PUBLISHED BY
bookboon

John Kyriazoglou

The CEO's Guide To GDPR Compliance

The guide for C-Suite Members to ensure GDPR compliance

JOHN KYRIAZOGLOU

THE CEO'S GUIDE TO GDPR COMPLIANCE

THE GUIDE FOR C-SUITE MEMBERS TO ENSURE GDPR COMPLIANCE

The CEO's Guide To GDPR Compliance:
The guide for C-Suite Members to ensure GDPR compliance
1st edition

ISBN 978-87-403-2229-3

CONTENTS

OVERVIEW

This guide contains a sample of measures and controls to support your senior management accountability responsibilities in meeting the privacy compliance requirements and obligations of the new European General Data Protection Regulation (GDPR) for your company or organization.

PREFACE: MAJOR HIGHLIGHTS OF GDPR

Thucydides: 'Errors that have been committed without intention should be forgiven'.

Introduction

On 25 May 2018, the EU General Data Protection Regulation ('GDPR' or 'the Regulation') will come into force, without the need for national laws to implement its provisions.

The EU General Data Protection Regulation (GDPR) represents a major change and radical improvement in the personal data protection compliance regime for data controllers and data processors for companies and organizations, called 'enterprises' in GDPR terms (as per Appendix 1), operating in the European Union.

Central in personal data protection is privacy protection of the rights of persons, called data subjects in the language of GDPR (as per Appendix 1). They must know what data are maintained on them, correct and improve their accuracy, limit their use, and be assured that confidentiality and integrity is maintained at all times.

These data may be processed by enterprises in manual and computerized systems that maintain and process valuable information, or provide services to multiple users concurrently, on the basis of the provision of security safeguards against unauthorized access, use, or modifications of any data.

Enterprises must protect manual and computerized systems against all types of security and privacy risks, abuse of personal data, unauthorized use, errors, illegal intrusions, disruption of operations, and physical damage, among other things.

The growing number of computer applications processing business transactions that involve using valuable information or assets and the ever-increasing number of criminal actions directed against them underscore the need for finding efficient and effective solutions to the computer security and privacy issues.

In the future, concerns for privacy and security of personal data must become integral in the planning and design of manual and computer systems and their applications.

People will appreciate doing business with companies and organizations that demonstrate a respect for their privacy rights. This will ultimately lead to a competitive advantage for businesses. Companies and organizations can see this as an opportunity to review and improve their personal information handling practices.

GDPR Highlights

The major highlights of this regulation relate to:

1. **Data protection principles**
   Organizations must ensure that all processing operations of personal data must adhere to and comply with the following principles:

   1. 'Lawfulness, fairness and transparency';
   2. 'Purpose limitation';
   3. 'Data minimisation';
   4. 'Accuracy';
   5. 'Storage limitation';
   6. 'Integrity and confidentiality'; and
   7. 'Accountability'.

2. **Data Protection Impact Assessments (DPIAs)**
   Organizations must undertake DPIAs when conducting risky or large scale processing of personal data.

3. **Consent**
   3.1. Consent to process data must be freely given and for specific purposes by data subjects.
   3.2. Data subjects must be informed of their right to withdrawn their consent.
   3.3. Consent must be explicit in the case of sensitive personal data or trans-border dataflows.

4. **Mandatory breach notification**
   4.1. Organizations must notify supervisory authority of data breaches 'without undue delay' or within 72 hours, unless the breach is unlikely to be a risk to individuals.
   4.2. If there is a high risk to data subjects, then such data subjects should also be informed.

5. **Data subject rights**
   There are several rights, such as:

   5.1. The right to be forgotten, i.e., the right to ask data controllers to erase all personal data without undue delay in certain circumstances.
   5.2. The right to data portability, i.e., the right of individuals that have provided personal data to a service provider, to require the provider to transfer or "port" the data to another service provider provided this is feasible.
   5.3. The right to object to profiling, i.e., the right not to be subject to a decision based solely on automated processing, etc.

6. **Data Protection by Design and by Default**
   6.1. Organizations should design data protection into the development of business processes and new systems.

7. **Personal data definitions**
   7.1. The GDPR applies to all personal data that is collected in the EU, regardless of where in the world it is processed. Any database containing personal or sensitive data collected within the EU will be in scope, as will any media containing personal or sensitive data. Any organisation that has such data in its systems, regardless of business size or sector, will have to comply with the GDPR.

   7.2. Personal data is anything that can identify a 'natural person' ("data subject"); and can include information such as a name, a photo, an email address (including work email address), bank details, posts on social networking websites, medical information or even an IP address, etc.

   7.3. This definition is critical because EU data protection law only applies to personal data. Information that does not fall within the definition of „personal data" is not subject to EU data protection law.

   7.4. 'Sensitive Personal Data' are personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.

More definitions of GDPR terms, such as biometric data, controller, processor, etc., are contained in Appendix 1.

8. **Administrative Fines for GDPR non-compliance**
   Article 83 GPDR includes requirements concerning penalties. When DPAs decide whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case, due regard shall be given to the following:

   - nature, gravity and duration of the infringement, the number of data subjects affected and the level of damage suffered by them
   - intent or negligence
   - action taken to mitigate the damage
   - degree of responsibility
   - any previous infringements
   - degree of cooperation with supervisory authority
   - categories of personal data affected
   - manner in which the infringement became known to the supervisory authority
   - compliance with previously ordered measures
   - adherence to approved codes of conduct pursuant or approved certification mechanisms
   - any other aggravating or mitigating factor.

   Administrative fines are up to €10,000,000 or, in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher, in case of a violation of:

   - obligations of the controller and the processor pursuant to Articles 8, 11, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 42 and 43
   - obligations of the certification body pursuant to Articles 42 and 43
   - obligations of the monitoring body pursuant to Article 41(4).

   Administrative fines are up to €20,000,000 or, in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher, in case of a violation of:

   - the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9
   - the data subjects' rights pursuant to Articles 12 to 22
   - the transfers of personal data to a recipient in a third country or an international organization pursuant to Articles 44 to 49
   - any obligations pursuant to Member State law adopted under Chapter IX (specific processing situations)
   - non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority.

Migrating to the new privacy regime

The exercise of proper corporate governance, control and management of personal data is fundamental to ensure, and be able to demonstrate, compliance with the GDPR for all companies and organizations.

Migrating effectively and efficiently to the new (GDPR) data protection and privacy regime will be challenging and require:

1. Great amounts of corporate resources (Management, legal, IT, human and financial resources, etc.);
2. Spiritual energy, motivation and inspiration; and
3. Engagement and full involvement of corporate management and employees.

The commitment of corporate resources for GDPR is the task of the board of directors of the company. See Appendix 2 for more on board responsibilities.

Adding spiritual energy, motivation and inspiration to your activities for better implementation of GDPR may be achieved by employing the B^4 workplace wellness model and by considering the ancient Greek sayings and quotations before each data protection activity.

Engaging and involving corporate management and employees in GDPR activities and improving their human skills and dexterities may be achieved by the execution of an improvement plan, as detailed in Appendix 3: Data Protection Team Improvement Plan.

B^4 Workplace Wellness Model

This workplace wellness model (B^4 workplace wellness model) for GDPR activities has four dimensions: Believing; Bonding; Belonging; and Benefiting.

Dimension 1: Believe. Believe (or have faith) in God, nature, yourself, your family, your company (its vision, mission, products, services, quality, personal and other data processed, etc.), your employees, your associates, your community, your country and your values and beliefs.

Dimension 2: Bond. Bond (or unite) with God, nature, your friends, your family, your employees, your associates, your community, your company (its vision, mission, products, services, quality, personal and other data processed, etc.), your country and your profession.

Dimension 3: Belong. Belong (or attach) to your family, your nation, your company (its vision, mission, products, services, quality, personal and other data processed, etc.), your employees, your associates, your community and your country.

Dimension 4: Benefit. Benefit (be of service or be good to) nature, yourself, your family, your company (its vision, mission, products, services, quality, personal and other data processed, etc.), your employees, your associates, your community, your country, your nation, others less advantaged, and your friends.

These four workplace wellness dimensions, will support you and your people fully in GDPR implementation and compliance, when all your data protection activities are permeated by their specific aspects.

