Payment Systems Regulator

Data Privacy Notice

V2.0

October 2026

PSR/OPS010/V2

Contents

1	Overview	3
2	General Data Processing Activities	4
3	Data processing for Regulatory, Compliance Monitoring and Enforcement Purposes	19
4	Glossary	26

1 Overview

How and why we use your personal data

1.1 The Payment Systems Regulator (PSR) respects your privacy and is committed to protecting your personal data. The PSR collects and processes personal data that it needs to carry out its statutory functions and to operate as a public body, including ensuring that it is staffed appropriately.

This privacy notice will inform you as to how we look after your personal data and tell you about your privacy rights and how the law protects you.

It aims to give you information on how we collect and process your data, including any data you may provide through our website.

It is important that you read this privacy notice together with any other privacy notice or fair processing notice we may provide or direct you to on specific occasions when we are collecting or processing personal data about you, so that you are fully aware of how and why we are using your data. This privacy notice supplements the other notices and is not intended to override them.

This privacy notice does not deal substantively with the processing of personal data for job applications. The Financial Conduct Authority (FCA) carries out Human Resources and recruitment functions on behalf of the PSR. To learn how the FCA handles personal data for job applications, read their applicant privacy notice.

Background

Controller – who we are

1.2 The PSR is the controller and responsible for your personal data (collectively referred to as "we", "us" or "our" in this privacy notice). Where the PSR is a joint controller with the Financial Conduct Authority (the "FCA"), each controller is responsible for its own compliance with the Data Protection Legislation.

The PSR is a registered data controller under the Information Commissioners Office ("ICO"), our registration number is ZA058079. The PSR is a wholly owned subsidiary of the FCA.

Third-party links

1.3 The PSR's website may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave the PSR website, we encourage you to read the privacy notice of every website you visit.

2 General Data Processing Activities

2.1 This section addresses our data processing activities for "general" purposes, that is for purposes other than processing for law enforcement purposes (which is dealt with in part 3).

The personal data we collect about you

- **Personal data**, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data). Depending on the purpose and context, we may collect, use, store and/or transfer different kinds of personal data about you which we have grouped together as follows:
- **Identity Data** includes first name, maiden name, last name, username, or similar identifier, marital status, title and date of birth.
- **Contact Data** includes billing address, delivery address, email address and telephone numbers.
- **Financial Data** includes bank account and payment card details and information about the financial status of you or your business, including ownership structures and shareholdings etc.
- **Transaction Data** includes details about payments to and from you.
- **Employment and Education Data** includes employment history, absence records, schools and universities attended and qualifications.
- **Family Data** includes details on family members, dependents and next of kin.
- Details of **complaints, incidents and grievances**.
- **Technical Data** includes internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access this website.
- **Profile Data** includes your feedback and survey responses.
- **Usage Data** includes information about how you use our website.

2.2 Save where specifically required in accordance with our operations and functions (as described in more detail below) or in relation to employment issues, we do not collect any special categories of personal data about you (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health and genetic and biometric data). We may however collect information about criminal convictions and offences. Such 'criminal offence data' shall be processed in compliance with Article 10 of the UK GDPR.

2.3 We do not knowingly collect data relating to children.

How is your personal data collected?

2.4 Depending on the purpose and context, we use different methods to collect data from and about you including through:

- **Direct interactions**. You may give us personal data such as your Identity, Contact and Financial Data by corresponding with us by post, phone, email or otherwise.
- **Third parties, other regulators or public bodies**. We may receive personal data from third parties including the participants of the payment systems we regulate, such as Pay.UK in its role as payment system operator of the UK's national retail payment system, Faster Payments. Other examples include regulators or public bodies. Our contractors may receive Technical Data from analytic providers within the European Union (EU) or based outside the EU, such as Google. Different levels of protection are afforded to data processed within the EU and outside of the EU. We shall ensure that all personal data received from outside of the EU is subject to appropriate safeguards.
- **Automated technologies or interactions**. As you interact with us, we may automatically collect Technical Data about your equipment, browsing actions and patterns. We collect this personal data by using cookies and other similar technologies. We may also receive Technical Data about you if you visit other websites employing our cookies. Please see our cookie policy for further details.

Purposes for which we will use your personal data

2.5 We will only use your personal data when the law allows us to. This section sets out a high-level summary of the purposes for which the PSR will process personal data. Further detail on the purposes and categories of personal data and lawful basis for processing can be found in the section below. Most commonly, we will use your personal data in the following circumstances:

a. Where we need to carry out a task in the public interest or in the exercise of official authority, such as where we are carrying out our statutory functions, including our monitoring functions.

b. Where we need to comply with a legal or regulatory obligation such as when dealing with Data Subject Access Requests or requests for information under the Freedom of Information Act.

c. To provide you with any information or services that you ask for, as well as to reply to your correspondence.

d. To maintain a record of our contact with you (as well as keeping track of our interaction with you, this helps us identify you if you contact us again and therefore provide a better level of service to you).

e. To identify and analyse issues, risks and emerging trends in relation to the firms and markets that we regulate.

f. Where we have otherwise obtained your consent.

Ways we may use your personal data and our legal bases for doing so

2.6 We have set out below, a summary description of the ways we may use your personal data, and which of the legal bases we would rely on to do so. Further detail in relation to our main areas of work can be found in the specific sections of this notice.

Note that we may process your personal data for more than one ground depending on the specific purpose for which we are using your data. Please contact us if you need more details about the specific legal grounds we are relying on to process your personal data.

