Data Protection in practice:

2018 - The new regime.

Paul Vane

Acting Information Commissioner

OFFICE OF THE INFORMATION COMMISSIONER

A Surveillance Society?...

WALKING THROUGH TOWN

TAKING OUT A LOAN

INTERNET BROWSING

AMAZON PURCHASE

DASH CAMS

SENDING A TEXT MESSAGE

CCTV

OPENING A STORE CARD

VISITING YOUR DOCTOR

USING A CASHPOINT

VISITING YOUR BANK

ENTERING A COMPETITION

MAKING A TELEPHONE CALL

USING A SWIPE ENTRY CARD

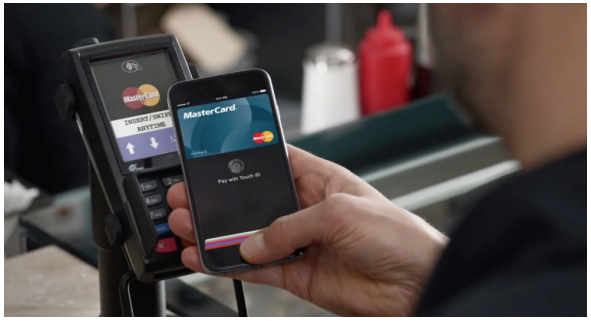
DRONES

OFFICE OF THE INFORMATION COMMISSIONER

WHERE WE WERE IN 1995

OFFICE OF THE INFORMATION COMMISSIONER

WHERE WE ARE IN 2018



OFFICE OF THE INFORMATION COMMISSIONER

The Data Protection(Jersey)Law 201-

KEY DEFINITIONS:

Data

Means information which is:

Automatically processed
or
Recorded with the intention of being automatically processed
or
Recorded as part of a relevant filing system

OFFICE OF THE INFORMATION COMMISSIONER

KEY DEFINITIONS:

Personal Data

Information which relates to a natural, living individual who can be identified, directly or indirectly by reference to identifiers such as:

- Name
- Identification number
- Location data
- Online identifier
- One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the person.

Examples:

- Name, address, data of birth
- IP addresses
- Physical description
- Metadata
- Cookie identifiers
- Biometric data
- Genetic data, DNA profile
- Anything that could identify a living person.

OFFICE OF THE INFORMATION COMMISSIONER

KEY DEFINITIONS:

Special Category Data

- **Racial or ethnic origin**
- **Political opinions**
- **Religious or philosophical beliefs**
- **Trade union membership**
- **Genetic and biometric data**
- **Physical or mental health**
- **Sexual life**
- **Criminal records and criminal activity (including allegations of)**

KEY DEFINITIONS:

Processing

Any operation or set of operations performed on personal data

Includes:

- Collecting
- Recording
- Organising
- Structuring
- Storing
- Adapting
- Altering
- Retrieving
- Consulting
- Using
- Disclosing
- Transmitting
- Disseminating
- Aligning
- Combining
- Erasing/Destroying

OFFICE OF THE INFORMATION COMMISSIONER

KEY DEFINITIONS:

Data Controller

A person who (either alone or in common with other persons) determines the purposes for which and the manner in which personal data are, or are to be, processed.

GDPR CHANGES FROM MAY 2018…

More stringent requirements on data controllers, particularly in respect of joint data controller arrangements.

OFFICE OF THE INFORMATION COMMISSIONER

KEY DEFINITIONS:

Data Processor

a person (other than an employee) who processes the data on behalf of the data controller

Examples:

- Cloud services provider
- External IT/HR organisation
- Customer Service Centre
- Accountancy firm
- Data storage facility

GDPR CHANGES FROM MAY 2018…

Specific requirements for processors with certain obligations placed upon them. Will impact on cloud providers and outsourced functions that previously fell outside the scope of the Law.

OFFICE OF THE INFORMATION COMMISSIONER

KEY DEFINITIONS:

Data Subject

The person to whom the information relates
i.e. YOU!

OFFICE OF THE INFORMATION COMMISSIONER

The Principles

The new Data Protection Principles under GDPR set enforceable standards for the collection and use of personal data.

