Standard Life EU General Data Protection Regulation (EU GDPR): FAQ

March 2018

Overarching: Privacy by design and default

Privacy by design is defined as an approach to embed privacy protection into the design specifications of technologies, business practices and physical infrastructures – this means building privacy into the design specs and architecture of systems and processes, both existing and new. GDPR requires all organisations to implement a wide range of technical and organisational measures to demonstrate they have considered and integrated data protection.

How does Standard Life integrate Data Protection? (An overview of the organisational measures in place to protect personal data.)

Standard Life's Protection of Information and Resilience Policy covers information security, physical security and business continuity; it also includes data protection and records management. This policy, in combination with other sub policies of the Group Operational Risk Framework, provides a clear structure for an effective internal control system to manage risks to the confidentiality, integrity and availability of information. The policy covers information held, processed and transmitted in electronic form.

We adopt a 'defence-in-depth' approach to cyber security where we utilise layers of controls across a breadth of security domains, in order to protect both our external perimeter and our internal customer assets from harm. We carry out regular security penetration testing to identify any vulnerability in our systems that could be used against us.

Access to data through our secure websites is protected by strong authentication mechanisms, and data is encrypted whilst in transit over the internet to your browser (using the industry standard SSL security protocol). In addition, our websites have authorised Extended Validation SSL Certificates in place, meaning users can be confident that they are accessing a trusted site (users will see a green address bar if a website is secured with an EV SSL Certificate).

Can you provide an overview of your governance structure for compliance with the Data Protection Act 1998, and provide details of how this will change post 25 May 2018?

We have a Data Governance and Privacy team responsible for ensuring Standard Life Aberdeen can evidence compliance with its data protection obligations. The Head of this team reports directly to the Chief Information Security Officer who in turn reports to the Chief Operations Officer for Standard Life group. The COO is a member of our Executive Committee with reporting line to the CEO.

Regular governance meetings are held at the various reporting lines to ensure continued oversight of our data management practices and controls.

We will be reviewing our governance structure as we prepare for GDPR and we will continue to retain senior accountability and oversight of our business processes and operational compliance with our data privacy obligations to ensure the ongoing security and privacy of your clients' personal information.

General Overview

What personal data or sensitive data does Standard Life process or hold, and what categories of Data Subjects does this relate to?

Personal Data

We will need to collect personal data about you, your clients and any person associated with or employed by you (the "Data Subject") when you complete the registration form to set up an adviser account with us and thereafter throughout the course of our business relationship with you.

We will only ever collect and use information which is personal to you, your clients where it is necessary, fair and lawful to do so.

Special Categories (Sensitive Data under DPA 1998)

We may collect special categories of data (as defined by the GDPR) about your clients, including information relating to a client's physical or mental health.

We will normally require your clients' explicit consent for this, and you should not provide us with any special categories data unless you have obtained your clients' explicit consent, or we require it to provide the agreed service or to fulfil our legal obligations.

What is the purpose of the processing of the personal data that Standard Life does?

We will collect and use you and your clients' information only where:

- your clients have given us their permission [consent] to send them information about products and services offered by other parts of Standard Life Aberdeen plc and/or selected third parties we have chosen to work with which we believe may be of interest and benefit to them
- it's necessary to provide the product or service you have requested on behalf of your client e.g. if you wish to invest in one of our pension or savings products, we will require some personal information including their name, address, date of birth and bank account details
- it's necessary for us to meet our legal or regulatory obligations e.g. to send your clients Annual Statements, tell them about changes to Terms and Conditions, or for the detection and prevention of fraud

- it's in the legitimate interests of Standard Life e.g. to deliver appropriate information and guidance so your clients are aware of the options that will help them get the best outcome from their product or investment; where we need to process your clients' information to better understand them and their needs so we can send them more relevant communications about the products they have with us and to develop new products and services; where we use artificial intelligence or computer algorithms to improve the products and services offered to you and your clients
- it's in the legitimate interests of a third party e.g. sharing information with discretionary fund managers who have been contracted by you.