Purpose/Activity	Type of data we will collect	Lawful basis for processing
To carry out our statutory functions, including our regulatory, compliance monitoring, enforcement and competition functions (but not including our functions as an employer – these are addressed separately below)	(a) Identity (b) Contact (c) Financial (d) Transaction (e) Profile (f) Employment and Education (g) Family (h) In limited cases, Special Categories of Personal Data	• To the extent of processing special categories of personal data, we rely on Article 9(2)(a), (e) or (g) of the GDPR as appropriate, that is that the data subject has given explicit consent, the processing relates to personal data which are manifestly made public by the data subject and/or processing is necessary for reasons of substantial public interest. • When dealing with Data Subject Access Requests, requests for information under the Freedom of Information Act or other statutory regimes so far as we process personal data in accordance with them, we rely on Article 6(1)(c) (processing is necessary for compliance with a legal obligation to which the PSR is subject). • For all other processing of personal data, including pursuant to and when monitoring compliance with directions or requirements which might lead us to take regulatory or enforcement action, we rely on Article 6(1)(e) of the GDPR, 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 the PSR.
To maintain contact details of stakeholders	(a) Identity (b) Contact	• Necessary for public interest (such as keeping interested parties informed about our work) (Article 6(1)(e) of the GDPR).
Maintaining contact details for journalists to receive and distribute information	(a) Identity (b) Contact (c) Profile	• Necessary for public interest (Article 6 (1)(e) of the GDPR).

Purpose/Activity	Type of data we will collect	Lawful basis for processing
To hold meetings, conferences, seminars, workshops and other PSR events	(a) Identity (b) Contact (c) Profile (d) In limited cases, Special Categories of Personal Data	• Necessary for public interest (such as keeping interested parties informed about our work and engaged with the PSR's work) (Article 6 (1)(e) of the GDPR). • To the extent of processing special category data, we rely on Article 9(2)(a) or (g) of the GDPR as appropriate, that is that the data subject has given explicit consent and/or processing is necessary for reasons of substantial public interest. For example, when you register to attend one of our events, we may collect details about your dietary and accessibility requirements.
To manage enquiries and complaints	(a) Identity (b) Contact (c) Complaints, incidents and grievances (d) Profile (e) In limited cases, Special Categories of Personal Data	• To the extent of processing special categories of personal data, we rely on Article 9(2)(a), (e) or (g) of the GDPR as appropriate, that is that the data subject has given explicit consent, the processing relates to personal data which are manifestly made public by the data subject and/or processing is necessary for reasons of substantial public interest. • For all other processing of personal data, we rely on Article 6(1)(e) of the GDPR, 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 the PSR.
To carry out consultations, discussions, market reviews, research and to gather and publish evidence and opinions	(a) Identity (b) Contact (c) Profile (d) In limited cases, Special Categories of Personal Data	• To the extent of processing special categories of personal data, we rely on Article 9(2)(a), (e) or (g) of the GDPR as appropriate, that is that the data subject has given explicit consent, the processing relates to personal data which are manifestly made public by the data subject and/or processing is necessary for reasons of substantial public interest. • For all other processing of personal data, we rely on Article 6(1)(e) of the GDPR, 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 the PSR.
To procure suppliers and process supplier payments	(a) Identity (b) Contact (c) Financial (d) Transaction	• Necessary for public interest (Article 6 (1)(e) of the GDPR). • Necessary for the performance of a contract or prior to entering into a contract (Article 6(1)(b) of the GDPR).

Purpose/Activity	Type of data we will collect	Lawful basis for processing
To establish, exercise or defend legal claims	(a) Identity (b) Contact (c) Financial (d) Transaction (e) Details of complaints, incidents and grievances (f) In limited cases, Special Categories of Personal Data	• Necessary for public interest (Article 6 (1)(e) of the GDPR). • Necessary for the performance of a contract or prior to entering into a contract. (Article 6(1)(b) of the GDPR). • To the extent of processing special categories of personal data we rely on Article 9(2)(f) of the GDPR, that is that processing is necessary for the establishment, exercise or defense of legal claims.
To pass personal information to accountants, consultants, lawyers, bankers, auditors, insurers and/or other professionals for the purpose of obtaining professional advice where appropriate	(a) Identity (b) Contact (c) Financial (d) Transactional	• Necessary for public interest. (Article 6(1)(e) of the GDPR). • Necessary to comply with our legal obligations (Article 6(1)(c) of the GDPR).
To administer and protect our business and the PSR's website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	(a) Identity (b) Contact (c) Technical (d) Profile	• Necessary for public interest. (Article 6(1)(e) of the GDPR). • Necessary to comply with our legal obligations (Article 6(1)(c) of the GDPR).
To use data analytics to improve our website, products/services	(a) Technical (b) Usage	• Necessary for public interest. (Article 6(1)(e) of the GDPR).