1. Fair, lawful and transparent processing
2. Use of data for limited purposes
3. Adequate, relevant and minimal data collection
4. Accurate and up to date information
5. Limitations on retention of data
6. Appropriate security, integrity and confidentiality of data

OFFICE OF THE INFORMATION COMMISSIONER

1 Fair, lawful and transparent processing

Fair:

- Obtained from a person who is authorised by law to supply it;
- Obtained from a person who is required to supply it under any law or international agreement that imposes an international obligation on Jersey.

Lawful:

- Must meet at least one of the conditions for processing in listed in Schedule 2 (for personal data), or Part 2 or Schedule 2 (for special category data)

Transparent:

- Must ensure data subjects can exercise their rights under the Law;
- Must act on the data subject's request wherever possible (e.*g. not possible because data subject not identified, or processing is exempt under Law*)
- Must provide certain information to the data subject.

Lawful Processing: First Principle (Cont'd):

Conditions for the processing of any Personal Data:

Schedule 2 – Part 1:

At least one of the following conditions must be satisfied before processing can commence:

- **Consent**
- **Performance of a contract to which the data subject is a party or has requested**
- **Vital interests** (of the data subject or any other natural person)
- **Public functions and administration of justice**
- **Legitimate interests** (not applicable to Public Authorities)

Lawful Processing: First Principle (Cont'd):

Conditions for the processing of Personal Data AND Special Category Data:

Schedule 2 – Part 2:

At least one of the following conditions must be satisfied before processing can commence:

- **Explicit consent**
- **Other legal obligations**
- **Employment, social security/services/care**
- **Vital interests** (of the data subject or any other natural person)
- **Non Profit Organisations** (with consent of data subject for 3rd party disclosures)
- **Information already made public** (by the data subject themselves)
- **Legal proceedings**
- **Public functions**
- **Public interest**
- **Medical purposes**
- **Public health**
- **Archiving and research**
- **Avoidance of discrimination**
- **Prevention/detection of unlawful acts**
- **Protection against, and publication about malpractice and mismanagement**
- **Provision of confidential counselling**
- **Insurance and pensions: determination and processing already underway**
- **Exercise of functions by a Police Officer**

Transparent Processing: First Principle (Cont'd):

Information to be provided to the data subject:

- Identity of the data controller
- Contact details of the Data Protection Officer (where applicable)
- Purpose for which the data are to be used
- Legal basis for the processing
- Details of to whom the data may be disclosed
- Details of any third country to which the data may be transferred
- How long the information will be retained for
- Information about how data subjects can exercise their rights under the Law
- How a data subject can withdraw consent
- Whether or not any of the data is to be subject to automated decision-making
- Details as to how to complain to the Information Commissioner
- Details of any legal/contractual obligation on the data subject to provide the data
- Details of the source of the data (if not obtained from the data subject)
- Any further information relating to the specific processing of their data to enable the processing to be fair.

>>TRANSPARENT PRIVACY POLICIES!!<<

OFFICE OF THE INFORMATION COMMISSIONER

The First Principle (Cont'd): **Consent**

Key points:

- **CONSENT** - *"Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, whether orally or in writing, signifies agreement to the processing of that data."* **(OPT-IN)**
- Mere silence or inactivity (e.g. Non-response) will not constitute a valid consent.
- Data subject must be aware of the identity of the data controller.
- Data controller must allow for separate consents for different processing activities.
- Data controllers bear the burden of proof that consent was actually given. Data controllers will need to review their consent forms.
- Specific rules for **CHILDREN's CONSENT** – Parental consent required for children under 13 in relation to internet services, e.g. Gaming websites designed for children, social media etc.

The First Principle (Cont'd): **Consent**

CONTROLLER MUST BE ABLE TO DEMONSTRATE:

- That consent was requested in a clear and easily accessible manner;
- Where the request was in writing, that the request was clearly distinguishable from other matters;
- Where the request was made electronically, that it did not unnecessarily disrupt the use of the service for the data subject;
- Where consent was required for the performance of a contract, that it was either necessary for the performance of that contract, or can be refused without prejudicing the performance of the contract;

The First Principle (Cont'd): **Consent**

CONTROLLER MUST BE ABLE TO DEMONSTRATE:

- That the data subject has been advised as to how to withdraw consent (**OPT-OUT**);
- That they have taken appropriate measures to verify that the person giving consent is who they say they are.
- That if consent is required for a child under 13, valid consent can only be given by a person with parental responsibility for them;
- That separate consent is required for each purpose.

