# Managing Data and its Implications

## Lecture Title: Implications on Business Part II


Lecturer: Angelito Sciberras

Date: 24 June 2024

Undergraduate Diploma

# The assignment questions

# Question 01

Your task is to critically analyse the concept of lawful basis for processing personal data within the framework of GDPR. In your response, address the following:

- Define what is meant by the term "lawful basis for processing personal data."
- Identify and explain at least three lawful basis for processing personal data as outlined in the GDPR.
- Discuss the significance of selecting an appropriate lawful basis for processing personal data.
- Provide examples illustrating instances where organisations have faced challenges or consequences due to improper selection or misuse of lawful basis for processing personal data.

# Question 02

Your task is to identify the data subject rights enshrined within the GDPR and explain their implications for organisations operating within the European Union or processing the personal data of EU residents. In your response, address the following:

- Define and explain the eight data subject rights enumerated in the GDPR.
- Briefly explain the procedure for handling data subject requests and ensuring timely response.
- Name at least 4 different data privacy information notices that an organisation must have to fulfil the right to information and list what information must be provided to the data subjects.

# Question 03

Your task is to analyse the implications of data breaches under the GDPR framework and examine the responsibilities of organisations in responding to and mitigating such incidents. In your response, address the following:

- Define what constitutes a data breach according to the GDPR and distinguish between different types of data breaches, including accidental and unlawful breaches.
- Outline the obligations of organisations under the GDPR regarding the notification and reporting of data breaches to supervisory authorities and affected individuals.
- Discuss strategies and best practices for organisations to include preventive measures against data breaches.

# The group presentation question

# Question

## Privacy Consideration when designing a website

Designing a company website with data capturing tools for recruitment and service booking entails significant privacy considerations. In a 20-minute presentation, explore the ethical and practical dimensions of privacy in this context. How can companies balance the need for data collection with respecting user privacy? What measures should be in place to ensure transparency and consent? Discuss potential risks, and show best practices from existing websites, for safeguarding user data in such websites.

# Managing Data and its Implications

## Lecture Title: Implications on Business Part II


Lecturer: Angelito Sciberras

Date: 24 June 2024

Undergraduate Diploma

# Last Lecture

- Most effected departments in a business
- Checklist
- Policies and Procedures a company shoud have
- Monitoring
- Data Inventory
- Data Processing Agreement
- Technical vs Organisational Measures
- IT Department

# Which of the following is a must-have from the GDPR compliance checklist?

a) Conduct regular employee training sessions on data protection

b) Conduct regular customer satisfaction surveys

c) Update the company logo on the website

d) Organize team-building activities for employees

# Which of the following is a must-have from the GDPR compliance checklist?

a) Review and update company social media policies

b) Review and update privacy notices and policies

c) Schedule regular team meetings

d) Conduct customer market research

# Which of the following is a must-have from the GDPR compliance checklist?

a) Implement measures to increase data collection

b) Implement measures to ensure data accuracy and minimize data collection

c) Implement measures to track employee attendance

d) Implement measures to increase data sharing

# Which of the following is a must-have from the GDPR compliance checklist?

a) Review and update data processing agreements with third-party service providers

b) Review and update the company's vacation policy

c) Review and update employee dress code

d) Review and update company mission statement

# Which of the following is a must-have from the GDPR compliance checklist?

a) Implement measures to ensure data security

b) Implement measures to improve office decor

c) Implement measures to enhance employee benefits

d) Implement measures to increase marketing efforts

# Which of the following is a must-have from the GDPR compliance checklist?

a) Appoint a Chief Executive Officer (CEO)

b) Appoint a Data Protection Officer (DPO)

c) Appoint a Chief Financial Officer (CFO)

d) Appoint a Chief Marketing Officer (CMO

# Which of the following is a must-have from the GDPR compliance checklist?

a) Establish procedures to respond to customer complaints only

b) Establish procedures to respond to data subject requests and complaints

c) Establish procedures to respond to employee complaints only

d) Establish procedures to respond to supplier complaints

# Most effected departments in a company?

- IT
- Human Resources
- Marketing (Sales)
- Finance

# HR Data

Give some examples of why an employer processes personal data.

