GANADO
ADVOCATES

# General Data Protection Regulation

Key Changes and Implications

March, 2018

# Overview

- Old regime deemed no longer fit for purpose;
- Enforceable from **25 May, 2018** ("*D-Day*"), two years after entry into force;
- Repeals and replaces the present Data Protection Directive (Directive 95/46/EC);
- Overrides conflicting national data protection laws;
- Scope for derogations and divergences (e.g. national security, processing of employee data);
- 'Wait and see' approach regarding the Data Protection Act (Chapter 440) and subsidiary legislation. Germany, for example, has enacted a new Federal Data Protection Act.

# Headline Features

## 1. Significantly Expanded Territorial Scope - A Global Law

(1) any processing by a controller or processor "established" in the EU, regardless if it takes place in the EU or not;

(2) controllers and processors based outside of the EU where the processing relates to:

(a) the offering of goods or services to individuals in the EU; or
(b) the monitoring of such individuals' behaviour.

## 2. Administrative Fines - Two Tiers

(1) Up to €10 million, or 2% annual global turnover – whichever is higher, or
(2) Up to €20 million or 4% annual global turnover – whichever is higher,

depending on the nature of the infringement. Discretionary rather than mandatory, case-by-case basis.

Factors to take into account, e.g. nature and gravity of the infringement, actions taken to mitigate damage.

# The EU GDPR Countdown Clock

http://www.gdprcountdownclock.com

## Time Until the EU GDPR comes into force


until May 25th 2018

The above includes weekends and public holidays.

ACT NOW - you have less time than you think!

# Definitions and Terminology

a. '**Personal data**': any information relating to an identified or identifiable natural person (the 'data subject').

Wide range of personal identifiers, both obvious (name, I.D.) and less so (GPS, IP address, mobile device ID.

'Identifiable': combination of identifiable elements.

b. '**Special Category Data**' (i.e. sensitive): information revealing a person's race, ethnic origin, politics, religion, trade union membership, or genetics, biometrics, health, sex life or sexual orientation.

Subject to additional protection and requirements (including processing justification).

c. '**Processing**' (broadly-defined): any operation or set of operations performed on personal data, such as collection, recording, adaptation or alteration, use, disclosure by transmission, dissemination etc.

# Definitions and Terminology (2)

d. '**Data Controller**': natural or legal person public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Exercises overall control over the 'why' (purposes) and the 'how' (means) of a data processing activity.

e. '**Joint Controllers**': Jointly determine the purposes and means of processing.

E.g. - CCTV cameras in a town centre which is operated by a local council jointly with the police,
- Business partners with a common customer database relating to the same product/service.

f. '**Data Processor**': a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

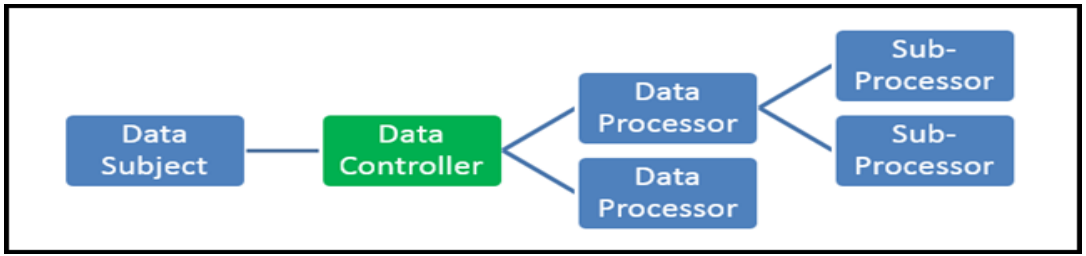
E.g. Employee payroll companies, customer services for utilities companies (ARMS on behalf of Enemalta).

g. '**Sub-processor**': third party to whom processor subcontracts or outsources its processing activities.

# Controller-Processor Relationship

Relationship must be governed by a contract or other legal act that is binding on the processor with regard to the processor and which incorporates those obligations contained in Article 28, GDPR.

('data processing agreement')




Controller or Processor ?

1. Courier Service (e.g. DHL): data to arrange delivery or tracking, content of mail or parcel.

2. Cloud Provider used by a company to store its data and records (hosting services).

3. Recruitment agency: collection of candidate info (e.g. C.Vs), sharing with business clients.

# Lawful Basis for Processing

## Six available lawful bases for processing

(a) Consent: data subject has consented to processing of their personal data for one or more specific purposes.

High standard for consent ('a clear affirmative act' and 'freely given, specific, informed and unambiguous'): **Opt-In**.

Individual ('granular') consent options for distinct processing operations. Consent may be freely withdrawn at any time.

Where there is an imbalance of power between the party giving consent and the party receiving it, consent will not be deemed to have been freely given under GDPR, i.e. invalid consent: **employer-employee relationship**.

(b) Contract: processing is necessary for -

(i) the performance a contract with the data subject (fulfil a contractual obligation); or
(ii) to take specific steps at the request of the data subject before entering into a contract (e.g. provide a quote).

Example: Employer processing employee bank account details or processing of address for delivery of online purchases.

# Lawful Basis for Processing (2)

(c) Legal obligation: processing is necessary for compliance with a legal obligation to which the controller is subject.

