dcm THE LEARNING EXPERTS

GDPR Refresher | 5 Years On

10am - 12pm

8th November 2023

Recorded

About Me

KARA OVINGTON

kara@dcmlearning.ie

dcm | Member Event

GDPR 5 years on...

- What have we learned?
- Article 6 Lawful Processing
- Special categories/ sensitive data
- RoPA – Record of Processing
- Role of the DPC
- Q&A

GDPR – 5 years on…

Introduction

The implementation of the General Data Protection Regulation (GDPR) ushered in a new era for data privacy. Billed as

“the most important change in data privacy regulation in 20 years”,

it was born out of a need to update our approach to protecting personal information.

Since its enactment five years ago, GDPR has given EU individuals greater control over their personal information while also imposing landmark restrictions on organisations regarding how they collect, store and use people’s data.

A holistic view of compliance

A holistic view of compliance
Although GDPR has bedded down in many ways, it continues to generate a high volume of activity for the regulator, for companies and for individuals.

In 2022 alone, the DPC fielded over 30,000 contacts from individuals — this is entirely separate from the organisational activity the office deals with on a day-to-day basis.

There were also 5,828 breach notifications, 61% of which arose from misdirected communications.

Stats

On 2 September 2021, the Data Protection Commission (DPC) announced it has imposed a €225 million administrative fine against WhatsApp Ireland Limited , as well as a reprimand and an order to bring its processing into compliance.

In December 2022 the DPC fined Meta Ireland a total of €390 million for breaches of the GDPR relating to its Facebook (€210 million) and Instagram (€180 million) services. In addition, the DPC also noted that Meta Ireland must bring its processing operations into compliance with the GDPR within a period of three months.t

Confirmed fines

Nov 2022

Data Protection Commission fines confirmed

30th November 2022

The Irish Data Protection Commission (DPC) yesterday had decisions to impose administrative fines on five different organisations confirmed in the Dublin Circuit Court

The decisions in relation to each of the five separate inquiries can be found below.

MOVE Ireland - August 2021 (€1,500)
Teaching Council - December 2021 (€60,000)
Limerick City and County Council - December 2021 (€110,000)
Slane Credit Union - January 2022 (€5,000)
Bank of Ireland Group plc - March 2022 (€463,000)

Deputy Commissioner Graham Doyle and Deputy Commissioner Cian O'Brien have provided an overview of these investigations, discussing the outcomes, fines and reprimands, in the latest DPC podcast - available here.

Ireland ranked second highest for GDPR fines - DLA Piper survey

Nearly €1.1 billion in fines have been imposed for a wide range of infringements of Europe's General Data Protection Regulation, a new survey shows today.