# Some examples...

- For payroll
- For benefits
- For insurance
- For background checks
- For training
- For legal reasons
- For disciplinary matters
- For performance reviews

# HR Data

Give some examples of personal data an employer processes.

# Some examples...

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth.
- Gender.
- Marital status and dependants.
- Next of kin and emergency contact information.

# Some examples...

- Next of kin and emergency contact information.
- National Insurance number.
- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension, and benefits information.
- Start date.

# Some examples...

- Location of employment or workplace.
- Copy of driving licence.
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process).
- Employment records (including job titles, work history, working hours, training records and professional memberships).
- Compensation history.

# Some examples...

- Performance information.
- Disciplinary and grievance information.
- CCTV footage and other information obtained through electronic means such as telephone calls' recordings.
- Information about your use of our information and communications systems.
- Photographs.

# HR Data

10:00

Give examples of processors directly involved with HR departments

# Some examples...

- Payroll Services
- HRM software
- Researchers
- Activity storage services (CCTV, access, tracking)

10:00

21 ACADEMY

Undergraduate Diploma

# Most effected departments in a company?

- IT
- Human Resources
- Marketing (Sales)
- Finance

# Direct Marketing vs Indirect Marketing

# What do we mean by “direct marketing” ?

# Direct Marketing

- In the UK DPA 2018 :

- “the communication (by whatever means) of advertising or marketing material which is directed to particular individuals”

# Direct Marketing

- Direct Marketing covers all advertising or promotional material.
- Including those promoting the aims or ideals of NGOs, charities and political parties.
  - E-mails
  - Print ads
  - Telephone Calls
  - Direct mail

# Indirect Marketing

- News articles and press
- Sponsorships
- Blog posts
- Social media pages
- Social media influencers
- Product placements
- Word-of-mouth
- Referrals

# Direct Marketing

- does not include “genuine market research”

- unless a survey includes promotional material

# Direct Marketing

- Genuine routine customer-care service messages do not count as direct marketing.

- E.g. correspondence on current contracts, past purchases, service interruptions etc.

# Direct Marketing

DATA PROTECTION LAW
cares about direct marketing

# Direct Marketing

- ...How is direct marketing regulated?
- **General Data Protection Regulation ('GDPR') - 2016/679**
- **Data Protection Act (Chap. 586)**
- **Processing of Personal Data (E-Communications Sector) Regulations (586.01)**
- **Processing of Child's Personal Data in relation to the Offer of Information Society Services Regulations (586.11)**

# GDPR | RECITAL 47

*“The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest."*

E.g. to profile your customers?

