

DATA PROTECTION & THE GDPR FOR SMEs

Advocate Davida Blackmore, Callington Chambers
Adrian Hayes, Office of the Information Commissioner
Alexia McClure, Jersey Business
Paul Byrne, LeanJsy

CALLINGTON
CHAMBERS



Topics


- How we got here
- Which law applies to you?
- What you need to do
- Key topics:
 - Marketing (inc. consent and legitimate interests)
 - Contracts between controllers & processors
 - Role as processor
 - The employment perspective
 - Privacy policies
 - Enforcement and breaches
- In practice
- Resources

Data protection law in Jersey

- Legislation in place since 1987
- Data Protection (Jersey) Law 2005

Change





Welcome to Amazon.com Books!

One million titles, consistently low prices.

(If you explore just one thing, make it our personal notification service. We think it's very cool!)

SPOTLIGHT! -- AUGUST 16TH

These are the books we love, offered at Amazon.com low prices. The spotlight moves EVERY day so please come often.

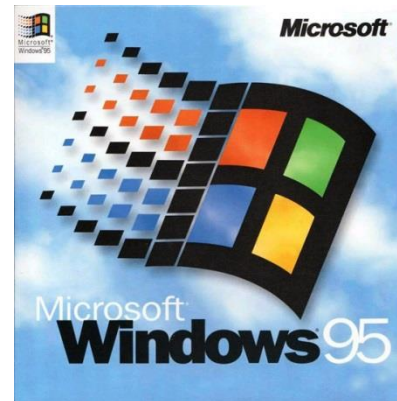
ONE MILLION TITLES

Search Amazon.com's [million title catalog](#) by author, subject, title, keyword, and more... Or take a look at the [books we recommend](#) in over 20 categories... Check out our [customer reviews](#) and the [award winners](#) from the Hugo and Nebula to the Pulitzer and Nobel... and [bestsellers](#) are 30% off the publishers list...



Now Open: Yahoo! Start Shop! [Remove the Snapple Gap to PLOP!](#) [Web Launch](#)

- Arts: Film, Music, Photography, Architecture, ...
- Business and Economy (Xref): Economy, American, Canadian, Euro, ...
- Computers and Internet (Xref): Internet, WWW, Software, Multimedia, ...
- Education: Universities, K-12, Courses, ...
- Entertainment (Xref): TV, Movies, Music, Theater, ...
- Government: Politics (Xref), Agencies, Law, Military, ...
- Health: Medicine, Drugs, Diseases, Fitness, ...
- News (Xref): World (Xref), Daily, Current Events, ...
- Recreation: Sports (Xref), Games, Travel, Amos, ...
- Reference: Literature, Dictionaries, Phrase Books, ...
- Regional: Countries, Regions, U.S. States, ...
- Science: CS, Biology, Astronomy, Experiment, ...
- Social Science: Anthropology, Sociology, Economics, ...
- Society and Culture: People, Transportation, Religion, ...



General data protection regulation (“GDPR”)

4.5.2016

EN

Official Journal of the European Union

L 119/1

I

(Legislative acts)

REGULATIONS

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 27 April 2016

on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

(Text with EEA relevance)

Key changes

- Enhanced data subject rights 😊
- Enhanced consent
- Privacy by design (building it in)
- Controllers and processors
- Co-operation with regulator, notification of data protection breaches and administrative penalties
- Data Protection Officer (“DPO”)

GDPR and Jersey?

GDPR applies to:

- Activities of an establishment in the EU
 - wherever the processing actually takes place
- Processing of EU data subjects by an entity:
 - Offering goods or services within the EU; or
 - Monitoring behaviour within the EU



Jersey law

The States of Jersey also introduced two new laws which came into force on 25 May 2018



DATA PROTECTION (JERSEY) LAW 2018

**DATA PROTECTION AUTHORITY
(JERSEY) LAW 2018**

Why did we follow the EU?

4.5.2016

EN

Official Journal of the European Union

L 119/61

Article 45

Transfers on the basis of an adequacy decision

1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

Which law applies to you?

- If you are not targeting/monitoring EU individuals, will likely only need to be concerned with Jersey law.
- If overlapping islands, may need to consider Guernsey law.

Preparation

- What?
- Where?
- Why?
- Who?