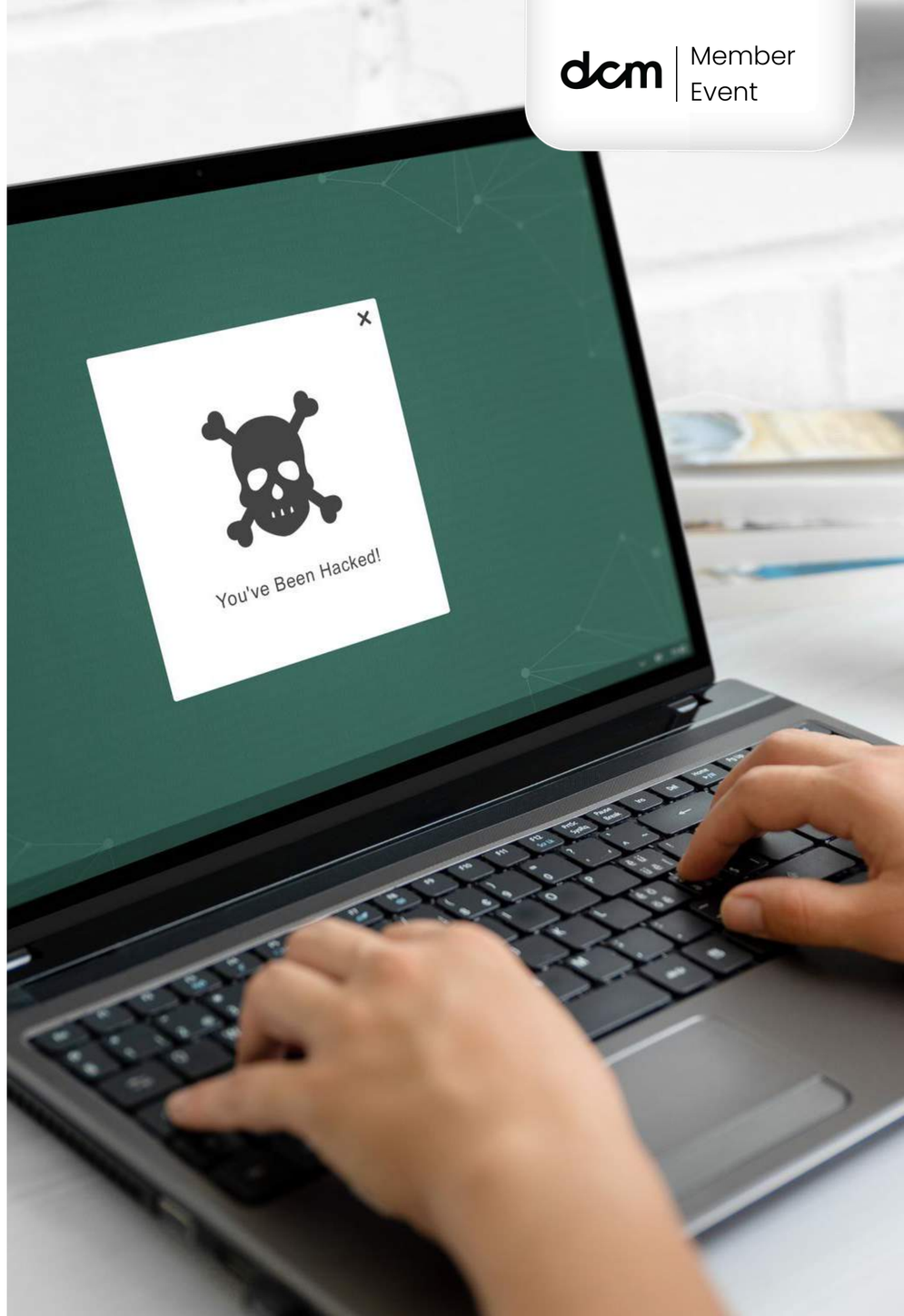
This represents a 594% annual increase in fines imposed since January 2021, according to international law firm DLA Piper's latest annual General Data Protection Regulation (GDPR) fines and data breach survey.

A total of 6,802 data breaches were reported to the Irish Data Protection Commission in the past 12 months, the survey shows.

Ireland recorded the sixth highest level of breach notifications across Europe and fourth highest on a per capita basis.

The survey shows that Luxembourg, Ireland and France top the rankings for the highest individual fines - €746m, €225m and €50m respectively.

Luxembourg and Ireland have each imposed record breaking fines moving them from the bottom to the top of the league tables.



Handling Personal Data

Article 5

GDPR checklist on how to handle personal data

In this GDPR checklist, we list the requirements for handling of personal data.

The data must be:

1. processed lawfully, fairly and in a transparent manner in relation to the data subject
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (also known as data minimization)
4. accurate and, where necessary, kept up to date
5. kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the personal data are collected
6. processed in a manner that ensures appropriate security of the personal data

You can find more on how to handle personal data in **Article 5 of the GDPR**

Article 6 Lawful Processing

For standard PII

1 Consent : IMPLIED – business cards
: INFORMED –privacy notice, cookies…
: EXPLICIT – direct marketing / outside E.U. / sensitive data

