ecosystm

TACKLING GDPR AND DATA PRIVACY

Claus Mortensen
Principal Advisor,
Digital Transformation & Privacy,
Ecosystm


The BUCK STOPS here!

DOES THE GDPR CONCERN YOU?

The GDPR applies to processing carried out by organisations operating **within the EU**. It **also applies to organisations outside the EU** that offer goods or services to individuals in the EU.

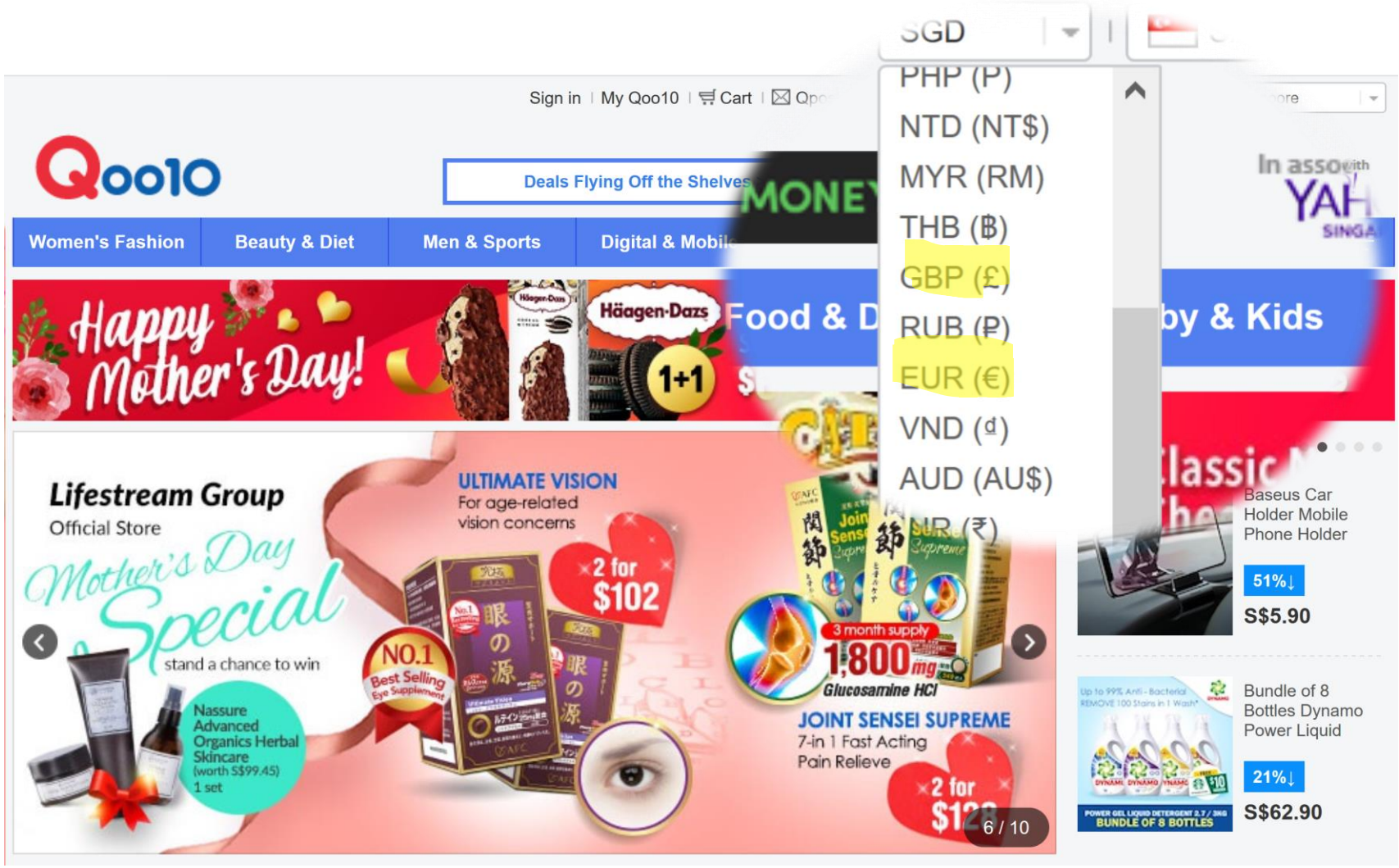
The **first "global" data protection law**.

(Singapore, the Personal Data Protection Act of 2012).

DOES THE GDPR CONCERN YOU?

Probably…. Yes!

…"intention" of dealing with residents or companies located within the EU.