Basis for processing

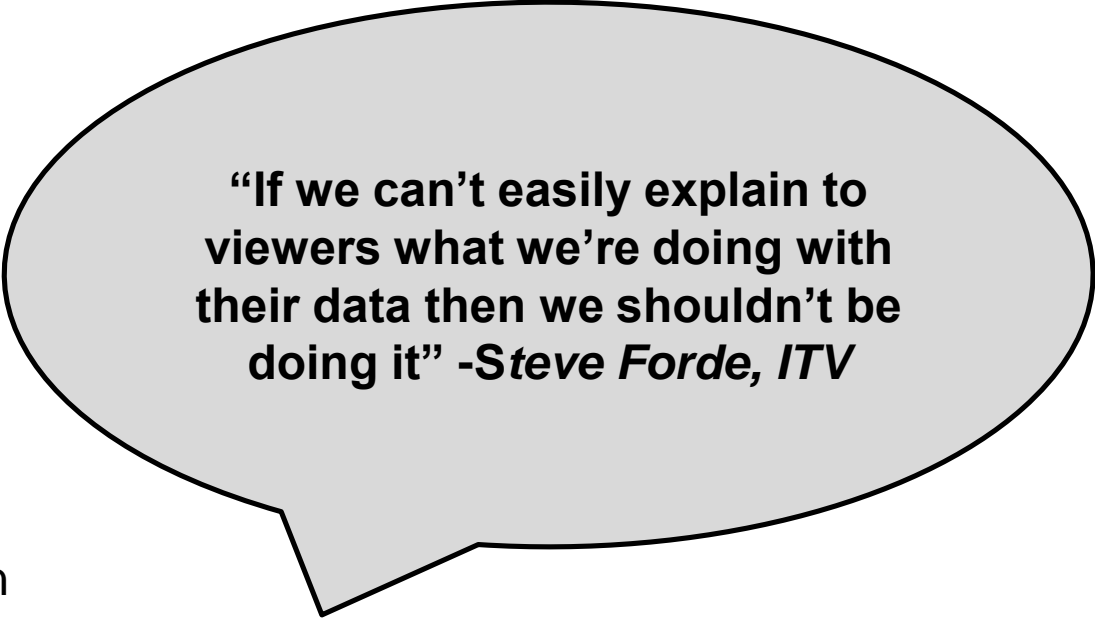
- Can only process data if one of the following applies:
 - **Consent:** the individual has explicitly allowed you to process their personal data for a specific purpose.
 - **Contract:** you need to process the data for the performance of a contract;
 - **Vital interests:** you need to protect someone's life.
 - **Public functions:** it's in the public interest or for your official functions, and you've got a legal basis
 - **Legitimate interests:** it's necessary for your legitimate interests or the legitimate interests of a third party.

Principles

- There are 6 principles of good data handling:
 - lawfully, fairly and transparently;
 - for specified, explicit and legitimate purposes and once collected, not used in a different way;
 - adequate, relevant and limited to what you need;
 - accurate and up-to-date;
 - to keep it for no longer than is necessary;
 - secure using appropriate technical or organisation measures.

Marketing

1. Freely given
2. Specific
3. Informed
4. Clear affirmative action



“If we can’t easily explain to viewers what we’re doing with their data then we shouldn’t be doing it” -*Steve Forde, ITV*

Consent

1. Is consent the most lawful basis for processing?
2. Is the request for consent in a obvious place and separate from main terms & conditions?
3. No pre-ticked tick-boxes!
4. Is the language clear and easy to understand?
5. Why do you want it?
6. What are you going to do with it?
7. When you've got it, how can you show that you obtained the information lawfully?
8. I don't consent anymore...
9. I'm a minor.

What should my consent look like?

- Name of organisation
- Name of any third parties relying on the consent
- Why you want the data
- What you're going to do with it
- Let me give consent for different things
- Specifically state that can withdraw at any time
- Contact details!

Managing consent

- Review
- Refresh
- Tools

Legitimate interests

- Is it the most appropriate basis?
- Legitimate interests assessment
 - Identify the legitimate interest
 - Show that processing is necessary to achieve it
 - Balance it against the individual's rights and freedoms.
- What is a legitimate interest?
- Need to put details in your privacy notice.
- Right to object is absolute.

Contracts with third parties

- If a controller uses a processor then you need a contract:
 - What and how long
 - Why
 - Types of data
 - Types of data subject
 - Obligations and rights of controller
- Must be in writing.



Contracts contd.