2 Performance of a contract

3 Legal obligations : drink aware…

4 Vital interests, where DS is incapable : eg death / severe harm

5 Public interests : gossip, media, CCTV, councils, police…

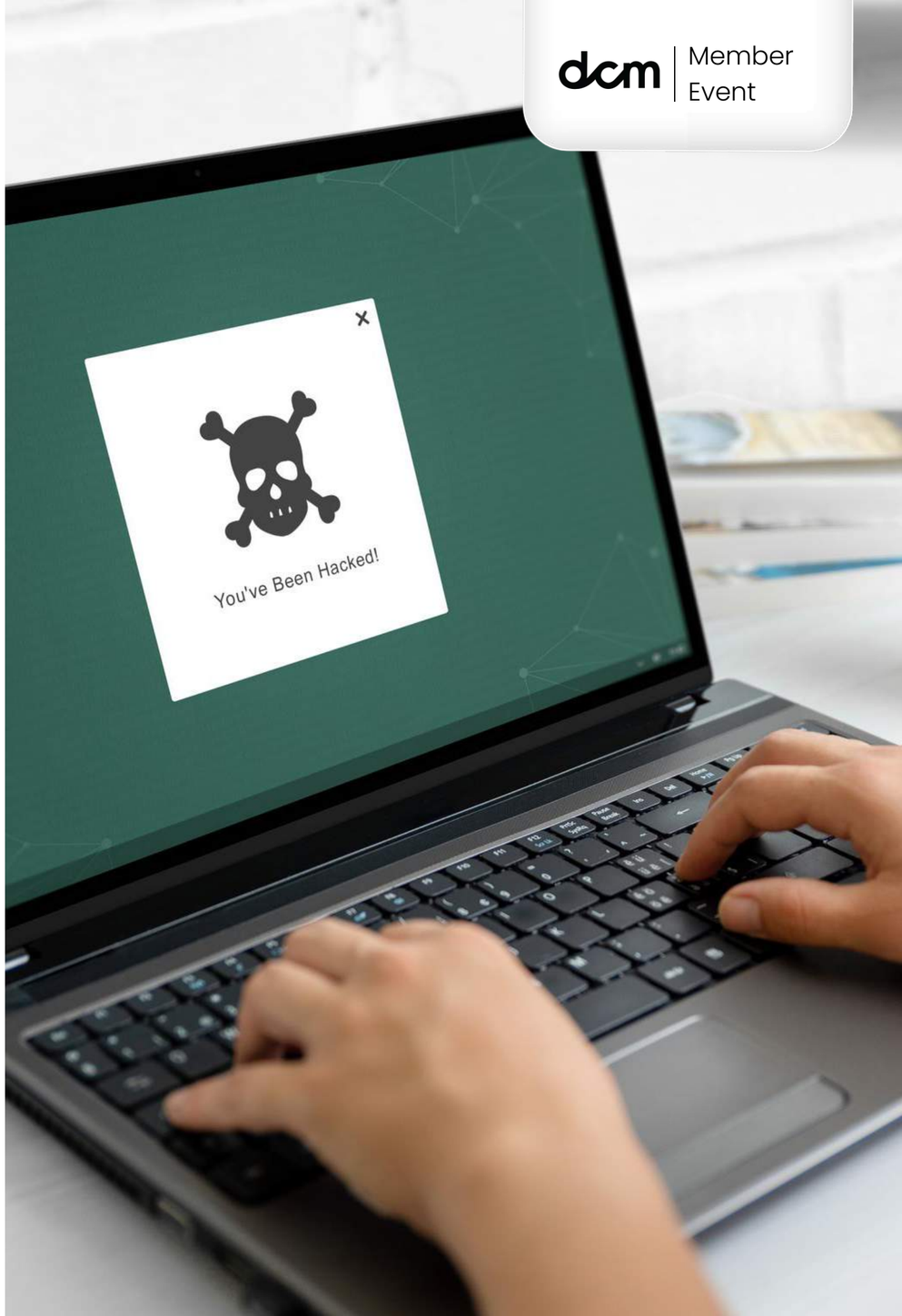
6 Legitimate interests : business as usual

7 Official authority

Special Categories / Sensitive Data

Article 9

- **Racial / Ethnic**
- **Political Opinion / Affiliation**
- **Religious or Political Beliefs**
- **Trade Union Membership**
- **Genetic / Biometric Data**
- **Health Related**
- **Sex-Life / Sexual Orientation**