Processing of sensitive personal data (special categories of personal data) and personal data relating to criminal convictions and offences

GDPR maintains the requirement for explicit consent to process sensitive data (subject to some exemptions).

GDPR prohibits the processing of personal data relating to criminal convictions unless there is local law to permit such processing.

Who can access sensitive personal data?

Security of all data is of paramount importance to us and we have robust controls in place to ensure this happens. Access to sensitive personal data is restricted only to those who have a lawful reason to process it.

Consent

When does Standard Life obtain consent from clients/members in order to process personal data?

Where consent is relied upon as the legal basis for processing, this will be captured, stored and used in line with the GDPR standards. Individuals will be able to withdraw their consent at any time.

Where the individual has given us consent to send them information about products or services offered by other companies in SLA plc and / or selected third parties we have chosen to work with.

Right of the Data Subject to be informed - privacy notice

Organisations must provide privacy notices to the Data Subject so that the Data Subject is aware of how their information will be used, and to ensure transparency of processing.

How will Standard Life provide Privacy Notices to clients/members?

When collecting personal information from your clients, we will present a Privacy notice or 'Fair Processing Notice' at that time e.g. when completing an application form for a product with us, using our mobile App or online dashboard. Our Privacy Policy will be updated whenever we make changes, and if these are important changes such as where data is being processed, we will contact individuals to let them know. You can find a copy of the Privacy Notice online: **https://www.standardlife.com/privacypolicy**

Data Subject access requests

GDPR grants Data Subjects further rights to access their personal information. Organisations are required to provide this information, where feasible, in an electronic format where the request is made electronically. From 25 May 2018, firms will no longer be able to charge for the provision of a Subject Access Request and must respond within 1 month.

Does Standard Life have operating procedures, guidance notes and templates to complete / provide information to meet the Subject Access Request requirements?

Yes, Standard Life has established processes in place to respond to Data Subject Access Requests. We are reviewing and (where necessary) enhancing these processes to comply with the GDPR.

Will Standard Life respond directly to the Data Subject?

Where Standard Life receives a request to provide a copy of the personal information for your client(s), we will respond directly to the requestor in relation to the personal information we process as the Data Controller.

Right to Data Portability

GDPR introduces a new right of Data Portability in certain circumstances. This right gives the Data Subject the ability to request, obtain and re-use the personal data the Data Subject has provided to a business, in a structured and commonly used machine-readable format, or ask for such information to be transferred to another Data Controller.

Will the right to Data Portability apply for the work Standard Life completes or the services Standard Life provides?

Yes. Data Portability will apply to the information provided to Standard Life in relation to your client and to a limited set of the personal information we process on your clients as defined by the regulation.

Data Portability relies on a structured, commonly used and machine readable format to facilitate the transmission of the data from one controller to another. As such, when a standard format is agreed within our industry, we will seek to implement this. Currently, of course, we can facilitate the transmission of pension schemes to / from Standard Life to another provider at your or your clients' request.

Right to rectification

Does Standard Life have a process for rectifying incorrect information?

Yes. Standard Life has established processes in place to respond to requests to correct inaccurate or incomplete information on individuals. We are reviewing and (where necessary) enhancing these processes to comply with the GDPR.

Right to erasure / Right to be forgotten

The right to erasure is also known as 'the right to be forgotten'. Data Subjects have the right to request the deletion or removal of personal data in certain circumstances. It is not an absolute 'right to be forgotten'.

Does Standard Life have a process in place for handling any requests to erase data?

Yes, Standard Life has a process for Erasure/Right to be forgotten. We are reviewing and (where necessary) enhancing these processes to comply with the GDPR.

Standard Life may not fulfil a request for erasure / right to be forgotten where we are bound by regulations or other laws to retain this personal data.

Right to Restriction of Processing

Does Standard Life have a process for handling any requests for restriction of processing?

Yes, we have a process for handling requests to restrict processing of personal information. We are reviewing and (where appropriate) enhancing these processes to comply with the GDPR.

