

Smart Pension Master Trust: Information Security and Compliance Fact Sheet for Participating Employers

This document addresses frequently asked questions about the Smart Pension Master Trust (SPMT), including how participating employer and employee data is safeguarded, and how business continuity and compliance are managed.

For further details on our information security certificates, policies, and controls, please visit our dedicated Trust Centre at <https://trust.smart.co/>.

About the Smart Pension Master Trust.....	1
How do we govern data protection?.....	1
How do we keep your data secure?.....	3
How do we ensure continuity of service?.....	4
How do we manage compliance?.....	4

About the Smart Pension Master Trust

What is the Smart Pension Master Trust?

SPMT is a pension scheme, authorised and regulated by The Pensions Regulator, that helps members save for their retirement.

Smart Pension Limited (SPL) is the scheme funder of SPMT, and EC2 Master Limited is the trustee of SPMT (the “Trustee”).

How do we govern data protection?

What are the data protection roles for the SPMT?

SPL and the Trustee are joint data controllers in relation to data held in respect of members of SPMT. There is an intra-group data sharing agreement between the various Smart Pension group companies (including the Trustee). As this agreement involves all of the Smart entities, this is not shared externally.

Are SPL and the Trustee registered with the Information Commissioner’s Office (ICO)?

Yes, both SPL and the Trustee are registered with the ICO. SPL’s ICO registration number is ZA070575 and provides Data Protection Officer (DPO) duties on behalf of SPMT. The Trustee’s ICO registration number is ZA135972.

Does the Trustee have a Privacy Policy?

The Trustee has a Privacy Policy which sets out its approach to collecting, using, processing and protecting personal data in the business to comply with its legal and regulatory obligations in respect of data protection. It serves as a transparent communication tool to inform SPMT members about their privacy rights and the practices employed by the Trustee and SPL regarding the handling of their personal data. A copy of the SPMT Privacy Policy can be found in our [Trust Centre](#).

Does the Trustee have a data protection programme in place to implement effective privacy controls?

The Trustee has a Data Protection Policy which sets out how it, and SPL, use tools and processes to embed privacy controls into new products, operations and processes that collect and use personal data. These include data protection impact assessments (DPIAs), maintaining records of processing activities, supplier due diligence, incident management, mandatory training and regular audit procedures.

Is a controller-to-controller agreement needed between a participating employer and SPL?

SPL and participating employers are independent data controllers and therefore controller-to-controller agreements between SPL and participating employers are not needed.

What is the position under the participation agreement?

Each participating employer joining SPMT enters into a participation agreement with SPL. By signing a participation agreement, each employer explicitly acknowledges and accepts our terms and conditions, which can be found on the Smart Pension website. Under the Scheme rules, an employer who has not signed a participation agreement becomes bound by both the Scheme rules and the participation agreement upon making their first contribution to SPMT.

Does SPL complete privacy risk assessments for handling personal data?

Yes, SPL uses DPIAs to help to identify and minimise the data protection risks of handling personal data, in order to negate risk and demonstrate GDPR compliance in respect of SPMT.

Does SPL have a programme in place to respond to data protection breaches?

SPL operates a data breach notification procedure (which is not publicly available) on behalf of the Trustee which sets out breach reporting requirements to the ICO and our clients. The SPL DPO has overall responsibility for ensuring clients impacted by a security incident resulting in data loss are notified within agreed timelines.

Does the Trustee have a Data Retention Policy?

The Trustee has a Data Retention Policy for SPMT. The Data Retention Policy is not publicly available but is consistent with the Trustee's legal obligations.

Who should I contact with any queries relating to data protection?

If you have any data protection or privacy questions that are not addressed in this FAQ document, please contact privacy@smartpension.co.uk.

How do we keep your data secure?

How do we manage information security?

SPMT leverages its cloud platform, Keystone, which is certified for ISO 27001 for information security and has successfully completed a SOC 2 Type II audit. This demonstrates that its security controls are both appropriately designed and operating effectively over time, forming a key component of SPMT's information security management program.

Our approach to information security follows the requirements set out in these standards. SPMT's compliance with the standard is independently audited on a regular basis. Our ISO report is not publicly available but a link to our certification can be found [here](#).

SPMT has a full suite of Information Security Policies and manages the risks associated with information security in line with its Risk Management Framework approved at board level.

How do we deal with cyber incidents?

We have a dedicated Cyber Security Team who work with incident managers in our Engineering Teams to mitigate cyber incidents and attacks, through our security incident process. There is an appropriate cyber security insurance policy in place, covering SPMT.

Do we have controls against distributed denial-of-service (DDoS) attacks?

We leverage a cloud supplier together with latest-generation security software to counter DDoS attacks and maintain service.

Do we have controls against malware?

We maintain a full suite of technical controls against malware, including firewalls and anti-virus software together with real-time monitoring and reporting of activity through a dedicated security operations centre.

How do we manage user access?

Access to the Keystone platform is governed by our Access Control Policy and strictly limited to colleagues who require it to perform their roles. This access is subject to regular review and independent audits.

Are there any restrictions on where Keystone can be accessed from?

Keystone can currently be accessed from any location. There are no geographical restrictions for Adviser, Member or Employer Accounts.

Do we encrypt data?

All data and databases are encrypted using our cloud supplier's standards. All data transmission by SPMT is encrypted.

Do we have a Patching Policy?

Yes, we have a Patching Policy and implement procedures to ensure that software updates are promptly deployed across all user devices.

How do we ensure continuity of service?

Do we have a Business Continuity Policy and Plan?

We have a Business Continuity Policy and enterprise wide Business Continuity Plans in place to ensure continued service in the event of a disruption.

What arrangements do we have for hosting participating employer data?

We use cloud computing services – providing access to a large number of data centres to deliver strong operational resilience and security.

Do we back up data?

We create daily backups of member data, allowing this to be recovered if necessary.

Do we carry out business continuity and disaster recovery testing?

We test business continuity plans on a regular basis, conducting full disaster recovery tests for the Keystone platform every six months. Test results are reviewed, to drive ongoing refinement and improvements of our disaster recovery arrangements.

Do we have a pandemic response plan?

We have plans in place for responding to a pandemic, incorporating lessons learned during the COVID-19 pandemic. All colleagues are enabled to work remotely to ensure that service is maintained in these circumstances.

How do we manage compliance?

Do we have an Anti-Money Laundering Policy?

We have a dedicated Anti-Money Laundering Policy and implement appropriate risk-based controls to meet its statutory obligations to prevent money laundering.

Do we have an Anti-Modern Slavery Policy?

We have a dedicated Anti-Modern Slavery Policy and require all third-party suppliers to be compliant with UK law in this area.

Do we have a Whistleblowing Policy?

We have a dedicated Whistleblowing Policy and provide our employees with an independent confidential whistleblowing service.

Do we comply with UK sanctions?

We are fully compliant with UK sanctions.

Do we provide compliance training for employees?

Yes, we operate a mandatory compliance training programme for all employees. This includes initial onboarding modules and quarterly updates covering key risk areas such as financial crime, data protection, cybersecurity, and whistleblowing.

For further details, please visit our dedicated Trust Centre at <https://trust.smart.co/>.