It is mainly your job and responsibility and part of your 'duty of care' duties as a business manager, corporate leader, board member or professional consultant, etc., to ensure that that an effective data protection framework with its constituent components and controls is implemented fully by your people to satisfy your company's needs and requirements for protecting the privacy of individuals (data subjects).

To ensure it is done, you need to implement a set of data protection activities and implement the appropriate policies and procedures (as per Parts 1 to 4) by defining '*what needs to be done*' and '*how to do it*'. To make certain it is done very well, you must involve and engage your people and explain well '*why to do it*' by giving them the ***rationale***, the ***motivation*** and the ***inspiration*** for doing what needs to be done.

'What' and 'how' engage the minds of your people. But it's the 'why' that captures their hearts.

The level of existing compliance will affect the enterprise resources that are required.

However, taking a positive approach, and embracing the changes to comply with the data protection principles of the GDPR, will improve customer trust, employee productivity, corporate records management and business opportunities, such as those associated with the digital economy as well as improve the lives of individuals.

The first thing that board directors and senior management must do, is to prepare their organization by utilizing the following questionnaire that reflects the aspects of board and management accountability, as the first and most critical issue in starting to prepare to implement the GDPR for their organization.

Board and management accountability

Organizations, through their boards and management structures and processes, must prove they are accountable, in terms of GDPR, by:

1. Establishing a culture of monitoring, reviewing and assessing data processing procedures.
2. Minimizing data processing and retention of data.
3. Building in privacy and security safeguards to data processing activities.
4. Documenting data processing policies, procedures and operations that must be made available to the data protection supervisory authority on request.

All enterprises (companies, organizations, etc.) are responsible for the protection of personal information and the fair handling of it at all times, throughout the organization and in dealings with third parties. Additionally, care in collecting, using and disclosing personal information is essential to continued consumer confidence and good will.

Management accountability is a common principle for companies and organizations across many disciplines; the principle embodies that organizations live up to expectations for instance in the delivery of their products and their behaviour towards those they interact with.

The General Data Protection Regulation (GDPR) integrates accountability as a principle which requires that organizations put in place appropriate technical and organizational measures and be able to demonstrate what they did and its effectiveness when requested.

Enterprise, and not Data Protection Authorities, must demonstrate that they are compliant with the law.

Such measures include:

1. Adequate documentation on what personal data are processed, how, to what purpose, how long;
2. Documented processes and procedures aiming at tackling data protection issues at an early state when building information systems or responding to a data breach;
3. The presence of a Data Protection Officer integrated in all aspects of personal data processing, etc.

Implementing GDPR Accountability

To discharge all board and management accountability responsibilities in complying with GDPR, a set of data protection activities must be designed, developed and implemented very effectively.

These contain activities and questionnaires with a sample of questions and measures that senior management and board directors can use to assess the basic level of compliance that currently exists within their enterprise.

The measures and questions do not go into great and very specific detail, but rather aim to ensure that a business is in control of personal information and its lawful processing.

For a more detail review and extended measures for GDPR implementation, the resources at the end of this book should be consulted (see Bibliography).

These data protection activities are structured in three chapters:

Chapter 1: Data Protection Management and Governance Activities

The objectives of the data protection activities of this part are:

1) to assign responsibility and accountability to the highest level of management for monitoring the implementation and assessment, and demonstrating, the quality of compliance and application of GDPR to external stakeholders and supervisory authorities, and
2) to raise and maintain awareness of data protection in all corporate staff and functions.

Chapter 2: Managing Information Security and Privacy Risks

The objective of the data protection activities of this part is to establish mechanisms (plans, policies, procedures and technological platforms, etc.) so that your company complies fully with the relevant obligations of GDPR related to privacy risk assessment, confidentiality, integrity, availability, resilience, recoverability and security of personal data processed by the company.

Chapter 3: Integrating Data Protection into Business Functions

The objective of these activities is to incorporate data privacy into the operations and practices of the enterprise consistent with the data protection and privacy policy, legal requirements of GDPR, and operational risk tolerance of the company.

These parts are complemented by five appendices: (GDPR Definitions, Board Responsibilities, Data Protection Team Improvement Plan and Technical and Organizational Data Protection Measures).

These are detailed next.

1 DATA PROTECTION MANAGEMENT AND GOVERNANCE ACTIVITIES

'As bees extract honey from thyme, the strongest and driest of herbs, so sensible men often get advantage and profit from the most awkward circumstances'.

– Plutarcht

1. **Overview**
   This part contains: (a) several quotations and a short story to inspire you and your team to act effectively; and (b) a set of data protection activities with controls and examples of relevant measures to be implemented to comply with the DP management and governance issues of GDPR (articles 5, 15 to 22, 24, 26, 27, 28, 30, 32 to 34, 36, 37 to 39 and recitals 58, 59, 61, 63 to 65, 67 to 70, 73 74, 77, 78, 84 to 86 and 156).

2. **Objectives**
   The objectives of the data protection activities of this part are:

   1) to assign responsibility and accountability to the highest level of management for monitoring the implementation and assessment, and demonstrating, the quality of compliance and application of GDPR to external stakeholders and supervisory authorities,
   2) to raise and maintain awareness of data protection in all corporate staff and functions, and
   3) to enable privacy reporting.

3. **Inspiring you and your DP team for action**
   To inspire yourself and your DP team to take action, it is wise to consider the meaning and guidance offered by the following ancient Greek sayings and short story related to governance. The essential message they convey will enlighten and add spiritual fluid to you and your team. This will support all your efforts in implementing the activities related to DP management and governance, in a more effective way.

Saying 1: 'Do not govern with arrogance' by the Seven Sages;

Saying 2: 'The worst misfortune you can get to know is when your country is governed by men without any value' by Dimocritus;

Saying 3: 'No government can maintain itself if it is based on injustice, betrayal and perjury' by Dimosthenis;

Saying 4: 'Friendship, freedom, justice, wisdom, courage and moderation are the key values that define a good society' by Plato;

Saying 5: 'You don't develop courage by being happy in your relationships every day. You develop it by surviving difficult times and challenging adversity' by Epicurus; and

Short story: The meaning of **Aesop's fable 'A mother crab and her son'** *that example by corporate leaders is more powerful than precept,* as detailed next: 'A mother crab criticized her son for walking sideways, whereupon the son asked his mother to show him how to walk straight. Of course the mother crab was unable to walk any straighter than her son, and soon apologized for criticizing what she herself was unable to do'.

In summary, the meaning of the above sayings and short story is: good data protection management and governance is best based on courage, justice and leading by example.

Tip: Considering these within the framework of the proposed workplace wellness model (of four dimensions: Believing; Bonding; Belonging; and Benefiting), will support you in motivating and inspiring yourself and your DP team so that you all best execute the following **DP management and governance activities** and reach your stated objectives listed above.

These data protection activities are detailed next.

4. **DP Management and Governance (DPMG) Activities**
   Implementing data protection management and governance controls to comply with the relevant GDPR articles referenced in this chapter entails the execution of a minimum set of activities as described next.

1.1 DPMG ACTIVITY 1: APPOINT DATA CONTROLLER

GDPR Compliance Requirements

The GDPR (articles 24, 26, 27 and 29) requires the data controller to implement appropriate technical and organisational measures to ensure and be able to demonstrate compliance with the GDPR. The appropriateness of these measures is based on a risk assessment that takes into account the nature, scope, context, and purposes of the processing as well as the risks of varying likelihood and severity for the rights and freedoms of individuals. There is a specific reference that, where proportionate in relation to the processing activities, data protection policies shall be implemented.

Your company's/organization's duty

1. Assign the duties and responsibilities of controller with a specific mandate for implementing GDPR to a competent company officer and have them approved by the board.
2. Ensure this person is well trained and has the adequate skills, support and knowledge.
3. Ensure all senior management levels involved (CEO, CIO, CRO, etc.) support this role.
4. Craft, approve and implement a GDPR Implementation Action Plan.
5. Craft and issue data protection instructions to staff.
6. Ensure all corporate roles and business areas (corporate security, risk management, HR, IT security, etc.) are assigned data protection responsibilities and are approved by the board.
7. Ensure these data protection roles are included in job descriptions of all staff involved in data protection.

Additional Information

For more information on implementing additional measures related to this DPMG activity, see:

1. Appendix 4: Technical and organizational data protection measures
2. Appendix 2: Board Responsibilities
3. Examples of other detail plans and policies described above are included in my books listed in the Bibliography.

