

We collect personal information about you in the following ways:

- information provided by you
- information obtained from third parties (where permitted under local laws), such as:
  - former employers
  - employment agencies
  - 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 sources
- information provided from your managers and peers
- information provided to us by public authorities, courts or tribunals
- 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.

4. How we use your personal data

We will only use your personal data when doing so satisfies both the law and our privacy principles.

As part of that commitment, we will only use your personal data if we have an appropriate reason for doing so. Those reasons can be one or more of the following:

- Where necessary to perform a contract with you;
- Where processing your data is in our legitimate interest, and that interest is not overridden by your own interests, rights or freedoms;
- Where we are obliged by law to process your personal data in a particular way or it is necessary in the public interest or your vital interest to do so;
- You have consented to our processing your personal data.

Even where we have an appropriate reason for processing your personal data, we must ensure that we do so in a manner which is fair to you, and does not go beyond the reasons why we first collected your data.

Purposes for which we will use your personal data

Below is a high level list of the activities we may undertake which could involve your personal data, along with our reasons for carrying them out. Where one of our reasons for a particular activity is our legitimate interest, we have also explained what those interests are.

For simplicity, we have shortened references to our reasons for processing your personal data to “Contract”, “Legitimate Interest”, “Law” and “Consent”.

Activity (with examples)	Reason	Our legitimate interest (if relevant)
Human resources management (recruitment, establishment, maintenance and termination of employment relationship, career development, training, education, talent management, performance management, appraisals and disciplinary and grievance management)	• Contract • Legitimate Interest • Law	• Ensuring we comply with our contractual, legal and regulatory requirements • Keeping our records up to date
Background checks before and during employment	• Legitimate Interest • Law • Consent	• Ensuring we comply with our contractual, legal and regulatory requirements • (where permitted) preventing risks to the business, where applicants are shown to have engaged in fraud, or otherwise illegal or seriously improper conduct
Staff administration and operational purposes (absences, pay, benefits, compensation, stock administration, business travel, maintaining employee directories, enabling access to our systems and resources, managing authorisation controls, ensuring the security of our systems and resources, maintaining and monitoring usage of internal networks and IT systems, management forecasts and planning changes in our group structure)	• Contract • Legitimate Interest • Law	• Ensuring we comply with our contractual, legal and regulatory requirements • Keeping our records up to date • Enabling the efficient management of our staff • Financial planning and analysis
Monitoring access to Fiserv premises (checking that you are adhering to the attendance rules under Fiserv policies and allowing us to take action, including disciplinary action, against staff who breach these policies)	• Legitimate interests • Law	• Enabling the efficient management of our staff and their working time • Compliance with a legal obligation relating to the employment relationship, in applicable countries, to keep records of staff attendance

Security management (verifying your identity, preventing fraud other illegal or criminal activity and dishonest or otherwise seriously improper conduct, misuse of our products or services as well as the security of our IT systems, architecture and networks, and the security of our premises and assets, protecting our intellectual property, confidential information, detecting or preventing any inappropriate behaviour or breach of policies including by conducting background checks and operating CCTV).	• Contract • Legitimate Interest • Law	• Ensuring we comply with our contractual, legal and regulatory requirements • Ensuring the security of company premises, assets and client information held by Fiserv • Ensuring health and safety of employees, on-site contractors or contingent workers and visitors • Preventing and detecting fraud, other unlawful, or seriously improper conduct. Where permitted, this includes sharing your personal data with and making checks with third party databases. These databases keep a record of fraudulent or other seriously improper conduct; this can be checked by other organisations and may result in others refusing to employ you. If we learn that you have engaged in fraudulent or other seriously improper conduct, this may mean that an offer of employment is withdrawn, or that we take disciplinary measures which could result in termination of employment.
Making contact in an emergency	• Legitimate Interest • Law	• Ensuring we comply with our contractual, legal and regulatory requirements
Monitoring your use of Fiserv systems: to check that these are used primarily for business purposes and in line with Fiserv policies and to take action against staff who breach these policies; to ensure we have sufficient technology capacity for the needs of the business and to see if staff are working in an efficient manner; and to ensure we are protected against cybersecurity threats such as malware	• Legitimate Interest • Law	• Ensuring we comply with our contractual, legal and regulatory requirements • Improving the efficiency of our business operations