Examples: (i) processing of due diligence documentation by subject persons;
(ii) processing of N.I. details by employers;

(d) Vital Interests: processing is necessary to protect the vital interests of the data subject or of another natural person.

(e) Public Task: necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (e.g. regulatory functions and powers).

(f) Legitimate Interests: processing is necessary for the purposes of the legitimate interests of the controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data ('**balancing of interests test**').

Relied on where another lawful basis is not available.

Examples: Monitoring user access to computer network, access card data or visitor logs(visitor data).

# Limitation and Retention

## Data Protection Principles

### Limitation of Purpose

Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes.

Personal data collected for one purpose should not be used for a new, incompatible, purpose.

### Data Retention

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 personal data are processed (after which, must be *erased* or *anonymized*).

Typical scenarios: withdrawal of consent, conclusion of contract, termination of employment.

Derogation where processing remains necessary for the '*establishment, exercise or defence of a legal claim*'.

Relevant Prescriptive Periods:

(i) Unfair dismissal action – 1 year;
(ii) Contractual action – 5 years;
(ii) Social Security – 10 years or 12 months from date on which evidence comes to knowledge of the Director General.

# Individual Rights

## Strengthened Rights

**1. Right to be Informed** (transparency)**:** applies even where the data is obtained from a 3rd party.

*Mandatory information*: identity and contact details of controller, purposes of the processing and lawful basis relied on, categories of data collected, recipients, possible data transfers, existence of individual rights (below), retention periods.

'Privacy Notice' - concise, intelligible, easily accessible, without expense and written in clear and plain language.

**2. Right of Access**: confirmation data is being processed, access to that data (provide a copy) plus supplementary info.

Right may be restricted under National Law where necessary to safeguard *inter alia* the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

**3. Right to Rectification**: Entitled to have personal data rectified if it is inaccurate or completed if it is incomplete.

**4. Right to Data Portability:** Entitled to receive the his/her processed personal data in a structured, commonly used and machine-readable format and to transmit that data to another controller without hindrance from the controller.

# Individual Rights (2)

**5. Right to Erasure** ('right to be forgotten'): Not an absolute right, individuals entitled to request deletion or erasure.

Controllers bound to fulfil an erasure request, or erase of their own motion, without undue delay where *inter alia*:

- consent has been withdrawn and no other lawful basis exists,
- the processing is no longer necessary for its stipulated purpose,
- the personal data was unlawfully processed,
- necessary to comply with a legal obligation.

Justified and permissible refusals, e.g. exercise or defence of legal claims, legal obligation which requires retention.

**6. Right to Restrict Processing**: Set grounds entitling the data subject to have the processing of his/her data restricted.

For example, where contested, processing should be restricted until the accuracy of the personal data is verified.

**7. Right to Object**: Right to object to, in particular, (i) any processing based on legitimate interests or the performance of task in the public interest / exercise of official authority and (ii) processing for direct marketing purposes.

Exemption applies in the case of '(i)', where either continued processing is necessary for the exercise or defence of legal claims or the controller is able demonstrate 'compelling legitimate grounds for the continued processing.

# Data Protection Officer

## Mandatory Appointment

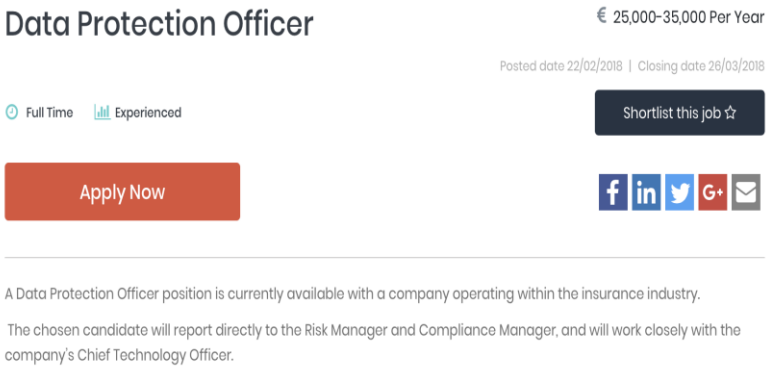
For all public authorities, and where the core activities of the processor or controller involve regular and systematic monitoring (all forms of 'tracking and profiling') of data subjects on a large scale, or where the entity conducts large-scale processing of special categories of personal data, like that which details race or ethnicity or religious beliefs.

Examples: Hospitals, Telecom Providers, Surveillance and Security Companies, Insurance Companies, Banks.

Who to appoint? Guidance from the EDPS:

a. Autonomy (no instructions regarding performance of duties);
b. No conflict of interest. Recommended that DPO should:

- not also be a controller of processing activities (e.g. head of HR),
- not be an employee on a short or fixed term contract,
- not report to a direct superior (but rather top management),
- have responsibility for managing his/her own budget.



# Thank you.

**www.ganadoadvocates.com**

**Important Notice:** This presentation is for informational purposes only and does not contain or convey legal advice. The information contained in these slides should not be used or relied upon in regard to any particular facts or circumstances without first obtaining specific legal advice.

In this presentation 'GANADO Advocates' refers to the law firm Ganado & Associates, Advocates, an association established under the laws of Malta. A full list of members is available upon request at the principal office of the firm at 171, Old Bakery Street, Valletta VLT1455, Malta.