# The Data Protection Landscape

## Before and after GDPR:
## General Data Protection Regulation

OPT-4

# Data Protection regulations across Europe

**Current regulations & guidance**

- European Directives 95/46/EC (Data Protection) and 2002/58/EC (Electronic Communications) led to different Regulations across EU member states
- In the UK we have:
  - The Data Protection Act 1998
  - Privacy and Electronic Communications (EC Directive) Regulations 2003
  - ICO Direct Marketing Guidance – this was issued to clarify ICO's requirements for compliance
- Other EU members have their own data protection regulations
- The current UK regulation is 'light touch' compared to some others regimes

**Under GDPR**

- There will be a single Regulation across the EU which will be passed into law in all EU member states
- There is limited 'directivisation' enabling certain requirements to be varied for individual member states
- GDPR 'compromise' text was agreed in December 2015 and is expected to go into member states laws in 2018

OPT-4

# Definition of Personal Data & Data Subject

**Current definition**

"personal data" means data which relate to a living individual who can be identified—

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual;

"data subject" means an individual who is the subject of personal data;

**Under GDPR -** A broader definition to take account of data across all consumer touchpoints:

'personal data' means any information relating to an identified or identifiable natural person 'data subject'; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

OPT-4

# Definitions for Data Controller and Data Processor

**Current definitions**

"data controller" means, subject to subsection (4), a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed;

"data processor", in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller;

**Under GDPR**

'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;

'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

OPT-4

# Definition of Processing

**Current definitions**

"processing", in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including—

(a) organisation, adaptation or alteration of the information or data,

(b) retrieval, consultation or use of the information or data,

(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or

(d) alignment, combination, blocking, erasure or destruction of the information or data;

**Under GDPR**

'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

OPT-4

# Definition of Consent

**Current definition**

"any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed".

**Under GDPR**

'the data subject's consent' means any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;

OPT-4

# Definition of Profiling

**Under GDPR**

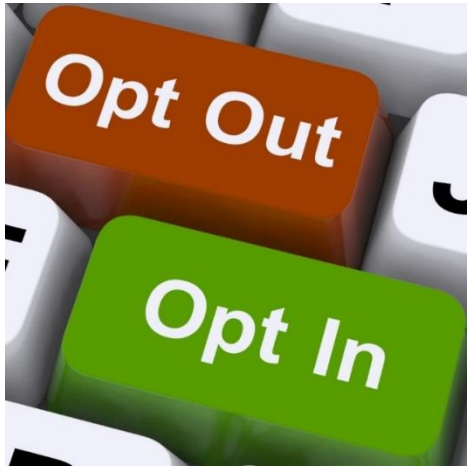
'profiling' means any form of automated processing of personal data consisting of using those data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

OPT-4

# 1. Consent for Marketing

**Current definition of consent**

- "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed"
- The data controller should be able to provide 'indicative copies' of data collection statements




**Under GDPR**

- Consent for marketing must be unambiguous
- Consent requires a clear affirmative action
  *'Silence, pre-ticked boxes or inactivity should therefore not constitute consent.'*
- Sensitive personal data requires explicit consent
- Consumers cannot be forced to give consent for further use of data when signing up to a service.
- Controller shall 'be able to demonstrate that consent was given'
  – in practice this means storing copies of your DP statements

OPT-4

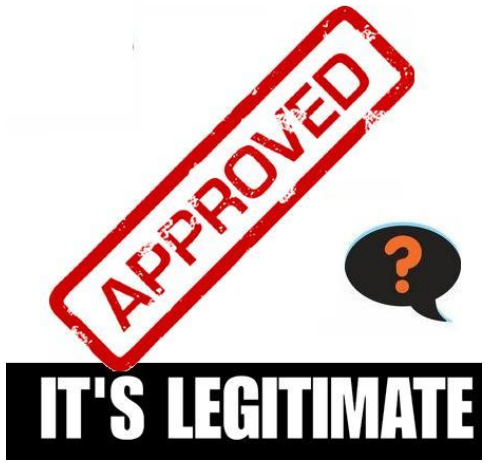
# 2. Processing under ‘Legitimate interests’

**Current position**

Data controllers have some flexibility for contacting individuals where consent has not been given, when it is in their ‘legitimate interests’

**Under GDPR**

- Some flexibility has been maintained under GDPR. The controller must be able to show how their own legitimate interests override the interests of the data subject.
- Data subjects have the right to object to processing under legitimate interests.
- The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest

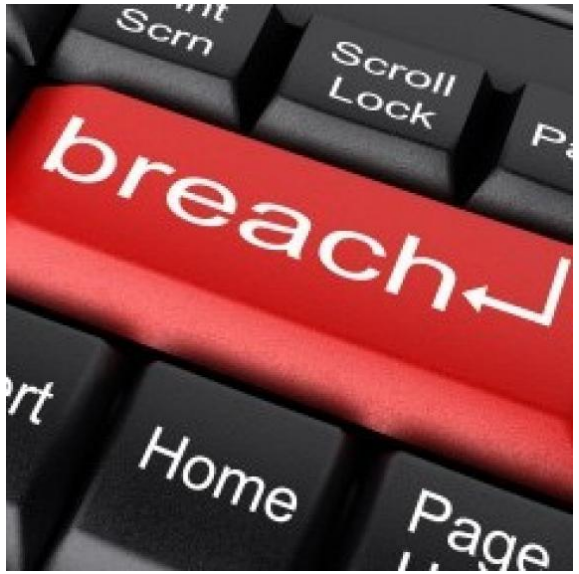



OPT-4

# 3. Data breaches

**Current position**

Data breaches do not need to be notified to the Regulator. Notification is optional but often advisable if the breach will affect consumers.