1.2 DPMG ACTIVITY 2: ASSIGN DATA PROTECTION OFFICER (DPO)

GDPR Compliance Requirements

The GDPR requires (Articles 37 to 39) the designation of a DPO in three specific cases:

a) where the processing is carried out by a public authority or body;
b) where the core activities of the controller or the processor consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale; or
c) where the core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

Your company's/organization's duty

1. Assign the duties and responsibilities of a DPO with a specific mandate for monitoring the implementation of GDPR to a competent company officer and have them approved by the board.
2. Ensure this person is well trained and has the adequate skills, support and knowledge.
3. Ensure all senior management levels involved (CEO, CIO, CRO, etc.) support this role.
4. Ensure this person sets up a system and implements activities to monitor GDPR compliance and maintain compliance documentation.
5. Ensure the details of this person are published in the privacy notice and communicated to the Data Protection Authority ad to employees and partners.

Additional Information

For more information on implementing additional measures related to this DPMG activity, see:

1. Appendix 4: Technical and organizational data protection measures
2. Appendix 2: Board Responsibilities
3. Examples of other detail controls, plans and policies described above and needed to implement the GDPR better are included in my books listed in the Bibliography.

1.3 DPMG ACTIVITY 3: SATISFY DATA PROTECTION PRINCIPLES

GDPR Compliance Requirements

The GDPR requires (main Article 5, other supporting articles: 6, 25 and 32 and recital 39) that the general principles that all processing activities must abide by, include: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage or retention limitation; integrity and confidentiality; and accountability. Also the accountability principle states that data controllers are responsible for and able to demonstrate compliance with the data processing principles.

Your company's/organization's duty

1. **Privacy Notice**. Update your privacy notices to include the required additional transparency/fair processing information to individuals.
2. **Data Governance Practices**. Update your data collection, data handling, security and data retention practices and policies to ensure compliance with the data protection principles (Article 5: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage or retention limitation; integrity and confidentiality; and accountability).
3. Require contractual assurances that any bought-in data lists are legally compliant with GDPR requirements.
4. Implement and maintain appropriate technical and organisational security measures, such as: pseudonymisation, encryption, security policies, data quality procedure, etc.
5. Establish and maintain a Personal data holdings inventory.
6. Implement Template consent forms
7. Conduct regular security testing
8. Keep testing records.
9. Keep documentary evidence to demonstrate compliance with the data protection principles for accountability purposes (e.g. processing records, data mapping, data governance frameworks, DPIAs).
10. Craft and issue data privacy and data protection guidelines.
11. Maintain awareness and communication on data protection issues and responsibilities.
12. Train relevant staff on data protection compliance best practice.
13. Keep training records.

Additional Information

For more information on implementing additional measures related to this DPMG activity, see:

1. Appendix 4: Technical and organizational data protection measures
2. Examples of other detail controls, plans and policies described above and needed to implement the GDPR better are included in my books listed in the Bibliography.

1.4 DPMG ACTIVITY 4: APPOINT DATA PROCESSOR

GDPR Compliance Requirements

The GDPR obliges (articles 28 to 36) data controllers to only outsource processing to those entities that have sufficient guarantees to implement appropriate measures to guarantee GDPR compliance and to have a contract or binding act that governs the relationship.

Article 28 also limits the ability of processors to subcontract without consent of the data controller, and what guarantees need to be in place in this arrangement.

Your company's/organization's duty

1. Ensure senior management assigns the duties and responsibilities of processor to a third company with a specific mandate and a contract for processing personal data according to GDPR.
2. Ensure that you have executed a due diligence before a contract has been signed with the third company.
3. Ensure the contract (see example in Appendix 10) contain terms and conditions (internal controls, security, confidentiality statements of employees, audit and inspection rights, etc.) to ensure compliance with GDPR obligations in processing the personal data of your company.

Additional Information

For more information on implementing additional measures related to this DPMG activity, see:

1. Appendix 4: Technical and organizational data protection measures.
2. Appendix 5: Controller-Processor Agreement.
3. Examples of other detail controls, plans and policies described above and needed to implement the GDPR better are included in my books listed in the Bibliography.

1.5 DPMG ACTIVITY 5: TRAIN STAFF ON DATA PROTECTION

GDPR Compliance Requirements

The GDPR (articles 5 and 39) sets out the tasks of the DPO, as follows: advise the Controller or Processor and its employees of data protection obligations; monitor compliance, including assigning responsibilities, awareness-raising and training of staff involved in processing operations and audits; advising on and monitoring DP impact assessments, cooperating and contacting the supervisory authority as required, and reviewing processing risk.

Your company's/organization's duty

1. Craft and implement an awareness, communication and training plan.
2. Ensure this plan is adequately supported (budget, resources, etc.).
3. Ensure this is executed to raise awareness and train all staff in the data protection responsibilities, policies and procedures implemented by the organisation to manage data privacy and information security risks.
4. Keep training records.

Additional Information

For more information on implementing additional measures related to this DPMG activity, see:

1. Appendix 4: Technical and organizational data protection measures.
2. Appendix 3: Data Protection Team Improvement Plan.
3. Examples of other detail controls, plans and policies described above and needed to implement the GDPR better are included in my books listed in the Bibliography.

1.6 DPMG ACTIVITY 6: ENABLE THE RIGHTS OF DATA SUBJECTS

GDPR Compliance Requirements

The GDPR requires (main articles 15 to 22 and recitals 58, 59, 61, 63 to 65, 67 to 70, 73 and 156) for controllers to ensure that the data subjects shall have several rights regarding their personal data processed by the company, such as: the right of access, the right to rectification, the right to erasure ('right to be forgotten'), the right to restriction of processing, the right to data portability, the right to object and the right to object to automated individual decision-making, including profiling, etc.

Your company's/organization's duty

1. Ensure mechanisms (strategies, plans, policies, procedures, software tools, etc.) are defined, developed and implemented to ensure the exercise of the rights of data subjects for their personal data processed and stored by the company.
2. Ensure these include:
   2.1. Personal Data Access Procedures.
   2.2. Personal Data Complaints Procedures.
   2.3. Personal Data Rectification Procedures.
   2.4. Personal Data Objection Procedures.
   2.5. Personal Data Portability Procedures.
   2.6. Personal Data Erasure Procedures.
   2.7. Personal Data Handling Information Procedures.

Additional Information

For more information on implementing additional measures related to this DPMG activity, see:

1. Appendix 4: Technical and organizational data protection measures
2. Examples of other detail controls, procedures, plans and policies described above and needed to implement the GDPR better are included in my books listed in the Bibliography.

1.7 DPMG ACTIVITY 7: DEMONSTRATE COMPLIANCE WITH GDPR

GDPR Compliance Requirements

The GDPR requires (articles 5, 24, 26, 28, 30. 32, 33 and 34 and recitals 74, 77, 78 and 84 to 86) the data controller to implement appropriate technical and organisational measures to ensure and be able to demonstrate compliance with the GDPR. The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.

Your company's/organization's duty

1. Implement appropriate technical and organisational measures to ensure and be able to demonstrate compliance with the GDPR.
2. Ensure these measures include:
   2.1. Mapping current processing activities (and populating an internal data processing register.
   2.2. Execution of internal data protection policies (security, retention, encryption, etc.).
   2.3. Maintaining records of processing according to article 30 of GDPR and a Personal Data Inventory.
   2.4. Providing notices to employees of all data collected and for what purpose.
   2.5. Managing customer marketing protocols and consents (cookies and online tracking and consent mechanisms, etc.).
   2.6. Managing other third-party data (supplier/business partner notices/consents/ data transfers to third parties, etc.).
   2.7. Managing data subject rights (responding to data subject rights, i.e. subject access, rectification, erasure, restriction of processing, data portability, right to object to certain types of processing and right to object to or obtain human intervention in certain automated decision making, etc.).
   2.8. Executing DPIAs, where required and including privacy by design and by default guidance principles in all systems, products and services.

Additional Information

For more information on implementing additional measures related to this DPMG activity, see:

1. Appendix 4: Technical and organizational data protection measures
2. Appendix 2: Board Responsibilities
3. Examples of other detail controls, plans and policies described above and needed to implement the GDPR better are included in my books listed in the Bibliography.

2 MANAGING INFORMATION SECURITY AND PRIVACY RISKS

'To make no mistakes is not in the power of man; but from their errors and mistakes the wise and good learn wisdom for the future'.