Article 9 Lawful Processing

For Special Category PII

1 Explicit consent - -Direct Marketing
-Outside EU
- Sensitive Data

2 Vital interests – Death, severe harm, D.S unable to give consent

3 Made public by the DS - Facebook, social media, phone book…

4 Public interests – Gossip, media, CCTV…

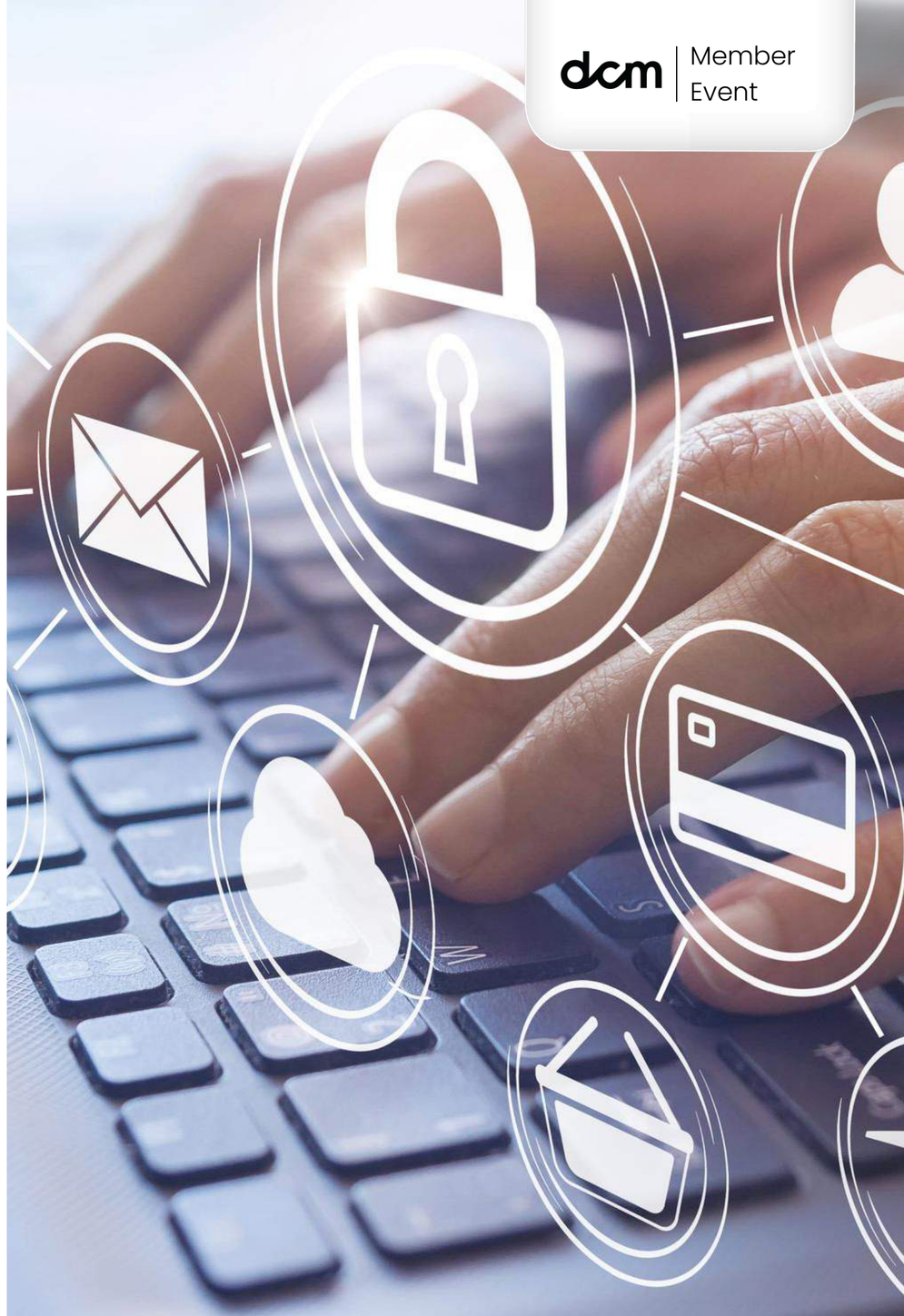
5 Public health & health of the DS – Viruses, foot & mouth, preventative, occupational medicine…

6 Employment – Social Security…

7 Member groups – not for profit, voluntarily join an organisation…

8 Legal claims – courts acting in their judicial capacity…

9 Archiving / stats / research – Census, national archive…



Test Your Knowledge

Q1 Which one of the following is the best example of special data?

a) Your name

b) Your phone number

c) Your ethnic origin

d) Your IP address

Q2 Who gives consent?

a) Data Processor

b) Data Subject

c) Supervisory Authority

d) Data Processor

RoPA – Article 30

Record of Processing

Record of processing activities (ROPA)
Your organisation has a formal, documented, comprehensive and accurate ROPA based on a data mapping exercise that is reviewed regularly.

