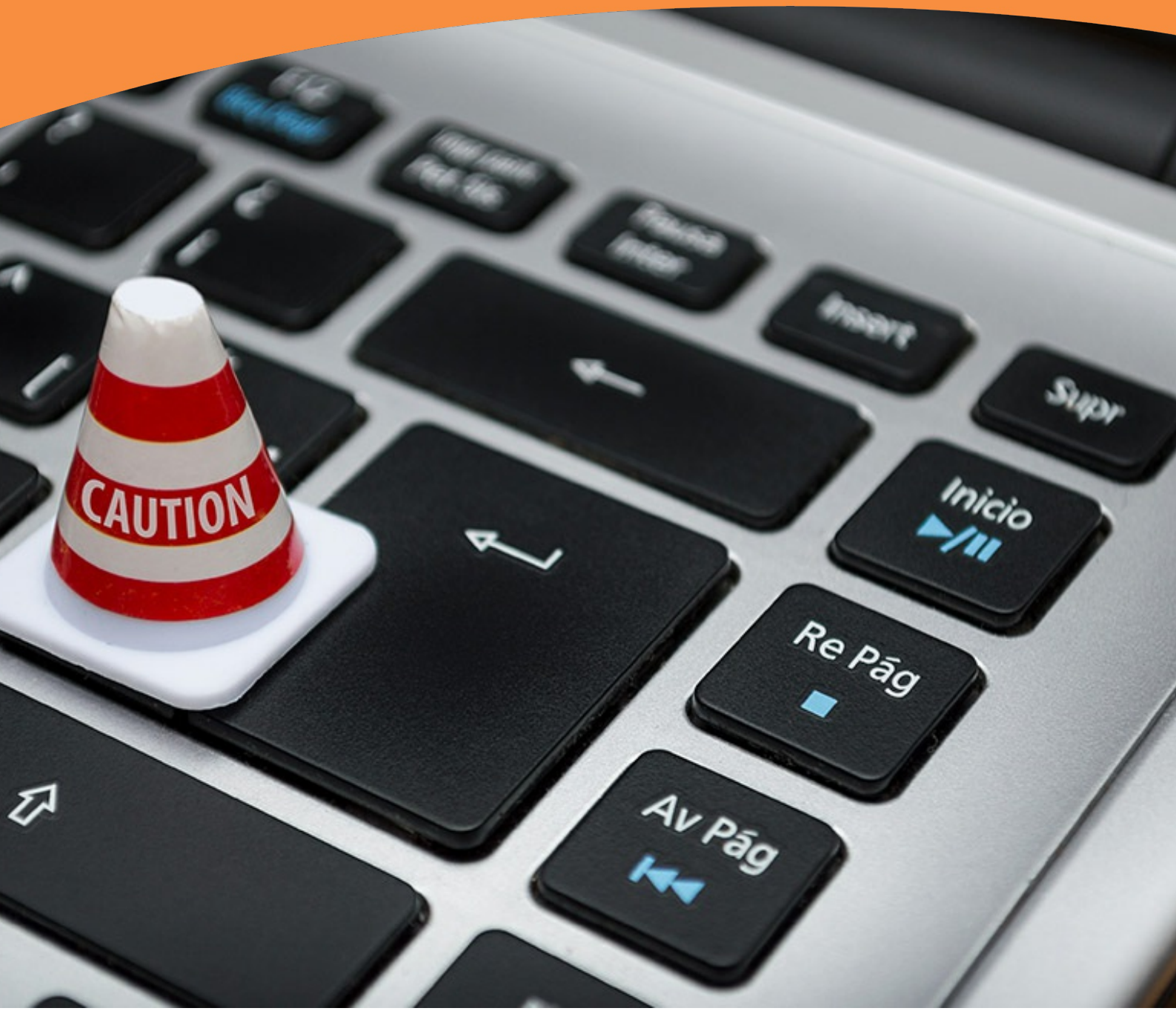
Data Protection (GDPR) Guide

Managing Personal Data Better

John Kyriazoglou



bookboon
The eBook company

JOHN KYRIAZOGLOU

DATA PROTECTION (GDPR) GUIDE

MANAGING PERSONAL DATA BETTER

Data Protection (GDPR) Guide: Managing Personal Data Better
1st edition

ISBN 978-87-403-2779-3

CONTENTS

1 GENERAL DATA PROTECTION REGULATION (GDPR)

Summary: This chapter describes, in general terms, the major highlights and impact of GDPR (European General Data Protection Regulation) on business operations, such as: The new data privacy regime in Europe, GDPR Highlights (Principles, DPIAs, Consent, etc.), Migrating to the new privacy (GDPR) regime, Examples of personal data, etc.

1.1 INTRODUCTION: THE NEW DATA PRIVACY REGIME IN EUROPE

On 25 May 2018, the EU General Data Protection Regulation ('GDPR' or 'the Regulation') is in full 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.

1.2 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.

8. **Administrative Fines for GDPR non-compliance**

8.1. 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.

8.2. 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).

8.3. 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.

1.3 MIGRATING TO THE NEW PRIVACY (GDPR) 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.

1.4 EXAMPLES OF PERSONAL DATA

Some indicative examples of personal data are:

- Name, telephone, address, etc.
- The E-mail address (Email)
- Information regarding customer requisitions / orders
- Participation in trade unions, etc.
- Text from a user to generated content, including Blogs, comments, photos and videos, etc.
- Sexual preferences, political beliefs, etc.
- Demographic data, such as age, gender, race, income.
- Examples of Personal Data
- Age or special needs of vulnerable natural persons
- Allegations of criminal conduct
- Any information collected during health services
- Bank account or credit card number
- Biometric identifier
- Credit card statements
- Criminal convictions or committed offences
- Criminal investigation reports
- Customer number
- Date of birth
- Diagnostic health information
- Disabilities
- Doctor bills

- Employees' salaries and human resources files
- Financial profile
- Gender
- GPS position
- GPS trajectories
- Home address
- IP address
- Location derived from telecommunications systems
- Medical history
- Name National identifiers (e.g., passport number)
- Personal e-mail address
- Personal identification numbers (PIN) or passwords
- Personal interests derived from tracking use of internet web sites
- Personal or behavioural profile
- Personal telephone number
- Photograph or video identifiable to a natural person
- Product and service preferences
- Racial or ethnic origin
- Religious or philosophical beliefs
- Sexual orientation
- Trade-union membership
- Utility bills

1.5 SENSITIVE PERSONAL DATA

Sensitive data are data relating to the

- "racial or ethnic origin"
- "political opinions"
- "religious or philosophical beliefs"
- "trade union participation"
- "health, social welfare, etc."

According to the GDPR (Article 9 Processing of specific categories of personal data) processing of personal data revealing racial or Ethnic Origin, political opinions, etc., is prohibited, unless other specific conditions exist, such as consent, legal interest, etc.

1.6 HOW SHOULD DATA PROTECTION WORK?

1. There should be limits on what data is collected and understood as personal data.
2. Personal information should be obtained by lawful and legitimate means, with the consent of the individual (data subject).
3. Personal information shall be correct, relevant to the purposes for which it is used, accurate, complete and up-to-date, etc.

1.7 EFFECTS OF INCORRECT MANAGEMENT OF PERSONAL DATA

The effect of any incorrect management of personal data by management and company employees and the consequent results include the following (as an example):

- Damage to the company's reputation
- Loss of the confidence of investors or customers
- Loss of sales
- Imposition of fines
- Other wrong management decisions
- Losses and errors on significant business and personal data that reduce overall employee productivity, as they take time to correct, etc.

1.8 HOW TO RECTIFY THE SITUATION

In order to comply better with the requirements of GDPR and avoid the effects of incorrect management of personal data outlined above, it is recommended that:

1) All Company employees should review and study very well the material (guidelines, actions, etc.) contained in this guide, and
2) Follow and comply to the best of their abilities with the instructions contained in the following chapters and the guidance and specific actions contained in the appendices of this guide.