General Data Protection Policy

GDPR Data Subject Requests

If you are an EU data subject, this portal allows you to retrieve or delete all of your personal data held by Amobee.

Request Status

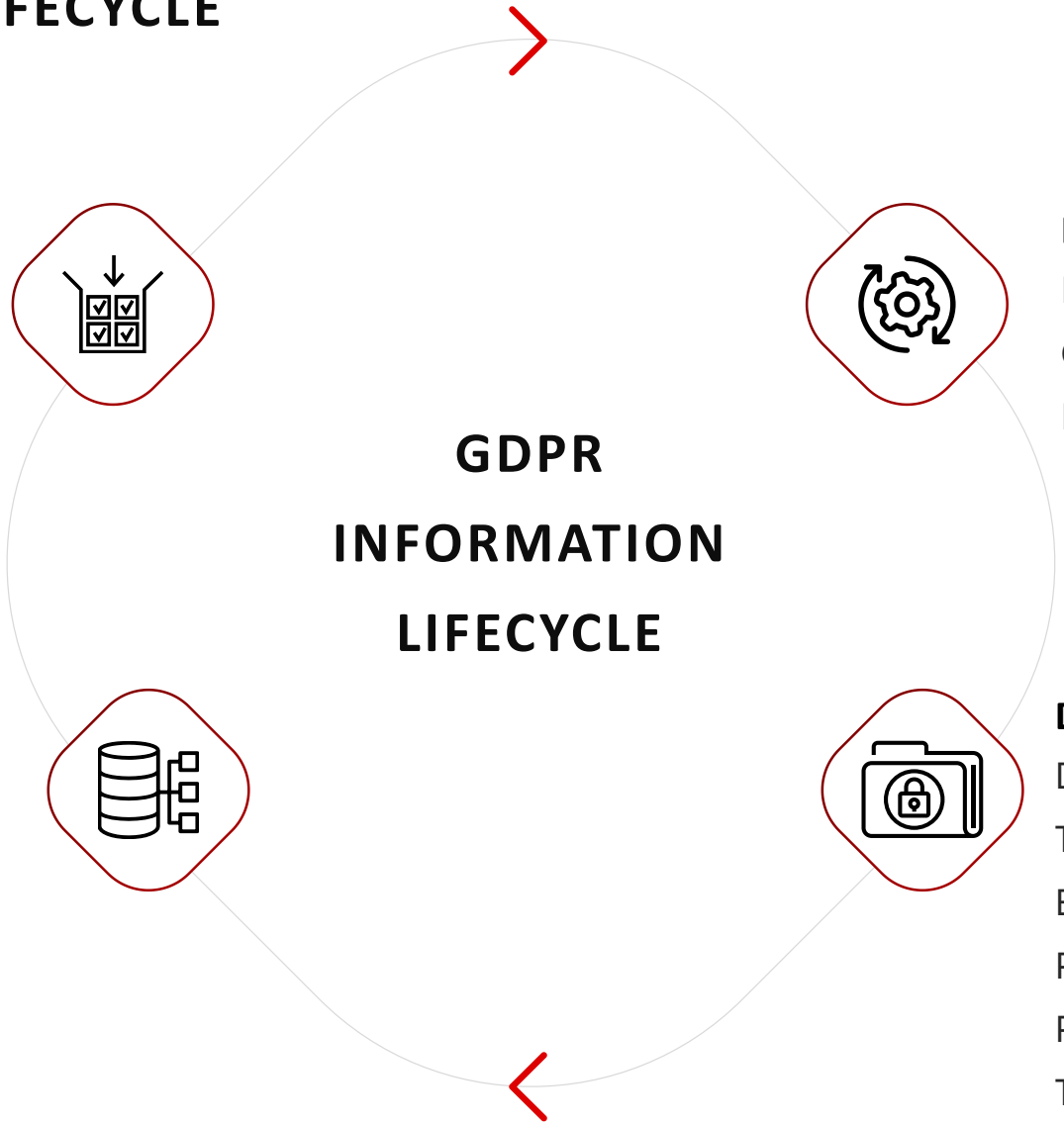
If you have previously made a data request, please enter your case number here to check the status of the request.

