CPP Group

Group Data Protection & Information Security Policy

Date of Issue: December 2021
Version Number: V3
Sponsoring Executive: Chief Executive Officer
Approved: 8th December 2021
Classification: Internal

Document Control

Approval & Review Period:

CPPGroup Plc board approval is required for this policy. This policy applies to all Companies within the Group.

This policy will be reviewed when there are material changes in the nature of areas being covered, the business's strategic direction or operational plans. As a minimum the policy will be reviewed at least annually.

Revision History

Date Issued:	Version No.	Reason for Change:
31/07/2019	1	Combination of data protection and information security policies.
18/08/2020	2	Annual review by SS. Minor changes
11/11/2021	3	Annual review by Global Data Manager Major changes- Adding Data protection sections and information security policies list

1. Purpose

This policy regulates the way in which CPPGroup (CPP), together with its affiliates and group companies obtains, uses, holds, transfers and processes data, and the management and delivery of information security. The scope of policy requirements is defined in line with the ISO27001 series of international standards for information security management.

Further, it describes individuals' rights in relation to their personal data as processed by CPP. This policy ensures that CPP is compliant with applicable local and international legislation and regulation.

This Policy applies to all personal data in any format stored (internally or by third parties on behalf of CPP) for use within CPP's operations, including wholly or majority owned and all associate businesses where CPP has management control. Personal data is any information (or combination of information) about a living person (data subject), which allows that person to be identified. Effective management of data and Information Security enables the business to:

- Ensure that information assets receive appropriate levels of protection
- Ensure that critical controls are appropriately defined and implemented
- Ensure compliance with relevant regulatory and statutory requirements

Failure in Data Management

There are a number of potential implications of data management failures including:

- Reparation to stakeholders/customers in respect of any compromised data
- Fines from regulators
- Loss of investor and customer confidence
- Loss of business opportunity
- Reputational damage

2. Scope

This policy covers all information held by and on behalf of CPPGroup and the handling rules must apply to all CPP's colleagues, directors, employees, agents, contractors, consultants, advisors, service providers and any third parties handling CPP's information.

3. Compliance

Breaches or violations of this policy will be taken very seriously by the company. Any colleagues who violate the policy, incorrectly certifying compliance with the policy or who knowingly or negligently allow personnel under their supervision to do so, may be liable to disciplinary action in accordance with CPP's disciplinary procedures.

4. Roles and responsibilities

Chief Executive Officer

- Approving the Data Protection Policy and any changes on an annual basis as a minimum, ensuring it remains aligned with the requirements of all data protection regulations
- Receiving and reviewing management information reports to monitor the effectiveness of the implementation of the Data Protection Policy

Global Data Manager

- Ensuring that CPP' policies are adequately defined and implemented to ensure compliance with all data protection regulations

- Challenge and oversight of procedures to ensure the compliance with the requirements of this policy
- Providing clarification and guidance on any aspect of compliance with all data protection regulations

Line Managers

- Ensuring adherence to this policy and associated procedures and processes within their teams and areas of the business
- Ensuring and monitoring that working practices within their areas of the business are compliant with all data protection regulations
- Establishing and maintaining documented procedures to ensure that anyone requesting Confidential or Personal Data, either in person, electronically or by telephone is appropriately authenticated before information is disclosed
- Establishing and maintaining documented procedures to ensure personal data relating to customers is kept accurate and up to date

All Employees (whether permanent, temporary, or contracted) are responsible for:

- Complying at all times with this policy and any associated procedures
- Reporting any actual or perceived breaches via Jira or Secure Force
- Acknowledge that they have read and understood CPP's Acceptable Use Policy before they are given access to company's systems
- Notifying the human resources department if their personal details change

If you are unsure about the application of these guidelines to the information you hold as part of your job, you should contact your Line Manager.

5. Information Security

Data and information security management is defined as the management of risks arising from loss or compromise of the confidentiality, integrity, and/or availability of CPP's data / information assets. This policy applies to information listed below and assets used in handling this information:

- Stored on databases, computers and transmitted across internal and public networks
- Stored on removable media such as CD-ROMs, USB devices, hard disks etc
- Stored on fixed media such as hard disks and disk sub-systems
- Printed or hand-written on paper, whiteboards etc
- Presented using audio-visual media
- Spoken during telephone calls, meetings or conversations
- Sent by text or other communication methods.

