GDPR – The Final Push

The EU General Data Protection Regulation (**GDPR**) will become effective on 25 May 2018.

An organisation that controls the collection or processing of personal identification information of any individual in the European Union (**EU**) shall be responsible for and must be able to demonstrate compliance with the data protection principles in the GDPR.

In its capacity as external corporate counsel, Radix Legal and Consulting (**RLC**) has assisted its clients in assessing their existing policies, procedures, and the controls against the GDPR requirements.

Why is urgent attention needed?

The consequences of non-compliance may be severely damaging for the business and may include:

1. fines of up to €20 million or 4% of total worldwide annual group turnover;
2. adverse publicity, reputational damage and lost customer trust;
3. missed opportunities and wasted resources;
4. increased scrutiny from regulators;
5. punitive damages from civil claims by individuals affected by violations;
6. criminal liability for directors and senior managers with a potential for imprisonment and substantial penalties; and
7. management distraction and the diversion of time effort and expense in dealing with litigation or investigation by supervisory authorities or implementing emergency corrective measures to allow business continuity.

What is the objective of GDPR?

The aim of the GDPR is to better protect EU individuals from privacy and data breaches and to give the individual more control over how their personal data is used by others. GDPR places specific legal obligations on a processor and controller of personal data.

Who is affected?

The GDPR applies to:

- EU-based establishment
  - Business established in the EU that process personal data in the context of the activities of the EU establishment, regardless of where the processing takes place; and

- Business not established in the EU that process EU data subjects' personal data in connection with offering goods or services or monitoring their behaviour.

- Non-EU Establishment
  - Non-EU business processing EU data subjects' personal data in connection with offering goods and services in the EU with the intent to target EU data subjects as customers; and
  - Non-EU business processing EU data subjects' personal data in connection with monitoring their activities or behaviour in the EU.

What are the key requirements?

Key principles for processing - The key requirements of the GDPR are captured in the following principles requiring that personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals;

(b) collected for specified, explicit and legitimate purposes;

(c) limited to what is necessary in relation to the purposes for which they are processed;

(d) accurate and, where necessary, kept up to date;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and

(f) processed in a manner that ensures appropriate security of the personal data.

Accountability – The GDPR requires that the controller shall be responsible for, and be able to demonstrate, compliance with the principles.

What next for the business?

1. Audit, review, implement - The Information Commissioner's Office (**ICO**) has suggested a simple checklist:
   - analysing and documenting the type of personal data the business holds;
   - checking procedures to make sure they cover all the rights individuals have;
   - identifying the lawful basis for processing activity;
   - reviewing consent procedures; and
   - implementing procedures to detect, report and investigate personal data breaches.

2. Record keeping - Data controllers and processors must keep certain records to be provided to the appropriate supervisory authority on request. A business must therefore implement a structure that will enable it to comply.

How RLC can help

1. Information audit – RLC will guide clients through the process of gathering the information needed to conduct a GDPR impact assessment. The information supplied must be accurate and complete as it will form the basis of the advice given.
2. Data Protection Impact Assessment - RLC will then conduct an assessment of the information supplied. This will include an assessment of the client's existing policies, procedures, and the controls against the GDPR requirements.
3. Data Protection Impact Assessment Report - Following the assessment, a report will be compiled that sets out our findings. We will specify the extent to which there may be non-compliance with the GDPR and make recommendations for what needs to be done to comply.

Elizabeth Uwaifo Managing Partner E: euwaifo@radixlc.com Phone: +44(0)20 3802 0031	Funmi Dele-Giwa Senior Associate E: fdele-giwa@radixlc.com Phone: +44(0)20 3802 0031
Mercy Etomi Legal and Regulatory Consultant and GDPR Practitioner E: metomi@radixlc.com Phone: +44(0)20 3802 0031	