2 CORPORATE DATA PROTECTION FRAMEWORK

Summary: This chapter describes the aspects of the Company's ('ABCX Ficticious Enteprise Inc.') Data Protection Framework, such as: Data Governance Operating Framework, Data Protection Model ('TRUST'), Commitment of the company, Compliance with Data Protection (DP) Principles, etc.

2.1 DATA GOVERNANCE OPERATING FRAMEWORK OF THE COMPANY

The Company (<name of company or organization), located in the municipality of the City of <name of city, etc.>, has, operates and employs specialized personnel, resources, computer and communications equipment, communications network, information systems and applications, data (financial, personal, etc.) and other online services, systems and equipment and telecommunication infrastructure with the purpose of:

1. The smoother and safest handling and fulfillment of its operational and other business needs and, inter alia,
2. More effective support for better service to its customers and safety of its employees and the public.

All departments, services and business functions of the company process personal data of data subjects (e.g., users, employees, etc.).

All of these data are organized and maintained in hard copy only or in digital form or in both forms, hard copy and digital.

The data in hard copy are stored in physical files at the company's offices.
Data in digital form are maintained by specific information systems and communications infrastructures, and stored in digital files in computer systems at the company's offices.

Full details for of these types (physical and digital) are contained in the Personal Data Inventory and the IT Assets Inventory of the Company.

2.2 DATA PROTECTION MODEL 'TRUST'

Description: The company's data protection model, 'TRUST', supports the processing of all personal data by promoting and implementing the following four values:

T - 'Transparency': we are open and clear on how to collect, use and process personal data.

R - 'Respecting Rights': we fully respect and satisfy the rights of data subjects.

U – 'Understanding Needs': we understand that the subjects are concerned about protecting their own Personal Data.

S - 'Security': we protect the Personal Data from abuse or unauthorized access, disclosure, loss, etc.

T -'Treatment ': we treat the data subjects on the basis of ethical principles and respect and in a way that is consistent with our corporate values.
*For an example of ethical principles, see 'DGC 11: Corporate Ethics Policy' in my book '**Data Governance Controls**' (www.bookboon.com).*

In order to serve the company's data protection model, 'TRUST', and to comply with the objectives of GDPR 'protection of individuals with regard to the processing of personal data and the free movement of such data', the company has established and applies in its day-to-day work the following practices related to the processing of personal data of individuals:

Practice 1. The company ensures that the data subjects (users, employees, partners, etc.) are always safe and cannot be harmed in any way by the company's activities.

Practice 2. The company establishes ethical behavioral patterns in transactions with all data subjects, establishes and implements a data quality policy (see Appendix 6. Data Quality Policy) and other relevant data governance controls ('*DGC 10: Data Governance Controls' in my book '**Data Governance Controls**' (www.bookboon.com).*

Practice 3. The company reduces internal conflicts by enhancing the sense of common purpose among the members of the company.

Practice 4. The company provides positive support to those people likely to be under pressure to behave improperly.

Practice 5. The company prevents unsound behavior by establishing sanctions and creating an environment that rewards good, kind and moral behavior.

Practice 6. The company implements appropriate quality, legal, organizational and technical measures in order to comply with GDPR, as best as possible.

Practice 7. The company ensures that data quality roles and responsibilities are executed (*see specific roles and responsibilities for Chief Data Officer, data quality officers, managers, ICT and administrative staff, data librarian, etc.) in 'DGC 10: Data Governance Controls' in my book '**Data Governance Controls**' (www.bookboon.com))* and that all employees and third parties sign a non-disclosure and confidentiality agreement and a declaration statement of conformity with GDPR.

*For more data governance policies and controls for all your enterprise data, see my book '**Data Governance Controls**' (www.bookboon.com).*

2.3 COMMITMENT OF THE COMPANY

The Company, within the framework of these values, undertakes to protect the personal data of the data subjects (individuals) in accordance with the provisions of the GDPR and other relevant laws and regulations.

All employees, workers, partners, directors, and board members (employees) of the Company are required to comply and share the responsibility to secure and protect personal information that is collected and processed by the company for legitimate purposes.

The Company, with specific job responsibilities (*see 'DGC 10: Data Governance Controls' in my book '**Data Governance Controls**' (www.bookboon.com)*), policies, procedures and practices, ensures that commitments and compliance with the company's data protection model ('TRUST') and the Data Protection Principles are fully respected and that the rights and other critical GDPR provisions set out below and in the other chapters of this Guide are met in an effective and efficient manner.

2.4 COMPLIANCE WITH DATA PROTECTION (DP) PRINCIPLES

First DP Principle: 'lawfulness, fairness and transparency'.
Personal data (PD) are subjected to fair and legitimate processing in a transparent way with respect to the data subject (GDPR Article 5, 1a).

Second DP Principle: 'purpose limitation'.
PD are only taken for one or more specific and legitimate purposes and are not further processed in any way incompatible with the purpose or purposes, etc. (GDPR article 5,1b).

Third DP Principle: 'data minimisation'.
PD are appropriate, relevant and limited to what is necessary for the purposes for which they are processed (GDPR Article 5, 1c).

Fourth DP Principle: 'accuracy'.
PD are accurate and, where necessary, updated, and all reasonable steps are taken to immediately delete or correct personal data that are inaccurate in relation to its purposes (GDPR Article 5, 1d).

Fifth DP Principle: 'storage limitation'.
PD are maintained in a form that permits identification of data subjects only for the time required for the processing of personal data, etc. (GDPR Article 5, 1e).

Sixth DP Principle: 'integrity and confidentiality'.
PD are processed in a way that guarantees the appropriate security of personal data, including their protection against unauthorized or unlawful processing and accidental loss, destruction or deterioration, using appropriate technical or organizational measures (GDPR Article 5,1f).

2.5 AUTHORITY, PURPOSE AND USE LIMITATION OF PD

According to GDPR companies and organizations may only use personal data either as specified in their public notices, in a manner compatible with those specified purposes, or as otherwise permitted by the data protection law.

To satisfy these requirements the company has taken the following actions:

a) Identifies the legal basis that authorize a particular personal data collection or activity that impacts privacy; and
b) specify in the respective notices the purpose(s) for which personal data are collected and used.

More details are documented in the company's PD Inventory.

2.6 DATA SUBJECTS

'Data Subjects' are defined to be the employees of the Company, other important relatives of employees of the company, users of the company's web sites, or third parties whose personal data are collected, are considered as data subjects for the purposes of this guide.

2.7 SATISFACTION OF REQUESTS OF DATA SUBJECTS

Individuals (citizens, consumers, customers, users, employees, etc.) referred to as data subjects under GDPR (or individuals), have different rights regarding the processing of their personal data which the company will fully satisfy, unless there are other legal conditions and actions that do not allow this.

These rights are:

1) **The right of access:** the right of individuals to access their personal data (GDPR Article 15).
2) **The right of rectification:** the right of individuals to correct their personal data if these are inaccurate or incomplete (GDPR Article 16).
3) **The right to erasure ('right to be forgotten'):** allowing a person to request the deletion or removal of his or her personal data if there is no good reason to continue processing (GDPR Article 17).

4) **The right to restrict processing:** when processing is limited, it is allowed to store personal data but not to process it further (GDPR Article 18).
5) **The right to be informed of the rectification, erasure or limitation:** data controllers must notify any beneficiary whose data is disclosed, of any correction, deletion or limitation of the processing carried out in accordance with Article 16, Article 17 (1) and Article 18, unless this proves impossible or involves a disproportionate effort (GDPR Article 19).
6) **The right to data portability:** allows individuals to acquire and re-use their personal data for their own purposes in various services (GDPR Article 20).
7) **The right of objection:** the right of individuals to refuse the use of their data for processing and direct marketing, including profiling (GDPR Article 21).
8) **Rights related to automated decision-making and profile creation:** individuals have the right not to be subject to a decision when it is based on the automated processing of their data (GDPR Article 22).