Purpose/Activity	Type of data we will collect	Lawful basis for processing
To use analytical tools and advanced technologies, including machine learning and artificial intelligence, to support the delivery of our statutory functions and make efficient use of our resources	(a) Identity (b) Contact (c) Technical (d) Usage (e) Profile (f) Other personal data, where necessary and proportionate for relevant to the specific purpose for which the tool is used	• Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the PSR (Article 6(1)(e) of the GDPR). • Where we use personal data in the development, testing or assurance of these tools, we will do so only where this is necessary and appropriate for the relevant purpose and with suitable safeguards.
To assist in collecting regulatory fees from fee payers	(a) Identity (b) Contact	• Necessary for public interest. (Article 6(1)(e) of the GDPR). • Necessary to comply with our legal obligations. (Article 6(1)(c) of the GDPR).
To pass personal information to Pay.UK, and the Bank of England, to enable them to engage with payment service providers in relation to the FPS reimbursement rules and the CHAPS reimbursement rules.	(a) Identity (b) Contact	• Necessary for the performance of a task carried out in the public interest and/or in the exercise of official authority vested in the PSR (Article 6(1)(e) of the GDPR).

Sharing of your personal data, international transfers, data security and retention

Sharing of your personal data

2.7 Depending on the purpose and context, we may have to share your personal data with Internal Third Parties and/or External Third Parties (as set out in the Glossary in part 4 of this privacy notice) for the purposes set out in the table in paragraph 3 above.

We require all third parties to respect the security of your personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

Further detail of when we may share personal information in relation to our main areas of work can be found under the specific sections of this notice.

2.8 The Government has announced plans to consolidate the Payment Systems Regulator (PSR) into the Financial Conduct Authority (FCA). While this transition is underway, the PSR and FCA are working closely together to support a smooth transfer of responsibilities.

During this period, FCA staff may increasingly support the delivery of PSR functions and services. Where needed, this may involve FCA staff receiving, sharing or processing personal data provided to the PSR. As a result, your contact for a PSR matter may be based at the FCA, and information you provide to the PSR may be received by, shared with, or processed by FCA staff where necessary to support PSR functions and services.

2.9 We may also use internally developed analytical tools and advanced technologies, and IT services provided by third parties through the cloud, including tools using machine learning and/ or artificial intelligence, to support our work. We may also use third-party cloud-based IT services for these purposes. Where a third-party provider processes providers process personal data for us, we require them to process it only for specified purposes, in accordance with our instructions and subject to appropriate contractual, technical and organisational safeguards.

International transfers

2.10 Given our role as a regulator, we occasionally share personal data with other regulators, public authorities and law enforcement agencies outside the UK or European Economic Area, where applicable. Before we transfer personal data outside the UK or European Economic Area, we deploy robust processes to ensure that appropriate safeguards are put in place to protect any personal data included in such a transfer. If you would like to obtain more details about the safeguards that we have in place with regard to any personal data about you that we may transfer to a particular country, please contact us.

Where any analytical tools, advanced technologies or related cloud services involve access to personal data from outside the UK or European Economic Area, where applicable EU, we will ensure that appropriate safeguards are in place before the transfer or access takes place.

Data security

2.11 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. Appropriate technical and organisational measures have been put in place to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. 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.

Where the FCA and PSR are joint controllers, each party will be responsible for complying with Data Protection Legislation. The FCA and PSR will assist each other in meeting their obligations under Data Protection Legislation, including consulting with each other and assisting each other in responding to suspected personal data breaches.

How we use your data when you contact us regarding a general enquiry

2.12 We process your personal data for various reasons which includes, addressing your enquiries or concerns, when you subscribe to our newsletters, or attend our online or in-person events or meetings, and when we have business relationship with you.

The personal data we use

2.13 When you contact us with a general enquiry, including by email, telephone, letter, and electronic contact form, we will ask for and/or use some personal data such as your name, email address, phone number and (if corresponding by letter) your address. We need this information if you contact us electronically (for example by email, webchat or contact form) so that we are able to respond to you. However, if you contact us by telephone, you are under no obligation to provide any personal data to us and you can carry out your call on an anonymous basis. (Though anonymous, your call will still be recorded for staff evaluation and training purposes, unless you specifically ask for the recording of your call to be paused. You can request that the recording is paused at any time during your call.)

When you contact us about a PSR matter, FCA staff may handle or support your contact may be handled or supported by FCA staff as part of the transition arrangements described in the "Sharing of your personal data" section. This may include support from FCA staff supporting PSR contact-handling functions, such as the FCA contact centre and switchboard.

Depending on the reason you contact us, we may also collect other personal data about you or other individuals that you may have chosen to provide.

How we collect personal data

2.14 People can contact us with a general enquiry in various ways, whether they are a firm, consumer or anyone else who wishes to ask us a question or report something to us. The homepage of the PSR website has details on how you can get in touch with us - including by email, telephone, letter, live web chats and electronic contact forms.

We offer a third-party translation service for individuals when English is not their first language. The company that provides this service does not record the calls or retain any information about individuals mentioned during the calls.

Depending on the reason you contact us, we may ask you to provide personal data about you or other individuals.

Why we collect personal data when you contact us

2.15 Depending on the purpose and context, we may use your personal data for a number of important reasons:

- to provide you with any information or services that you ask for, as well as to reply to your correspondence;
- to analyse the use and performance of our Correspondence function, such as where in the country users of our helpline come from, what type of questions they are asking, and whether the service was able to give them useful information or guidance;
- to maintain a record of our contact with you (as well as keeping track of our interaction with you, this helps us identify you if you contact us again);
- to quality assess the service provided to you by our Correspondence staff, identify any areas for improvement and develop staff training;
- to identify and analyse issues, risks and emerging trends in relation to the firms and markets that we regulate; and
- to process any complaints made against us by you or relating to our interaction with you.

