CIPS Data Protection Policy

Contents

1 Overview 3
2 Principles of data protection ..... **Error! Bookmark not defined.**
3 Objectives 3
3.1 Establish lawful basis ..... **Error! Bookmark not defined.**
3.2 Collect data for explicit and legitimate purpose 4
3.3 Select data that is adequate and relevant 4
3.4 Maintain accurate records 4
3.5 Appropriate retention period for information 4
3.6 Information Security ..... **Error! Bookmark not defined.**
4 Upholding the rights and freedoms 5
4.1 Information and rights for data subjects 5
4.2 Breach management 6
4.3 Data Protection Impact Assessment 6
4.4 Subject Access Request 6
5 Governance 6
6 Audit and review 7
7 Training and exercise 8
8 Definitions 8
9 Related policies and procedures 9
10 Further information 9

1 Overview

The Chartered Institute of Procurement & Supply (CIPS) is the leading voice of the procurement and supply profession. With a global community of over 200,000 in 150 countries, we set the standards for the profession and are the only regulated body in the world to promote a Code of Conduct; the international model for purchasing and supply practice. CIPS is the Data Controller and Data Processor of the information that you provide to us as a member and to access our services and training.

CIPS and its subsidiary company, CIPS Corporate Services Limited, are registered as Data Controllers under the UK Data Protection Act 2018 [registration numbers: Z7413243 and Z5706326 respectively].

CIPS Data Protection Policy sets out how we respect the personal information that we collect and hold in the course of carrying out our role representing the procurement and supply profession, our clients and members. We are committed to ensuring that the privacy of our members, business partners and staff is protected and upholding the principles of data protection.

The General Data Protection Regulation, effective from May 25 2018 and incorporated in the Data Protection Act 2018, harmonises data protection rules across EU member states. It applies to data processing carried out by individuals and organisations operating within the EU, but also applies to organisations outside the EU that offer goods and services to EU citizens. The GDPR significantly enhances the rights of data subjects in the processing of their personal data and strengthens the current system.

2 Purpose

CIPS as Data Controller and in cases, Data Processor, must be able to demonstrate compliance with data protection law. This policy outlines CIPS framework in upholding Article 5 of the GDPR and Data Protection Principles in that data shall be:

- processed lawfully, fairly and in a transparent manner
- collected for specified, explicit and legitimate purposes
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary for the purposes for which the personal data are processed
- processed in a manner that ensures appropriate security

3 Objectives

Adhering to data protection principles, CIPS will manage data throughout the information life cycle and will seek to audit and review its processes and procedures in data handling. With constant regard to continuous improvement, the data protection management system will adopt best practice principles and GDPR requirements. This management process will be achieved by adopting the following policy objectives.

3.1 Process data lawfully and fairly

CIPS must have a 'lawful basis' or 'grounds for processing' before legally processing personal data.
There are 6 different grounds for processing:

- Consent - the individual/data subject has freely given their consent to the processing and data must be collected through a clear affirmative action.
- Contractual - processing is necessary for the performance of a contract or agreement to which the individual is party or is required prior to entering into a contract.
- Legal requirement - processing is necessary for compliance with a legal obligation to which the individual is subject.
- Public interest - 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 data controller.
- Legitimate interests - processing is necessary for the purposes of the legitimate interests of the organisation or a third party where the interest and rights and freedoms of the individual are not overridden and the data is used in ways which people would reasonably expect.
- Vital interests - processing is necessary to protect the vital interests of the individual or of another person.

Where processing is intended to require Special Categories of personal data (see definitions), a specific condition permitting such processing must also be identified as laid out in the GDPR & Data Protection Act 2018.

Once legal grounds for processing have been established, its activities will be included within the Data Asset Inventory – Article 30.

3.2 Collect data that is necessary and for a legitimate purpose

CIPS will ensure that personal data collected is necessary for processing and not further processed in a manner that is incompatible with those purposes; under GDPR further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

CIPS will communicate in a clear and transparent manner ensuring that all data subjects are informed of the purpose for their data being processed and only use their personal data in a way that the data subject expects and with accordance to their rights.

3.3 Select data that is adequate and relevant

CIPS will ensure that the data processed will be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed and those purposes will be transparent and clear. If intentions are to use the data for any other purpose data subjects are informed and have the right to object.

3.4 Maintain accurate records

CIPS will ensure that data is accurate and, where necessary, kept up to date. All data subjects will be provided with the means to update their personal data and every reasonable step will be taken to erase or rectify without delay inaccurate records.

Records will be restricted if there is any dispute over their accuracy until a time where the data has been rectified and authorised as an accurate account of the subject's data.