2.8 PRIVACY NOTICE

To meet the GDPR requirements the company has implemented an effective privacy notice to the public and to individuals regarding:

- Its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personal data;
- Authority for collecting personal data;
- The choices, if any, individuals may have regarding how the company uses personal data and the consequences of exercising or not exercising those choices; and
- The ability to access and have personal data amended or corrected if necessary;

Describes the following regarding collection and use:

- The personal data the company collects and the purpose(s) for which it collects that information;
- How the company uses personal data internally;
- Whether the company shares personal data with external entities, the categories of those entities, and the purposes for such sharing;
- Whether individuals have the ability to consent to specific uses or sharing of personal data and how to exercise any such consent;
- How individuals may obtain access to their personal data; and
- How the personal data will be protected.

2.9 DATA PROTECTION REQUIREMENTS FOR THIRD PARTIES

For a variety of business and public interest reasons companies and organizations may share personal data with third parties.
These parties include other public, international, or private sector entities as well as external service providers.
External service providers provide a variety of services to all companies and organizations. These providers include contractors, maintenance and service providers, cloud service providers, information providers, application service providers, network service providers, Internet service providers, outsourcing service providers, information processors, and other organizations providing information system development, information technology services, and other outsourced applications.

According to GDPR companies and organizations may only use third parties, in a manner compatible with this regulation and on the basis of a specific contract.

The company has revised the existing contracts with all relevant third parties to fully comply with GDPR.
*For an example of Controller-Processor Agreement, see 'DGC 6: Controller – Processor Agreement' in my book '**Data Governance Controls**' (www.bookboon.com).*

2.10 DATA PROTECTION IMPACT ASSESSMENT

Organizational data protection risk management processes operate across the life cycles of all business processes and systems that collect, use, maintain, share, or dispose of personal data.

Data protection must be designed into management systems by default. Privacy impact assessments (PIAs) – or what the GDPR calls data protection impact assessments (DPIAs) must be done for technologies and processes that are likely to result in a high risk to the rights of data subjects.

The company, in order to comply with GDPR, undertakes the following actions related to DPIAs:

1. Documents and implements a data protection risk management process that assesses protection and privacy risks to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personal data; and
2. Conducts Data Protection Impact Assessments (DPIAs) for information systems, programs, projects, or other business activities that may pose a protection or privacy risk in accordance with applicable law, or any existing company/organizational policies and procedures.

2.11 BREACH OF PERSONAL DATA

1) **Manage breach**. In the case of existence or suspicion of a personal data breach, the company, as the Controller, shall take action, such as:
    1) isolate the breached system or systems,
    2) identify and eliminate the causes of the beach,
    3) implement improvements to restore systems to production, and
    4) analyze the impact that may occur as the result of the system failures, data breaches, etc.

2) **Informing Data Protection Authority.** If a personal data breach takes place, the controller (the company) notifies without delay and, if possible, within 72 hours from the moment the controller becomes aware of the fact of breach of personal data to the competent supervisory authority under GDPR Article 55.
3) **Announcement of the breach of personal data to the data subject.** In the event that a personal data breach has occurred, which may, in the judgment of the controller (the company), pose a high risk to the rights and freedoms of the individuals, the company shall, without delay, notify in writing, by registered mail, the breach of the personal data to the data subjects concerned.

*For an example of a Personal Breach Plan, see 'DGC 7: Personal Data Breach Incident Response Plan' in my book '**Data Governance Controls**' (www.bookboon.com).*

2.12 DATA PROTECTION AND PRIVACY ENHANCED SYSTEM DESIGN AND DEVELOPMENT

'Data Protection and Privacy Enhanced System Design and Development' is defined as the process of designing and developing Information Systems and other products and services on the basis of two inter-related concepts: 'Privacy by Design' and Privacy by Default'.

'Privacy by Design' means that each new product, system, service or business process that makes use of personal data must take the protection of such data into consideration. An organization needs to be able to show that they have adequate security in place and that compliance is monitored. In practice this means that the IT department of the specific company must take privacy into account during the whole life cycle of the system or process development.

'Privacy by Default' simply means that the strictest privacy settings automatically apply once a customer acquires a new product or service. In other words, no manual change to the privacy settings should be required on the part of the user. There is also a temporal element to this principle, as personal information must by default only be kept for the amount of time necessary to provide the product or service.

These mean that companies and organizations must design information systems to support data protection and privacy by automating privacy controls. To the extent feasible, when designing organizational information systems, organizations must employ technologies and system capabilities that automate privacy controls on the collection, use, retention, and disclosure of personal data. By building privacy controls into system design and development, organizations mitigate privacy risks to personal data, thereby reducing the likelihood of information system breaches and other privacy-related incidents.

The company, in order to comply with GDPR, undertakes the following actions related to 'Privacy by Design' and Privacy by Default':

1. Implements technical and organizational measures to show that they have considered and integrated data protection and privacy compliance measures into their data processing activities;
2. Adopts appropriate staff policies such as the use of pseudonymisation to ensure compliance with data minimization obligations;
3. Conducts periodic reviews of systems to determine the need for updates to maintain compliance with the data protection act the organization's privacy policy;
4. Monitors, regardless of whether automated data protection and privacy controls are employed, information system use and sharing of personal data to ensure that the use and sharing is consistent with the authorized purposes identified in GDPR;
5. Documents, by the IT function, the decisions taken during the development of each IT system;
6. Ensures that all electronic documents (such as spreadsheets, presentations, PDF files and Word documents, etc.) containing personal data are developed and used by taking into considerations the privacy by default and privacy by design principles; and
7. Implements electronic document transmission security technologies that incorporate logging, reporting and tracking of digital documents as they are transferred to enable you to maintain an audit trail of all personal data.

2.13 DESTRUCTION OF DATA

Any information (financial, personal, etc.) that has been declared obsolete on the basis of internal data protection and data retention procedures is destroyed in a secure and legal manner, in accordance with the company's relevant policy.

2.14 DATA PROTECTION OFFICER

1) The Company's Data Protection Officer (DPO) is <<Name and surname>>.
2) The Data Protection Officer is responsible for monitoring compliance with the Internal Actions of the Company and the Personal Data Protection Regulation (GDPR) and acts as the central point of contact for any matter concerning the protection of personal data.
3) The DPO is responsible for informing the Company and training staff and associates for their duties arising from this Regulation and the law applicable to personal data.
4) The DPO monitors the GDPR compliance issues of the Company.
5) The DPO communicates with the Data Protection Authority on personal data protection issues that arise in the Company.
6) The DPO undertakes the coordination and management of responses to security incidents related to personal data (e.g. unauthorized access or disclosure, etc.).
7) The DPO is informed of the requests of the data subjects for exercising their rights.
8) The DPO advises Company Management and Personnel and serves as a contact point for Personnel, Third Parties, and the Company for issues related to the protection of personal data.

2.15 AWARENESS AND TRAINING OF EMPLOYEES

1) The company ensures, through the Data Protection Officer, the awareness and training of its staff with regard to their obligations, roles and responsibilities in the processing of the personal data in the performance of their duties.
2) The training takes place at regular intervals in the form of primary training and is renewed and supplemented in relation to the needs arising from the assessment of the situation related to data protection on an ongoing basis.
3) New recruits, in the context of their initial education, receive training on the legislation on personal data (GDPR), this guide and other general obligations related to personal data protection.
4) Employees wishing to exercise these rights must contact the Company's Data Protection Officer.

2.16 DATA PROTECTION MONITORING AND AUDITING

Companies and organizations monitor and audit data protection and privacy controls and internal protection and privacy policies, procedures, controls and practices.

The company, in order to comply with GDPR, undertakes the following actions related to Data Protection Monitoring and Auditing:

1. Identifies and addresses gaps in data protection and privacy compliance, management, operational, and technical controls by conducting regular assessments (e.g., external audits, internal audits, internal risk assessments, etc.).
2. Monitors for changes to applicable data protection and privacy laws, regulations, and policies;
3. Tracks programs, projects, services, information systems, and applications of the company that collect and maintain personal data to ensure data protection and privacy compliance;
4. Ensures that access to personal data held by the company is only on a *need-to-know* basis;
5. Ensures that personal data is being maintained and used only for the legally authorized purposes identified in the public notice(s);
6. Implements technology to audit for the security, appropriate use, and loss of personal data;
7. Performs reviews to ensure physical security of documents containing personal data;
8. Assesses compliance by all external service providers with data protection and privacy requirements; and
9. Ensures that corrective actions identified as part of the assessment and review process are tracked and monitored until audit findings are implemented effectively.

