



EUGDPR.ORG.UK



# GDPR Information Day

Andrew Dent  
07771915010

EUGDPR.ORG.UK 

---

## What does Data Protection Mean to You?



EUGDPR.ORG.UK



# GDPR: IT'S ABOUT YOU

"Your rights as an EU Citizen, regardless of where in the world your data is being processed"



@CliffGibson

## The History of Data Protection

- 1950 EU Convention on Human Rights introduces privacy
- 1980 OECD guidelines on trans border data flows
- 1981 EU Treaty 108 - the 8 principals for protecting personal data
- 1995 EU Data Protection Directive
- 1998 Human Rights Act (Article 8 'right to privacy')
- 1998 Data Protection Act (DPA 1998)
- 2016 EU GDPR approved, becomes law 25<sup>th</sup> May 2018



## Data Protection Principles

1. **Processed lawfully, fairly and in a transparent manner**  
(lawfulness, fairness, transparency)
2. **Collected for specified, explicit and legitimate purposes**  
(purpose limitation)
3. **Adequate, relevant and limited to what is necessary**  
(data minimisation)
4. **Accurate and, where necessary, kept up to date**  
(accuracy)
5. **Retained only for as long as necessary**  
(storage limitation)
6. **Processed in an appropriate manner to maintain security**  
(integrity and confidentiality)

**Accountability**





## YOUR RIGHTS AS A DATA SUBJECT

- **Right to be informed**
- **Access (Subject Access Request or DSAR)\***
  - \* DSAR – 1 month to comply.
  - \* Fees are abolished
- **Correction (rectification)**
- **Erasure ('right to be forgotten')**
- **Restriction of processing**
- **Data portability**
- **Right to object**
- **Right to Compensation**



# Data Controller

---

EUGDPR.ORG.UK 

## Controller

“The organisation that determines the purposes and means of processing the personal data”



---

## Data Processor



### Processor

“A natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.”



EUGDPR.ORG.UK



---

**Joint and Severable Liability**

**€20 million**

**Or**

**4% of worldwide turnover**

EUGDPR.ORG.UK



## Protecting Personal Data

What is the largest cause of data breaches?





Security

## Human error remains the weakest link in data protection

A number of recent email gaffes have drawn the attention of the ICO



Jason Murdock

@Jason\_A\_Murdock

04 September 2015



0 Comments



Email blunders indicate that human error is a security risk to business

Recent blunders have shown that human error remains one of the most prevalent security and data protection risks for businesses of all sizes, regardless of how much money they invest in a security infrastructure, email encryption and secure data storage.

This week a high-profile example hit the headlines when an **email error at the 56 Dean Street sexual health clinic** in London exposed the names and email addresses of nearly 800 patients signed up to an HIV treatment newsletter.