The lawful basis for us using personal data in these ways

2.16 We use this personal data to respond to queries or reports from firms and members of the public, and to improve the quality of our service, under Article 6(1)(e) of the UK GDPR (it is necessary for performance of a task carried out in the public interest). We do not usually explicitly ask for any special categories of data from people who contact us but, depending on the nature of the correspondence and the information the individual chooses to give us, it is possible that some special categories of personal data may be included in the information that we collect or record. To the extent that we do process any special categories of personal data as part of our complaints handling work, we do so under Article 9(2)(g) of the UK GDPR (it is necessary for reasons of substantial public interest) and Section 10(3) of the DPA 2018, in that it meets a condition in Part 2 of Schedule 1 of the DPA 2018.

When our Correspondence function shares personal data

2.17 The FCA speech and text analytics tool transfers information to be stored on virtual servers which can be accessed by third-party technical support teams in the United States of America (USA) and India, where necessary and explicitly allowed by us. To ensure that adequate protection is in place for any personal data being accessed outside the EU in this way, we have implemented robust contractual and security safeguards with the third-party provider. It is not intended that any personal data held by the PSR should be accessed by the third-party technical support teams in this way. Backups of the information are stored on physical servers by the same third party in the UK. If you would like to obtain more details about these safeguards in relation to your personal data, please contact us.

Information collected by our Correspondence teams:

- may be shared with the FCA, for example where there is a request under the Freedom of Information Act or otherwise in relation to one of the areas where the FCA provides the PSR with services. A list of services provided by the FCA to the PSR can be found in the Glossary under the definition of Internal Third Parties;
- may be shared with External Third Parties, for example other domestic and international regulators where appropriate and required in the context of our role as a regulator and public body;
- is occasionally shared with other third-party providers that assist with specific PSR campaigns or act as a supplementary contact point if required; and
- is occasionally shared with research companies to undertake thematic reviews and other research exercises.

Other than that, the information will be shared internally within other areas of the PSR as required, such as a relevant PSR project team and/or teams undertaking research and analysis as appropriate. The information may also be used by other areas of the PSR to identify and analyse emerging trends and risks and, more generally, to help us to fulfil effectively our statutory functions and relevant legal obligations.

Change of purpose

2.18 When you contact us with a general inquiry, we will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact us.

If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

How we use personal data in our surveys, consultations, market reviews, studies and other research work

2.19 Here we set out how and why we use personal data to enable us to conduct our research work.

The personal data we use

2.20 The PSR may undertake a range of research work when performing its statutory functions, including to advance any of its objectives. Such research work includes conducting surveys and consultations, issuing discussion papers, conducting market reviews or studies, and responding to super complaints. In conducting such work, we try to keep our collection of personal data to a minimum. We use anonymised data as

far as possible and only ask for personal data where we believe it is necessary for the purpose of the exercise in question.

The type of personal data that we typically use as part of our research work is normally limited to contact details (of the person completing a PSR information request, questionnaire or survey or responding to a consultation or discussion paper) and personal views and opinions of consumers and those who submit questionnaires, surveys and consultation responses to us.

We also occasionally, where required for the purposes of a specific project, use financial information, dates of birth and location data as part of our research, although this is usually either aggregated or pseudonymised by us when used in research.

How we collect this personal data

2.21 We collect personal data in a variety of ways to conduct our research work. To get a holistic and accurate view of the markets, understand consumer behaviour and properly identify issues, trends and risks, we collect personal data from third parties as well as from individuals directly.

Below are some examples of how and from where we collect personal data for this purpose:

- information requests, questionnaires and surveys by us and by our third-party research providers;
- social media analytics tools which gather information (such as X, Facebook, blogs, forums and mainstream media) to analyse real-time consumer opinions; and
- data collection and public consultation and discussion papers for market reviews and reports, all of which are published on our website.

Why we use this personal data

2.22 We use this personal data to ensure that we are able to fulfil our statutory functions and obligations under applicable law and, in particular, to help us:

- understand how well competition and innovation is working in particular payment systems;
- Understand how well the interests of users are being promoted in the development and operation of payments systems.
- identify areas of concern, inform our strategic thinking as a regulator and help us decide if we need to intervene or publish guidance;
- manage and prioritise decision making within the PSR in a way which reacts appropriately to emerging risks and trends; and
- build strong relationships with consumer groups, the industry, media and stakeholders to reflect our accountability to Parliament, enrich our insight, enhance our credibility and maximise our usefulness to the public.

The lawful basis for us using this personal data

2.23 Our research work is essential to enable us to understand the payment systems that we regulate and to carry out effectively our statutory functions and obligations as a regulator of payment systems.

The lawful basis for collecting and using personal data will depend on the specific context in which we collect it. If it is necessary for the performance of a task carried out in the public interest, we can use this personal data under Article 6(1)(e) of the UK GDPR and Section 8(c) of the DPA 2018. Where you have agreed to take part in PSR research, or responded to a discussion paper or consultation, and agreed for us to use your personal information, we may also rely upon the lawful basis of consent.

To the extent that we use any special categories of data in our research work, we do so under Article 9(2) (a),(e) or (g) of the UK GDPR (the data subject has given explicit consent, processing relates to personal data which are manifestly made public by the data subject or it is necessary for reasons of substantial public interest) and Section 10(3) of the DPA 2018, in that it meets a condition in Part 2 of Schedule 1 of the DPA 2018.