2.17 DATA PROTECTION REPORTING

Through internal and external data protection and privacy reporting, companies and organizations promote accountability and transparency in organizational data protection and privacy operations. Reporting also helps companies/organizations to determine progress in meeting data protection and privacy compliance requirements and privacy controls, compare performance across all business functions and systems, identify vulnerabilities and gaps in policy and implementation, and identify ways and methods to become more effective in data protection.

The company, in order to comply with GDPR, undertakes the following actions related to Data Protection Reporting:

1. Reports report personal data breaches to their supervisory authority and in some cases, affected data subjects, in each case following specific GDPR provisions.
2. Maintains an internal breach register.
3. Develops or updates the internal breach notification procedures, including incident identification systems and incident response plans, which they regularly test, review and improve;
4. Ensures, via the data protection officer that the company IT staff implement appropriate technical and organizational protections to render the data unintelligible in case of unauthorized access; and
5. Reviews the company's insurance policies are revisited to assess the extent of their coverage in case of breaches.

2.18 PERSONAL DATA AND IT ASSETS INVENTORIES

The personal data and IT assets inventories facilitate and enable companies and organizations to design, develop and implement effective organizational, administrative, technical, and physical security policies and procedures to protect personal data and related information systems and to mitigate risks related to personal data protection and privacy exposure.

The company, in order to comply with GDPR, undertakes the following actions related to personal data and IT assets inventories:

1. Documents the existing personal data of the company and assigns the responsibility of managing it to a company manager.
2. Documents the existing IT Assets of the company and assigns the responsibility of managing it to the IT manager of the company.

2.19 FILING A COMPLAINT

The data subject has the right to file a complaint with the Local Data Protection Authority (url of data protection authority of company's location or county) in the event of a violation, breach or unauthorized access of his or her personal data.

2.20 POLICY VIOLATION

Any alleged or actual violation of the Privacy Policy and other data protection policies and procedures of the Company's should be communicated to any member of the Company's Management as well as to the Controller and the Data Protection Officer.

*For examples of additional data governance controls for all your enterprise data, see my book '**Data Governance Controls**' (www.bookboon.com), and the controls described in it, such as:*
DGC 5: Technical and Organizational Data Protection Measures
DGC 6: Controller – Processor Agreement
DGC 7: Personal Data Breach Incident Response Plan
DGC 8: Data Protection Technology Strategy
DGC 9: IT Security Strategy
DGC 10: Data Protection Policy
DGC 12: Data Governance Controls.

3 PERSONAL DATA MANAGEMENT OBLIGATIONS FOR EMPLOYEES

Summary: This chapter contains the most basic employee obligations for the best protection and management of the Company's personal data processing under the General Data Protection Regulation (GDPR), such as: Understand Personal Data Definitions, Security, confidentiality and disclosure of personal data, etc.

Legal Data Management Employee Obligations
All company employees, on the basis of the above principles, requirements and guidelines (see previous chapter), in the exercise of their duties in the management of personal data, must fully respect and follow the guidelines outlined next and also execute the following obligations (OBL), to their best ability:

3.1 OBL 1. UNDERSTAND PERSONAL DATA DEFINITIONS

Definition 1: '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;

Definition 2: ' Sensitive data ' refers to the circumstances of specific processing situations, including those relating to the processing of specific categories of personal data such as:

'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;

'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data;

'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;

personal data revealing the racial or ethnic nature of the ethnic origin, political opinions, religious or philosophical beliefs or participation in a trade union, as well as the processing of genetic data, biometric data for the purpose of undeniable identification of a person, data relating to health or data relating to the sexual life of a natural person or sexual orientation.

3.2 OBL 2. SECURITY, CONFIDENTIALITY AND DISCLOSURE OF PERSONAL DATA

Employees must preserve and protect the security, confidentiality and privacy of personal data that are brought to their knowledge:

a) in the exercise of their duties (*see specific roles and responsibilities for managers, ICT and administrative staff, data librarian, etc.) in 'DGC 10: Data Governance Controls' in my book '**Data Governance Controls**' (www.bookboon.com))* or
b) in the event of their (personal data) occurrence and / or
c) to which personal data they have access and / or
d) whose personal data they process,

throughout their term of office in the company, but also after the termination of such employment for any reason, whatsoever.

Employees must respect the confidentiality of personal data which come to their knowledge and which they process in the course of their duties or at the same time, and not to disclose, transmit or otherwise disclose them to third parties only if this is strictly necessary in the performance of their duties solely and for the purpose of carrying out the work entrusted to them or required by a relevant provision of law.

'Third party' means any natural or legal person, including, but not limited to, the other members of the company, the external associates and suppliers of the Company, as well as persons in the family, friendly and social environment of the employees.

Also all employees should study, review and comprehend the impact of the risks contained in Appendix 1: Information security and data privacy risks and implement additional security controls listed in the following:

Appendix 2: Guidance on safeguarding of confidential information
Appendix 3: Information Systems Security actions
Appendix 4: Clean Desk and Screen policy
Appendix 5. FAX Management Controls.

3.3 OBL 3. FOLLOWING INSTRUCTIONS AND SUPPORTING MANAGEMENT

Employees must manage the personal data collected by the company, by following the instructions of the Data Protection Officer, their manager and other company executives, and by taking the technical and organizational security measures for the personal data indicated to them as described in this guide and other company policies and procedures.

Employees must generally provide any assistance to Company management in order to:

a) protect the confidentiality,
b) protect the security and privacy of personal data which they or third parties have directly or indirectly revealed or otherwise made available to an unauthorized user or holder; and
c) cooperate with and support management to retrieve possession of personal data as soon as possible and to prevent further unauthorized use or disclosure or otherwise violation of the security of personal data held.

3.4 OBL 4. AVOIDING BENEFIT TO STAFF OR OTHER PARTIES

Employees must not use, without written authorization of the Company, for their personal benefit or purposes or for the benefit or purposes of any third party, personal data held and managed by the Company.

In particular, to respect and protect the confidentiality and privacy of data of specific categories brought to their knowledge in the exercise of their duties and not to disclose, post, disseminate, or display them by any means of communication or reproduction of files or their contents (but not limited to sending e-mail, uploading to social media, sending via viber, photocopy or personal data files for personal purpose, etc.).

3.5 OBL 5. UNFAIR ACTIONS TO PERSONAL DATA

Employees must not make an unlawful or unauthorized action related to the personal data processed by the company, included in an electronic or physical file of any type of form, such as:

- Access,
- Harm,
- Collection,
- Posting,
- Organization,
- Structuring,
- Saving,
- Adaptation or Change,
- Recovery,
- Use,
- Dissemination of any kind,
- Correlation,
- Combination,
- Restriction,
- Deletion or Destruction, etc.

3.6 OBL 6. CONTACT WITH MANAGEMENT AND THE DATA PROTECTION OFFICER

Employees must contact the Company's Data Protection Officer for:

1) any queries relating to the protection of personal data,
2) for any matter of personal data brought to their attention in the course of their duties and in general, during their hours of work,
3) for requests from data subjects and any other person,
4) for exercising the rights conferred by the General Data Protection Regulation 679/2016 (access, correction, deletion, limitation of processing, portability, complaint to the Supervisory Authority, etc.),
5) for complaints about the protection of personal data, omissions and
6) non-compliance with technical and organizational security measures for personal data.

Employees must inform their manager and the Data Protection Officer of the Company in a timely manner, not later than 2 hours,

1) of any breach of personal data comes to their knowledge as well as
2) for any violation of the security of the physical and / or electronic file of personal data in general, which results in or may result in accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to the Company's personal data files.

3.7 OBL 7. LEGAL DISCLOSURE OF PERSONAL DATA

Employees must, in case they are legally required to disclose personal data beyond what is required in the course of their duties, provide the Company with written notice immediately prior to such disclosure, unless such notice is contrary to or prohibited by any provision of law.