Ways to meet your expectations:

•You record processing activities in electronic form so you can add, remove and amend information easily.

•Your organisation regularly reviews the record against processing activities, policies and procedures to ensure that it remains accurate and up to date, and you clearly assign responsibilities for doing this.

•You regularly review the processing activities and types of data you process for data minimisation purposes.
Have you considered the effectiveness of your accountability measures?

•Would staff say that you have effective processes in place to keep the record up to date, accurate and make sure that the data is minimised?

•Could staff explain their responsibilities and how they carry them out in practice?

RoPA – Article 30…

Record of Processing

ROPA requirements

Your ROPA contains all the relevant requirements set out in Article 30 of the UK GDPR.
Ways to meet our expectations:

•The ROPA includes (as a minimum):

- your organisation's name and contact details, whether it is a controller or a processor (and where applicable, the joint controller, their representative and the DPO);
- the purposes of the processing;
- a description of the categories of individuals and of personal data;
- the categories of recipients of personal data;
- details of transfers to third countries, including a record of the transfer mechanism safeguards in place;
- retention schedules; and
- a description of the technical and organisational security measures in place.

•You have an internal record of all processing activities carried out by any processors on behalf of your organisation.

RoPA – Article 30…

Record of Processing

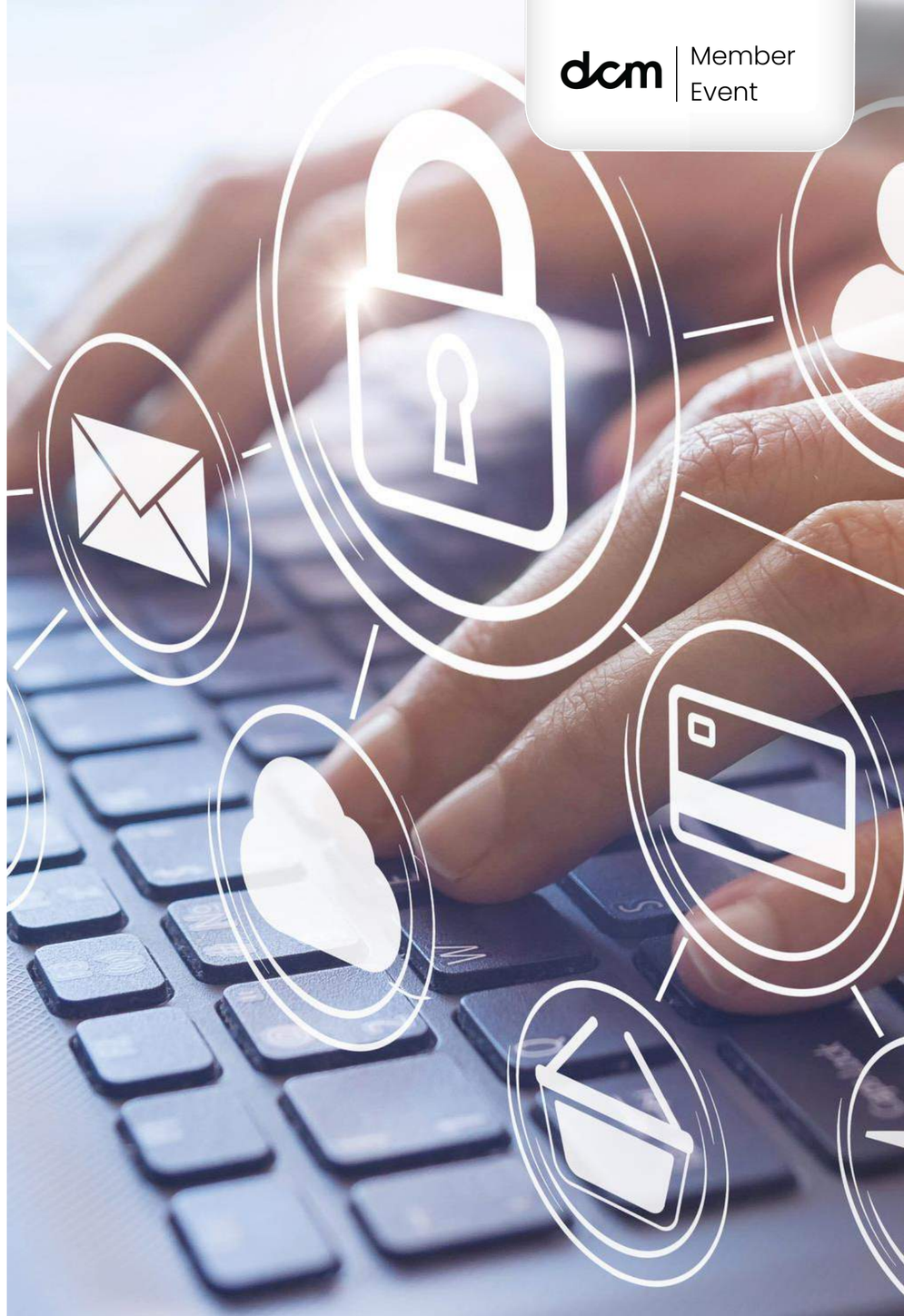
Good practice for ROPAs