– Plutarch

1. **Overview**
   This part contains: (a) several quotations and a short story to inspire you and your team to act effectively; and (b) a set of data protection activities with controls and examples of relevant measures to be implemented to comply with the Information and Privacy requirements of GDPR (articles 5, 28, 30, 32 to 36, 39, 40, 47, 55 to 58, 64 and recitals 49, 73, 78, 85 to 88, 92, 94, 95 and 108).

2. **Objective**
   The objective of the data protection activities of this part is to establish mechanisms (plans, policies, procedures and technological platforms, etc.) so that your company complies fully with the relevant obligations of GDPR related to privacy risk assessment, confidentiality, integrity, availability, resilience, recoverability and security of personal data processed by the company.

3. **Inspiring you and your DP team for action**
   To inspire yourself and your DP team to take action, it is wise to consider the meaning and guidance offered by the following ancient Greek sayings and short story related to controlling human conduct. The essential message they convey will enlighten and add spiritual fluid to you and your team. This will support all your efforts in implementing the activities related to managing information and privacy risks, in a more effective way.

   Saying 1: 'We can control our thoughts, beliefs and attitudes, but everything else is to some extent out of our control – other people's perceptions and behaviour, the economy, the weather, the future and the past. If you focus on what is beyond your control, and obsess over it, you will end up feeling helpless. Focus on what you can control, and you will feel a measure of autonomy even in chaotic situations' by Epictitus;

Saying 2: The goal of life is happiness, i.e. living in agreement with Nature' by the Cynics, like Diogenes, etc.;

Saying 3: 'Nobody can escape God's attention, when they design evil acts' by Menander; and

Short story: The meaning of Aesop's fable 'The Travelers and the Plane-Tree' *that some people (such as managers, professionals, company executives, etc.) underrate their best blessings and do not feel grateful for anything given to them by God or their customers or their employees regarding security*, as detailed next:

'Two Travelers, worn out by the heat of the summer's sun, laid themselves down at noon under the wide spreading branches of a Plane-Tree. As they rested under its shade, one of the Travelers said to the other, "What a singularly useless tree is the Plane! It bears no fruit, and is not of the least service to man." The Plane-Tree, interrupting him, said, "You ungrateful fellows! Do you, while receiving benefits from me and resting under my shade, dare to describe me as useless, and unprofitable?"'

In summary, the meaning of the above sayings and short story is: good data protection information and privacy risk management is best based on focusing what you can control, implementing controls that do not harm nature and engaging and being grateful to all people as well as God's blessings (as we as a company are moral and benefit society).

Tip: Considering these within the framework of the proposed workplace wellness model (of four dimensions: Believing; Bonding; Belonging; and Benefiting), will support you in motivating and inspiring yourself and your DP team so that you all best execute the following **DP information and privacy (DPIP) risk management activities** and reach your stated objectives listed above.

These data protection activities are detailed next.

4. **DP information and privacy risk management (DPIP) Activities**
   Managing information security and privacy risks so that you comply with the GDPR articles referenced in this chapter entails the execution of a minimum set of activities as described next.

2.1 DPIP ACTIVITY 1: MAINTAIN DATA PRIVACY PROTECTION AND INFORMATION SECURITY POLICIES AND PROCEDURES

GDPR Compliance Requirements

The GDPR (main articles 5, 32 to 34, supporting articles 28, 30 and 40 and recitals 49 and 83) requires an "appropriate" level of security based on the state of the art and costs of implementation, processing activities, and risk of varying likelihood and severity to individuals' rights and freedoms, such as:

Pseudonymisation; encryption; the ability to ensure the confidentiality, integrity, availability, and resilience of systems and services processing personal data; the ability to restore availability of and access to data in the event of an incident; regular tests of the effectiveness of security measures, etc.

Your company's/organization's duty

1. Implement a basic data privacy and information security policy also supported by other complementary organizational and technical measures, policies, procedures and tools to protect personal data.
2. Ensure these identify:
   2.1. The level of risk to the individual posed by the processing.
   2.2. The level of security.
   2.3. System and data resilience.
   2.4. Actions to maintain access in the event of a technical or physical incident.
   2.5. Other complementary organizational and technical security (e.g. encryption), data protection and privacy policies and procedures (e.g. pseudonymization) required.
3. Ensure all security and data protection policies and procedures are regularly tested, reviewed and updated, properly documented and applied effectively.
4. Ensure staff are trained to monitor security events effectively.
5. Ensure security and privacy measures are regularly tested, and evaluated.
6. Ensure company executes security penetration testing periodically.

Additional Information

For more information on implementing additional measures related to this DPIP activity, see:

1. Appendix 4: Technical and organizational data protection measures
2. Examples of other detail controls, plans and policies described above and needed to implement the GDPR better are included in my books listed in the Bibliography.

2.2 DPIP ACTIVITY 2: ESTABLISH A DATA PROTECTION INCIDENT AND BREACH RESPONSE PROCESS

GDPR Compliance Requirements

The GDPR (main articles 33–34, supporting articles 55 to 58 and recitals 73 and 85–88) makes it mandatory for data controllers to notify supervisory authorities in the event of a data breach that poses a "risk of harm", without undue delay and where feasible within 72 hours. Also to notify data subjects of breaches that result in a "high risk" for the rights and freedoms of individuals.

Your company's/organization's duty

1. Craft and implement a personal data incident and breach response process.
2. Ensure this process contains policies and procedures:
   2.1. To monitor all security incidents.
   2.2. To enable it to report a breach to the regulator within 72 hours of becoming aware of it.
   2.3. To notify the individuals affected.
   2.4. To record incidents in a personal data breach register.
   2.5. To establish a personal data breach organization.
   2.6. To enable processors to report breaches to the company.
   2.7. To train staff on monitoring and resolving incidents.
   2.8. To maintain all documentation and upgrade compliance files, as needed.

Additional Information

For more information on implementing additional measures related to this DPIP activity, see:

1. Appendix 4: Technical and organizational data protection measures
2. Examples of other detail controls, plans and policies described above and needed to implement the GDPR better are included in my books listed in the Bibliography.

2.3 DPIP ACTIVITY 3: EXECUTE A DATA PROTECTION IMPACT ASSESSMENT (DPIA) FOR SYSTEMS, PROJECTS, PROCESSES AND PRODUCTS

GDPR Compliance Requirements

The GDPR (main article 35, supporting articles 9, 10, 36, 39, 57 and 64 and recitals 92, 94 and 95) requires data controllers to assess the impact of processing operations on the protection of personal data where the processing is likely to result in a high risk for the rights and freedoms of data subjects. When carrying out the DPIA, the controller must seek the advice of the Data Protection Officer (when designated).

Your company's/organization's duty

1. Craft and implement a DPIA process.
2. Ensure the DPIA process includes a methodology, policy, procedures and guidance to staff.
3. Ensure the company uses it when it implements new technologies which will or could result in a high risk to the rights and freedoms of individuals.
4. Ensure the DPO is consulted on issues related to data protection impact assessments.
5. Ensure staff are trained on all aspects of executing a DPIA.
6. Ensure data subjects and the data protection authority are consulted, as required.

Additional Information

For more information on implementing additional measures related to this DPIP activity, see:

1. Appendix 4: Technical and organizational data protection measures
2. Examples of other detail controls, plans and policies described above and needed to implement the GDPR better are included in my books listed in the Bibliography.

2.4 DPIP ACTIVITY 4: IMPLEMENT DATA PROTECTION BY DESIGN AND BY DEFAULT IN SYSTEMS, PROCESSES AND PRODUCTS

GDPR Compliance Requirements

The GDPR (main article 25, supporting article 47 and recitals 78 and 108) requires data controllers, at the time of determining the means of processing as well as when actually processing, implement appropriate technical and organisational measures (e.g., pseudonymisation) to implement the data protection principles set out in Article 5 (such as data minimisation) and integrate necessary safeguards into the processing to meet the GDPR requirements.

Data controllers must also implement data protection by default, i.e. implement appropriate technical and organisational measures to ensure that, by default, only personal data necessary for each specific purpose are processed. The concept of "necessary" informs the amount of data collected, extent of processing, and retention and accessibility of data.