3.8 OBL 8. EMPLOYEE TERMINATION

In the event of termination in any way of the Employment Contract of the Employee with the Company, at the initiative of any of the parties, the Employees acknowledge that:

- They have no right to process the personal data held by the Company and
- They have no right to access the physical and electronic personal data files of the Company, including the Company's electronic mail, and
- are therefore required:

1) to deliver immediately to the Company any electronic records or documents containing personal data held by them or third parties,
2) to provide a written attestation stating:

    - that they have not kept any documents, electronic records or any other form of copies of the personal data held by the Company;
    - that they have returned all physical records;
    - that they have removed from any electronic device in their possession (mobile phone, PC, portable storage devices, etc.) any personal data file in which they have physically or electronically accessed during their collaboration with the Company; and
    - that they have not transferred out of the Company's facilities without authorization or instructions from the legal representative or Data Protection Officer or any person authorized to do so, any document, record, object or file containing personal data including photocopies or copies of any type and form,

3) to refrain from any malicious action such as destruction, deletion, reproduction, copying, disclosure, dissemination, etc., any personal data contained in a physical and / or electronic record of the Company,
4) to generally refrain from any breach in any way of the security, confidentiality and privacy of the Company's personal data,
5) to abide by the above obligations for an indefinite period of time after the termination of their employment contract with the Company in any way, and
6) to fully comply with the actions set out in this guide and the policies of the company.

4 PERSONAL DATA MANAGEMENT ACTIONS FOR EMPLOYEES

Summary: This chapter contains the most basic daily employee actions for the best protection and management of the Company's personal data processing under the General Data Protection Regulation (GDPR), such as: Personal Data Collection Actions, Personal Data Maintenance Actions, etc.

4.1 DATA LIFE CYCLE

All company employees, on the basis of the principles, requirements and guidelines stated in previous chapters, in the exercise of their daily duties in the management of personal data (PD), must fully use the actions outlined next, to their best ability.

These actions relate to all steps of the company's general data life cycle of:

1. Collecting Data
2. Maintaining Data
3. Using Data
4. Storing Data
5. Publishing Data
6. Purging Data
7. Securing Data.

On the basis of all above, data protection model, GDPR principles, etc., the adoption and using of the following actions for the processing of personal data is recommended as a good practice by all employees of the company.

4.2 PERSONAL DATA COLLECTION ACTIONS

1) **Overview**: The actions outlined below relate to the first step (Collecting Data) of the 7-step data life cycle of the company.
There are three main ways, in general, that data can be collected or captured, and these are:

1. Data Acquisition: the ingestion of already existing data that has been produced by an organization outside the specific enterprise
2. Data Entry: the creation of new data values for the specific enterprise by human operators or devices that generate data for the enterprise
3. Signal Reception: the capture of data created by devices, typically important in control systems, but becoming more important for information systems with the Internet of Things, etc.

The company, as documented in the PD and IT Asset Inventories, uses the first 2 ways (data acquisition and data entry), without the use of any devices in the collection process.

In order to comply better with the GDPR requirements, the following actions are recommended to be used by all company employees in this regard.

2) **Practical Tips**

Practical Tip 1: It is good practice, *at least once a year*, for all company employees, to review the corporate policies and procedures and any changes *related to GDPR and privacy/security issues (e.g., data retention, data deletion, legal basis of processing, etc.)* affecting their duties in their specific business function and particularly anything that impacts personal data processed within their own department or corporate function.

Practical Tip 2: In carrying out their daily *or ad-hoc* PD collection duties by executing the actions outlined next, it is good practice, for all company employees, to review and consider:

a) the data subjects concerned (office employees, crew members, suppliers, consultants, surveyors, technicians, etc.),
b) the business function involved (crewing, technical, office administration, etc.),
c) the data flows and the process (forms, document, policies, procedures, systems, etc.) recorded in the company's PD and IT Assets Inventories and
d) the data quality policy (see Appendix 6. Data Quality Policy) and other relevant data governance controls (*see 'DGC 10: Data Governance Controls' in my book '**Data Governance Controls**' (www.bookboon.com)*.

3) **PD Collection Actions**

PD Collection Action #1. Ensure effective collection of personal data

Ensure that you collect personal data in the most effective way, by:

1. Confirming to the greatest extent practicable upon collection or creation of personal data, the accuracy, relevance, timeliness, and completeness of that information;
2. Collecting personal data directly from the individual to the greatest extent practicable;
3. Checking for, and correcting as necessary, any inaccurate or outdated personal data used by its functions, projects, programs or systems;
4. Requesting that the individual or individual's authorized representative validate personal data during the collection process; and
5. Requesting that the individual or individual's authorized representative revalidate that personal data collected is still accurate at the time of the next encounter.

PD Collection Action #2. Dealing with sensitive data

The collection and processing of specific categories of personal information ("sensitive data") shall be avoided unless there is a definitive and proven need for it.

PD Collection Action #3. Consent

PD collected for processing must always have the explicit consent of the data subject. Non-action, such as the pressure of a submit button, is not considered a clear consent.

PD Collection Action #4. Informing data subject

PD shall be collected and processed only for the reasons communicated to the data subject at the point of collection.

PD Collection Action #5. Collection minimization

PD collected must be limited to what is required for the specific purpose.

PD Collection Action #6. Data accuracy

In reasonable cases personal information must always be accurate. The continued processing of erroneous personal information after an update is considered a violation of the principles of GDPR.

PD Collection Action #7. Expiration date

Collected personal information must have an expiration date that is defined as the point at which the processing must be completed for the purpose of the personal data collected.

A vague expiration date is no longer acceptable.

4.3 PERSONAL DATA MAINTENANCE ACTIONS

1) **Overview**: The actions outlined below relate to the second step (Maintaining Data) of the 7-step data life cycle of the company.

   Once data have been collected or captured, by any means and methods, they usually must be maintained.

   Data Maintenance is about processing the data and often involves tasks such as data accuracy, data quality, integration, cleansing, enrichment, *creation of data values via inductive logic (*expert experience, judgement, and/or opinion, etc.) analytics, modeling, deductive logic, encryption, pseudonymization, etc.

   We only deal here with the first 2 tasks of data maintenance, as the Law (GDPR) requires the Company to take reasonable steps to ensure that personal data (PD) are kept accurate and up-to-date and are of the highest quality.

The more important is that personal data is accurate, the greater the effort the Company has to make to ensure its accuracy.

The following actions are recommended to be used by all company employees in this regard.

2) **Practical Tips**

Practical Tip 1: It is good practice, *at least once a year*, for all company employees, to review the corporate policies and procedures and any changes *related to GDPR and privacy/security issues (e.g., data retention, data deletion, legal basis of processing, etc.)* affecting their duties in their specific business function and particularly anything that impacts personal data processed within their own department or corporate function.

Practical Tip 2: In carrying out their daily *or ad-hoc* PD maintenance duties by executing the actions outlined next, it is good practice, for all company employees, to review and consider:

a) the data subjects concerned (office employees, crew members, suppliers, consultants, surveyors, technicians, etc.),
b) the business function involved (crewing, technical, office administration, etc.),
c) the data flows and the process (forms, document, policies, procedures, systems, etc.) recorded in the company's PD and IT Assets Inventories and
d) the data quality policy (see Appendix 6. Data Quality Policy) and other relevant data governance controls (*see 'DGC 10: Data Governance Controls' in my book '**Data Governance Controls**'* (www.bookboon.com).

3) **PD Maintenance Actions**

PD Maintenance Action #1. Ensure data accuracy.
It is the responsibility of all Company employees who personally process the data to take reasonable steps to ensure that they are kept as accurate and up-to-date as possible.

PD Maintenance Action #2. No data redundancy.
The data will be stored in a few locations as necessary. You should not create unnecessary additional groups or data files.

PD Maintenance Action #3. Confirm subject identity.
You must take every opportunity to ensure that the data is updated. For example, by confirming the data subjects' data when they call.