**Under GDPR**

- Data breaches must be notified to the Regulator 'without undue delay' and 'not later than 72 hours'
- Exclusion: Organisations do not need to notify if the breach is 'unlikely to result in risk for the rights and freedoms of individuals'
- Individuals must be notified 'without delay' if the breach is likely to result in a 'high risk' to individuals rights and freedoms.

OPT-4

# 4. Data Protection Officer

**Current position**

There is no current requirement for organisations to have a Data Protection Officer.

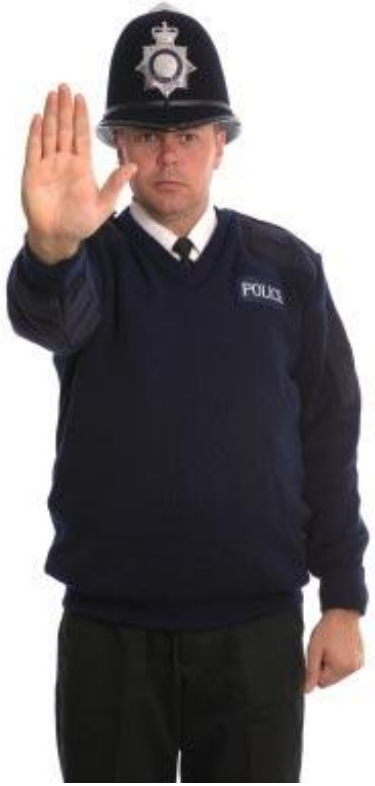
**Under GDPR**

Organisations will require a DPO if

- If the organisation has 250+ employees
- Smaller organisations only need a DPO is if their processing is ‘likely to result in a risk to data subjects’
- Public authorities and bodies are required to have a DPO
- A group of organisations may appoint a single DPO
- Organisations will have 12 months’ leeway to appoint DPO.
- They may be employed or can be contracted in from a service provider

**Role of a DPO**

- They will oversee the protection of personal data
- Carry out Data Protection Impact Assessments
- DPO must report direct to the highest level of management and may not be dismissed or penalised for carrying out their job (they have legal protection)




OPT-4

# 5. Data Protection Impact Assessments

**Current position**

Currently no requirement to carry out assessments of the impact of data processing.

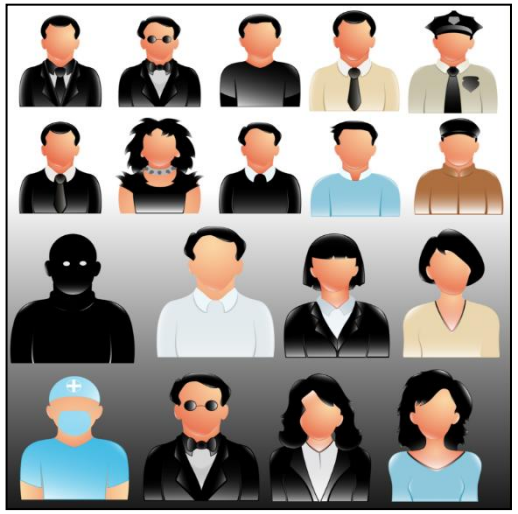
**Under GDPR**

- Data Protection Impact Assessments to be carried out if the planned processing is likely to result in a high risk to rights and freedoms of individuals - including where processing involves ‘new technologies’ or ‘large scale processing‘
- Assessments are not retrospective to the Regulation as long as there was compliance with the prior Directive
- Assessments must be carried out prior to processing to ensure that risks are mitigated and compliance with the Regulation is demonstrated
- Assessment is required when examining the legitimate interests and reasonable expectations of the data subject
- The supervisory authority shall publish a list of the kind of processing operations which require assessment and may also publish a list of those which do not require assessment.


OPT-4

# 6. Profiling

- Profiling is referred to within ‘Automated individual decision making’
- Profiling includes personal preferences, interests, behaviours, location or movements
- Data subjects must be informed about the existence of profiling on or before the time of the first communication, using explicit wording clearly and separately from other information. Organisations may use the Privacy Policy to notify consumers.
- Data subjects have the right to object to profiling, including its use in direct marketing, but not if it is necessary for a contract
- They must be informed of the consequences if they object.