Your company's/organization's duty

1. Craft and implement data protection by design and by default (dpdd approach) in your systems, processes and products.
2. Ensure your company uses it (dpdd approach) when it implements new systems, processes and products.
3. Ensure staff are trained on using this (dpdd approach).
4. Ensure this approach includes:
   4.1. The application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, legal basis for processing and processing of special categories of personal data.
   4.2. Measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules.

Additional Information

For more information on implementing additional measures related to this DPIP activity, see:

1. Appendix 4: Technical and organizational data protection measures
2. Examples of other detail controls, plans and policies described above and needed to implement the GDPR better are included in my books listed in the Bibliography.

2.5 DPIP ACTIVITY 5: ISSUE REPORTS ON DATA PROTECTION MANAGEMENT ISSUES

GDPR Compliance Requirements

The GDPR (main article 39 and recital 97) requires the DPO: to advise the Controller or Processor and its employees of data protection obligations; monitor compliance, including assigning responsibilities, training and audits; advising on and monitoring DP impact assessments, cooperating and contacting the supervisory authority as required, and reviewing processing risk.

Your company's/organization's duty

1. Craft and implement a policy on information security and privacy reporting.
2. Ensure your DPO regularly reports on data protection issues directly to the highest level of management.
3. Ensure this report is issued on a pre-defined or ad-hoc basis and frequency (monthly, quarterly, etc.).

Additional Information

For more information on implementing additional measures related to this DPIP activity, see:

1. Appendix 4: Technical and organizational data protection measures
2. Examples of other detail controls, plans and policies described above and needed to implement the GDPR better are included in my books listed in the Bibliography.

3 INTEGRATING DATA PROTECTION INTO BUSINESS FUNCTIONS

'What we achieve inwardly will change outer reality'.

– Plutarch

1. **Overview**
   This part contains: (a) several quotations and a short story to inspire you and your team to act effectively; and (b) a set of data protection activities with controls and examples of relevant measures to be implemented to comply with the DP integration issues of GDPR (articles 24, 39 and 88 and recitals 64, 66, 71, 74, 75, 77, etc.).

2. **Objective**
   The objective of these activities is to incorporate data privacy into the operations and practices of the enterprise consistent with the data protection and privacy policy, legal requirements of GDPR, and operational risk tolerance of the company.

3. **Inspiring you and your DP team for integration actions**
   To inspire yourself and your data protection (DP) team to take action, it is wise to consider the meaning and guidance offered by the following ancient Greek sayings and short story related to harmony. The essential message they convey will enlighten and add spiritual fluid to you and your team. This will support all your efforts in implementing the activities related to integrating DP into your business functions, in a more effective way.

   Saying 1: 'Pursue harmony' by the Seven Sages;

   Saying 2: 'Harmony is a blend or composition of contraries' by Aristotle;

   Saying 3: 'The logical man thinks, the wise man doubts and the man who does not know anything is always certain' by Aristotle;

   Saying 4: Heraclitus: 'Opposition brings concord. Out of discord comes the fairest harmony' by Heraclitus; and

   Short story: The meaning of **Aesop's fable** 'The Shipwrecked Man and the Sea' *that Harmony includes opposites and that resolving conflicts in integrating data protection in all functions of a business must be done with grace by managers,* as detailed next:

'A shipwrecked man, having been cast upon a certain shore, slept after his buffetings with the deep. After a while he awoke, and looking upon the Sea, loaded it with reproaches. He argued that it enticed men with the calmness of its looks, but when it had induced them to plow its waters, it grew rough and destroyed them. The Sea, assuming the form of a woman, replied to him: "Blame not me, my good sir, but the winds, for I am by my own nature as calm and firm even as this earth; but the winds suddenly falling on me create these waves, and lash me into fury"'.

In summary, the meaning of the above sayings and short story is: good data protection integration is best based on pursuing harmony, using logic and been grateful to all staff affected by these activities.

Tip: Considering these within the framework of the proposed workplace wellness model (of four dimensions: Believing; Bonding; Belonging; and Benefiting), will support you in motivating and inspiring yourself and your DP team so that you all best execute the following **DP integration activities** and reach your stated objectives listed above.

These data protection activities are detailed next.

4. **Data Protection Integration (DPI) Activities**
   Integrating data protection into all functions of your company or organization so that you comply with the relevant GDPR articles referenced in this chapter entails the execution of a minimum set of activities as described next.

3.1 DPI ACTIVITY 1: INTEGRATE DATA PROTECTION IN ALL BUSINESS FUNCTIONS

GDPR Compliance Requirements

The GDPR (main article 24, supporting article 39 and recitals 64, 66, 71, 74, 75, 77, etc.) requires the data controller to implement appropriate technical and organisational measures to ensure and be able to demonstrate compliance with the GDPR. The appropriateness of these measures is based on a risk assessment that takes into account the nature, scope, context, and purposes of the processing as well as the risks of varying likelihood and severity for the rights and freedoms of individuals. There is a specific reference that, where proportionate in relation to the processing activities, data protection policies shall be implemented. Also the data controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default.

Your company's/organization's duty

1. Craft and implement policies and procedures for the protection of personal data used in the workplace for all business function (HR, Marketing, production customer support, etc.).
2. Locate all personal data in your business functions.
3. Review the personal data processed by each business function.
4. Review all internal plans, policies and procedures related to the functions processing personal data.
5. Ensure these include: A data protection policy, a personal data privacy policy, a risk mitigation plan, a privacy readiness assessment plan, privacy management software tools and self-assessments of privacy management.
6. Ensure relevant are staff are issued instructions on how to deal with personal data and are trained effectively.

Additional Information

For more information on implementing additional measures related to this DPI activity, see:

1. Appendix 4: Technical and organizational data protection measures
2. Examples of other detail controls, plans and policies described above and needed to implement the GDPR better are included in my books listed in the Bibliography.

3.2 DPI ACTIVITY 2: INTEGRATE DATA PROTECTION INTO IT APPLICATION SYSTEMS AND INFRASTRUCTURE

GDPR Compliance Requirements

The GDPR (main article 24, supporting article 39 and recitals 64, 66, 71, 74, 75, 77, etc.) requires the data controller to apply the regulation (GDPR) to all data (manual as well as computerized). In terms of IT application systems and infrastructure, this obliges the data controller to implement appropriate technical and organisational measures to protect all these resources and to ensure and be able to demonstrate compliance with the GDPR.

Your company's/organization's duty

1. Locate and document the personal data processed by each IT Application system.
2. Locate the personal data stored in storage units, network locations and data bases.
3. Craft and implement policies and procedures for the protection of personal data in IT Application systems and IT infrastructure.
4. Ensure your policies and procedures include integrating security and privacy into the process of information system development.

Additional Information

For more information on implementing additional measures related to this DPI activity, see:

1. Appendix 4: Technical and organizational data protection measures'
2. Examples of other detail controls, plans and policies described above and needed to implement the GDPR better are included in my books listed in the Bibliography.

3.3 DPI ACTIVITY 3: INTEGRATE DATA PROTECTION IN DIGITAL DEVICES

GDPR Compliance Requirements

The GDPR (main article 24, supporting article 39 and recitals 64, 66, 71, 74, 75, 77, etc.) requires the data controller to apply the regulation (GDPR) to all data (manual as well as computerized). In terms of digital devices, this obliges the data controller to implement appropriate technical and organisational measures to protect all these resources and to ensure and be able to demonstrate compliance with the GDPR.

Your company's/organization's duty

1. Craft and implement policies and procedures for the protection of personal data processed and stored in portable storage units, smart devices and digital media for work-related purposes.
2. Locate and document the personal data processed and stored on these devices and media.
3. Ensure the use of encryption and pseudonymization, as required, by these units, devices and media.
4. Ensure these policies and procedures are followed and their use monitored.
5. Maintain a data inventory for the personal data for these units, devices and media.

Additional Information

For more information on implementing additional measures related to this DPI activity, see:

1. Appendix 4: Technical and organizational data protection measures
2. Examples of other detail controls, plans and policies described above and needed to implement the GDPR better are included in my books listed in the Bibliography.

3.4 DPI ACTIVITY 4: INTEGRATE DATA PROTECTION IN PRACTICES RELATED TO MONITORING EMPLOYEES' COMMUNICATIONS

GDPR Compliance Requirements

The GDPR (article 88) requires the data controller to protect the personal data of employees during employment in all its aspects: recruitment; performance of employment contracts; discharge of legal obligations; management, planning and organisation of work; workplace equality and diversity; health and safety; and employment rights and benefits.