2 What do you use personal information for?

- Personal data shall be collected for specified, explicit and legitimate purposes and once collected, not processed in a manner incompatible with those purposes.

Examples to which this Principle applies:

- **Marketing**
- **Database trading**

OFFICE OF THE INFORMATION COMMISSIONER

3 How much information do you collect from your customers?

- Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose or purposes for which they are processed.

Examples to which this Principle applies:

- **Customer surveys**
- **Job application forms**
- **Data collection forms (job applications)**
- **Marketing**

***Data minimisation**: Data controllers can only collect as much information as they need for the purpose, nothing more.*

OFFICE OF THE INFORMATION COMMISSIONER

4 How accurate is the information you hold?

- Personal data shall be accurate and, where necessary, kept up to date, with reasonable steps being taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Examples to which this Principle applies:

- **Client file reviews**
- **Personal files**
- **Marketing**

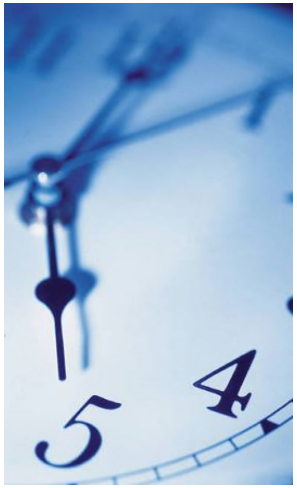
OFFICE OF THE INFORMATION COMMISSIONER

5 How long do you keep information for?

- Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed.

Examples to which this Principle applies:

- **Retention periods**
- **Regular data audit**
- **Records management processes**
- **Archive/weed policies**



OFFICE OF THE INFORMATION COMMISSIONER

6 Integrity and Confidentiality

- Personal data must be processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures.

Examples to which this Principle applies:

- **Robust security policies**
- **Applies also to data processors**
- **Article 21 applies: Security of personal data**

OFFICE OF THE INFORMATION COMMISSIONER

Cross-border transfers of personal data

A controller or processor must not transfer personal data to a third country or international organisation unless that country or organisation has adequate protections in place for the rights and freedoms of data subjects.

Accepted levels of protection:

- **Adequacy status from the EC**
- **Exceptional circumstances approved by the Commissioner (Urgency procedure)**
- **One of the exceptions applies:**
  - Court order
  - Explicit consent of the data subject
  - Performance of a contract between the controller and the data subject
  - Transfer by, or on behalf of the JFSC
  - Vital interests of the data subject
  - Public register
  - Public authorities

OFFICE OF THE INFORMATION COMMISSIONER

Data Protection Officers

A controller and processor must appoint a DPO in any case where:

- Processing carried out by a Public Authority
- Processing requires systematic and regular monitoring of data subjects on a large scale
- Core activities of the business require the processing of special category data on a large scale
- Required by law

What or who is a DPO?

- Practical experience in field of data protection
- Acts independently
- Reports to highest level of management
- Point of contact for the controller

OFFICE OF THE INFORMATION COMMISSIONER

Enforcement

Regulatory actions under the Data Protection (Jersey) Law 201-

- Enforcement notices
- Information Notices
- Fining powers (up to £10million for serious breaches)
- Informal resolutions (undertakings)