Notification obligation for rectification or erasure of personal data, or restriction of processing

How does Standard Life comply with the requirement to notify the recipients of the personal data in the event of any rectification or erasure of personal data or restriction of processing?

We will contact any third parties / recipients of your [clients'] personal data to notify of any requests to rectify / erase / restrict processing.

Automated decision making and profiling

GDPR defines profiling as any form of automated processing intended to evaluate certain personal aspects of an individual, in particular to analyse or predict their performance at work; economic situation; health; personal preferences; reliability; behaviour; location; or movements. Data Subjects have the right not to be subject to a decision based solely on automated processing where it produces a legal effect or significantly affects the Data Subject.

Does Standard Life complete any profiling?

We use automated processing where it is in our legitimate interests, focused on understanding your clients better, helping us communicate with you and them, and to assist us in improving our products and services offered to your clients:

- Tailoring products and services e.g. placing your clients in groups with similar customers to make decisions about the products and services we may offer you to help meet your needs
- When designing and enhancing our online services to help meet your clients' requirements for ongoing guidance and support

Data protection impact assessments

GDPR requires organisations to consider privacy risks and data protection obligations as part of the implementation of any organisational, technical or systematic change. Data Protection Impact Assessments (DPIAs) (also known as Privacy Impact Assessments or PIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow organisations to identify risks and fix issues at an early stage.

Have Standard Life implemented a Data Protection Impact Assessment/Privacy Impact Assessment (DPIA/PIA) Process?

Does Standard Life have and maintain DPIA guidelines and templates?

Standard Life have existing processes where we assess the potential impact of processing on an individual's privacy - we have an established DPIA process with standard templates in place for use across the business and operational / IT & Change areas - we are currently reviewing our existing processes and will strengthen these further (where appropriate) in our preparation for GDPR.

Data Protection Officer

GDPR requires that firms processing large amounts of personal data have a Data Protection Officer (DPO) in certain circumstances.

Does Standard Life have a DPO in place and does that person meet the requirements of the DPO under the GDPR? If so, please provide their contact details.

Standard Life group have a Chief Information Security Office (dpoffice@standardlife.com), who are accountable for data protection, security and liaison with the relevant regulators.

Record of processing activities and new principle of accountability

GDPR requires organisations in certain circumstances (either when they have more than 250 employees or the processing could result in a high risk to the rights and freedoms of individuals, or processing involves sensitive data or data relating to criminal convictions and offences) to maintain a record of all their processing activities, with certain prescribed information to include who has access to personal data, what information this includes, and where that information is stored.

Where does Standard Life store records and information?

The majority of your clients' information is processed in the UK and European Economic Area (EEA).

However, some of your clients' information may be processed by us or the third parties we work with outside of the EEA, including countries such as the United States, Philippines and India.

Where your clients' information is being processed outside of the EEA, we take additional steps to ensure that their information is protected to at least an equivalent level as would be applied by UK / EEA data privacy laws e.g. we will put in place legal agreements with our third party suppliers and do regular checks to ensure they meet these obligations.

For how long are records retained?

We will keep your clients' personal information only where it is necessary to provide them with our products or services whilst they are a customer.

We may also keep their information after this period but only where required to meet our legal or regulatory obligations. The length of time we keep their information for this purpose will vary depending on the obligations we need to meet.

Security of processing

What security measures and controls do Standard Life have in place? How do Standard Life identify and mitigate cyber vulnerabilities?

The security of your clients' information is always of paramount importance to us and we will always act in you and your clients' best interests, making robust risk decisions that protect them. Like all financial services companies, we operate in a challenging, constantly evolving cyber-crime environment. We have a strong commitment to our security and IT capabilities, including long-term security programmes, partnerships with third party specialists and a dedicated internal IT function. These are designed to protect our customer and corporate assets / information from misuse, the effects of crime and the impact of a significant disruption to our operations.

Our security policy set is aligned with ISO27001 standards.