Your company's/organization's duty

1. Craft and implement procedures to integrate data protection into communications monitoring practices, such as the personal use of e-mail, internet and telephone.
2. Obtain, consent, inform and engage employees, as requited.

Additional Information

For more information on implementing additional measures related to this DPI activity, see:

1. Appendix 3: Data Protection Team Improvement Plan
2. Examples of other detail controls, plans and policies described above and needed to implement the GDPR better are included in my books listed in the Bibliography.

4 RECOMMENDED GOOD PRACTICES

Conclusion

In today's 21st century digital and seamlessly connected world, the relationship between individuals (citizens, customers, consumers, partners, patients, etc.) and enterprises of all types and kinds (private companies, non-profits, single-owner businesses, public sector organisations, etc.) has deepened beyond the fundamental supply of goods and services.

People now view enterprises through their own lens of personal values and principles.

They expect the companies and state authorities that they deal with to act with values, principles and ethics that reflect high levels of trust and integrity.

How companies and organisations manage and protect the personal data with which they are entrusted is one way in which they can prove that the person's well-being is at the heart of their business.

This means being very clear about what personal information is being collected, how it will be processed, stored and used and the rights that the persons (data subjects) have to approve, correct, change or erase their own personal data.

The full implementation of the GDPR offers a golden opportunity for boards and senior management to use this regulation as a high-priority catalyst for business change and initiate a culture of customer respect that permeates the organisation and offers a competitive advantage.

Making an organisation GDPR compliant can be a difficult task because it includes reviewing all the business processes and information architectures (applications, as well as data), in all data handling and processing stages and in all exchange contexts.

Beyond the technology and legal procedures made necessary by the GDPR, boards and senior management should establish what is being done to develop a culture of customer privacy and data protection.

Helping staff to work according to good data protection practice also reduces the risk of inadvertent weakening of the procedures that are in place.

Employees should be encouraged to feel that they have a valuable role to play in supporting customer privacy and building trust.

In conclusion, the following good practices to improve your data protection and privacy measures and controls are recommended for your review and consideration and potential implementation after customization to your enterprise's requirements, needs and expectations.

Recommended Good Practice 1: Security and Privacy

1.1. Develop an integrated approach to all aspects of information security policy and privacy practices for your enterprise systems and data.
1.2. Always train your people to follow your security and privacy policies and procedures and engage them to report any suspected security and privacy breaches.
1.3. Set up review procedures for old enterprise business records, based on a policy of destroying business records unless there is a strong reason or regulation (pension, health, etc.) for keeping them.

Recommended Good Practice 2: Accuracy of data

2.1. Your people should always give a full explanation on all forms of communication (telephone, paper, online, etc.) of why personal data are needed, who is going to use it, what other sources of information may be used and what choice the data subject has.
2.2. Your enterprise should use every opportunity to check that a data subject's contact details are correct (e.g., address, telephone number, email address, etc.).
2.3. Your enterprise responsible officer should also set a schedule for checking other elements of the information held about a data subject according to the likelihood of frequent changes, etc.

Recommended Good Practice 3: Authorization

3.1. Instruct your enterprise people to never share personal information obtained in the course of their employment with anyone unless they have explicit authorization to do so.
3.2. Also instruct them to always follow security and authorization procedures, particularly when dealing with enquirers about personal data over the telephone.

Recommended Good Practice 4: Managing privacy requests and complaints

4.1. Your enterprise should set a timetable for dealing with a subject access request and keep a log of each stage.

4.2. Your enterprise responsible officer should make direct contact with the data subject to establish what information he or she wants and to get any information you need to process the request.

4.3. The complaints by the data subjects should be dealt with in accordance with the normal complaints procedure.

APPENDIX 1: GDPR DEFINITIONS

Summary

This appendix contains the definitions of the following terms:

- Binding corporate rules
- Biometric data
- Consent
- Controller
- Data concerning health
- Data protection officer
- Data Subject
- Encrypted Data
- Enterprise
- Genetic data
- Personal data
- Personal data breach
- Processing
- Processor
- Pseudonymisation
- Special categories of personal data
- Third party

For more definition of GDPR terms, see:

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Binding corporate rules

Reference: GDPR article 4(20), 47, 49, 57, 58, 64 and recitals 107, 108, 110 and 168.

Definition: 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.

Biometric data

Reference: GDPR article 4(14) and recital 51 of GDPR.

Definition: 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data. This includes photographs, finger-prints, facial recognition, iris scans, etc. The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person.

Consent

Reference: GDPR articles 4(11), 6, 7, 8, 9, 22, 49 and recitals 32, 33 and 38.

Definition: 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Controller

Reference: GDPR articles 4(7) and recital 18.

Definition: 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data concerning health

Reference: GDPR article 4(15).

Definition: 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

Data protection officer

Reference: GDPR articles 37 to 39, recital 97 and ARTICLE 29 DATA PROTECTION WORKING PARTY

Website: http://ec.europa.eu/justice/data-protection/index_en.htm

16/EN WP 243 rev.01, Guidelines on Data Protection Officers ('DPOs'), Adopted on 13 December 2016, as last Revised and Adopted on 5 April 2017.

Definition: '…a person with expert knowledge of data protection law and practices should assist the controller or processor to monitor internal compliance…'.

Data Subject

Reference: GDPR Articles 3 to 5, etc., and recitals 11, 23, 24, 28, 33, 39, etc.

Definition: a natural person whose data is processed by a controller or processor.

Encrypted Data

Reference: GDPR Articles 6 and 32.

Definition: personal data that is protected through technological measures (encryption software and related procedures, etc.) to ensure that the data is only accessible/readable by those with specified access.

Enterprise

Reference: GDPR article 4(18).

Definition: 'enterprise' means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity.

Genetic data

Reference: GDPR article 4(13).

Definition: 'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

Personal data

Reference: GDPR article 4(1) and recital 26.

Definition: 'personal data' means any information relating to an identified or identifiable 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.

Personal data breach

Reference: GDPR article 4(12).

Definition: '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.

Processing

Reference: GDPR articles 4(2).

Definition: 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processor

Reference: GDPR articles 4(8).

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

Pseudonymisation

Reference: GDPR articles 4(5).

Definition: 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Special categories of personal data

Reference: GDPR article 9 and recitals 51 to 56.

Definition: Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

Third party

Reference: GDPR article 4(10).

Definition: 'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

APPENDIX 2: BOARD RESPONSIBILITIES

The role and the responsibilities of the board of directors, in general terms, are to:

1. Internal controls: Establish the internal control framework, system, environment and process and ensure that this control system operates effectively and efficiently.
2. Data protection: Appoint a controller to implement all required measures and controls for GDPR and a Data Protection Officer to monitor compliance to GDPR.
3. Adequacy of board: Ensure that an effective Board of Directors is in place and that the Board possesses within its membership the appropriate skills, know-how and dexterities to enable it to fulfill its duties and responsibilities.
4. Appointments: Elect the Chief Executive Officer and replace if necessary, and elect all other executive officers on the recommendation of the Chief Executive Officer.
5. Reviews: Review annually review and evaluate, on a continuous basis, the Corporate Strategic Plans (overall, business unit, functional, etc.), the organization's security and data protection practices, community involvement and corporate social responsibility activities, and the Annual Capital and Operating Budgets.
6. Decision-making: Under established policies and procedures, approve critical decisions not delegated to management, such as: major acquisitions, divestitures, capital investments, IT systems, loans, and strategic plans.
7. Committees: Through its committee system provide supervision regarding certain activities of the Company, such as: benefits, audit, compliance, compensation, finance, community relations, personnel management, security, etc. Also they establish additional committees from time to time as may be necessary to fulfill the needs, duties and responsibilities of the Board. Monitor and perform an evaluation at least annually to determine whether the Board and its Committees are functioning effectively.
8. Fraud control: Select members to constitute an Audit Committee. Manage conflicts of interest. Serve as external liaison with external auditors. Direct the internal audit process. Serve as a direct internal control entity in relation to the fraud actions of senior management. Act as a spokesperson for the organization in relation to fraud committed by senior management.

   Select members to constitute an Audit Committee.