OFFICE OF THE INFORMATION COMMISSIONER

Enforcement

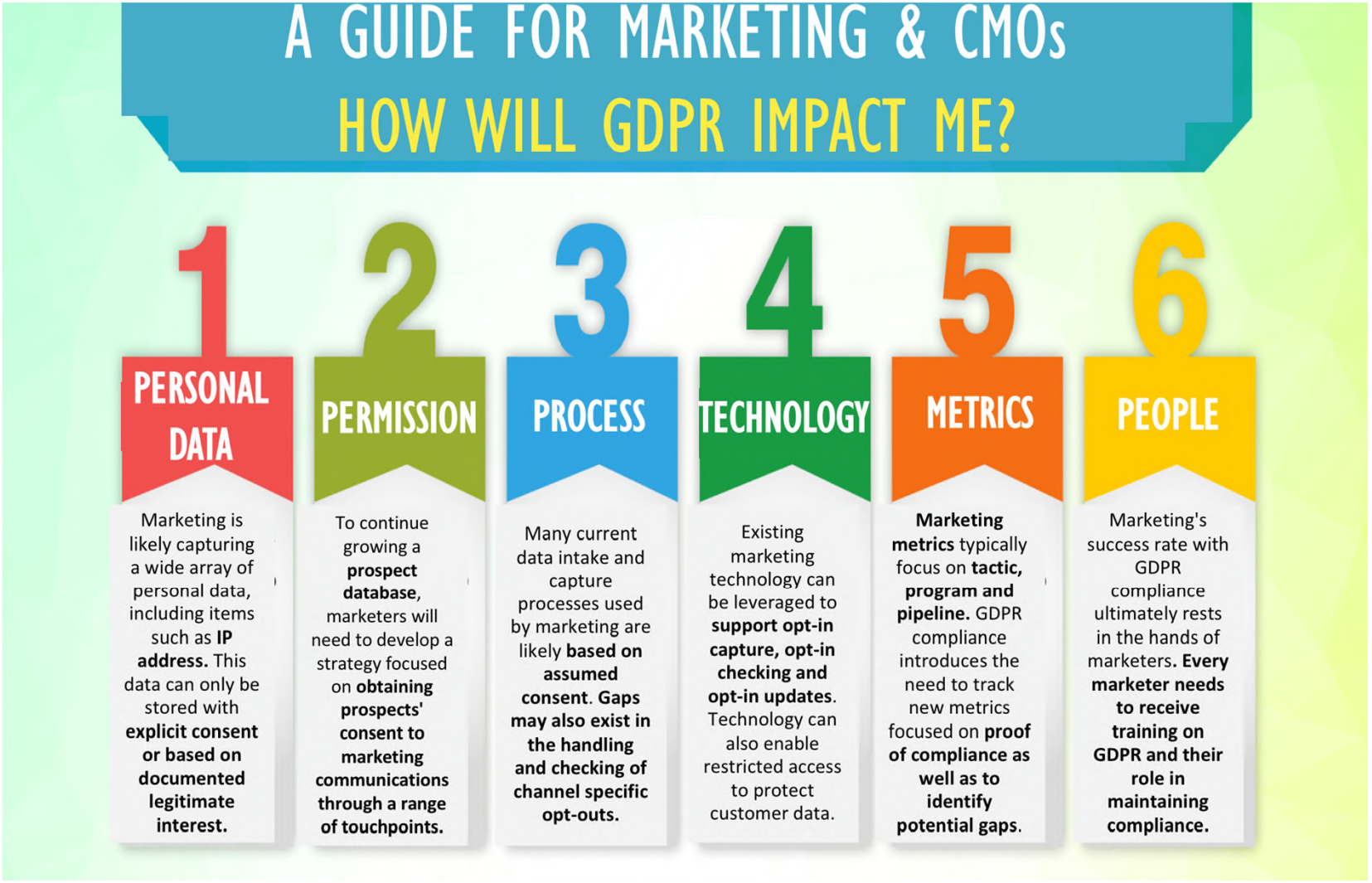
In addition, the AG can bring prosecutions for the following:

Offences under the Data Protection (Jersey) Law 201-

- Unlawful obtaining/disclosure of personal data (Art.71)
- Requiring certain records to be produced (Art.72)
- Providing false information to the Authority (Art.73)
- Obstructing the Authority or Information Commissioner (Art.74)

Offences under the Data Protection Authority (Jersey) Law 201-

- Failing to register (Art.17)
- Failing to comply with an Enforcement/Information Notice (Art.25)



OFFICE OF THE INFORMATION COMMISSIONER

Thank you

Paul Vane

Acting Information Commissioner
Brunel House
Old Street
St. Helier
Jersey
JE2 3RG

Telephone: 716530

Direct E-Mail: p.vane@dataci.org

General E-Mail: www.dataci.org

OFFICE OF THE INFORMATION COMMISSIONER