5. 1 Information Security Policy Areas

CPP defines policy in a wide variety of information security-related areas which are described in detail in a comprehensive set of policy documentation that accompanies this overarching information security policy.

Each of these policies is defined and agreed by one or more people with competence in the relevant area and, once formally approved, is communicated to an appropriate audience.

The table in **Annex 1** shows the individual policies within the documentation set and summarises each policy's content and the target audience of interested parties.

5.2 Information Security - Specific Requirements

- All CPP's information assets are to be protected and managed in line with the agreed risk appetite, the value of the information and the risks applicable to the asset. This must be reviewed in an annual risk assessment process.
- Customer data must be protected from external and internal threats in accordance with best practice when designing systems, applications, products and processes.
- Data is to be retained in line with the data retention policies and only stored in approved secure locations.
- Adequate resources are to be provided to ensure that customer data is protected throughout its entire lifecycle when in the care of CPP or its suppliers.
- Access to CPP systems and information assets is to be approved and reviewed on a regular basis by line managers.
- All employees, contractors or third parties with access to CPP information are to be screened according to the local HR process.
- All suppliers with access to CPP information (including customer information) or CPP systems, should have appropriate due diligence performed on a regular basis.
- All CPP premises or premises where CPP information is stored, processed, or transmitted are to be secured against unauthorised digital or physical access.
- Information systems should ensure reliability and resilience is in line with the value of the information processes or the business services provided.
- Compliance to ISO27001, PCI DSS and Data Protection Regulations must be maintained along with contractual, legal and regulatory requirements as applicable to the business strategy.
- Breaches and Incidents are to be managed in a documented process. All colleagues have a responsibility to report security weaknesses or incidents.
- Onboarding new Suppliers/Business Partners need to be compliant with Supplier Policy

6. Personal data – Specific Requirements

6.1 Definitions

Personal data means any information relating to a natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special category data is personal data that needs more protection because it is sensitive. Example: racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation, data of vulnerable individual.

Data controller means the natural or legal person, public authority, agency, or any other body which, alone or jointly with others, determines the purposes and means of the processing.

Data processor means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

Processing (collection, recording, organising, structuring, storage, adaptation or alteration, retrieval, consultation, use, archiving).

Data subject is a living individual who can be identified from the personal data or from additional information held, or obtained, by CPP. For example, a CCTV image which can identify someone when linked to building access control codes.

6.2 Data Protection Principles

There are 6 key principles relating to the processing of personal data:

Lawfulness, fairness, and transparency
Data should be processed lawfully, fairly and in a transparent manner in relation to the data subject

Purpose limitation
Data should be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

Data minimisation
Data should be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed

Accuracy
Data should be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay

Storage limitation
Data should be kept for no longer than is necessary for the purposes for which the personal data are processed. Please refer to the Data Retention Policy for further details.

Integrity and confidentiality
Data should be processed in a manner that ensures appropriate **security** of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures

6.3 Individual's Rights

Data subjects have rights in relation to the way we handle their personal data. These include the following rights:

The right to be informed
Individuals have the right to be informed about the collection and use of their personal data. CPP must provide individuals with information including purposes for processing their personal data, retention periods for that personal data, and who it will be shared with. This is called 'privacy information'.

The right of access
The right of access, commonly referred to as ***subject access request (SAR)***, gives individuals the right to obtain a copy of their personal data, as well as other supplementary information. It helps individuals to understand how and why CPP is using their data, and check if we are doing it lawfully. All subject access request should be forwarded to Head of Operations Immediately.
Processes and training must be in place in each country to ensure compliance with data subject rights (in line with applicable regulations). who wishes to exercise their rights under data protection law as appropriate. We will communicate with data subjects in a concise, transparent, and easily accessible form and without undue delay. Appropriate privacy notices must be shared with data subjects, informing them of the business relevance and intended uses of data that is collected about them.

The right to rectification
Individuals have the right to have inaccurate personal data rectified. An individual may also be able to have incomplete personal data completed – although this will depend on the purposes for the processing.

The right to erasure
Individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.

The right to restrict processing
Individuals have the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data.

The right to data portability
Individuals have the right to receive personal data they have provided to a controller in a structured, commonly used and machine-readable format. It also gives them the right to request that a controller transmits this data directly to another controller.