***3-Part-Test must be documented***

# 3-Part-Test

**1 Purpose**

**Is it in Your Interests?**
**Is it Lawful?**
**Is it Ethical?**

**2 Necessity**

**Is it Proportionate?**
**Are There Alternatives?**

**3 Balance**

**Is it High-Risk?**
**What's the Impact?**

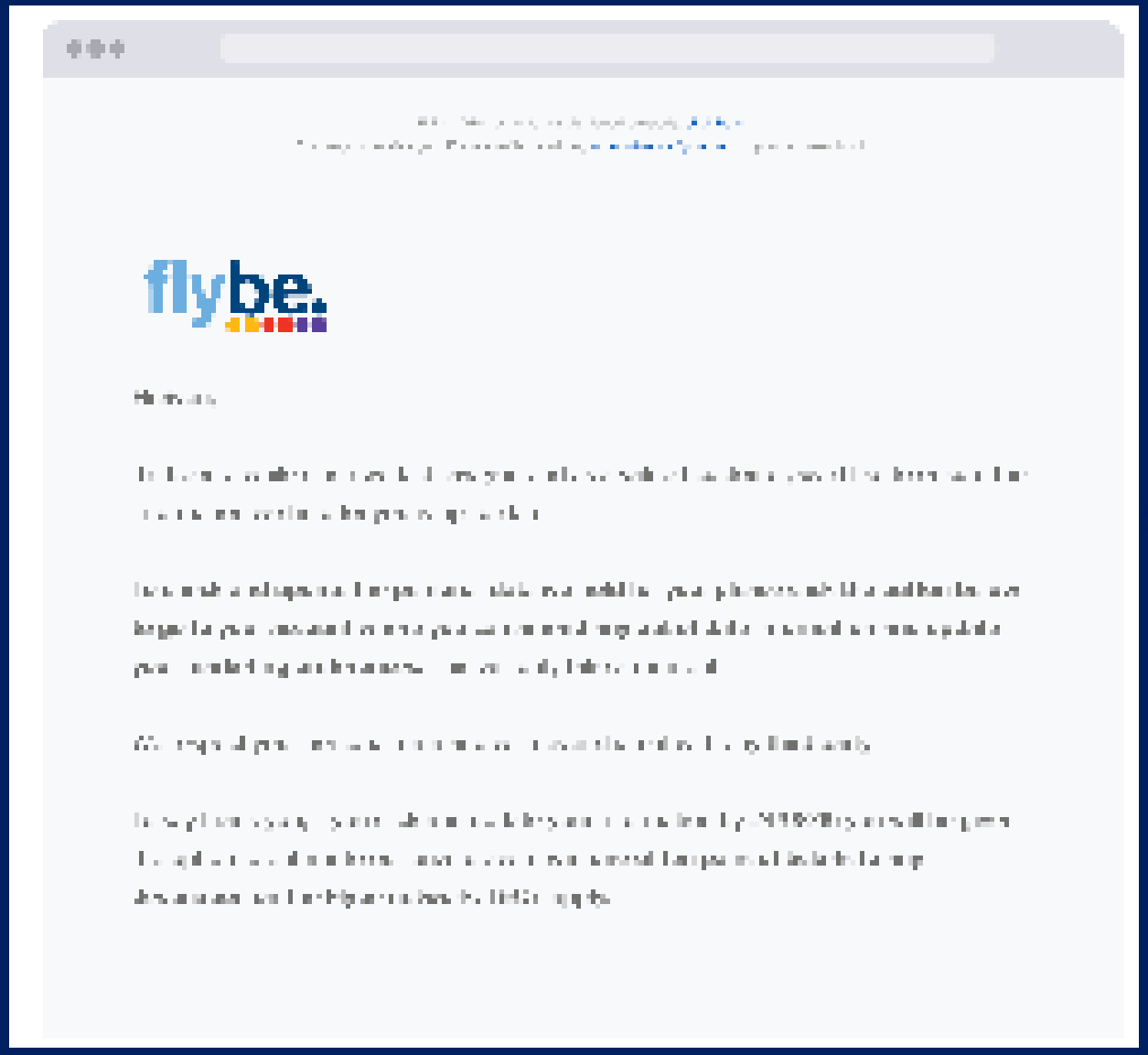
# GDPR | Article 21(2) | Right to Object

*"Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing."*

# GDPR | Article 21(2) | Right to Object

*“Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.”*

>> Therefore >> NO possibility to contest




£70,000

# Processing of Personal Data (E-Communications Sector) Regulations

1. Transpose older EU Directives.

2. Is likely to be replaced by a new Regulation.

# Processing of Personal Data (E-Communications Sector) Regulations

Includes key rules on:

1. **Direct Marketing**

2. **Web Cookies - (essential tools for Online Behavioural Marketing)**

## (1) Direct Marketing

# DO NOT SPAM.

# (1) Direct Marketing

**DO NOT SPAM.**

**… You cannot send unsolicited communication for the purpose of direct marketing by means of**

**(a) an automatic calling machine; or**

**(b) a facsimile machine; or**

**(c) electronic mail**

**to a subscriber or user (including legal entities), unless with the prior consent in writing**

## (1) Direct Marketing

*Unsolicited = a message that has not been specifically requested.*

# DO NOT SPAM.

**… You cannot send unsolicited communication for the purpose of direct marketing by means of**

**(a) an automatic calling machine; or**

**(b) a facsimile machine; or**

**(c) electronic mail**

**to a subscriber or user (including legal entities), unless with the prior consent in writing**

## (1) Direct Marketing

*It applies also to **marketing leads** which might not include actual product/services info.*