Potential and/ or actual litigation or investigations or requests concerning you, us or any group company or its officers	• Legitimate Interest • Law	• Ensuring we comply with our contractual, legal and regulatory requirements • Defending our legal rights • Keeping our records up to date
Potential disclosures to third parties in the context of mergers and/or acquisitions, Joint Ventures or other corporate restructuring	• Legitimate Interest • Law	• Improving the efficiency of our business operations • Growing our business
Carrying out obligations under client contracts (co-listening, recording of telecommunications between contact centre agents and clients' customers, providing recordings to clients and/or client's customers)	• Legitimate Interest	• Performance of client contracts • Quality assurance • Fraud prevention
Carrying out employee surveys, developing and carrying out marketing activities for products and services of the company (including introducing client referral programs)	• Legitimate Interest • Consent	• Assessing how employees relate to the company and enhance engagement • Growing our business

Treatment of special categories of personal data

We know that certain types of your personal data require higher levels of protection. The circumstances in which we are allowed to use special categories of personal data are more limited than other types of personal data. They are:

- in a few circumstances, with your explicit consent;
- where we need to use the data in connection with employment;
- where it is needed in the substantial public interest (such as in connection with our pension scheme or access to certain controlled facilities such as data centres).

We may also use special categories of your personal data where necessary in connection with legal claims, where doing so is needed to protect your (or someone else's) interests or where you have made the information publicly available.

Access to special categories of personal data will be limited to those who:

- need access to such data to perform normal job responsibilities or to provide services to us; and
- are bound by our policies, contract or other legal obligation to use and disclose the data only as we instruct them.

Examples of scenarios where we will process special categories of personal data are our records of your leaves of absence, medical records and sickness certificates to ensure Data Subjects' health and safety in the workplace and to ensure meaningful equal opportunity monitoring and reporting (where relevant). Prior to joining us, we carry out pre-employment background checks. To the extent permitted by local law, background checks may include credit history, medical reports and criminal record checks to comply with legal, contractual and regulatory requirements and in some cases also searches against international sanctions lists. These checks are conducted as a condition of employment and may be repeated during your employment.

In some cases, we use fingerprint and palm recognition technology to allow controlled access to our facilities that house customer data to ensure that we meet our obligations to our customers, ensure their data is protected and to prevent fraud.

To the extent possible, your Employee ID number (or other unique identifier) will be used as the identifier for you instead of your name for identification purposes. All special categories of personal data will be encrypted if transmitted electronically or secured in packaging if hard copy is sent by mail or delivery service and if faxed, the fax sending and receiving machines must be located in secure rooms.

Failure to comply with our policies as regards the use of data and all applicable privacy laws, or to undergo training, as appropriate, will amount to a serious misconduct, which may lead to the termination of employment or end of your assignment.

If you have any questions or concerns regarding this notice or our privacy policies and practices, please contact the Data Protection Officer at ***dpo@fiserv.com*** or the Global Privacy Office at ***dataprivacyoffice@fiserv.com***.

5. Automated Decisions and Monitoring in the Workplace

An automated decision is one made solely by automated means without any human involvement.

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.

We also have software on our Fiserv devices and hardware that monitor your access to our systems, premises, facilities and communications. For example, as permitted by local law, we check which apps and files you use and which websites you visit and we check email addresses and content. We also look at how long you spend on different tasks online. We do this to check if Fiserv policies are being followed, such as about use of our systems or working location; to ensure the security of our systems and information; to comply with legal, regulatory or contractual requirements and to look at how efficiently staff are working. The BUDDY portal lets you see information on how efficiently you are working. Reports from BUDDY about how you work are only shared with managers at a group level. We will only access or monitor your use of systems or premises to allow managers to review performance at work as part of their regular performance reviews, to conduct customer reviews or where we suspect a breach of our policies. No decision is made as a result of monitoring without human involvement.

You can contact our Data Protection Officer for more information on automated decision making. Please also see **Your individual legal rights** below.

6. Who we share your personal data with

Where we are permitted to, we may share your personal data with other Fiserv group companies and any of the following:

- 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, risk management agencies and law enforcement agencies where we reasonably consider this is necessary to prevent and/or detect crime;
- 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 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.

Where we do share your personal data with third parties, we will only do so where they will apply appropriate security measures to the data they receive from us.

7. International transfers

We share your personal data within the Fiserv group, including those outside the European Economic Area (EEA).

We ensure your personal data is protected by requiring group companies to apply our global policies and procedures and to legally commit to our privacy principles when processing your personal data.