Different rules apply to the processing of personal data for certain research and statistical work under the UK GDPR and the DPA 2018. This means that if we ensure that appropriate safeguards are in place, including adopting technical and organisational measures (such as, where possible, pseudonymisation techniques), we are entitled to use for research or statistical purposes information that we have already collected from you for a different purpose. We would not use personal data in this way if it was likely to cause substantial damage or distress to individuals. We also do not use this research or statistical data to make decisions about or take measures against particular individuals. All our research work is conducted in the public interest.

The rules about research and statistical work in the UK GDPR and the DPA 2018 also mean that certain rights that you may have in respect of your personal data under the UK GDPR (such as the right to restrict or object to processing activity) may not apply to the personal data that we use about you as part of our research work. If you would like more information about this, please contact us.

When we share personal data used to undertake our research work

2.24 Given our role as a regulator, where necessary and appropriate, we may share personal data with other regulators, public authorities and law enforcement agencies both inside and outside the UK and the EU.

In most cases, we publish responses to our surveys, consultation papers, market reviews/studies and other research work, along with our conclusions and associated report, on our website. That said, in the majority of cases and where possible, we remove any personal data from the responses and associated reports that we share or make public in this way.

We may also use third-party research agencies and data analytics tools to help us with our research work.

When this personal data is transferred outside the EU

2.25 It is rare for us to transfer personal data collected as part of a research exercise in the UK. However, as mentioned above, given our role as a regulator we occasionally share personal data with regulators, public authorities and law enforcement agencies outside the EU.

We may use third party research agencies, data analytics tools and other third-party suppliers to help us with our research work. Some of these third parties transfer data outside the EU in their provision of services to us.

Before we transfer personal data outside the EU, we deploy robust processes to ensure that appropriate safeguards are put in place to protect any personal data included in such as transfer. If you would like to obtain more details about the safeguards that we have in place with regard to any personal data about you that we may transfer to a particular non-EU country, please contact us.

How we use personal data in our competition work

2.26 Here we set out how and why we use personal data to enable us to perform our competition work.

2.27 The PSR is a concurrent regulator alongside the Competition and Markets Authority (CMA) for payment systems in the UK. The PSR has the power to apply and enforce the Chapter I and Chapter II prohibitions under the Competition Act 1998 (CA98), which mirror the concepts of Articles 101 and 102 of the Treaty on the Functioning of the European Union (TFEU).

The PSR also has the power (under the Company Directors Disqualification Act 1986) to apply to the court for an order disqualifying a director from acting as director, if the company of which he is a director has breached competition law.

Whilst carrying out our competition work or monitoring activity we may be provided with your personal information. This may consist of:

- your name and other identity data;
- your email address and other contact data;
- your email or personal correspondence held by the company or business under investigation; and/or
- other personal information held by the company or business under investigation.

The lawful basis for us using this personal data

2.28 The lawful basis for collecting and using your personal data will depend on the specific context in which we collect it. When we are exercising our competition functions we use this personal data under Article 6(1)(e) of the UK GDPR (it is necessary for the performance of a task carried out in the public interest) and Section 8(c) of the DPA 2018 and, to the extent that we use any special categories of personal data or criminal

records, under Article 9(2)(g) (it is necessary for reasons of substantial public interest) and Sections 10(3) and (5) of the DPA 2018 (it is necessary for the exercise of the PSR's statutory functions and it meets a condition set out in Parts 1, 2 or 3 (as applicable) of Schedule 1 of the DPA 2018).

When we share personal data we hold in relation to our competition work

2.29 There are a number of reasons we may need to share personal data with other parties. For example, we may share information with the parties involved in investigations and their legal representatives. We may share your personal information with other regulators such as the CMA or the European Commission (EC), if we are required to do so in accordance with the specified purposes. These other regulators will handle any personal information sent to them in accordance with their own privacy notices.

When this personal data is transferred outside the EU

2.30 It is rare for us to transfer personal data collected as part of our competition work outside the EU. However, given our role as a regulator we may occasionally share personal data with regulators, public authorities and law enforcement agencies outside the EU.

How we use your personal data when you attend one of our events

2.31 Here we set out how and why we use personal data when you register or otherwise agree to attend a meeting, seminar, conference, workshop or other PSR event.

Why we collect personal data

2.32 As a regulator, we hold a range of events from time to time which are necessary to carry out our statutory functions in the public interest (such as keeping interested parties informed about our work and to assist stakeholders in engaging with our work).

When you register or otherwise agree to attend one of our events, we will collect personal information from you, including:

- Your name;
- Job title;
- Your company email address;
- Company address;
- Company phone number; and
- IP address of the device you use to access our website.

In addition, when you register or otherwise agree to attend one of our events, where appropriate, we may also collect details about your dietary and accessibility requirements.

Occasionally photographs and video footage may be taken at our events and used for post-event publicity.

The lawful basis for us using this personal data

2.33 The lawful basis for collecting and using your personal data is Article 6(1)(e) of the UK GDPR (it is necessary for the performance of a task carried out in the public interest) and Section 8(c) of the DPA 2018 and, to the extent that we collect and use any special categories of personal data, we would rely upon Article 9(2)(a) (the data subject has given explicit consent) and/or Article 9(2)(g) of the UK GDPR (the processing is necessary for reasons of substantial public interest) as appropriate.

When we share personal data

2.34 When we hold a PSR event, we will usually share your details (full name, position & company name) with other participants. We may circulate an attendee list in advance of the event including a table plan where appropriate. We may also share this information with other UK or EU regulators where this is relevant to their work.