APPENDIX 3: DATA PROTECTION TEAM IMPROVEMENT PLAN

Objective of this plan

The main objective of the Data Protection (DP) Team Improvement Plan is to improve the organizational and operational aspects of the people working in the data protection teams that are working in implementing efforts of GDPR for the company.

Action 1: Scope the DP problem

You have to know what the DP performance problem is with your team.
Assess their environment and concerns against your business requirements for GDPR and DP issues.
Identify the general and specific DP issues involved in solving the specific GDPR implenetation problem.
Document the problem and the solution, in terms of specifications, needs, expectations, demands and resources required for GDPR implementation.

Action 2: Organize the DP team

Assign DP project manager or team manager or function manager.
Develop terms of reference.
Define each detail team and the roles within that DP team.
Assign specific DP responsibilities.
Develop and issue DP project schedule and DP reporting mechanisms.

Action 3: Link DP team to strategy

Set clear vision, mission and values; establish targets for the DP project, team, function, etc., and its expectations.
Inform DP team members of the desired outcomes and measures of success.
Invite each member to be a part of the DP team and communicate the goals and why they were selected.

Action 4: Enable DP team culture

Build commitment and trust by valuing the contribution of each member of the DP team.
Build sympathy for each person's challenges.
Ensure the competence of the whole DP team, as well as each member.
Empower the DP team by allowing the members to work within the prescribed guidelines with each other to accomplish the goals.
Resolve conflicts.

Action 5: Establish DP communications

Craft and implement DP communication policy and associated procedures.
Ensure clarity and accountability for all types of DP communications.
Ensure DP team shares information and develops an open mind.

Action 6: Monitor DP activities

Establish regular DP monitoring.
Review progress.
Identify issues, and resolve problems.
Close the DP project when all DP project activities have been concluded successfully.

Action 7: Manage DP team performance

Develop DP performance policy for DP manager and team members.
Link this policy with corresponding corporate performance system.
Award DP manager and team members when performance targets are met.
Manage DP performance issues.

APPENDIX 4: TECHNICAL AND ORGANIZATIONAL DATA PROTECTION MEASURES

These measures include organizing, designing, developing implementing, monitoring and improving a set of measures to comply with the data protection principles (article 5) and with articles 32 to 34 of GDPR.

1. Organizational data protection measures

These measures include organizing, designing, developing, implementing, monitoring and improving:

1) Security and privacy responsibilities of the Board of Directors
2) Security and privacy responsibilities of Senior Management
3) Appointment and responsibilities of Controller
4) Appointment and responsibilities of Data Protection Officer
5) Personnel Management System (Security and privacy aspects)
6) Contracts with third-party software providers
7) Data protection specifications with third-party data processing companies
8) Instructions for the security and safeguarding of confidential information
9) Information Systems Security and privacy Rules
10) Cyber Security Insurance Program
11) Reporting mechanisms for security incidents and privacy violations
12) Certification (ISO, PCI, SOX, ITIL, etc.)
13) Provision of controller and data protection officer details to data protection authority

2. Technical data protection measures

2.1. Methodologies (DPIA, Data Protection by Design and by Default)

1) Methodology of Security and Privacy Integration in Information Systems Development
2) Methodology for the Development of Security Strategy for IT
3) Methodology for analyzing and managing information and privacy risks (DPIA)
4) **Methodology for integrating data protection into products and services**

2.2. Plans

1) Information Security Strategic Plan
2) Business Continuity Plan
3) Data Protection and Security Plans
4) Data Protection Program
5) Data Protection Awareness, Communication and Training Plan
6) Personal Data Requests, Complaints and Correction Plan
7) Third Party Risks Management Plan
8) Data Protection Integration Plan
9) Data Quality Improvement Plan
10) Data Security Management Plan
11) Social Media Governance Plan
12) Information Security Management Plan
13) Information System Security Development Plan
14) Privacy Complaints Plan
15) **IT Disaster Recovery Plan**

2.3. Data Protection Policies and Procedures:

1) Data Protection Policy
2) Encryption Policy
3) Pseudonymization Policy
4) Data Minimization Practices Policy
5) Minimum Personal Data Definition Policy
6) Continuous Evaluation of Personal Data Collection Policy
7) Personal Data Transformation Techniques Policy
8) Personal Data Documentation Procedure
9) Corporate Files and Records Retention Policy
10) Data Classification Policy
11) Data Quality Policy
12) Information Security Manual
13) Web Site Policy
14) Data Protection Guidelines
15) Cookies Policy

2.4. IT Security Policies and Procedures

1) IT Security Policy
2) Backup and Recovery Policy and Procedures
3) IT security events and breaches monitoring Procedure

2.5. Procedures for Evaluation and Improvement of Data Protection Measures

1) Procedure for Implementing the Data Privacy Policy
2) Procedure for executing internal audits for data protection
3) Procedure to support the implementation of external audits
4) Procedure for carrying out specific assessments and studies
5) Procedures for the implementation of Data Protection Impact Assessments
6) Procedures for the implementation of Data Protection by Design and by Default

2.6. Physical and Environmental Protection

1) Physical Security Measures
2) Environmental protection measures

2.7. Software and Technical Infrastructure

1) Data loss prevention (DLP) software
2) Software tools for aggregation, data masking, pseudonymisation, or anonymization
3) Encryption software technology
4) Intrusion Detection and Prevention System
5) Consent technical infrastructure
6) Technical infrastructure for enabling rights of data subjects (access, portability, rectification, deletion, etc.)

APPENDIX 5: CONTROLLER-PROCESSOR AGREEMENT

Overview

This appendix describes the GDPR requirements of processors that process personal data and details an example of such a Controller-Processor contract.

Introduction

Any enterprise (private company, public organization, non-profit, etc.) that is subject to the EU General Data Protection Regulation (GDPR) as a Controller will need to have in place an appropriate contract (Controller-Processor Agreement) with any third party that it shares data with where that third party is a Processor as defined under GDPR.

GDPR is quite specific about the duties of the Controller and the Processor. Article 28 (3) of GDPR stipulates that there must be a contract in writing between the Controller and Processor which clearly sets out:

1. The subject matter of the processing and its duration;
2. The nature and purposes of processing;
3. The types of personal data, any particular special categories of data and the obligations and rights of both parties, etc.

Failure to have in place a suitable Controller-Processor Agreement is a breach of the law under GDPR.

This means that Controllers:

1. Should be carrying out an audit of their existing contracts with Processors to establish if those contracts already comply with GDPR; and
2. Should be putting in place due diligence and procurement requirements in respects of contracts that are going to be entered into to which GDPR will apply.

GDPR Requirements

Articles 28 to 36 set out issues that must be addressed in the Controller-Processor Agreement which include that the Processor:

1. Must cooperate with the relevant Data Protection Authorities in the event of an enquiry;
2. Must report data breaches to the Controller without delay;
3. May need to appoint a Data Protection Officer;
4. Must keep records of all processing activities;
5. Must comply with EU trans-border data transfer rules;
6. Must help the Controller to comply with data subjects' rights;
7. Must assist the Controller in managing the consequences of data breaches;
8. Must have adequate information security in place;
9. Must not use sub Processors without consent of the Controller;
10. Must delete or return all personal data at the end of the contract at the choice of the Controller; and
11. Must inform the Controller if the processing instructions infringe GDPR.

An example of such a contract is detailed next.

Controller-Processor Agreement Example

1. Parties to the agreement

Between:

1) 'XYZ' Private Corporation ('The Company') <*complete details, such as: incorporated by xxx, address, etc.*> named the 'Controller', and
2) 'Processor-xyz company' <*complete details, such as: incorporated by xxx, address, etc.*> named the 'Processor').

2. Scope of the agreement

2.1. 'Personal data' shall include all data relating to individuals and which is processed by the Processor on behalf of 'The Company' in accordance with this Agreement.
2.2. 'The Company' uses the services of the Processor to process personal data <*describe what data and what processing to be done*>.
2.3. Both parties have agreed to enter into this Agreement to ensure compliance with the European Union General Data Protection Regulation (EU GDPR, termed 'the Act') in relation to all such processing.

3. Terms of Agreement

It is agreed as follows:

3.1. Processing. The terms of this Agreement are to apply (a) to all forms and types of data processing carried out for 'The Company' by the Processor and (b) to all personal data held by the Processor in relation to all such processing whether such personal data is held at the date of this Agreement or received afterwards.