We outline below some of our key security controls and practices:

- As a key area of risk for Standard Life Aberdeen, cyber security receives significant ongoing focus from our Board and senior management. This is reflected in the significant ongoing investment we make to continually enhance our cyber-related resources and capabilities.
- Our cyber security policy and standards are aligned with industry good practice standards and the UK Government's 'Cyber Essentials' scheme.
- We fully recognise the increasing and constantly evolving external cyber threat environment and we strive to be responsive to, and stay ahead of, these threats and challenges through our regularly updated security strategy and programme which is designed to address specific risks quickly and to continue evolving our sustainable cyber security capability.
- We adopt a defence-in-depth approach to cyber security whereby we utilise layers of controls across a breadth of security domains in order to protect both our perimeter and our internal assets from harm. We carry out regular vulnerability scanning and penetration testing to identify any vulnerabilities in our systems and network that could be used against us. All findings are measured on a Red, Amber, Green status and are actioned accordingly to close any vulnerability.
- Internal and external audit and specialist third party consultants conduct regular, independent assurance and benchmarking exercises across our business to ascertain the effectiveness of our security control environment, our security strategy and programme, and our governance processes.
- We have dedicated Cyber Intelligence, Cyber Response and Financial Crime teams in place to effectively deal with emerging cyber threats and criminal campaigns. Our response plans are tested regularly.

Given the above, we believe that our security framework fully adheres to industry good practice, and provides a control environment that effectively manages risks to the confidentiality, integrity and availability of our information assets (and related systems).

Do Standard Life have a Business Continuity Policy?

Yes. Standard Life have a Business Continuity Policy in place and a robust Business Continuity Plan.

Personal data breaches and notification

GDPR will introduce a new requirement for organisations to report data breaches to the ICO within 72 hours, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of the Data Subject. Organisations must also notify the Data Subject of the data breach if there is a high risk to the Data Subject. Processors must notify controllers without undue delay of any data breaches.

What is Standard Life's internal process for breach reporting, and how does Standard Life intend to comply with the GDPR?

Any data protection breaches are managed locally in line with our agreed processes and regular reporting to the Chief Information Security Office (CISO). If a material breach, this would be escalated immediately to the CISO for awareness and actions agreed, as appropriate, including any notification to the regulator(s) where required.

Data transfers

Transfers of personal data outside of the EU can only be made in certain circumstances, usually by way of appropriate safeguards set out in the GDPR or based on a decision by the Commission.

Do Standard Life transfer data outside the EU?

The majority of your clients' information is processed in the UK and European Economic Area (EEA).

However, some of your clients' information may be processed by us or the third parties we work with outside of the EEA, including countries such as the United States, Philippines and India.

Where your clients' information is being processed outside of the EEA, we take additional steps to ensure that their information is protected to at least an equivalent level as would be applied by UK / EEA data privacy laws e.g. we will put in place legal agreements with our third party suppliers and do regular checks to ensure they meet these obligations.

Is data encrypted/anonymised when being transferred?

We believe that our security standards fully adhere to industry good practice, and provides a control environment that effectively manages risks to the confidentiality, integrity and availability of our information assets (and related systems).

All data in transit is protected by TLS encryption which uses the strongest cipher settings available for the source browser.

Staff communications and training

Privacy by Design requires the organisations to embed the GDPR into their systems, processes and controls and in the event of any changes. Staff will need to be trained and aware of requirements of the GDPR, and how this impacts on their work.

What data protection and information security training do Standard Life staff receive on their data protection obligations in respect of data handling and processing?

A Data Protection eLearning module is mandatory for all staff on an annual basis. All staff are informed in their Terms of Employment and annual training is provided. Local education sessions are held and we issue regular communications to staff via our intranet to ensure staff are kept abreast of developments in security processes and potential external threats.

Standard Life Assurance Limited is registered in Scotland (SC286833) at Standard Life House, 30 Lothian Road, Edinburgh EH1 2DH. Standard Life Assurance Limited is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.
www.standardlife.co.uk

GEN3086 0318 © 2018 Standard Life Aberdeen. Images reproduced under licence. All rights reserved.