We may share the attendee list with the venue, where required, such as for security and fire regulation purposes. We may share dietary and accessibility requirements with the venue or other parties where necessary for the event.

How we use your personal data in our regulatory fee collection

2.35 Here we set out how and why we use personal data when our regulatory fees are collected from the industry.

Why we collect personal data

2.36 Under the Financial Services (Banking Reform) Act 2013, the FCA raises fees to recover the costs of carrying out our statutory functions and passes them to us. This will include:

- Your name;
- Your job title;
- Your company email address; and
- Your company phone number

The lawful basis for us using this personal data

2.37 The lawful basis for collecting and using your personal data is Article 6(1)(c) (it is necessary under legal obligation) and (e) (it is necessary for the performance of a task carried out in the public interest) under the UK GDPR.

When we share personal data

2.38 The FCA process the collection of PSR regulatory fees and so we will share names and contact details with the relevant parts at the FCA, such as their revenue team.

3 Data processing for Regulatory, Compliance Monitoring and Enforcement Purposes

Exercising our statutory powers

3.1 This section explains how and why we use personal data when exercising our statutory powers to fulfil our regulatory, compliance, monitoring and enforcement functions.

3.2 Our approach to exercising our statutory powers is to hold the industry to account. We will take formal regulatory action to regularise industry behaviours, in line with our payment system objectives; for example, where we have identified areas of regulatory concern and:

1. the solutions proposed by industry do not take into account criteria or measures we have set, or do not satisfactorily address our concerns;
2. industry or individual regulated parties are behaving in a way which could run counter to our existing directions;
3. progress against any priorities we have set for industry is too slow; or
4. the outcomes we expect to be delivered, in relation to those priorities, are not being delivered satisfactorily.

We monitor industry progress closely and ensure that our approach remains fit for purpose in light of changes in the market, law and regulation.

We will use enforcement action where appropriate in response to industry behaviours which are either contrary to, or have fallen short of, our expectations and to deter future compliance failures. For example, where industry or individual participants are failing to comply with requirements of domestic or EU legislation for which the PSR is the competent authority, including failure to comply effectively or on time with directions that we have given.

In order to ensure that we are properly able to perform our regulatory, compliance, monitoring and enforcement functions and advance the payment system objectives we also have powers to gather information and conduct formal investigations ('Investigations').

Not every regulatory concern or suspected compliance breach that we become aware of will result in the use of our formal information gathering and investigative powers. We may also gather information and make enquiries of regulated parties on an informal basis.

Likewise, not every use of our formal information gathering and investigative powers results in us taking regulatory or enforcement action. The way in which we process

personal data will depend on the nature of our Investigations and the outcomes which we decide are most appropriate.

Where the making of enquiries or an Investigation relates to either a regulatory or civil matter, processing is subject to the GDPR. Processing in the context of a criminal investigation or proceedings will be subject to provisions of the DPA 2018, which implements the LED into UK law. The PSR is a competent authority for the purposes of the enforcement provisions of the DPA 2018.

Processing personal data

3.3 Examples of the ways in which we may process personal data when carrying out our regulatory, compliance, monitoring and enforcement functions include:

- gathering and analysing information such as end user complaints, whistleblowing information, communications and market monitoring data;
- issuing information requests, on either a voluntary basis or using our formal information gathering powers, including for monitoring purposes in respect of compliance with our directions or requirements, and receiving the responses to these;
- in the case of the Faster Payments APP scams reimbursement requirement, receiving business contact information from Pay.UK to engage with parties regarding suspected compliance failures;
- conducting an investigation and exercising, through appointed Investigators, additional information gathering powers;
- managing projects where there is a prospect of taking regulatory action and run enforcement cases, including evidence analysis and storage in line with our statutory obligations, preparing project/case documentation, and managing proceedings before the PSR's Enforcement Decisions Committee, other tribunals, appeal bodies, and civil or criminal courts;
- engaging with parties who are the subject of enquiries/an investigation being conducted by us, including evidence-gathering, fulfilling disclosure obligations and holding discussions to agree appropriate outcomes;
- in the case of enforcement action into a suspected compliance failure, making a determination about that failure, considering appropriate sanctions and calculating penalties;
- fulfilling money laundering reporting obligations;
- cooperation with domestic and overseas authorities; and
- publishing outcomes resulting from regulatory or enforcement action.

The information that we have provided in this notice (particularly in relation to sharing information with third parties) is not exhaustive. If you want to understand more about how we use personal data or you have any particular questions about our enforcement processing activities, please contact us.

The personal data we use

3.4 Given the nature of our work, we use a variety of personal data (including special categories of personal data and criminal offence data) to exercise our enforcement functions and we may access a variety of personal data in the course of performing our regulatory, compliance, monitoring and enforcement functions, which may include:

- names, addresses, contact details, dates of birth, National Insurance numbers;
- racial or ethnic origin;
- employment history;
- location data;
- online identifiers, including IP addresses, cookie identifiers from third party websites;
- criminal records and allegations of criminal offences
- information relating to a person's health;
- information relating to a person's economic identity, including credit ratings, financial information and banking records;
- an individual's political opinions or religious and philosophical beliefs; and
- an individual's personal views and opinions, including recordings and transcriptions of interviews undertaken as part of an investigation.

As an organisation, we have robust policies in place to ensure that we do not use more information than we need. In the case of our enforcement work, it is often necessary to have a broad range of information to enable us to effectively and efficiently meet our responsibilities as a regulator and law enforcement authority, including detecting and investigating offences.