- Agreements must contain following:
 - Will only act on written instructions of controller
 - Will ensure that people working for you keep everything confidential
 - Will keep everything safe
 - Will only engage sub-processor with prior consent of controller and a written contract
 - Will assist controller with any subject access requests/when they need assistance generally
 - Will delete/return data to controller when requested at end of contract
 - Will make available all information to show compliance (including submitting to audits/inspections)

[Art.19(4) of the DPJL]

If you're a Processor

- Register with the Authority (and pay £)
- Can't use sub-processor without controller saying it's ok
- Need to have make sure that keep things safe
- Keep records of processing activities. Doesn't apply if fewer than 250 employees UNLESS the processing
 - is likely to result in a risk to the rights and freedoms of data subjects;
 - is not occasional; OR
 - includes special category data (health/race/biometrics etc)
- Confidentiality
- Tell controller without undue delay after becoming aware of a breach
- Appoint a data protection officer if required
- Don't send data out of Jersey unless it's safe/appropriate;
- Co-operate the Authority

[Part 4 of the JDPL
Art.22]

Employment

- If you're an employer:
 - Look at your privacy policy
 - Employee handbook
 - Contracts of employment

Stuart Franklin

Date **21 July 2017**

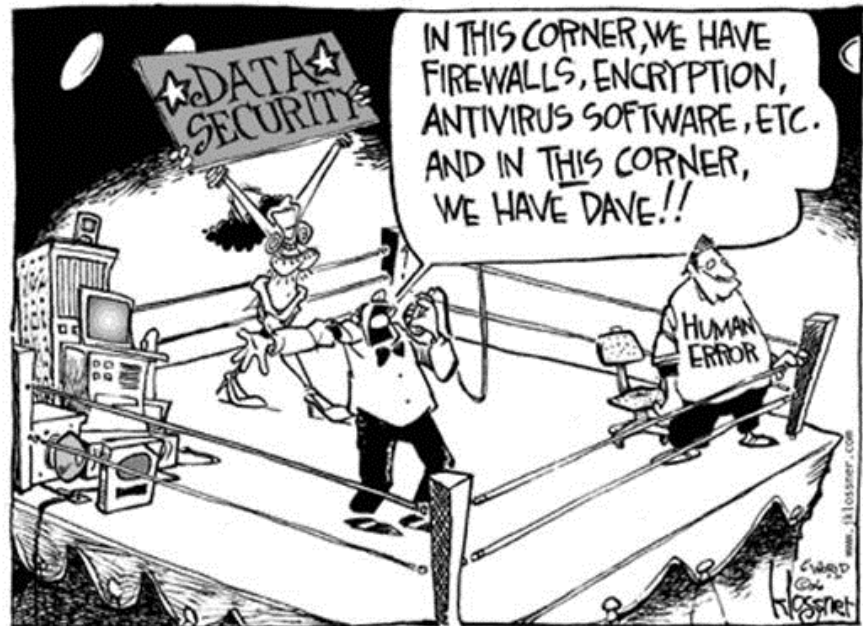
Type **Prosecutions**

Stuart Franklin has been prosecuted at Birmingham Magistrates' Court for the offence of unlawfully disclosing personal data. The defendant, who at the time worked at a Walsall based domestic services company, emailed the CVs of 26 job applicants to a third party company without his employer, the data controller's, consent.

Mr Franklin pleaded guilty to the offence under section 55 of the Data Protection Act, and was fined £573, ordered to pay £364 prosecution costs and a £57 victim surcharge.

Employment contd.

- Training (again)
- Employer obligations
 - Special category data
 - Security
 - Access
- DSARs



Privacy Policies

- What?
- Why?
 - Must make certain information available to data subjects (fair and transparent)
- How?
 - Just one document?
 - Set out approach to DP
 - Transparent (what, why, where and who)
 - Complaints/contact details
 - CLEAR LANGUAGE

Breaches

Enforcement



OFFICE OF THE
INFORMATION
COMMISSIONER

www.oicjersey.org

Penalties

- Two-tiers in the GDPR
 - 2% of global annual turnover (for undertakings) or €10m
 - 4% of global annual turnover for the preceding year (for undertakings) or €20m.
- Jersey (and Guernsey) Law:
 - Tier 1 = £5,000,000
 - Tier 2 = £10,000,000
 - BUT An administrative fine must not exceed £300,000 or 10% of the person's total global annual turnover or total gross income in the preceding financial year, whichever is the higher.