PD Maintenance Action #4. Updating data by subjects.
The Company will make it easier for data subjects to update the information held by the Company and will satisfy all access requests in compliance with GDPR.

PD Maintenance Action #5. Continuous effort in accuracy.
The data must be updated as inaccuracies are discovered. For example, if you can no longer contact the stored phone number of a data subject, it should be removed from the Company's database.

PD Maintenance Action #6. Ensure data quality.
Processed personal data must be of quality, accurate, and, to the extent necessary, up-to-date. Personal data that are inaccurate or incomplete should be deleted or corrected. Ensure that you follow the company's quality actions and process.

PD Maintenance Action #7. Monitor quality.
The company's data quality procedure should be monitored by senior management and should be followed by all staff.

PD Maintenance Action #8. Quality in Spreadsheets and Information Systems.
The company's information systems should be developed with data quality and error correction actions incorporated into all Excel Spreadsheets, computer programs, etc., and these actions should be documented, reviewed and improved on a periodic basis.

4.4 PERSONAL DATA USE ACTIONS

1) **Overview**: The actions outlined below relate to the third step (Using Data) of the 7-step data life cycle of the company.

   Once data have been collected or captured and maintained, they are usually put to productive use in support of company business functions and transactions and to satisfy data subject requests for access to their personal data.

   Data Use is about applying data as information to tasks that the specific enterprise needs to run and manage itself.

   Personal data (PD) have no value to the Company unless the company can use them. However, when someone accesses or uses personal data for a purpose, these data may be at higher risk of being lost, corrupted, stolen or harmed in some way.

To avoid any or all of these and comply with the requirements of GDPR, the following actions should be applied by all employees in using personal data.

2) **Practical Tips**

Practical Tip 1: It is good practice, *at least once a year*, for all company employees, to review the corporate policies and procedures and any changes *related to GDPR and privacy/security issues (e.g., data retention, data deletion, legal basis of processing, etc.)* affecting their duties in their specific business function and particularly anything that impacts personal data processed within their own department or corporate function.

Practical Tip 2: In carrying out their daily *or ad-hoc* PD use duties by executing the actions outlined next, it is good practice, for all company employees, to review and consider:

a) the data subjects concerned (office employees, crew members on ships, suppliers, consultants, surveyors, technicians, etc.),
b) the business function involved (accounting, crewing, technical, office administration, etc.),
c) the data flows and the process (forms, document, policies, procedures, systems, etc.) recorded in the company's PD and IT Assets Inventories and
d) the data quality policy (see Appendix 6. Data Quality Policy) and other relevant data governance controls (*see 'DGC 10: Data Governance Controls' in my book '**Data Governance Controls**'* (www.bookboon.com).

3) **PD Use Actions**

PD Use Action #1. Ensure purpose of processing of data.
An employee who has access to personal data must process the data only for the purpose of the processing (legal aspects documented in PD Inventory) and may not share, distribute or otherwise disclose personal data to third parties unless he has received a mandate from the Company.

PD Use Action #2. Computer screens. When working with personal data, you should ensure that your computer screens are always locked when they are left unattended.

PD Use Action #3. E-Mail. Personal data should not be shared informally. In particular, you should never send them by e-mail, as this form of communication is not secure.

PD Use Action #4. Encryption. Personal data must be encrypted before being transferred electronically to authorized external contacts.

PD Use Action #5. Central Store. You should not store copies of personal data on your own computers. Always have access to and use the central copy of any data.

PD Use Action #6. Mobile Phones. Avoid using (personal or corporate) mobile phone while working for personal purposes. In any case, the conversation on the mobile phone for personal purposes should be limited to what is absolutely necessary and may take place at the time of the break and with the necessary discretion.

PD Use Action #7. Internet Navigation. Use the computers and equipment of the Company for purposes related to the performance of your duties, and avoid navigating on websites that are not related to the processing of their work, including the use of social media on the job. It is strictly forbidden to navigate on websites with illegal or unethical content as well as to navigate to insecure websites in general.

PD Use Action #8. Professional e-mail for personal purposes. Abstain from using professional e-mail (business correspondence) for personal purposes as well as for acts of unlawful interference, including the exercise of competitive activity.

PD Use Action #9. Inspection of professional correspondence.
The Company reserves the right to occasionally inspect professional correspondence, in particular to identify any illegal activity of the employee, after informing the employees to be audited. It is explicitly recognized that business correspondence is a property of the Company, which retains the right to keep and use it after the end of the employment relationship.

PD Use Action #10. No backup on personal devices. Do not exceed your duties in the exporting, or unauthorized disclosure, or using for personal purposes, or copying on personal devices and media (e.g. Flashdisks) of any personal data contained in electronic and / or physical files that are property of the Company.

PD Use Action #11. Remote work. In the case of remote work and remote access to the Company's network, employees must refrain from accessing computers that do not meet the necessary security requirements (e.g. they do not have an antivirus protection system) and must restrict each remote access only to what is strictly necessary for the performance of their duties.

PD Use Action #12. Breach. All employees, in the event of a breach of the above security requirements, must immediately inform the Company.

PD Use Action #13. Satisfying Data Subject Requests
Ensure that your company executes the following:

1. Provides individuals the ability to have access to their personal data maintained in its system(s) of records;
2. Implements a system and the required technology, forms and tools to enable the data subjects to exercise their rights (access, deletion, correction, portability, etc.) in your company's records and systems.

PD Use Action #14. Manage Complaints

1. Ensure that your company implements a complaints management process for receiving, responding and monitoring of complaints, concerns, or questions from individuals about the organizational data protection and privacy practices and that all complaints received are reviewed and appropriately addressed in a timely manner.
2. Ensures that you and all other necessary employees who may receive complaints recognize them and know how to deal with them effectively.

4.5 PERSONAL DATA STORAGE ACTIONS

1) **Overview:** The actions outlined below relate to the fourth step (Storing Data) of the 7-step data life cycle of the company.

Once data have been collected or captured, maintained and used, they are usually stored to support the business functions and transactions of the company.

Data Storage is about keeping the data in an environment where the data are used in an active production mode, and the removal of these data from all active production environments to a data archive, to be restored when a need occurs, to an environment where they can be put to productive use again.

To ensure that personal data are stored in the most secure way and comply fully with the requirements of GDPR, the following actions are recommended to be used by all company employees in this regard.

2) **Practical Tips**

Practical Tip 1: It is good practice, *at least once a year*, for all company employees, to review the corporate policies and procedures and any changes *related to GDPR and privacy/security issues (e.g., data retention, data deletion, legal basis of processing, etc.)* affecting their duties in their specific business function and particularly anything that impacts personal data processed within their own department or corporate function.

Practical Tip 2: In carrying out their daily *or ad-hoc* PD storage duties by executing the actions outlined next, it is good practice, for all company employees, to review and consider:

a) he data subjects concerned (office employees, crew members, suppliers, consultants, surveyors, technicians, etc.),
b) the business function involved (accounting, crewing, technical, office administration, etc.),
c) the data flows and the process (forms, document, policies, procedures, systems, etc.) recorded in the company's PD and IT Assets Inventories and
d) the data quality policy (see Appendix 6. Data Quality Policy) and other relevant data governance controls (*see 'DGC 10: Data Governance Controls' in my book '**Data Governance Controls**' (www.bookboon.com)*.

3) **PD Storage Actions**

PD Storage Action #1. Retention period. Personal data must be stored only for as long as necessary, taking into account the purposes for which they were collected and the applicable legal storage periods.

PD Storage Action #2. Safe storage for data on paper. When the data are stored on paper (physical files), you must store them in a safe place where unauthorized people cannot see them.

PD Storage Action #3. Printing data. When not required, printing documents or files containing personal data should be stored in a locked drawer or archive cabinet.