How this personal data is collected

3.5 To fulfil our enforcement functions, we collect personal data from a variety of sources as described below.

From subjects of enquiries and Investigations

3.6 To perform our regulatory and enforcement functions, we may begin by requesting specific information from subjects of investigations. We may also rely on information that has previously been provided to the PSR, including information which we have compelled persons to provide (using our statutory powers), information which persons have provided voluntarily, and information which persons are obliged to report to us.

From government departments and other public authorities such as regulators and the police

3.7 We may receive information as part of our enquiries and investigations and intelligence and law enforcement work through our cooperation arrangements with other authorities, both domestic and overseas.

From other third parties

3.8 We may receive or request information from a variety of third parties to perform our functions. Given the nature of our work, it is often necessary to pull together a lot of information to ensure that we are able to identify and act when regulatory or enforcement action is required. Examples of other parties and sources that we could receive information from include:

- end users and whistleblowers;
- consumer bodies;
- trade bodies;
- social media, third party websites and commercial databases;
- credit reference agencies;
- third party contractors; and
- participants in designated payment systems.

Why we use this personal data

3.9 We use this personal data to enable us to carry out the specific regulatory compliance, monitoring and enforcement functions for which we are legally responsible. These duties arise under various statutes such as the Financial Services (Banking Reform) Act 2013; the Financial Services and Markets Act 2023; the Competition Act 1998 and in Articles 101 and 102 of the Treaty on the Functioning of the European Union in relation to participation in payment systems; the Payment Services Regulations 2017; the Payment Card Interchange Fee Regulations 2015; and the Payment Accounts Regulations 2015. Our duties include the ability to take regulatory action and to take enforcement action under regulatory, civil and criminal law. We have the power to conduct competition Investigations into businesses which may be acting anti-competitively.

The lawful basis for us using this personal data

3.10 We use this personal data under Article 6(1)(e) of the UK GDPR (it is necessary for the performance of a task carried out in the public interest) and Section 8(c) of the DPA 2018 and, to the extent that we use any special categories of personal data or criminal records, under Article 9(2)(g) of the UK GDPR (it is necessary for reasons of substantial public interest) and Sections 10(3) and (5) of the DPA 2018 (it is necessary for the exercise of the PSR's statutory functions, it meets a condition set out in Part 2 of Schedule 1 and we have an appropriate policy in place for such use).

We may also use personal data for law enforcement purposes under Section 35(2)(b) of the DPA 2018 (it is based on law and is necessary for the performance of a task carried out by us for that lawful purpose) and, to the extent that we use any special categories of personal data, under Section 35(5) (it is strictly necessary for law enforcement, it meets a condition set out in Schedule 8 of the DPA 2018 and we have an appropriate policy in place for such use).

When we share personal data we hold for compliance, monitoring and enforcement purposes

3.11 There are a number of reasons we may need to share personal data with other parties. For example, we share information with the parties subject to our enquiries and Investigations and their legal representatives. We may also share personal data with overseas regulators and/or domestic law enforcement bodies (such as police authorities and the National Crime Agency) and with other relevant organisations (such as Interpol, the Home Office, HM Revenue & Customs (HMRC) and overseas authorities with similar functions). In some circumstances, where appropriate, we may choose to share this information (for example, for the purposes of furthering an investigation) and in others we are obliged for legal reasons to share the information. In the case of competition investigations, it would be usual to share the information with relevant competition authorities.

We may also share information with participants in designated payments systems to enable them to comply with our directions. In the case of the APP scams reimbursement requirement, we may also pass personal information to Pay.UK and the Bank of England to enable them to engage with payment service providers in relation to the FPS reimbursement rules and the CHAPS reimbursement rules.

In the majority of cases, the law allows us to share this information without obtaining the consent of the individuals involved. Where the law does require this, we ensure that adequate consent is obtained in accordance with the UK GDPR and the DPA 2018.

When personal data is transferred outside the EU by us for the purposes of exercising our statutory powers

3.12 Given the international nature of our work, where necessary and appropriate we may share personal data with third parties, most commonly regulators and law enforcement agencies, outside the EU. We will only transfer personal data outside the EU if permitted by UK GDPR or DPA 2018. We have robust processes to ensure that appropriate safeguards are in place to protect any personal data included in such transfers. If you would like to obtain more details about our procedures for transferring personal data to countries outside the EU, please contact us.

Learn about your rights

3.13 Under the DPA 2018 and UK GDPR, you have certain rights regarding your personal data. For more details, see Individual Rights guidance. You can:

a. request access, deletion, or correction of your data,

b. object to how we use your data,

c. ask for your data to be transferred to another organisation, and

d. complain to the Information Commissioner's Office if dissatisfied.

3.14 As a public authority and regulator carrying out functions in the public interest, we may rely on exemptions specified in the DPA 2018 that could affect any rights requests you submit. If exemptions are applied, we will inform you of the relevant exemption, its justification, and the potential impact on your request.

3.15 Additionally, when processing personal data for law enforcement purposes, information may be withheld if necessary to prevent prejudice to the detection and investigation of criminal offences.

3.16 We assign responsibilities among joint controllers and, if needed, notify or refer individuals to other controllers for rights requests.

Data retention

3.17 Our retention schedule (available on request) sets out how long we hold all information, including any personal data used for each of the areas mentioned in this privacy notice.