AT THE HEART OF THE MATTER - ARTICLE 5

The GDPR sets out seven key principles:

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

GDPR INFORMATION LIFECYCLE



DATA COLLECTION

Lawfulness
Fairness
Transparency
Purpose limitation
Data minimisation
Consent

DATA PROCESSING

Purpose specific
Consent specific
Notifications

DATA MANAGEMENT

Access
Right to rectify data
Right to be forgotten
Data transfers
Compliance
Accountability

DATA STORAGE & SECURITY

Duration
Types of data
Encryption
People
Process
Technology
Data loss

AWARENESS OF CLOUD RISK

AVERAGE APAC ORGANISATION HAS
3 current cloud solutions

EXPECTED TO BE
5 by 2020

Store sensitive data on Public Cloud

51%

Feel Public Cloud security features are sufficient

45%

FINES IMPOSED – FIRST 9 MONTHS

FINES

Number of imposed fines

SAs from 11 EEA countries imposed a total of €55,955,871 fine

Based on information provided by SAs from 11 EEA countries

Germany: Based on information provided by 4 regional SAs

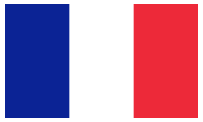
THE AREAS OF ENFORCEMENT – CASES SO FAR

Violation of the obligation to **implement adequate security measures** (Article 32 GDPR). **EUR 20,000**

Purpose limitation. Lack of legitimate interests. Video surveillance was **not sufficiently marked**, violating the transparency obligation. **EUR 4,800**

Violation of the obligation to **implement adequate security measures** (Article 32 GDPR). **EUR 400,000**

Must anonymise data. Taxi company failed to anonymise customer data. **EUR 160,000**



Google **failed to satisfactorily inform users about how their data is collected and used** in serving advertisements and marketing messages. Google also **failed to properly obtain user consent** for the purpose of using their data to serve them personalised ads. **EUR 50,000,000**

Only 0.25% of data breach cases fined under GDPR

May 10, 2019

Digi.me has revealed that only a minuscule percentage of data breach cases closed by the data protection regulator under General Data Protection Regulation (GDPR) have resulted in monetary penalties

The data, which was obtained by digi.me under the Freedom of Information Act, shows that 11,468 self-reported data breach cases were closed by the Information Commissioner's Office (ICO) between the implementation of the GDPR on 25 May 2018 and the end of March 2019. Public records displayed on the ICO website show that during this period a total of 29 monetary penalties were issued by the regulator – a penalty rate of 0.25%.

CAN FINES BE ENFORCED HERE? (1)

Article 27. Representatives of controllers or processors not established in the Union

… appoint a representative in the Union if they process personal data

Unless:

- ..only occasionally
- no large-scale processing of “special categories” of personal data
- …unlikely to result in a risk to the rights and freedoms of data subjects.

CAN FINES BE ENFORCED HERE? (2)

Article 50 - International cooperation for the protection of personal data

1. In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:

a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;....

SINGAPORE DOES NOT CURRENTLY HAVE ANY RECIPROCAL ENFORCEMENT ACTS COVERING EU COUNTRIES

WHO'S ACCOUNTABLE?

CHBM Centro Hospitalar Barreiro Montijo EPE

In its defense, the hospital argued that it used the IT system provided to public hospitals by the Portuguese Health Ministry.