PD Storage Action #4. Electronic data protection.
When data is stored electronically, you must protect it from unauthorized access, accidental deletion, and malicious hacking attempts by:

1) Protecting them with strong passwords that change regularly and never share with employees.
2) Not storing data on removable media (such as a USB drives).
3) Not storing data in Cloud Storage Units or Cloud Computing Systems.
4) Not storing data directly on laptops or other mobile devices such as tablets or smart phones, unless they are encrypted.
5) Saving data only on designated drives and servers.
6) Placing servers containing personal data in a secure location (special computer room area) away from the general office space.
7) Backing up regularly, according to the company's routine backup procedures.
8) Protecting all servers and computers containing data by, at least, an approved security software system and a firewall, etc.

4.6 PERSONAL DATA PUBLISHING ACTIONS

1) **Overview**: The actions outlined below relate to the fifth step (Publishing Data) of the 7-step data life cycle of the company.

   Once data have been collected or captured, maintained, used, and stored, they are usually published (or shared) for various needs in order to support the business functions and transactions of the company.

   Data Publication (including data sharing) is about sending the personal data to a location or system outside the specific company.

   To ensure that personal data are published (or shared) in the most secure way and comply fully with the requirements of GDPR, the following actions are recommended to be used by all company employees in this regard.

2) **Practical Tips**

   Practical Tip 1: It is good practice, *at least once a year*, for all company employees, to review the corporate policies and procedures and any changes *related to GDPR and privacy/security issues (e.g., data retention, data deletion, legal basis of processing, etc.)* affecting their duties in their specific business function and particularly anything that impacts personal data processed within their own department or corporate function.

Practical Tip 2: In carrying out their daily *or ad-hoc* PD publishing (sharing) duties by executing the actions outlined next, it is good practice, for all company employees, to review and consider:

a) the data subjects concerned (office employees, crew members, suppliers, consultants, surveyors, technicians, etc.),
b) the business function involved (accounting, crewing, technical, office administration, etc.),
c) the data flows and the process (forms, document, policies, procedures, systems, etc.) recorded in the company's PD and IT Assets Inventories and
d) the data quality policy (see Appendix 6. Data Quality Policy) and other relevant data governance controls (*see 'DGC 10: Data Governance Controls' in my book '**Data Governance Controls**' (www.bookboon.com)*.

3) **PD Publishing Actions**

PD Publishing Action #1. Using processors. When you use processors to process personal data you must do this on a basis of a controller-processor contract with all the necessary precautions outlined in the specific contract with the specific processor.

PD Publishing Action #2. Transfers out of E U. Personal data must never be transferred outside the European Union unless the legal conditions provided for by the Regulation are in place.

PD Publishing Action #3. Sending personal data by e-mail.
When you have the required approval from the company and you send an email with personal data of employees, partners, affiliates, citizens, customers or third parties, you are very careful that you send them to the right recipient, always recording the actions taken on a log, and always adding a password in the corresponding excel or word document.

PD Publishing Action #4. No disclosure.
You do not share any company data with unauthorized people in any way, including financial details of the company, personal data and information of citizens, customers, users, etc., such as telephones, emails, addresses, etc.

PD Publishing Action #5. Using FAX.
When you have the required approval from the company and you use a FAX machine to send any personal data of employees, partners, affiliates, citizens, customers or third parties, you are very careful that you send them to the right recipient, always recording the actions taken, etc.
See also 'Appendix 5. FAX Management Controls' for more details.

PD Publishing Action #6. Using Post Office.
When you have the required approval from the company and you use the postal services to mail any personal data to any recipient, you use the registered mail and you keep the receipt on file.

PD Publishing Action #6. Using Courier.
When you have the required approval from the company and you use a courier to send any personal data to any recipient, you ensure that your company has a contract with the specific courier company with confidentiality and GDPR compliance clauses in it.

4.7 PERSONAL DATA PURGING ACTIONS

1) **Overview**: The actions outlined below relate to the sixth step (Purging Data) of the 7-step data life cycle of the company.

   Up to this step, data have been collected or captured, maintained, used, stored and published (or shared).

   The next step is to purge (or delete) them, especially if the data have reached the end of their life-cycle, i.e., there is no further legitimate need to maintain and process them for any reason, what-so-ever.

   Data Purging (or Data Deletion) is the total removal of every copy of the personal data from the specific enterprise.

   To ensure that personal data are purged (or deleted) in the most secure way and comply fully with the requirements of GDPR, the following actions are recommended to be used by all company employees in this regard.

2) **Practical Tips**

   Practical Tip 1: It is good practice, *at least once a year*, for all company employees, to review the corporate policies and procedures and any changes *related to GDPR and privacy/security issues (e.g., data retention, data deletion, legal basis of processing, etc.)* affecting their duties in their specific business function and particularly anything that impacts personal data processed within their own department or corporate function.

   Practical Tip 2: In carrying out their daily *or ad-hoc* daily PD purging duties by executing the actions outlined next, it is good practice, for all company employees, to review and consider:

a) the data subjects concerned (office employees, crew members, suppliers, consultants, surveyors, technicians, etc.),
b) the business function involved (accounting, crewing, technical, office administration, etc.),
c) the data flows and the process (forms, document, policies, procedures, systems, etc.) recorded in the company's PD and IT Assets Inventories and
d) the data quality policy (see Appendix 6. Data Quality Policy) and other relevant data governance controls (*see 'DGC 10: Data Governance Controls' in my book '**Data Governance Controls**'* (www.bookboon.com).

3) **PD Purging Actions**

PD Purging Action #1. Data deletion. When the period of storage of the personal data expires, you must delete them in a permanent and secure manner.

PD Purging Action #2. Reports and media deletion. You must cut or shred printed reports and destroy digital media containing personal data using special equipment, and discard them safely when they are no longer needed.

PD Purging Action #3. Returning company equipment. After termination of the employment contract, employees are required to return any equipment (such as computers, mobile phones, etc.) that they have which has been granted by the Company and is the property of the Company after deleting any file or documents containing personal data from the specific equipment.

PD Purging Action #4. Deleting Personal Data on Personal Equipment. In the event that employees use personal equipment (mobile phones, computers) for business purposes in the performance of their duties, they must, upon terminating their employment contract, for any reason whatsoever, give written assurance to the company that they have deleted all personal data and all professional correspondence (e.g. e-mail or other electronic messages, etc.) from their personal equipment.

4.8 PERSONAL DATA SECURITY ACTIONS

1) **Overview**: The actions outlined below relate to the seventh step (Securing Data) of the 7-step data life cycle of the company.

The company's general data life cycle of: Collecting Data, Maintaining Data, Using Data, Storing Data, Publishing Data and Purging Data is supported by the actions of Securing Data.

This is due to the requirements of GDPR which state that the Company must take reasonable steps to ensure that personal data (PD) are fully secure in all their processing steps within the specific company.

In this regard, the Company applies appropriate technical and organizational measures to protect personal data from accidental or unlawful destruction, accidental loss or alteration, unauthorized disclosure or access and any other illegal processing.

These measures were designed on the basis of a risk analysis and a Data Protection Impact Assessment (DPIA) developed by a GDPR Compliance Advisor on behalf of the company.

To ensure that personal data are processed in the most secure way and comply fully with the requirements of GDPR, the following actions are recommended to be used by all company employees in this regard.

2) **Practical Tips**

Practical Tip 1: It is good practice, *at least once a year*, for all company employees, to review the corporate policies and procedures and any changes *related to GDPR and privacy/security issues (e.g., data retention, data deletion, legal basis of processing, etc.)* affecting their duties in their specific business function and particularly anything that impacts personal data processed within their own department or corporate function.

Practical Tip 2: In carrying out their daily *or ad-hoc* daily PD security duties by executing the actions outlined next, it is good practice, for all company employees, to review and consider:

a) the data subjects concerned (office employees, crew members, suppliers, consultants, surveyors, technicians, etc.),
b) the business function involved (crewing, technical, office administration, etc.),
c) the data flows and the process (forms, document, policies, procedures, systems, etc.) recorded in the company's PD and IT Assets Inventories and
d) the data quality policy (see Appendix 6. Data Quality Policy) and other relevant data governance controls (*see 'DGC 10: Data Governance Controls' in my book '**Data Governance Controls**'* (www.bookboon.com).