3.5 Appropriate retention period for information

CIPS will not store data for any time longer than necessary or if the data subject withdraws consent or objects to its processing (unless there is another legal ground to justify its retention). In order to manage the process

of establishing and keeping records for a suitable period, CIPS has a Retention Policy and process that outlines the assessment and categorisation of data for storage and deletion.

3.6 Securing personal data

CIPS depends on information and communications technology systems to operate global membership and administrative functions. Security of these systems, the hardware and networks on which they reside and the data which they host is necessary both to honour CIPS obligations to providers of data (students, members, suppliers, partners and staff) as required under the GDPR (Articles 25 and 32) and to protect CIPS systems and data from damage loss or corruption whether it be accidental or deliberate.

Where personal data is to be transferred outside of the EU, referred to as a Third Country Transfer, CIPS will only do so where one of the conditions specified in the GDPR (Articles 44-50) are fulfilled, such as binding corporate rules, the existence of an adequacy decision (including EU-US Privacy Shield) or a legal agreement specifying the standards to be adhered to.

CIPS Information Security Policy in conjunction with CIPS Acceptable Usage Policy outlines the activities taken to protect data within the organisation.

4 Upholding the rights and freedoms

4.1 Information and rights for data subjects

Individuals can request that we make changes in how their data is handled and we must respond promptly should a request be made.

- Right to be informed – we must communicate clearly and use plain language in all our external messaging when initially collecting the data or at first opportunity
- Right of access - we must have in place processes to respond to requests for what information we are holding (Subject Access Requests)
- Right to rectification - we must ensure we correct inaccurate information in the data we are processing without delay
- Right to erasure – we may be required to delete the data and stop processing it or publishing it (often called the Right to be Forgotten)
- Right to restrict processing – where the accuracy or lawful processing is challenged then temporary limits on the processing are required
- Right to data portability – we may be asked to provide the personal data we hold, securely and in a machine-readable format, so it can be moved, copied or transferred to be used across different services
- Right to object – individuals have the right to object to processing where our lawful basis is legitimate interests or where we directly market to them
- Rights related to automated decision making - if there is additional profiling or automated decision making based on the data we hold that then an individual can object

CIPS Subject Access Request (SAR) guideline outlines how an individual can contact CIPS to initiate the SAR process.

4.2 Subject Access Request

CIPS collection of personal data is handled in accordance with the CIPS Privacy Statement. All staff are expected to follow this policy and demonstrate a commitment to protecting others' privacy.

Requests from data subjects (see definitions) are called Subject Access Requests. The process for making a request is set out in the CIPS published guidance 'Making a Subject Access Request'. This is a simple checklist to guide you on the steps to make sure you recognise and handle a request (SAR) effectively, and in compliance with the data subject's rights and CIPS internal processes. The information is provided free of charge.

4.3 Breach management

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- access by an unauthorised third party through their direct action or lax internal security procedures or practices
- deliberate or accidental action or inaction by a member of staff
- sending personal data to an incorrect recipient, e.g. wrong copy recipient to an email
- USB stick, laptop or phone containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data

CIPS breach management procedure is outlined in the CIPS Breach Management Process document.

4.4 Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA) is a methodology or tool used to identify and reduce the privacy risks of individuals when planning projects or policies that involve the processing of personal data. Privacy by design means that CIPS identifies and minimises the data protection risks of a project or new initiative. CIPS manages all new data assessments through its DPIA management process.

5 Governance

CIPS has the following governance framework in place to manage Data Protection Compliance:

Data Controller:
Any person, or organisation, who makes decisions about how and why data is processed. A data controller must be a person recognised in law and they are responsible for compliance. CIPS is a Data Controller.

Senior Leadership Team (SLT):

- Responsible officers of all organisation-wide data protection
- Oversight of Data Compliance Management Group

Data Compliance Management Group

- Ensuring that there are adequate and competent resources available to support Data Protection Processes
- Updating Article 30: processing activities documentation
- Establish roles and responsibilities including appointment of one person with responsibility for the GDPR Breach Management Process
- Conduct management reviews of the GDPR Breach Management Process ensuring it is fit for purpose and seeking continual improvement
- Commitment to GDPR Breach Management Process and supporting implementation throughout the organisation
- Signing off audit processes and alignment with CIPS Data Protection Policy
- Review training and testing outcomes
- Reporting to SLT and GBT where applicable: including incident reports

Data Protection Officer:
Assigned under Article 37.1B: Chair of the Data Compliance Management Group.