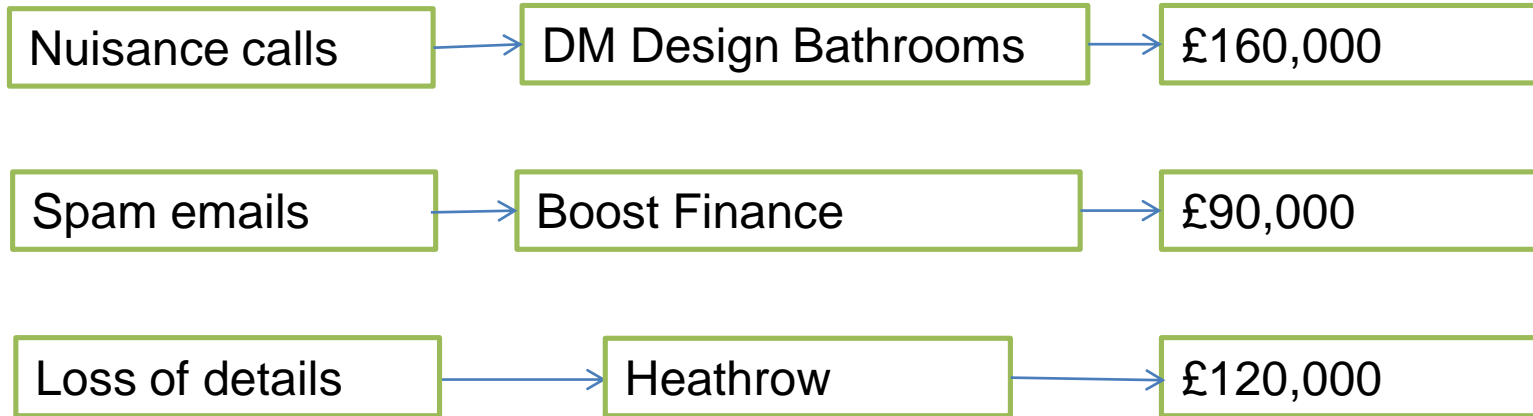
Penalties

- Things the Authority thinks about:
 - How bad the breach was, how many individuals affected and the level of damage suffered by them;
 - Was it on purpose or by mistake;
 - Steps taken to deal with the breach;
 - The seniority of the person who committed the breach;
 - Previous breaches/issues;
 - How well the organisation cooperates with the Authority;
 - Types of data affected;
 - How Authority found out about it;
 - Any thing else +ve / -ve

Stop!



Penalties continued...



Heathrow
Our company



Boost **FINANCE**


DMDESIGN
KITCHENS, BEDROOMS & BATHROOMS

In practice



LEAN-JSY
EFFICIENT & EFFECTIVE

Resources

 OFFICE OF THE INFORMATION COMMISSIONER

Enter your search term here...

[About Us](#) | [General Information](#) | [Data Protection \(2005 Law\)](#) | [Data Protection \(New Law\)](#) | [Freedom of Information](#) | [How to Complain](#) | [Online Registration](#)

Home > Data Protection (New Law)

Data Protection (New Law)

The Data Protection (Jersey) Law 2018 and the Data Protection Authority (Jersey) Law 2018 came into effect on 25 May 2018. This page includes legislation, resources, infographics and useful links to other websites to assist organisations in working towards compliance. More information

Please click on the sections below to view more:

GUIDANCE

- Guidance for States Members
- Guidance on Transitional Provisions
- The Data Protection Principles
- Key Definitions
- Guidance for SMEs
- Guidance on Breach Reporting
- Duties of Data Controllers
- Guidance on Registration of Controllers and Processors
- Guidance on Sanctions
- Guidance on Criminal Offences and Civil Remedies

- GDPR Briefing Paper
- GDPR Next Steps Flyer
- Infographic: 6 GDPR Myths
- Infographic: 6 Essential Steps to GDPR
- Infographic: 6 Initial Steps
- Infographic: Becoming Compliant – 6 Steps
- Infographic: 6 Things to Know About Cookies
- Infographic: GDPR for SMEs
- Infographic: GDPR for Start-ups
- Infographic: What GDPR Means for HR
- Infographic: 6 Things About GDPR and

<https://www.oicjersey.org/wp-content/uploads/2018/05/2018.05.22-Guidance-for-SMEs.pdf>

 OFFICE OF THE INFORMATION COMMISSIONER

 OFFICE OF THE INFORMATION COMMISSIONER

**GUIDANCE:
GUIDE FOR SMEs**

Thank you & discussion

Advocate Davida Blackmore, Partner
davida.blackmore@callingtonchambers.com
01534 510250

CALLINGTON
CHAMBERS

Adrian Hayes, Manager - Enforcement
a.hayes@oicjersey.org
01534 716530



Alexia McClure, Head of Operations
Alexia.McClure@jerseybusiness.je
01534 610300



Paul Byrne, Director
p.byrne@lean-jsy.co.uk
01534 752982