The right to object
Individuals the right to object to the processing of their personal data at any time. This effectively allows individuals to stop or prevent you from processing their personal data.

Rights in relation to automated decision making and profiling
Automated individual decision-making is a decision made by automated means without any human involvement.

6.4 Privacy by design

CPP has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect, or process personal data will be subject to due consideration of privacy issues, including the completion of ***Data Protection impact assessments (DPIA)*** link to DPIA form.
For more information, please visit Coco for a DPIA procedure or contact the Global Data Manager.

7. Monitoring & Reporting

The data council consisting of country data leads, nominated by Country CEO's meets quarterly and acts as the strategic data management forum for the Group businesses. The data council provides support to the local country leadership team in the monitoring and reporting of country related data protection issues.

A Virtual Information Security Team (VIST) consisting of country security leads, nominated by Country CEO's, will provide support to the local country leadership team in monitoring and reporting of local country related information security issues.

Local data leads, VIST members and the country CEO should attest compliance with the policy on an annual basis using the Group Assurance dashboard.

The Head of Internal Audit will issue formal reports to the The Board . The reports cover the key risks and incidents within the Group along with relevant MI. Internal audit performs a review of the information security environment and data protection processes at least once every two years, ensuring that controls are managed appropriately and are effective.

8. Breaches and Security incidents reporting

All data and information security breaches must be reported via the business incident management process, escalated through line management and, where appropriate raised at the GRCC. In circumstances where the policy cannot be met, this is escalated through line management with the risks clearly documented.

A personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. If there is a personal data breach it should be reported in line with Breach policy without undue delay and, where feasible, not later than 72 hours after having become aware of so that CPP can report it to the ICO where appropriate.

Please report data breaches to Secure Force link and security incident to IT Service Desk via Jira link.

Annex 1 - Information Security Policies:

Policy Title	Areas addressed	Target audience
Acceptable Use Policy	Business use of the Internet and IT devices, Internet account management, security and monitoring and prohibited uses of the Internet service	All employees must be aware and comply with Acceptable use policy
Mobile Device Policy and BYOD (Bring Your Own Device)	Care and security of mobile devices such as laptops, tablets and smartphones, whether provided by CPP or the individual for business use	Users of company-provided and BYOD (Bring Your Own Device) mobile devices
Access Control Policy	User registration and deregistration, provision of access rights, external access, access reviews, password policy, user responsibilities and system and application access control	Employees involved in setting up and managing access control
Password Policy	A password policy is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly	All employees
Cryptographic Policy	Risk assessment, technique selection, deployment, testing and review of cryptography, and key management	Employees involved in setting up and managing the use of cryptographic technology and techniques
Physical Security Policy	Secure areas, paper and equipment security and equipment lifecycle management	All employees
Backup Policy	Backup cycles, cloud backups, off-site storage, documentation, recovery testing and protection of storage media	Employees responsible for designing and implementing backup regimes
Logging and Monitoring Policy	Settings for event collection. protection and review	Employees responsible for protecting CPP's infrastructure from attacks
Pen testing and Vulnerability Management Policy	Vulnerability definition, sources of information, vulnerability assessments	InfoSec and Data Governance/Compliance teams
Network Security Policy	Network security design, including network segregation, perimeter security, wireless networks and remote access; network security management, including roles and responsibilities, logging and monitoring and changes	Employees responsible for designing, implementing and managing networks (NetSec)

Secure Development Policy (SDLC Policies)	Business requirements specification, system design, development and testing and outsourced software development	Software development team
Purchasing Policy/Supplier Process	Due diligence, supplier agreements, monitoring and review of services, changes, disputes and end of contracts	Employees involved in setting up and managing supplier relationships
Retention Policy	Retention period for specific record types, use of cryptography, media selection, record retrieval, destruction, and review	Employees responsible for creation and management of records
Data Protection Policy	Applicable data protection legislation, definitions and requirements	All employees
Clear Desk and Clear Screen Policy	Security of information shown on screens and printed out. Part of Acceptable Use Policy	All employees
Information Classification Policy	Security procedures on data processing	All employees
BCP / DR	Process involved in creating a system of prevention and recovery from potential threats to a company. The plan ensures that personnel and assets are protected and are able to function quickly in the event of a disaster	All employees