# DO NOT SPAM.

**… You cannot send unsolicited communication for the purpose of direct marketing by means of**

**(a) an automatic calling machine; or**

**(b) a facsimile machine; or**

**(c) electronic mail**

**to a subscriber or user (including legal entities), unless with the prior consent in writing**

# (1) Direct Marketing

**DO NOT SPAM.**

… You cannot send unsolicited communication for the purpose of direct marketing by means of

(a) an automatic calling machine; or

(b) a facsimile machine; or

(c) electronic mail

to a subscriber or user (including legal entities), unless with the prior consent in writing

# What do we mean by “electronic mail” ?

# Electronic Mail

"**electronic mail**" means **any text, voice, sound or image** message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient;


# (1) Direct Marketing

**DO NOT SPAM.**

… You cannot send unsolicited communication for the purpose of direct marketing by means of

(a) an automatic calling machine; or

(b) a facsimile machine; or

(c) electronic mail

to a subscriber or user (including legal entities), unless with the prior consent in writing

# (1) Direct Marketing

**DO NOT SPAM.**

**… You cannot send unsolicited communication for the purpose of direct marketing by means of**

**(a) an automatic calling machine; or**

**(b) a facsimile machine; or**

**(c) electronic mail**

**to a subscriber or user (including legal entities), unless with the prior consent in writing**

# Consent

…. GDPR

- freely given + informed + clear + specific
- positive action
- Generic consent covering “any third party” = very likely insufficient

# Consent - expires?

- The law doesn’t impose time-limits
- Consent does not remain valid for ever.
- Must be assessed on a case-by-case basis : is it still reasonable to treat it as an ongoing indication of the person’s wishes?
- e.g. was consent given in the context of a specific campaign or service that might have ended?

## (1) Direct Marketing

**BUT**

**[soft-opt-in]**

Where a person has obtained from his customers their contact details for electronic mail in relation to the sale of a product or a service, in accordance with the Act, that same person may use such details for direct marketing of its own similar products or services;

**In Malta It is still not clear whether the exception applies to enquires by potential customers.**
E.g. on a Web Form
E.g. by requesting a quotation

**UK : Some form of negotiation is required showing interest, even asking for a quote.**

# BUT
## [soft-opt-in]

Where a person has obtained **from his customers** their contact details for electronic mail in relation to the sale of a product or a service, in accordance with the Act, that same person may use such details for direct marketing of its own similar products or services;

**This is specific.** If you use other personal data, you would need to assess the grounds separately.

# BUT

## [soft-opt-in]

Where a person has obtained from his customers their **contact details** for electronic mail in relation to the sale of a product or a service, in accordance with the Act, that same person may use such details for direct marketing of its own similar products or services;

*"Any text, voice, sound or image message"*

NB The exception doesn't apply to FAX or Automated Calls

# BUT

## [soft-opt-in]

Where a person has obtained from his customers their contact details for **electronic mail** in relation to the sale of a product or a service, in accordance with the Act, that same person may use such details for direct marketing of its own similar products or services;

# BUT

## [soft-opt-in]

Where a person has obtained from his customers their contact details for electronic mail in relation **to the sale of a product or a service**, in accordance with the Act, that same person may use such details for direct marketing of its own similar products or services;

# BUT

## [soft-opt-in]

Where a person has obtained from his customers their contact details for electronic mail in relation to the sale of a product or a service, **in accordance with the Act**, that same person may use such details for direct marketing of its own similar products or services;

**PROVIDED THAT** customers shall be given the opportunity to object, free of charge and in an easy and simple manner, to such use of electronic contact details at the time of their collection and on the occasion of each message where the customer has not initially refused such use;

**PROVIDED THAT**

customers shall be given the **opportunity to object**, free of charge and in an easy and simple manner, to such use of electronic contact details at the time of their collection and on the occasion of each message where the customer has not initially refused such use;

**PROVIDED THAT** customers shall be given the opportunity to object, **free of charge** and in an easy and simple manner, to such use of electronic contact details at the time of their collection and on the occasion of each message where the customer has not initially refused such use;

