goodcorporation

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. It is based on the EU General Data Protection Regulation.

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, which is referred to in the organisation's code of conduct.

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

MG3: Both the complete policy and a summary of the policy are made public.

MG4: The organisation has readily accessible privacy notices in place which include the legal basis for processing data, data retention periods and a data subject's right to complain and to whom. The information provided in the privacy notice is given in a clear, concise and easy to understand language.

MG5: 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.

MG6: The responsible person has a reporting line to the board.

MG7: Senior management champions and sets the tone on data protection.

MG8: Adequate resources are devoted to implementing and monitoring data protection.

2. Risk assessment

RA1: Regular risk assessments consider data protection risks and impacts on privacy, and the effectiveness of mitigation measures, both within the organisation and in association with third parties. Assessments are conducted at least annually.

RA2: Data protection and privacy are considered by design and by default in respect of any new activities and products, including privacy impact assessments where necessary.

3. Security environment

Physical security

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

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

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, amend, 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 a policy on the use of private and/or employee-owned devices.

IS7: 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.

IS8: Specific training on information systems security is organised for all employees.

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 or where liability might arise.

LE2: Changes to the applicable data protection legislation are communicated clearly and speedily to the relevant people within the organisation. The impact of any changes on the organisation's policies and processes is constantly evaluated.

LE3: Where legally required, the organisation has registered with the appropriate data protection authorities in the different jurisdictions in which it operates.

LE4: The legal implications of any data transfers, including cross-border data transfers, have been considered, and there is a system in place to ensure that data transfers do not compromise the adequate protection of personal data.

LE5: Where any third parties process data on the organisation's behalf, the legal implications of this have been considered and the obligations for each relevant party are clearly set out in a contractual manner.

5. Operational data practices

OP1: Where the organisation relies on consent as the legal basis for processing personal data, it obtains subjects' free, specific, informed and unambiguous consent prior to gathering the data.

OP2: The organisation has systems in place to ensure the recording of any consent given and the existence of an effective audit trail.

OP3: The organisation records and regularly reviews its processing activities using a data map or inventory, including the purpose and legal basis for that processing, and information about where data has originated and where it is shared.

OP4: If the organisation buys data, it ensures that data subjects have consented to the use to which the data is being put.

OP5: The organisation collects only such information that it requires for its stated purpose, and strives to minimise any data collection to that which is strictly necessary.

OP6: The organisation communicates its data protection policies and practices and what it will use the data for and why, at all data collection points.

OP7: The organisation communicates its policy on how long it will keep data and how it will dispose of it.

OP8: The organisation obtains subjects' consent prior to disclosing or selling their data to third parties and explains the purpose of the disclosure.

OP9: 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.

OP10: The organisation has systems in place to verify data subjects' ages and to obtain parental or guardian consent for any data processing where necessary.

OP11: Privacy notices are adapted to the needs of children or other vulnerable individuals where their data is being processed.

OP12: There is a policy on the use of CCTV and audio recording which is made available to all those who could be recorded.

OP13: Information collected is used only in the ways for which the organisation has explicit permission.

OP14: There are processes which govern the monitoring of employees' use of internet, email and other communications systems.

OP15: The organisation has a clear process to review any personal data it holds.

OP16: The organisation has a system in place to consider the most appropriate way of sharing data, including where appropriate by way of pseudonymisation.

OP17: Data is kept up to date as necessary and a system is in place to identify inaccuracies and, where relevant, to correct them.

OP18: There are rules governing the download, printing or other removal of data, whether hard-copy or electronic, from the organisation's secure sites.

OP19: The organisation recognises data subjects' right to erasure and has a system in place which addresses such requests.

OP20: Data is disclosed to third parties only by those with authority to do so.

OP21: Data is held for a defined period of time or until the need for it has passed and then the data is securely suppressed or deleted.

OP22: Processes exist to destroy data or to render it irrecoverable. Confidential waste is properly handled.

OP23: Data is securely erased from equipment prior to the equipment's disposal.

OP24: The organisation has additional safeguards in place for the processing of sensitive personal data.

OP25: Where the organisation processes data on behalf of other organisations, it only acts on the documented instructions of that organisation.

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: The person designated as being responsible for data protection within the organisation receives specific training and is aware of a data protection officer's tasks and responsibilities.

ME3: There are regular communications campaigns to raise employees' awareness of data protection.

ME4: Data protection policies and procedures are readily accessible for employees' reference.

ME5: Employees are subject to written contractual confidentiality obligations.

ME6: Disciplinary processes are used to support observance of data protection policies.

7. Managing routine access by third parties

TP1: The organisation communicates its data protection policies and standards clearly to service providers and business partners.

TP2: The organisation ensures that service providers or business partners can sufficiently assure that their data protection practices are adequate prior to instructing them to collect, handle or destroy data on its behalf.

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: The organisation imposes sanctions where service providers or business partners fail to meet its required standards for data protection.

8. Managing requests

RQ1: Protocols are in place governing the disclosure of data (credentials, criteria, legal advice, requirements placed on recipient etc.).

RQ2: The organisation responds to public authorities' requests for data constructively and responsibly.

RQ3: There are clear processes in place to respond to data subjects' requests, including:

- for access;
- to have inaccuracies corrected;
- to prevent direct marketing;
- to prevent automated decision-making and profiling; and
- for data portability.

RQ4: Systems are in place which clearly establish the decision-making process in response to any type of request, and such systems are understood within the organisation.

9. Breaches

BR1: IT systems and data storage facilities are regularly checked for any data breach.

BR2: Staff are aware of whom they should speak to if they suspect a data breach.

BR3: There is a confidential means of reporting data protection concerns.

BR4: The organisation has a protocol governing data breaches, that includes information on how to respond and how to inform the affected data subjects as well as notify the relevant authority of the breach in a timely fashion and without undue delay.

BR5: The organisation investigates the causes of data breaches and takes remedial action.

BR6: The organisation works proactively with authorities investigating potential breaches.

10. Monitoring and review

MR1: The documentation requirements for the various sets of data are regularly reviewed and a clear process is in place to identify the organisation's record keeping obligations.

MR2: There is a regular review by senior management of the effectiveness of existing data protection measures.

MR3: There are periodic audits of the management of data protection.

MR4: The organisation conducts periodic unannounced simulations of breaches and attacks which could potentially compromise data protection and privacy.

MR5: There is a periodic report to the board on data protection, along with information and indicators on data breaches.