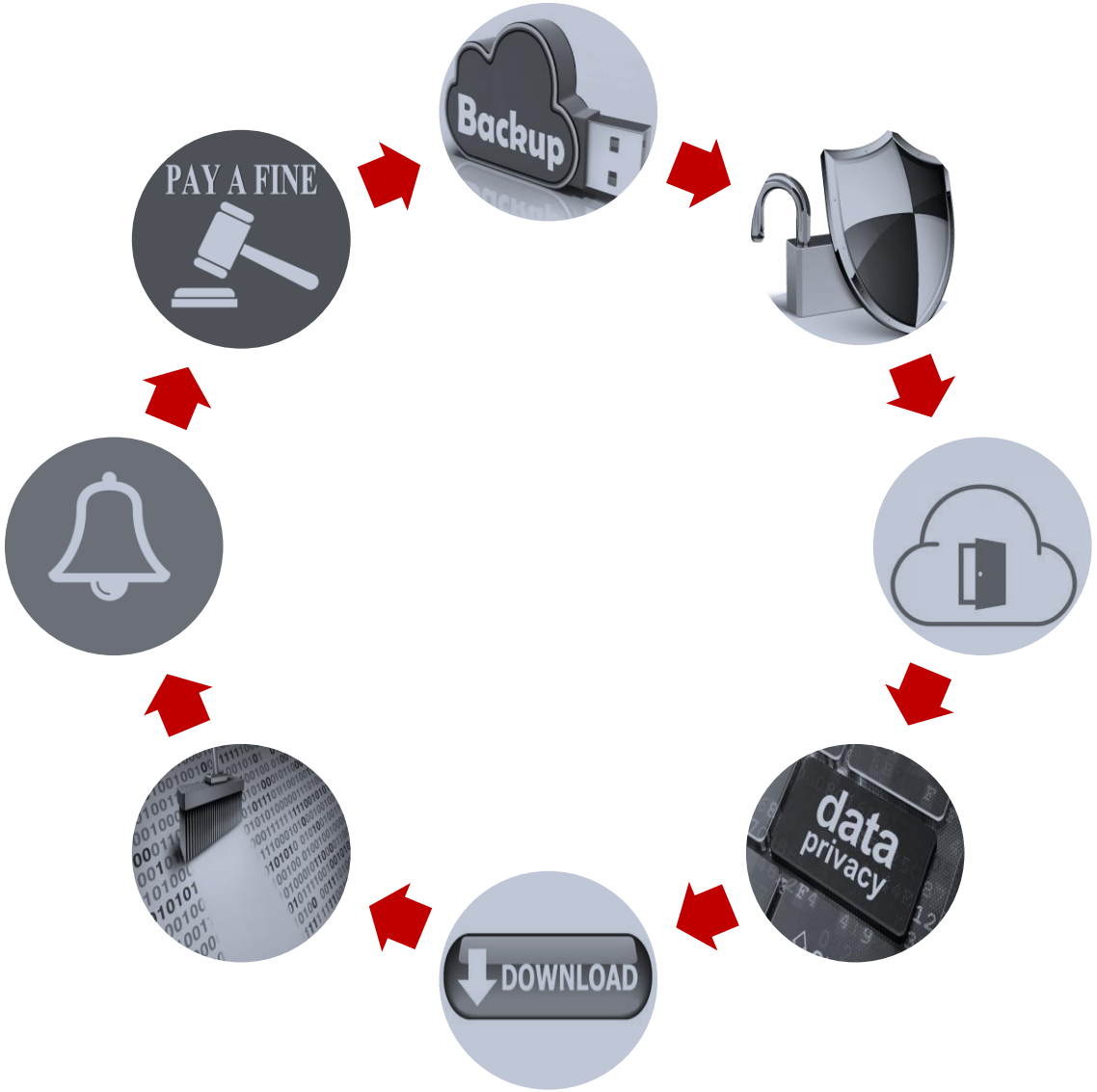
The CNPD decided that it was the hospital's responsibility to ensure that the IT system it uses complies with the GDPR.

YOU CAN'T PASS THE BUCK!

EUR 400,000

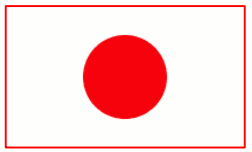
QUESTIONS FOR YOUR CLOUD PROVIDER (AND YOURSELF)

- Where is your data stored, mirrored and backed up?
- How is your data protected?
- Who has access?
- How private is your data?
- Can all the data be retrieved?
- Can all the data be deleted?
- How will your cloud provider notify you of breaches, data loss etc.?
- Internal liability and penalties



GDPR AS BLUEPRINT

Australia – the Privacy Amendment (Notifiable Data Breaches) to Australia's Privacy Act came into effect in February 2018.



Japan – Japan's Act on Protection of Personal Information – amended May 2017.

Japan and the European Commission reached an agreement on "reciprocal adequacy".

Brazil – Brazil's Lei Geral de Proteçao de Dados (LGPD) was modelled directly after GDPR.

South Korea's Personal Information Protection Act – September 2011. Similar to GDPR.

USA – no federal data privacy law applicable to all industries.

California Consumer Privacy Act (CCPA).
US Government Accountability Office (GAO) recommends federal law similar to GDPR.

India – Personal Data Protection Bill has been drafted.

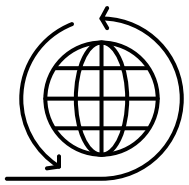
KEY TAKEAWAYS

ASK QUESTIONS AND DEMAND ANSWERS!

You need full transparency and clear answers from your outsourcing partners

THE EU CAN'T GET TO YOU….YET

Unless you're already present in the EU. And change is coming…



FUTURE GLOBAL BLUEPRINT

See compliance with GDPR as "futureproofing"

THE BUCK STOPS WITH YOU!

You can't outsource accountability

ecosystm

THANK YOU

Claus Mortensen
Principal Advisor
claus.mortensen@ecosystm360.com