- Inform and advise senior leadership of their obligations under data protection
- Promote a culture of data protection throughout the organisation
- Review policies and procedures to ensure they are fit for compliance
- Advise on data protection procedures and best practice
- Monitor and report on compliance to senior leadership
- Maintain accurate records and documentation
- Point of contact for data protection for all internal and external contacts
- Investigate breaches and recommend remedial and mitigating actions
- ICO point of contact
- Advise and assist in the DPIA process

Data Processor:
Any person, or organisation, who acquires records and processes personal data or who processes data on behalf of the Data Controller. An organisation can be both a Data Controller and Data Processor even where they may appoint third parties to carry out elements of data processing on their behalf, such as Cloud Computing services. CIPS is both Controller and Processor. Our third parties who handle data for us are also Data Processors.

6 Audit and review

The Data Protection Officer as chair of the Data Compliance Management Group performs and audit and review function. This policy outlines the GDPR requirements and objectives for the audit and the policies and processes will be reviewed at least on an annual basis to ensure future proofing and suitability and compliance.

All breaches will be reviewed on a case by case basis and will document the mitigating actions and steps to remedy the breach and return to security and protection of data. All process will be reviewed to ensure that CIPS operates within regulation timeframes for responding and reporting on all SARs and breach investigations.

7 Training and exercise

CIPS will ensure that training and information will be made available to all data processors. Training will be given to all new personnel and third party data processors. The Data Protection Officer will ensure that all training will remain current and fit for purpose.

8 Definitions

Data Subject
A living person who is the subject of personal data. The individual who has enhanced rights under data protection law.

Personal Data
Any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

Processing
Processing of data means any operation or set of operations which is performed on personal data, which includes but is not limited to, collection, storage, use, recording, disclosure or manipulation of data whether or not by automated means.

Data Breach
A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Organisations are required to report a data breach that creates a risk to the rights and freedom of the individuals concerned, to the Information Commissioner's Office (ICO) within 72 hours of the breach occurring or when made aware of the breach. If the individuals are at high risk of potential harm, then they must also be notified. Example: A computer account is hacked, and data listing contact details is accessed; or a member of staff takes unencrypted data out of the office against acceptable use policy and loses it.

Data Protection Officer (DPO)
This is the role in an organisation which has responsibility for ensuring that personal data is protected and that the organisation is compliant with the legislation. There should be a degree of independence so the DPO reports direct to the highest management level of the organisation as a part of the organisation's governance.

Binding Corporate Rules
A set of binding rules designed to allow organisations to transfer personal data from the EU to the organisation's related operations outside the EU but within the organisation. BCRs must demonstrate adequate safeguards and be authorised by the appropriate lead authority in the EU to vouch for data compliance.

Cross border processing
The processing of data by a Controller or Processor who operates in more than one EU member state, or the processing of data in one member state of subjects resident in one or more member state.

Privacy Shield
Prior to GDPR, the EU-US and Swiss-EU Privacy Shield Frameworks impose stronger obligations on US organisations to protect personal data of data subjects in EU. The privacy Shield, and now GDPR, requires the

US to monitor and enforce protection, and to cooperate with the Supervisory Authorities. This is administered by the Department of Commerce and the Federal Trade Commission.

Data Protection Authority
Also known as a Supervisory Authority. The national authority in every EU member state that enforces data protection in that member state. In the UK it is the Information Commissioner.

Data Privacy Impact Assessment
A methodology or tool used to identify and reduce the privacy risks of individuals when planning projects or policies that use or protect personal data.

Privacy by Design
The principle of the inclusion of data protection from the onset of the designing and planning of systems, rather than as a later addition.

Subject Access Request
The request by an individual to have access to, and information about, the personal data that a Controller holds. Application is by a subject access request that is free of charge.

Special Categories of Personal Data
This is sensitive data that requires more protection. It includes information revealing: race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life or sexual orientation.

Third party
Any person or organisation other than the Data Subject and the Data Controller. A third party can also be a Data Controller and a Data Processor.

9 Related policies and procedures

Supporting policies

Policy	Location
CIPS Information Security Policy	INT
CIPS Acceptable Usage Policy	INT
CIPS Retention Policy	EXT/INT
CIPS SAR Guidelines	EXT/INT
CIPS DPIA Process	INT
CIPS Breach Management Process	INT

10 Further information

ICO resources on breach management and reporting a personal data breach to the ICO:
https://ico.org.uk/for-organisations/resources-and-support/getting-ready-for-the-gdpr-resources/pdb/

ICO Guide to Personal Data Breaches:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

Contracts between controllers and processors:
https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf

Article 29 Working party Guidelines on Personal Data Breach Notification:
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

How to report a breach to ICO:
https://ico.org.uk/for-organisations/report-a-breach/

The European Data Protection Board, which will replace the Article 29 Working Party, may issue guidelines, recommendations and best practice advice that may include further guidance on personal data breaches. CIPS should look out for any future guidance.

https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/enforcement/what-european-data-protection-board-edpb_en