The GoodCorporation Data Protection Framework

GoodCorporation has developed this framework to help organisations ensure that all personal data they obtain in the course of their operations is properly protected and is used responsibly.

It is primarily designed to cover the protection of personal data, but can also be applied to commercial data of other kinds.

This framework can be used to design, embed or evaluate an organisation's data protection system and culture.

For evaluation purposes, it can be used internally as a checklist or as the basis of an external review. GoodCorporation's independent assessment process looks at four levels of evidence for each practice in the framework and assesses each practice against a five-point scale:

The assessor checks:

that a policy exists
policy documents are reviewed

that a system is in place to implement the policy
systems are examined

that records exist that show that the system works in practice
a sample of records is reviewed

that stakeholders agree that the system works in practice
interviews are held with employees and other relevant stakeholders

The assessor awards a grade:

best practice
the policy and system are examples of best practice

no action required
the policy and system work well

improvement recommended
there is a policy and system that work but potential improvements have been identified

action required
there is a policy and system but they do not always work and require corrective action to reduce risk

significant action required
there is no policy or system, or it has largely broken down, and significant action is required to reduce risk

GoodCorporation helps businesses understand and manage their ethical risks by advising on best practice, helping them build appropriate practice into their operations and evaluating how well their processes are working.

Business ethics have been GoodCorporation's sole focus since its foundation in 2000. Having completed over 500 assignments across 60 countries, GoodCorporation possesses unrivalled benchmark data and real insight into how different companies and industries meet business ethics challenges. This experience and data underpin the methodologies we have developed to support our clients in implementing the highest management standards.

The GoodCorporation Data Protection Framework

The organisation is committed to protecting all personal data that it obtains in the course of its operations and to taking a responsible attitude to the use of such data.

1. Management and governance

MG1: There is a written and clearly articulated policy on data protection.

MG2: The policy and the measures in place have been formally approved by the board.

MG3: A summary of the policy is made public.

MG4: There is a named person responsible for data protection who is made known to employees and signposted as a source of guidance on data protection queries.

MG5: The responsible person has a reporting line to the board.

MG6: Senior management champions and sets the tone on data protection.

MG7: Adequate resources are devoted to implementing and monitoring data protection.

2. Risk assessment

RA1: An annual risk assessment considers data protection risks and the effectiveness of mitigation measures, both within the organisation and in association with third parties.

RA2: Risk assessments conducted on new activities consider data protection.

3. Security environment

Physical security

PS1: Buildings where data is stored are properly secured, with access controlled.

PS2: Hard-copy files and servers are kept in locked rooms, cabinets or storage facilities, with access controlled.

PS3: There is protection for equipment containing data from environmental hazards including fire, flood and power failure.

Information systems security

IS1: Access to electronic data is regulated by user identification and authentication.

IS2: Data access controls (including read, write, modify, move, copy and delete privileges) and, where necessary, security levels are in place and regularly reviewed.

IS3: Changes to the systems that store and process data are properly controlled and subject to segregation of duties.

IS4: Laptops, smart phones and other portable devices are encrypted and if appropriate have remote memory wipe facility.

IS5: There is a policy on the use of USBs, hard drives and other external devices.

IS6: There is independent testing of the robustness and appropriateness of the IT security controls and the person responsible for data protection is informed of the results.

4. Legal environment

LE1: There is a process to monitor and comply with the applicable legal requirements in all the jurisdictions in which the organisation handles data.

LE2: The organisation has registered with the appropriate data protection authorities in the different jurisdictions in which it operates.

LE3: The legal implications of any data transfers, including cross-border data transfers, have been considered.

LE4: The legal implications of the use of any third parties to handle data on the organisation’s behalf have been considered.

5. Operational data practices

OP1: The organisation obtains the subjects’ free, informed consent prior to gathering data.

OP2: If the organisation buys data, it ensures that the data subjects have consented to the use to which the data is being put.

OP3: The organisation collects only the information that it requires for its stated purpose.

OP4: The organisation communicates its data protection policies and practices, what it will use the data for and why, at all data collection points.

OP5: The organisation communicates its policy on how long it will keep data and how it will dispose of it.

OP6: The organisation obtains subjects’ consent prior to disclosing or selling their data to third parties and explains the purpose of the disclosure.

OP7: The organisation makes reasonable efforts to explain to vulnerable people their rights and to guide them on sensible precautions they can take to protect their data.

OP8: There is a policy on the use of CCTV and audio recording which is made available to all those who could be recorded.

OP9: Information collected is used only in the ways for which the organisation has explicit permission.

OP10: There are processes which govern the monitoring of employees' use of internet, email and other communications systems.

OP11: Data is kept up to date where this is necessary to avoid harm or detriment to the data subject.

OP12: There are rules governing the temporary or permanent removal of data, whether hard-copy or electronic, from the organisation's secure sites.

OP13: Where relevant, the organisation recognises the data subject's right to be forgotten.

OP14: Data is disclosed to third parties only by those employees with authority to do so.

OP15: Data is held for a defined period of time or until the need for it has passed and then deleted.

OP16: Processes to destroy data render it irrecoverable. Confidential waste is properly handled.

OP17: Data is securely erased from equipment prior to the equipment's disposal.

6. Managing employees who handle data

ME1: Employees receive periodic training on data protection and, where relevant, on how to handle data protection queries.

ME2: There are periodic communications campaigns to raise employees' awareness of data protection.

ME3: Data protection policies and procedures are readily accessible for employees' reference.

ME4: Employees are subject to contractual confidentiality obligations.

ME5: Disciplinary processes are used to support observance of data protection policies.

7. Managing third parties

TP1: The organisation ensures that service providers' or business partners' data protection practices are adequate prior to instructing them to collect, handle or destroy data on its behalf.

TP2: The organisation imposes adequate contractual obligations on service providers or business partners relating to data protection.

TP3: The organisation actively manages its service providers or business partners to ensure data is properly protected.

TP4: The organisation conducts spot checks on service providers or business partners to ensure compliance with its standards.

TP5: Sanctions are imposed where service providers or business partners fail to meet the organisation's required standards for data protection.

8. Managing requests for disclosure

RD1: Protocols are in place governing disclosure of data (credentials, criteria, legal advice, requirements placed on recipient etc.).

RD2: The organisation responds to public authorities' requests for data constructively and responsibly.

RD3: There are processes to respond to data subjects' requests for access.

9. Breaches

BR1: Staff are aware of whom they should speak to if they suspect a data breach.

BR2: There is a confidential means of reporting data protection concerns.

BR3: The organisation has a protocol governing data breaches, that includes information on how to respond and how to inform and compensate the affected data subjects.

BR4: The organisation investigates the causes of data breaches and takes remedial action.

BR5: The organisation works proactively with authorities investigating potential breaches.

10. Monitoring and review

MR1: There is a regular review by senior management of the effectiveness of the data protection measures in place.

MR2: There are periodic audits of the management of data protection.

MR3: There is a periodic report to the board on data protection, along with information and indicators on data breaches.

www.goodcorporation.com