HOME > CYBERSECURITY > DEEPER DIVE: HUMAN ERROR IS TO BLAME FOR MOST BREACHES

## Deeper Dive: Human Error Is to Blame for Most Breaches



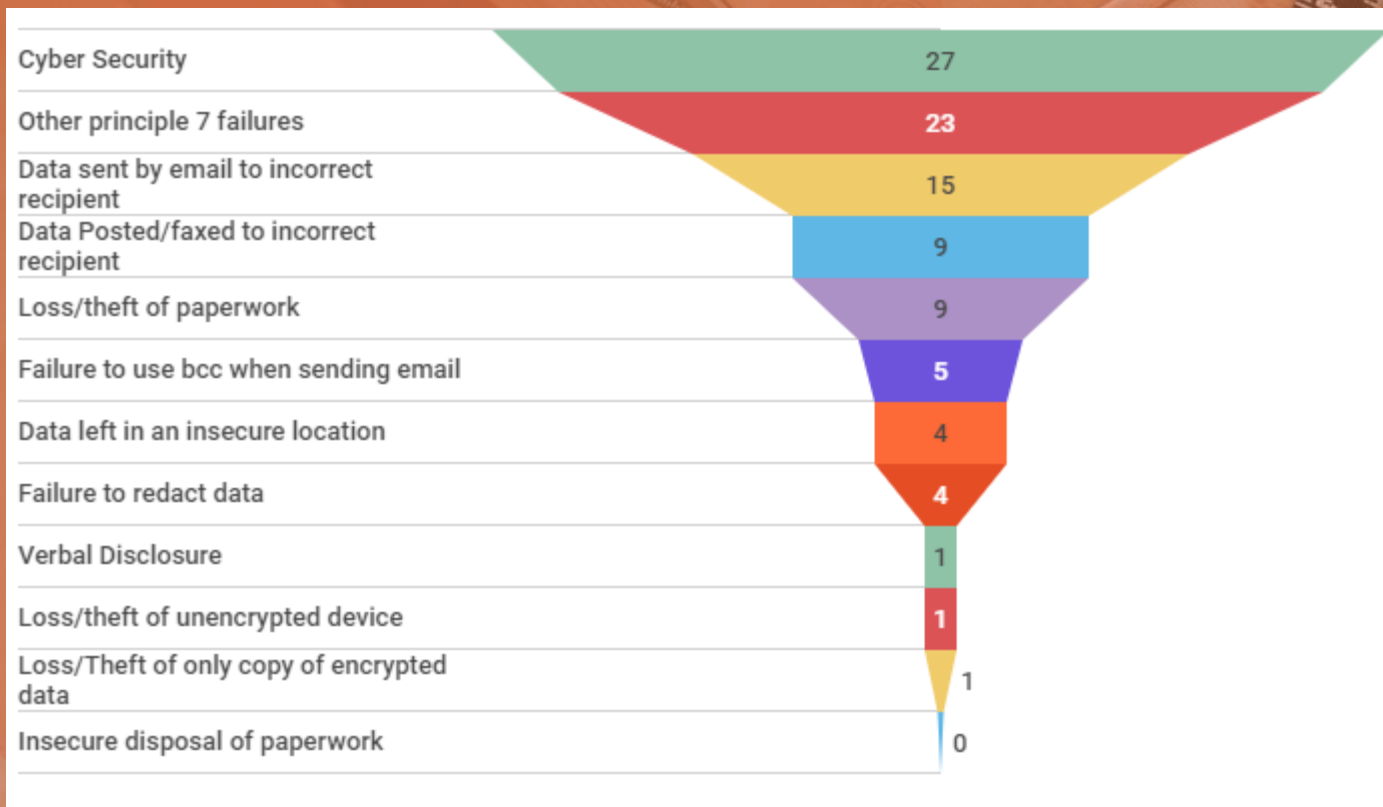
By Will R. Daugherty on April 25, 2016

POSTED IN CYBERSECURITY, INCIDENT RESPONSE, ONLINE PRIVACY

Each year, as companies implement the latest security technologies, attackers develop and launch new tactics, techniques, and procedures to circumvent those technologies. While investment in security defense and detection technologies is an essential component to building an effective defense-in-depth strategy, the reality is that most breaches can be traced back to human error. In our [2016 Data Security Incident Response Report](#), we looked back at the more than 300 incidents that we handled in 2015 to identify the top causes. Identifying and understanding the constantly evolving causes of security incidents, which vary among industries, allows us not only to better advise organizations on how to proactively become what we call "compromise ready," but also enables us to use these "lessons learned" to help organizations effectively respond to incidents when they do occur.

Last year, we identified human error as the leading cause of incidents (37 percent), followed by phishing/malware (25 percent), external theft of a device (22 percent), and employee theft

EUGDPR.ORG.UK





EUGDPR.ORG.UK 

How long do I have to report a breach?

**72 hours**



EUGDPR.ORG.UK



CNN Money

**HACKER?**



EUGDPR.ORG.UK







## What can we do to protect our data?

- Use really long passwords
  - Use different passwords for
    - Work
    - Social Media
    - Bank Accounts
  - Use only approved data sharing systems
  - Use only approved applications.
  - Only used encrypted USBs
  - Shred sensitive documents
- 
- Keep personal and work data separate



EUGDPR.ORG.UK



DAILY  
DOT COM  
DOL COW

FOX10tv.com

9:42 57°

## How does GDPR effect my Company?

This is a change in culture – there is no technological magic bullet.

Data Protection Officer

- Independent, not necessarily full time and can be outsourced.

Data Compliance team;

- Data Processors – (administrators)
- IT
- Department Heads or nominees

Regular agenda item on board meetings.

Review your third party contracts and controls (customers and suppliers).

Be seen to be making progress towards “Data Protection By Design and Default”.



# Data Protection Officer

The difference between the regulation and member state law

◆ Table of contents ◆

Info / Regulation / Dossier

## Article 37 EU GDPR

### "Designation of the data protection officer"

=> Recital: [97](#)

=> administrative fine: [Art. 83 \(4\) lit a](#)

=> Dossier: [Data Protection Officer](#)

**1. The controller and the processor shall designate a data protection officer in any case where:**

(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

(b) the **core activities** of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

=> Recital: [24](#)

=> Dossier: [Extensive Processing](#)

(c) the **core activities** of the controller or the processor consist of processing on a large scale of special categories of data pursuant to [Article 9](#) and personal data relating to criminal convictions and offences referred to in [Article 10](#).