These polices are called "binding corporate rules", a copy of them can be found here. Where our binding corporate rules do not apply to a group company for any reason, your data is processed in accordance with an alternative data transfer mechanism.

Some of our external third parties are based outside the European Economic Area (EEA) so their processing of your personal data will involve a transfer of data outside the EEA. These third parties include software support suppliers, software developers, cloud-based service providers, professional service providers and other IT service providers with servers or personnel located in the US, India or other locations.

Whenever we transfer your personal data out of the EEA to an external third party, we ensure it is protected by using one of the following safeguards:

- ensuring data is transferred only to a country that has laws that protect your personal data in the same way as it would be in the EEA.
- using a contract approved by the European Commission (sometimes called Model Clauses).

8. How we keep your data safe

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.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

You can contact us to obtain further details of the safeguards applicable to your personal data.

9. 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 unauthorised 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 for as long as reasonably necessary afterwards. There are also certain types of information which are required to be retained for a certain period by law.

10. Your individual legal rights

Under certain circumstances, you have rights under data protection laws in relation to your personal data. There may be legal or other reasons why we cannot, or are not obliged to, fulfil a request to exercise your rights. We will confirm what they are if that is the case.

You have a right to:

- **Access**. You are entitled to ask us if we are processing your personal data and, if so, for a copy of the personal data we hold about you and to check that we are lawfully processing it, as well as obtain other information about our processing activities.

- **Correction**. If any personal data we hold about you is incomplete or inaccurate, you can require us to correct it, though we may need to verify the accuracy of the new data you provide to us.
- **Erasure**. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law.
- **Object**. Where our reason for processing your personal data is for a legitimate interest you may object to processing if you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes.
- **Restriction**. You may ask us to suspend our use of your personal data in the following scenarios:
    - if you want us to establish the data's accuracy;
    - where our use of your personal data is unlawful but you do not want us to erase it;
    - where you need us to hold your data for a longer period than we usually would, because you need it to establish, exercise or defend legal claims; or
    - you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.
- **Transfer**. Where it is possible, we will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to personal data provided by you which you initially provided consent for us to use or where we used the information to perform a contract with you.
- **Withdraw consent.** Where our reason for processing is based on your consent, you may withdraw that consent at any time. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

You also have the right not to be subject to automated decision making that significantly affects you. The exercise of this right is not available to you in the following cases:

- The automated decision is required to enter into, or perform, a contract with you.
- We have your explicit consent to make such a decision.
- The automated decision is authorised by local law of an EU member state.

However, in the first two cases set out above, you still have the right to obtain human intervention in respect of the decision, to express your point of view and to contest the decision.

How to make an Individual Rights Request

Individuals may contact Fiserv to request that we take some action in connection with their personal data. Requests should be referred to the DPO: ***dpo@fiserv.com***

No fee usually required

You will not have to pay a fee to exercise any of your rights relating to your personal data. However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure you are entitled to exercise a right in respect of your personal data. This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

Processing your Information Request

We will respond to all legitimate requests promptly and, in any event, within any timeframes prescribed by applicable local laws. In general, we must respond to queries within one month from the receipt of the request, so it is important that requests are identified and sent to ***dpo@fiserv.com*** as soon as possible. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

In the event that we are not able to provide the information you requested, we will provide you with a written explanation for our decision. For example, we are not required to comply with a request to *erase* data if processing the data is necessary to: exercise freedom of expression and information; comply with law or legal claims; act in the interest of the public health or public interest; or support scientific or historical research purposes or statistical purposes.

Any transmission of your personal data will be handled in a secure manner.

11. Complaints Handling Procedures

Should you have any complaints or enquiries related to:

- Our handling of your individual rights as a data subject;
- Our compliance with our binding corporate rules;
- Our privacy practices generally;

you may contact our Data Privacy Hotline at **+1 800-368-1000**, which is available 24 hours per day. The Hotline is the most appropriate contact for an urgent concern, such as a potential breach regarding your personal data, and we will work together with the Data Protection Officer to resolve your concerns.

Alternatively, you may contact our Data Protection Officer and local privacy officers at ***dpo@fiserv.com***.

You also have the right to make a complaint at any time to a data protection authority (for more information go to *https://edpb.europa.eu/about-edpb/board/members_en* and *https://ico.org.uk/global/contact-us/*.