3.2. Services. The Processor is to carry out <*describe services in detail – as per Annex 1*> and provide 'The Company' with the Deliverables as set out in Annex 2 and process personal data received from 'The Company' only on the express written instructions of designated persons of 'The Company'.

3.3. Support. The Processor shall comply at all times with the Act and shall not perform its obligations under this Agreement in such way as to cause 'The Company' to breach any of its applicable obligations under the Act.

3.4. Confidentiality. All personal data provided to the Processor by 'The Company' or obtained by the Processor in the course of its work with 'The Company' is strictly confidential and may not be copied, disclosed or processed in any way without the express written authority of 'The Company'.

3.5. Compliance. The Processor agrees to comply with any reasonable measures required by 'The Company' to ensure that its obligations under this Agreement are satisfactorily performed in accordance with all applicable legislation (EU GDPR, other national laws, etc.) from time to time in force and any best practice guidance issued by the Data Protection Authority.

3.6. Security. The Processor agrees to implement appropriate technical and organizational security measures (as detailed in Annex 3) and take all steps necessary to protect the personal data against unauthorized or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure, and promptly supply details of such measures as requested from 'The Company'.

3.7. Data breaches – reporting. In the event of a suspected or actual data breach or breach of security measures or breach of the confidentiality obligation or loss of confidential data, the Processor shall notify 'The Company' immediately, but no later than 24 hours after the incident was first discovered.

3.8. Data breaches – measures. The Processor shall take all measures reasonably necessary to prevent or limit unauthorized examination, change, and provision or otherwise unlawful processing and to stop and prevent any future breach of security measures, breach of the confidentiality obligation or further loss of confidential data, without prejudice to any right 'The Company'.

3.9. Audit. Without any prior notice, permit persons authorized by 'The Company' to enter into any premises on which personal data provided by 'The Company' to the Processor is processed and to inspect the Processor's systems to ensure that sufficient security measures are in place.

3.10. Data subjects. The Processor agrees to provide 'The Company' with full co-operation and assistance in relation to any complaint or request made by data subjects.

3.11. Data transfers to third parties. The Processor agrees not transfer any personal data provided to it by 'The Company to any third party without the written consent of 'The Company'.

3.12. Data transfers to 'The Company'. The Processor shall transfer all personal data to 'The Company' on the Controller's request in the formats, at the times and in compliance with the specifications agreed with 'The Company'.

3.13. Liability. The Processor shall be liable for and shall indemnify 'The Company' against each and every action, proceeding, liability, cost, claim, loss, expense, including reasonable legal fees and disbursements on a solicitor and client basis and demand incurred by 'The Company' which arise directly or in connection with the Processor's data processing activities under this Agreement.

3.14. Deletion. The Processor agrees that in the event that it is notified by 'The Company' that it is not required to provide any further services to 'The Company' under this Agreement, it, at the Controller's request, shall destroy all such information using a secure method which ensures that it cannot be accessed by any third party and shall issue the 'The Company' with a written confirmation of secure disposal.

3.15. Monthly reporting. The Processor shall compile a monthly report on security management within two working days after the beginning of the next calendar month, which will include the following aspects in relation to the processing of personal data of 'The Company': Number of transactions processed; Number of personal data breaches; Number, status, progress and analysis of security incidents; Measures taken in the area of security management in connection with security breaches and incidents; and General measures taken in the area of personal data security.

3.16. Measures by Supervisory Authority. If the supervisory authority imposes a measure or fine on 'The Company' and if the cause of the measure or fine being imposed is attributable to the Processor's failure to comply with the arrangements made in the Processor Agreement, 'The Company' can recover all costs for this measure or fine from the Processor. Furthermore, 'The Company' has the right to terminate the Agreement with immediate effect in the above situation without 'The Company' being entitled to any form of damages.

3.17. Copyright. All copyright, database rights and other intellectual property rights in any personal data processed under this Agreement shall belong to 'The Company'. The Processor is licensed to use such data only for the term of and in accordance with this Agreement.

3.18. Laws. This Agreement shall be governed by the laws of <*add country*>.

SIGNED for and on behalf of 'The Company' by:

Print Name: .....
Position: .....
Signature: .....
Date: .....

Company Seal: .....

SIGNED for and on behalf of The Processor by:

Print Name: .....
Position: .....
Signature: .....

Date: .....

Company Seal: .....

Annex 1: Description of services.

The Processor is to carry out <*describe services in detail – as per Annex 1*> and provide 'The Company' with the Deliverables as set out in Annex 2, etc.

Annex 2: Description of deliverables.

<*describe services in detail1*>

Annex 3: Security Measures to be adopted by the Data Processor

1. The Processor will ensure that in respect of all personal data it receives from or processes on behalf of 'The Company' it maintains security measures to a standard appropriate to: the harm that might result from unlawful or unauthorized processing or accidental loss, damage or destruction of the personal data; and the nature of the personal data.
2. <*Provide a list of security measures, for example:*>.
   2.1. Security policy.
   2.2. Implementation of appropriate standard security safeguards (such as NIST SANS, etc.).
   2.3. Implementation of Physical and Environmental Security Control Actions
   2.4. Implementation of Data Communications Security Control Actions
   2.5. Implementation of Personal Computers and Office Equipment Security Control Actions
   2.6. Implementation of Security Administration Control Actions.

For more details, see: 'Chapter 2: Data Security Controls' in my book **'**Data Protection Specialized Controls: Data Protection and Privacy Guide – Vol IV'
http://bookboon.com/en/data-protection-specialized-controls-ebook

BIBLIOGRAPHY

1. Books by John Kyriazoglou:

1.1. DATA PROTECTION AND PRIVACY MANAGEMENT SYSTEM DATA PROTECTION AND PRIVACY GUIDE – VOL I
http://bookboon.com/en/data-protection-and-privacy-management-system-ebook

1.2. DP&P STRATEGIES, POLICIES AND PLANS DATA PROTECTION AND PRIVACY GUIDE – VOL II
http://bookboon.com/en/dpp-strategies-policies-and-plans-ebook

1.3. DATA PROTECTION IMPACT ASSESSMENT DATA PROTECTION AND PRIVACY GUIDE – VOL III
http://bookboon.com/en/data-protection-impact-assessment-ebook

1.4. DATA PROTECTION SPECIALIZED CONTROLS DATA PROTECTION AND PRIVACY GUIDE – VOL IV
http://bookboon.com/en/data-protection-specialized-controls-ebook

1.5. SECURITY AND DATA PRIVACY AUDIT QUESTIONNAIRES DATA PROTECTION AND PRIVACY GUIDE – VOL V
http://bookboon.com/en/security-and-data-privacy-audit-questionnaires-ebook

1.6. 'IT Strategic & Operational Controls', 2010, IT Governance
https://www.itgovernance.co.uk/shop/product/it-strategic-and-operational-controls

1.7. 'Business Management Controls: A Guide', 2012
http://www.acfe.com/products.aspx?id=4294984471
https://www.itgovernance.co.uk/shop/product/business-management-controls

2. Article 29 Working Party documents

2.1.Press release Privacy Shield
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610170

2.2. Guidelines on the right to "data portability" (wp242rev.01)
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233

2.3. Guidelines on Data Protection Officers ('DPOs') (wp243rev.01)
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

2.4. Guidelines on the Lead Supervisory Authority (wp244rev.01)
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611235

2.5. Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01)
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

2.6. Guidelines on Personal data breach notification under Regulation 2016/679 (wp250)
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

2.7. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251)
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

2.8. Guidelines on the application and setting of administrative fines (wp253)
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237

2.9. Guidelines on Consent (wp259)
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611232

2.10. Guidelines on Transparency (wp260)
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611232

Disclaimer

The material, concepts, ideas, plans, policies, procedures, forms, methods, tools, etc. presented, described and analyzed in all chapters and appendices, are for educational and training purposes only. These may be used only, possibly, as an indicative base set, and should be customized by each organization, after careful and considerable thought as to the needs and requirements of each organization, taking into effect the implications and aspects of the legal, national, religious, philosophical, cultural and social environments, and expectations, within which each organization operates and exists.

Every possible effort has been made to ensure that the information contained in this book is accurate at the time of going to press, and the publishers and the author cannot accept responsibility for any errors or omissions, however caused. No responsibility for loss or damage occasioned to any person acting, or refraining from action, as a result of the material in this publication can be accepted by the publisher or the author.