3) **PD Security Actions**

PD Security Action #1. Breach reporting.
Security breaches, which compromise the confidentiality or security of personal data processed by the Company, should be reported immediately to any member of the Company's Management as well as to the controller and the Data Protection Officer.

PD Security Action #2. Do not open attachments.
Never open email attachments. Even if you know the recipient, you should send the attachment to an IT specialist for scanning before you read it.

PD Security Action #3. Antivirus updating.
Update your antivirus. In all cases, you must request your IT department for specific instructions. Do not do things you do not fully comprehend.

PD Security Action #4. Use a strong password. In all cases you must comply with the instructions of the IT department. Generally speaking, you must have created a powerful password to enter the company's computer. Codes like 1234, abcd, 1234qwe etc ... are the first choices in a hacker list. Example of strong passwords are: k @ l1m3rA {}.

PD Security Action #5. Using original e-mail.
You never send any data to an email you receive from a supposed data subject (citizen, user, client, etc.) unless you make certain that the specific subject has used the same email for the first (original) communication with you.

PD Security Action #6. Subject identification. Do not give any personal data by phone if you do not identify the data subject (citizen, client, etc.).

PD Security Action #7. Understand risks.
You should study, review and comprehend the impact of the risks contained in Appendix 1: Information security and data privacy risks

PD Security Action #8. Security in Information Systems.
The company's information systems should be developed with security actions incorporated into all computer programs and these actions should be documented, reviewed and improved on a periodic basis.

PD Security Action #9. Review and practice additional security controls.
You should study, review, comprehend and comply with the guidelines and actions listed in the following:
Appendix 2: Guidance on safeguarding of confidential information
Appendix 3: Information Systems Security actions
Appendix 4: Clean Desk and Screen policy
Appendix 5. FAX Management Controls.

APPENDIX

Summary: This appendix contains a list of information and data privacy risks and a set of additional controls related to the better protection of the security and privacy of personal data.

Contents

APPENDIX 1: INFORMATION SECURITY AND DATA PRIVACY RISKS

1. Risks in buildings and Infrastructure

1. Serious building damage (large fire, flood, terrorist activity, extended power outage, etc.).
2. Air conditioning system failure.
3. Overheating system.
4. Fire in the data center.
5. Local fire.
6. Power outages.
7. Voltage surge – sparks.
8. Unauthorized access to the data center (Data Centre).
9. Damage (unintentionally) by non-suitably trained personnel.
10. Intentional damage/sabotage.
11. Hardware/software theft.

2. Risks in equipment and network

1. Serious equipment system failure (circuit, power supply, problem with fixed software segment (Firmware).
2. Local network failures resulting in loss of access to users/administrators/interfaces.
3. Wider network failures resulting in loss of access to users/administrators/interfaces.
4. Lack of system resources (CPU, memory, disk, IO) causing system failure or low performance.

3. Risks in system and network access

1. Malware (virus software, worms, trojan horses, etc.).
2. Network intrusion/ hacking.
3. Stealing passwords from a user.
4. Access by using dormant account.
5. Improper access to an account.
6. External partners.
7. Improper use of computers.
8. Improper use of access to the Internet.
9. Improper electronic correspondence (Email).

4. Application and Compliance risks

1. Unauthorized application development.
2. Changes in application.
3. Incoming data errors.
4. Deletion of necessary data.
5. Data spill of personal data.
6. Absence of support for internal controls.
7. Failure to implement security policies and procedures.
8. Non-compliance with the regulations.

5. Risks of data management and processing

1. Incomplete documentation of data processing.
2. Not efficient management of encryption keys.
3. Non-efficient management of user access rights.
4. Not efficient management of unstructured data (word documents, emails, etc.).
5. Not effective monitoring of the personnel who manages company data.
6. Not effective monitoring of information security incidents and events and data breaches in company data.
7. Non-effective implementation of data theft prevention measures of the company **that have been stored in equipment (servers), personal computers (laptops), media (digital media) and devices (mobile and smart devices)**.
8. Non-effective implementation of the Company's data transfer prevention measures **on personal computers (laptops), media (digital media) and devices (mobile and smart devices)**.
9. Non-effective implementation of data destruction measures of the company **that have been stored on personal computers (laptops), media (digital media), devices (mobile and smart devices) and prints**.

6. Risks of data subjects (GDPR)

1. Risk of non-compliance with the principles of processing of personal data (Article 5 and 89)
2. Risk of non-compliance with the requirements of article 6 (Legality of processing)
3. Risk of non-compliance with the requirements of articles 7 and 8 for the consent of individuals
4. Risk of non-compliance with the requirements of articles 9 and 10 for the processing of sensitive and criminal personal data
5. Risk of non-compliance with the requirements of article 12 to inform data subject rights
6. Risk of non-compliance with the requirements of articles 13 and 14 (information in policy privacy)
7. Risk of non-compliance with the requirements of articles 15 – 22 (access, rectification, deletion, mobility, etc. individuals ' personal data)
8. Risk of non-compliance with the requirements of article 34 (breach of personal data).

Appendix 2: Guidance on safeguarding of confidential information. This is detailed in my book 'Data Governance Controls' (www.bookboon.com) (DGC 1: Guidance on safeguarding of confidential information).

Appendix 3: Information Systems Security actions. This is detailed in my book 'Data Governance Controls' (www.bookboon.com) (DGC 2: Information Systems Security actions).

Appendix 4: Clean Desk and Screen policy. This is detailed in my book 'Data Governance Controls' (www.bookboon.com) (DGC 3: Clean Desk and Screen policy).

Appendix 5. FAX Management Controls. This is detailed in my book 'Data Governance Controls' (www.bookboon.com) (DGC 4: FAX Management Controls).

Appendix 6. Data Quality Policy

The primary objective of the **Data Quality** Policy is to provide guidelines all staff of the enterprise regarding the procedures and practices used to ensure quality of the data collected, processed and archived by all information systems and business functions.

An example of such a policy is described next.

Company 'AXYZ-Fictitious Enterprise Corporation' Data Quality Policy

'Company 'AXYZ' implements a data quality management system according to well-accepted international standards that cover the whole range of the activities of the company.

The main data quality elements of the company are:

1. Install a continuous improvement program for data quality.
2. Implement procedures to ensure the full application of the following seven characteristics of good data quality: Accuracy; Validity; Reliability; Timeliness; Relevance; Completeness; and Compliance.

   2.1. Accuracy: Data should provide a clear representation of the activity; Data should be in sufficient detail; and Data should be captured once only as close to the point of activity as possible.

   2.2. Validity: Data should be recorded and used in accordance with agreed requirements, rules, standards and definitions to ensure integrity and consistency.

   2.3. Reliability: Data collection processes must be clearly defined and stable to ensure consistency over time, so that data accurately and reliably reflects any changes in performance.

   2.4. Timeliness: Data should be collected and recorded as quickly as possible after the event or activity; and Data should remain available for the intended use within a reasonable or agreed time period and in accordance with the relevant regulation.

   2.5. Relevance: Data should be relevant for the purposes for which it is used; Data requirements should be clearly specified and regularly reviewed to reflect any change in needs; and the amount of data collected should be proportionate to the value gained from it and consent should be obtained as per regulatory requirements.

   2.6. Completeness: Data should be complete.

   2. 7. Compliance: Data must comply with regulations on data protection and data security.
3. Observe the data quality management procedures on a continuous basis in order to ensure their exact implementation and continuous improvement.
4. Enable employee participation in all aspects of data quality.
5. Respond as quickly as possible to operational problems and requests related to data collected, processed and archived.
6. Improve personnel satisfaction with continuous enhancement of their skills as regards data quality.
7. Monitor the needs by various tools and mechanisms for the creation and provision of new products and services with particular emphasis to the use of personal data.
8. Provide the required leadership and support to data quality.
9. Roles and responsibilities should be assigned for data quality to all staff levels of the company and should be included in their employment contracts and job descriptions'.

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
   1.8. The CEO's Guide To GDPR Compliance: The guide for C-Suite Members to ensure GDPR compliance, bookboon.com, 2017
   https://bookboon.com/en/the-ceos-guide-to-gdpr-compliance-ebook

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.