To make a rights request

3.18 You should use the Data Protection Rights Request form to exercise these rights. We require additional proof of identity before providing a response. You can also email us or write to us at: Information Disclosure Team, Financial Conduct Authority, 12 Endeavour Square, London, E20 1JN.

To make any FOIA request

3.19 You should refer to FCA | Freedom Information. If you are unhappy with how we handled your rights or FOIA request, you can make a complaint to us – please see the 'How to make a complaint' section below.

How to make a complaint

3.20 Please carefully consider the below guidance on how to make specific complaints to avoid any delays in our responses.

a. Request for Data Protection Rights Request or Freedom of Information Act (FOIA) or write to us at: Information Disclosure Team, Payment Systems Regulator, 12 Endeavour Square, London E20 1JN. If you are dissatisfied with our response, you have the right to lodge a complaint with the Information Commissioner's Office.

b. To complain about how the PSR has handled your personal data or complete a printable form (PDF) or write to us: Data Protection Compliance Team (Risk and Compliance Oversight Division), Payment Systems Regulator, 12 Endeavour Square, London E20 1JN. We will acknowledge your complaint within 30 days. If your complaint is complex or unclear, we may request clarification. Complex cases may require more time, and we will inform you of any delays. If you are dissatisfied with our response, please reach out to us at first instance. You have the right to lodge a complaint with the Information Commissioner's Office.

c. To complain about Complaints about the PSR or visit our website for more detail.

d. To complain about financial product or service you have received, and when you should get in touch with the Financial Ombudsman Service.

Our Data Protection Officer

3.21 As a public authority, and a Data Controller, the PSR has an appointed Data Protection Officer (DPO), who oversees our internal data protection compliance. You can contact the DPO via email or write to: Data Protection Team (R&CO), Payment Systems Regulator, 12 Endeavour Square, London, E20 1JN.

If you have any particular questions or any feedback about our privacy notice, please email us.

4 Glossary

Item	Definition
Comply with a legal or regulatory obligation	means processing your personal data where it is necessary for compliance with a legal or regulatory obligation that we are subject to.
Controller	means someone that makes decisions about how and why they process your personal data. The controller is responsible for making sure it is used in accordance with the Data Protection Legislation.
Data Protection Legislation	means primarily + the Data Protection Act 2018 (DPA), the UK General Data Protection Regulation (UK GDPR), and the Data (Use and Access) Act 2026. These laws regulate how organisations and the government process personal information to protect individual privacy.
Data Subject Access Request	means a request made by, or on behalf of, a data subject in accordance with rights granted pursuant to the GDPR and DPA 2018 to access their personal data.
DPA 2018	means the Data Protection Act 2018.
UK GDPR	means the General Data Protection Act Regulation as it applies in the UK
LED	means the Law Enforcement Directive (EU 2016/680).
Public interest	means processing your personal data for the performance of a task carried out in the public interest or in the exercise of official authority vested in us.
Processing	means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Pseudonymisation	means the process of distinguishing individuals in a dataset by using a unique identifier which does not reveal their "real world" identity.
Special categories of personal data	means the special categories of data are specifically listed in the UK GDPR. They include race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health information, or information about a person's sex life or sexual orientation. Previously referred to as 'sensitive personal data'

Item	Definition
Internal Third Parties	The FCA, acting either as joint controller with the PSR or as processor based in the UK, provides services to the PSR, including in relation to the following: • Internal Policies and controls: • IT and system administration services; • Printing and reprographics; • Mail and courier services; • Estate management, physical security and meeting rooms and conference suites; • Corporate protection and resilience/business continuity; • Cyber resilience; • Correspondence • Advice and support on information disclosure, including processing requests for information under the Freedom of Information Act and Data Subject Requests related to the PSR and processing and managing suspected personal data breaches on our behalf. The PSR will generally remain the decision-maker in such cases. Where the FCA and PSR are joint controllers, each party will be responsible for complying with the Data Protection Legislation. The FCA and PSR will assist each other in meeting their obligations under the Data Protection Legislation, including consulting with each other and assisting each other in responding to Data Subject Requests and suspected personal data breaches; • Management accounting; • Procurement; • Internal Auditing; • Human resources; and • Other back-office services to ensure the effective operation of the PSR.

Item	Definition
External Third Parties	• Other regulators, public authorities and law enforcement agencies in the UK and EU, such as the Bank of England, the Competition and Markets Authority and the EU. On rare occasions, it may include other regulators, public authorities and law enforcement agencies outside the EU. • FCA service providers acting as processors based in the UK and Hungary, India and the USA who provide IT and system administration services. • Professional advisers acting as processors, joint controllers or, in the case of external counsel, data controllers, including accountants, consultants, lawyers, bankers, auditors and insurers based in the UK who provide accountancy, consultancy, legal, banking, audit and/or insurance and similar services. • Third-party providers of cloud-based IT services, analytical tools and advanced technologies, including machine learning and artificial intelligence tools, where they act as processors or sub-processors and are subject to appropriate safeguards. • HMRC, regulators and other authorities acting as processors or joint controllers based in the UK who require reporting of processing activities in certain circumstances. • Service providers such as media firms, regulators, survey conductors, travel co-ordinators, and cyber security companies. • Participants in designated payment systems such as Pay.UK, in its role as operator of Faster Payments.

© The Payment Systems Regulator Limited 2026
12 Endeavour Square
London E20 1JN
Telephone: 0300 456 3677
Website: www.psr.org.uk

All rights reserved