OPT-4

# 7. The rights of data subjects

**Current position**

- Right to object to processing for direct marketing
- Right to be forgotten (e.g. Google's online search results)
- Subject Access Requests

**Under GDPR**

- Right to object to processing for direct marketing continues
- New right to object to processing for legitimate interests
- The right be forgotten becomes 'The right to erasure' which enables data subjects to request personal data concerning him or her to be erased 'without undue delay'. Controllers must inform data processors of any erasure request.
- Subject Access Requests must be free of charge (pay for copies only)

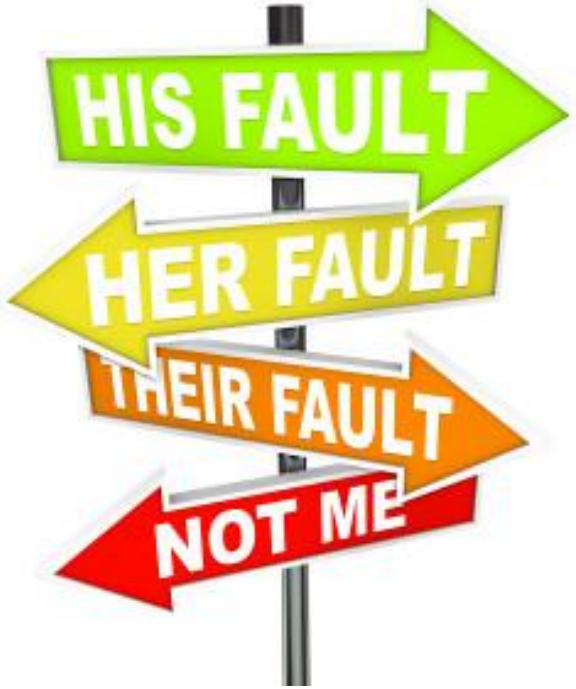

OPT-4

# 8. Controller and processor liability

**Current position**
Data controllers bear the responsibility when things go wrong.

**Under GDPR**

- Both controller and processor will be held responsible for any damage suffered
- To ensure effective compensation, where both controller and processor are involved each party shall be held liable for the entire damage
- Controller or processor shall be exempted if they can prove they are ‘not in any way responsible’.




OPT-4

# 9. International marketing

**Current position**

- Regulation differs across each EU member state making it difficult and costly to manage pan-European data-driven marketing

**Under GDPR**

- Regulation will be broadly the same across EU, with only small differences from 'directivisation'
- Businesses trading within Europe will benefit from harmonisation as the Regulatory framework will standardised across the EU – an equal playing field.
- They can employ common processes and practices across borders.
- Global businesses trading in Europe will also benefit in the same way.

**Safe Harbor**

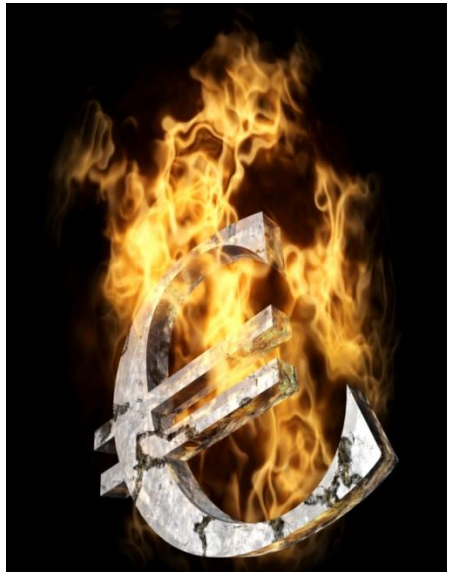
- In October 2015 a new ruling declared the Safe Harbor Agreement on transatlantic data sharing between the US and the EU to be invalid. A new transatlantic data agreement is possible, but until then businesses should evaluate alternative legal frameworks if they wish to ensure compliant data transfers with the US.

OPT-4

# 10. Enforcement and penalties for non-compliance

**Current position**

- ICO may name and shame or impose an enforcement notice
- Monetary penalty notices can have a value up to £500,000
- Criminal prosecutions may be made.



**Under GDPR**

- A warning or reprimand may be issued to the data controller
- An order to comply can be issued
- **A new tiered structure to penalise non-compliance, with fines rising up to €20 million or 4% of annual worldwide turnover**
- Member states may lay down their own rules on criminal sanctions.

OPT-4

# So what can you do now?

It’s all about planning ahead…

- Review your consent statements and how consent is stored and processed on your data systems. Will you be compliant under GDPR, e.g. have you been using pre-ticked boxes? Start planning ahead ready for the new consent requirements.
- Will your current CRM system be fit for storing & processing consent under GDPR?
- Think about how you could enable consumers to opt-out of profiling or processing under legitimate interests. Plan how to enable the right of erasure.
- Will you need to boost your compliance resources? Consider if / when you should you recruit a DPO. Do you need specialist compliance support to get ready for GDPR?
- Review contracts with data processors. Will they be ready to take on their new liabilities?

# Status of advice given

The information provided and the opinions expressed in this document represent the views of Opt-4 Ltd. They do not constitute legal advice and cannot be construed as offering comprehensive guidance to the Data Protection Act 1998 or other statutory measures referred to in the course of consultation.



OPT-4