Privacy Policy for third party suppliers

September 2022

Contents

In this Policy:

"Controller", "Processor", "Data Subject", **"Personal Data Breach", "Supervisory Authority"**, **"Subprocessor"** and **"Third Country"** shall have the same meanings defined in the Supplier Contract and **"Processed"** and **"Process"** shall be interpreted in accordance with the meaning of **"Processing"**.

"SRM" means a FIL Supplier Risk Manager.

"Supplier Contract" means the contract for the provision of supplier services between the supplier and FIL.

This Policy applies to the Processing of personal information, including sensitive personal information.

The supplier must ensure that:

- a nominated data privacy contact and sufficient resource is in place, with the necessary skills and knowledge to discharge data privacy accountability under the Supplier Contract,
- personal information Processed on behalf of FIL is compliant with both the Supplier Contract and this Policy, and
- risk based monitoring plans are established and embedded.

Requirements

Fair, lawful, and transparent Processing:

The supplier must only Process personal information in a lawful, fair and transparent manner.

Purpose limitation:

The supplier must not Process personal information in a way that is incompatible with the original purposes for which it is Processed.

Record of processing activity:

The supplier must:

- maintain proper records of processing of FIL personal information as required under applicable Data Protection/Privacy laws, and
- in consultation with the FIL Global Privacy Compliance function make the relevant elements of the record of processing available to relevant Data Privacy Supervisory Authorities within 72 hours of FIL's request.

Privacy Risk Assessments:

Where relevant the supplier must conduct a risk assessment (throughout the lifecycle of the relationship) to assess, manage and evidence privacy risk and how they are being mitigated in relation to the specific activity the supplier is providing services for.

Where the risk assessment identifies a high level of risk and these cannot be mitigated, the supplier must consult with the FIL Supplier Risk Manager ("SRM") and FIL Global Privacy Compliance.

Data Privacy Impact Assessments:

The supplier must provide assistance to FIL with any Data Privacy Impact Assessment and consultations with the relevant Supervisory Authorities.

Data minimisation:

The supplier must ensure that the personal information it Processes on behalf of FIL is adequate, relevant, and limited to those purposes necessary for which it is Processed.

Accuracy:

The supplier must ensure that all personal information is accurate, complete and up to date and must take all reasonable steps to ensure that inaccurate or incomplete personal information is erased, de-identified or rectified without undue delay having regard to the purposes for which it is Processed.

Data retention:

The supplier must not retain personal information in a form that permits identification of the Data Subject for longer than is necessary and must dispose of personal information securely upon expiry of the retention period, or securely return the personal information to FIL, in line with the requirements as set out in the Supplier Contract.

Data Subject rights:

The supplier must Process personal information in accordance with the rights of the Data Subject in accordance with applicable data privacy legislation.

Subject Access Requests (SARs):

The supplier must manage any subject access request received directly from the Data Subject, identifying, and providing the information as requested within the relevant timeframe as set out by applicable data privacy legislation. The supplier must notify the SRM without delay where the request is not fulfilled within the required timeframe and record the failure.

When providing the information to FIL to support the request the supplier must not alter, erase, block or withhold any information that the requestor would be entitled to.

Privacy complaints received from Supervisory Authorities:

The supplier must with immediate effect forward any complaint relating to privacy matters received from data privacy Supervisory Authorities, to the SRM. The supplier must support FIL, as required in the investigation and drafting of the response to any Supervisory Authority.

Other privacy rights:

The supplier must have appropriate processes to address all other relevant rights requests, such as:

- Rectification of inaccurate personal information, and
- Erasure of personal information, no longer required

Data security:

When processing personal information, the supplier must ensure an appropriate level of security to the risk that is presented. This must include protection against unauthorised or unlawful Processing, disclosure of or access to personal information and against accidental or unlawful loss, destruction, alteration or damage, using appropriate technical and organisational measures.

The Supplier must not take any steps to deliberately facilitate access to FIL Personal Data by any Public Body.

Management & reporting of Personal Data Breaches:

The supplier must report personal information incidents to FIL via the SRM without undue delay upon Supplier or Supplier's Affiliate becoming aware of or suspecting a Personal Data Breach, and must provide the following information,

- Description of the nature and the details of the Personal Data breach,
- Details of a contact at the supplier to support,
- Consequences of the Personal Data Breach, and
- Remediating actions to resolve this occurrence and to prevent reoccurrence.

Requests for Disclosure of Personal data:

The supplier must ensure requests for disclosures of personal information from Regulators, Government, Local Authorities and/or Law Enforcement agencies are:

- Authenticated - to establish the requestor is who they say they are
- Validated – to confirm the requestor is entitled to all of the information being requested
- Informed and consulted with FIL via the SRM prior to disclosure
- Responded to securely, and
- Retained to ensure that an audit trail is maintained which includes a clear explanation as to the rationale for disclosure

Provide appropriate training to all employees:

The supplier must ensure that all relevant employees receive privacy training when they commence employment and that this training is renewed annually to ensure that they fully understand the privacy requirements of Processing personal information in line with applicable data privacy legislation and this Privacy Policy as it relates to their role.

International data transfers:

The supplier must not transfer personal information Processed in the UK or European Union ("EU") to Third Countries, territories or international organisations, unless adequate measures are in place, and:

- The European Commission has determined that the Third Country has an adequate level of data protection.
- The transfer is made with appropriate safeguards (technological and organisational measures and standard contractual clauses)

All suppliers must provide FIL with details of: all Subprocessors who are based in third countries; the Processing that they undertake; whether they are a controller, processor, (or both); what personal information they are Processing; in which country, and under which transfer mechanism. Suppliers must, via the SRM, be able to provide this information without delay.