Your organisation's ROPA includes links to other relevant documentation, such as contracts or records as a matter of good practice.

Ways to meet our expectations:

•The ROPA also includes, or links to, documentation covering:

- information required for privacy notices, such as the lawful basis for the processing and the source of the personal data;
- records of consent;
- controller-processor contracts;
- the location of personal data;
- DPIA reports;
- records of personal data breaches;
- information required for processing special category data or criminal conviction and offence data under the Data Protection Act 2018 (DPA 2018); and
- retention and erasure policy documents.



Powers of DPC

Homepage | Data Protection Commission

Data Controllers & Data Processors have joint liability for Data Breaches

Data Subjects have the right to sue…

- For material and non-material damage
- Separately or jointly (class actions)
- The Data Collector and/or the Data Processor
- The Supervising Authority if they do not take action when a complaint is raised
- The regulations do not give an upper limit that can be awarded by the courts

The Supervising Authority can impose administrative fines

- Intended to be **"effective, proportionate, and dissuasive"** (Article 83)
- Maximum fine – €20M or 4% previous years global turnover for tier 1 breaches (Article 83)
- Maximum fine – €10M or 2% previous years global turnover for tier 2 breaches (Article 83)
- Can be mitigated by demonstrating that an effective and robust framework is in place to protect personal data

Test your knowledge

Q1 Which of the following is a role described by the GDPR?

a) Data Processor

b) Data Privacy Official

c) Data Commissioner

d) None of the above

Q2 Which one of the following is a right?