=> Recital: [91](#)

=> Dossier: [Extensive Processing](#)

**2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.**

=> Dossier: [Establishment](#), [Group Of Undertakings](#)

**3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.**

=> Dossier: [Group Of Undertakings](#)

**4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.**

=> Dossier: [Opening Clause](#)

**5. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in [Article 39](#).**

=> Recital: [97](#)

**6. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.**

**7. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.**

=> Article: [39](#)

=> Dossier: [Reporting to supervisory authority](#), [Obligation](#)

## Data Protection Officer

The difference between the regulation and member state law

*Data Protection Bill [HL]*

41

*Part 3 – Law enforcement processing*

*Chapter 4 – Controller and processor*

---

### *Data protection officers*

#### **69 Designation of a data protection officer**

- (1) The controller must designate a data protection officer, unless the controller is a court, or other judicial authority, acting in its judicial capacity.
- (2) When designating a data protection officer, the controller must have regard to the professional qualities of the proposed officer, in particular—
  - (a) the proposed officer’s expert knowledge of data protection law and practice, and
  - (b) the ability of the proposed officer to perform the tasks mentioned in section 71.
- (3) The same person may be designated as a data protection officer by several controllers, taking account of their organisational structure and size.
- (4) The controller must publish the contact details of the data protection officer and communicate these to the Commissioner.

#### **70 Position of data protection officer**

15



# The role of the Data Protection Officer

---

EUGDPR.ORG.UK 

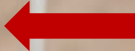
- **Independent – cannot be a processor**
- **Single point of contact for Supervisory Authority and Data Subjects**
- **Assist with Subject Access Requests**
- **Advise on reportable breaches**
- **Keep you up to date on GDPR changes**
- **Protected by the legislation (whistle blower)**





# Project phases and timeline

We are here



10 weeks



25<sup>th</sup> May



1) Raise awareness and gather information

2) Plan and Prioritise

3) Implement changes

4) Embed change, train and re-train



EUGDPR.ORG.UK



## 1) Raise awareness and gather information

- Inform decision makers on the impact of the GDPR.
- Gather information on current practices
- Conduct information audit
- Review systems and procedures
  - Line of Business Applications
  - Office 365
  - General Files/folders

EUGDPR.ORG.UK



1) Raise awareness and gather information

2) Plan and Prioritise

- Build Privacy and compliance programme and structure
- Identify and map information flows
- Conduct Data Protection Impact Assessments (DPIA) for riskier activities
- Identify and prioritise



EUGDPR.ORG.UK



1) Raise awareness and gather information

2) Plan and Prioritise

3) Implement changes

- Review and strengthen technical and security measures
- Internal procedures for breach notification, access requests etc.
- Review and update privacy policies and notices
- Review and audit commissioning supply chain and update contracts
- Implement privacy by design and by default
- Implement changes to key systems
  - Line of Business Applications
  - Azure Threat Management
  - Microsoft Cloud App Security
  - Azure Information Protection

- 1) Raise awareness and gather information
- 2) Plan and Prioritise
- 3) Implement changes
- 4) Embed change, train and re-train




**GDPR Executive Guidelines**



**GDPR for Data Handlers**



- 1) Raise awareness and gather information
- 2) Plan and Prioritise
- 3) Implement changes
- 4) Embed change, train and re-train



Send to a complete stranger

Most security breaches happen because of distractions or mistakes.

Always check email addresses, contents and attachments before you click 'Send'.

**ico.**

Think. Check. Share.

Personal information?

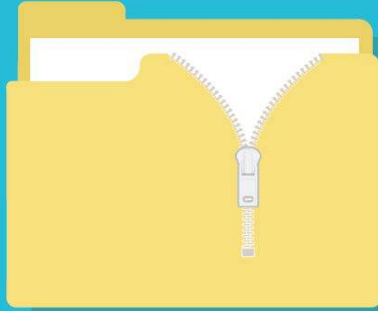
**Think.**

**Check.**

**Share.**

**ico.**

Are you securely zipped?



When sending information out of the office – make sure it's securely encrypted.

**ico.**

Think. Check. Share.

# Summary

---

EUGDPR.ORG.UK 

- GDPR is a change in organisational culture
- There is no technical magic bullet
- Fines have the potential to be severe

- Individuals can be personally fined
- Departments need to work to embed a culture of:

“Data Protection by Design and by Default”



EUGDPR.ORG.UK



# How can we help you?

## Compliance Pack

- Registration with ICO
- Policies, Procedures and Document Control
- Privacy Notices
- Subject Access Request Procedures
- Training on and assistance in Data Flow Mapping
- Training on and advice on Data Protection Impact Assessments
- Data Protection E-Learning for Execs and Handlers
- Advice on sub-contract data processing

EUGDPR.ORG.UK



# How can we help you?

## Data Protection Officer Service

- Formal registration as Data Protection Officer for your organisation
- Telephone and remote advice on all things Data Protection
- Point of contact for Data Subject and Information Commissioner
- Annual Compliance Audit
- Subject Access Request and Breach Management charged on time and materials basis.



EUGDPR.ORG.UK



For more information  
Please contact  
[sales@eugdpr.org.uk](mailto:sales@eugdpr.org.uk)