**PROVIDED THAT**

customers shall be given the opportunity to object, free of charge and **in an easy and simple manner**, to such use of electronic contact details at the time of their collection and on the occasion of each message where the customer has not initially refused such use;

**PROVIDED THAT**

customers shall be given the opportunity to object, free of charge and in an easy and simple manner, to such use of electronic contact details **at the time of their collection and on the occasion of each message** where the customer has not initially refused such use;

# Direct Marketing - Unlawful

- Disguising or concealing the identity of the e-mail sender
- e-mails that do not contain a valid email address for recipients to request that communications stop
- Marketing e-mails that encourage recipients to visit websites that contravene these rules

# Direct Marketing Important

- Make sure you are very transparent & upfront (even with customers).
- If you rely on consent, make sure you get different opt-ins for different forms of communications.
- Make sure you keep  clear records of consents.

# Why is it important to keep a log of who opted out?

# Direct Marketing Important

- Make sure you keep a ‘do not contact’ list of anyone who objects or opts out.
- Be sure to check applicable laws !! – Market research!!
- Look out for industry-specific rules. (e.g. igaming)

# Direct Marketing Important

- If you pay someone to do your marketing..... you are both responsible to comply...

- If you apply Automated-Decision-Making (with legal or similar effects)
- ... double check your position.

- Look out for industry-specific rules. (e.g. igaming)

# Marketing FAQs

# Question 1

The GDPR obviously covers email and email communications - does it also include telephone and postal communication?

Postal communication - door to door

Robo calling

Consent and GDPR compliance by list vendor

# Question 2

Is double opt-in a guidance or a law? Does GDPR include ‘double opt-in’? i.e. A website visitor said “OK” passively, but do I need to confirm their consent? Surely single consent is enough?

# Question 3

What about my contact database? Can I still email these people?

# Question 4

How can I profile my data under GDPR to send personalised and targeted marketing material?

Automated Decision Making

Purpose Limitation

# Question 5

## How can you be sure to be compliant?

| | |
|---|---|
| 1 | lawful, fair and transparent |
| 2 | specific, explicit and legitimate purpose |
| 3 | adequate, relevant and limited to what is necessa |
| 4 | accurate & up to date |
| 5 | storage limitation |
| 6 | integrity and confidentiality |

# Question 6

Does GDPR Block Advertisers from Running Competitions? How Do Marketers Deal With Consent in a Random Prize Draw?

Highlight each piece of data collected during the competition and what you are doing with it.

An individual dropping their business card into a prize draw

# Question 7

Can we still ask people to refer friends or does it go against GDPR?

Never:

- record a referred friend's personal data
- send any message to a referred friend
- record any data about a referred friend until they have become your user and provided clear consent
- use cookies or beacons to build profiles of referred friends or to track their behaviour in any way

# Question 8

What happens to the mailing list in the case of sale or acqusition of a business? Can I sell or buy the data?

- Information to data subjects
- New owner obliged to use that data according to Privacy Notice
- Otherwise data subjects to be informed with change of purpose

# Question 9

Can you buy a marketing list/database ?

Yes (but with lots of caution), if the list was lawfully obtained for that purpose.

[consent is the ground to rely on]

# Question 10

Can you sell a marketing list/database ?

Yes (but with lots of caution), if the list was lawfully obtained for that purpose.

[consent is the ground to rely on]

# Question 11

Can a company use the same list for multiple brands?

Yes (with caution), if the list was lawfully obtained for that purpose + the customers are fully aware at the time of consent.

[do not rely on exception]

# Question 12

Can I send emails about points to members of my loyalty scheme?

Opinion : You should be able rely on legitimate interest or contract to send periodic updates on points/vouchers to members.

# Question 13

Can I send marketing emails to members of my loyalty scheme?

Opinion : You should be able rely on the soft-opt-in in relation to marketing on your similar products and customers.

21 ACADEMY

# Undergraduate Diploma in Business Administration

# Managing Data and its Implications

## Lecture Title: Implications on Business Part II


Lecturer: Angelito Sciberras

Date: 24 June 2024

Undergraduate Diploma