a) The right to be protected

b) The right of access

c) The right to review

d) The right to respite

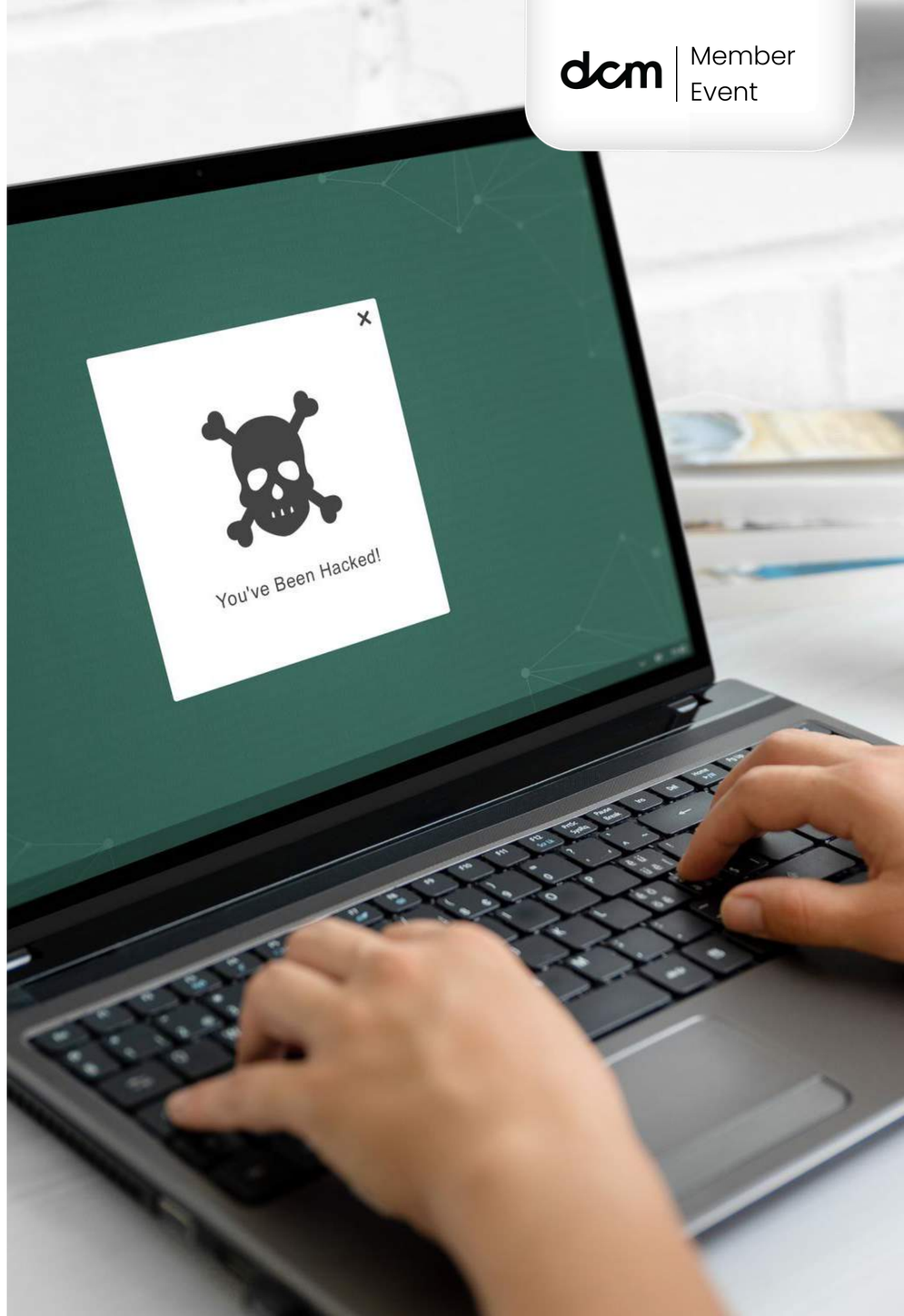
Q3 The main focus of the GDPR is…?

a) International trade

b) Trade internal to the EU

c) People and their personal information

d) People and their ability to access information



Test your knowledge

Q4

Under GDPR, organisations in breach of GDPR can be fined up to a maximum of:

a) 8% of annual global turnover
b) 2% of annual global turnover
c) 3% of annual global turnover
d) 4% of annual global turnover

Q5

Which one of the following does NOT fall under GDPR?

a) Holding a person's email address and mobile phone number in a database
b) Storing peoples' pictures in a manual filing system
c) Displaying photographs of portraits of 15th Century kings on a website
d) Holding details of your associates on a corporate mobile phone

Q6

Whilst performing a backup, a data server disk crashes and both the data and the backup are lost. The disk contained personal data.

What kind of issue is this known as?

a) Data breach
b) Security breach
c) Security incident
d) Technical breach

Test your knowledge

Q7
If someone wants to know what data an organisation holds on them they can make a…?
a) DPIA
b) Subject Access Request
c) Information Request
d) Personal Information Profile Study

Q8
Which one of the following contain the legal basis for GDPR?
a) Recitals
b) Principles
c) Articles
d) Directives

dcm | Member Event

Thank you!

Please use the QR code to take you to our feedback page ☺