**GDPR – The Way Forward**

**How will GDPR affect my business?**

The EU General Data Protection Regulation (Regulation (EU) 2016/679) ("**GDPR**") will come into effect in the UK and across the European Union ("**EU**") on 25 May 2018. The GDPR applies to the processing of personal data:

(1) in the context of the activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU or not[1],

(2) of data subjects that are in the EU, or by a controller or processor not established in the EU where the processing activities are related to[2]:

   a. The offering of goods and services to EU data subjects, regardless of whether payment is required from the data subject; or

   b. The monitoring of their behaviour while within the EU; and

(3) by a controller not established in the EU, but in a place where Member State law applies by virtue of public international law.[3]

**Penalties**

From 25 May 2018, organisations subject to the GDPR face enforcement risks for non-compliance and the penalties for non-compliance are steep.

- The Information Commissioner's Office ("**ICO**") has the power to issue organisations with fines of up to €10 million or 2% of global turnover for certain categories of breaches and up to €20 million or 4% of global turnover for other categories of breaches[4].
- Other penalties established by EU countries for infringements (in particular for infringements which may not fall under the above), including criminal penalties.[5]
- Damages in private lawsuits by supervisory authorities and data subjects. Data subjects have a right to compensation for any damages (material and non-material )[6].

**Applicability to Non-EU Established Businesses**

A business that is not established in the EU may nevertheless be exposed to penalties for failure to comply

[1] Article 3(1)
[2] Article 3(2)
[3] Article3(3)
[4] See Article 83
[5] Article 84 and Recitals 149, 152
[6] Articles 78, 79, 80 and 82.

with GDPR. It is prudent for non-EU companies that may have to hold, process, or store personal data or information of individuals in the EU to assess the applicability of the GDPR to their operations.

**Applicability to Small Businesses**

A small business for GDPR purposes is a firm with less than 250 employees.

GDPR applies to all businesses that fall within the remit of the regulations, irrespective of their size. Every business, big or small, will have to comply with the requirements of the GDPR regarding the secure collection, storage and usage of personal information. Failure to comply will expose the business to fines or other penalties.

However it is recognised that resources are limited in small businesses and they may pose less of a risk to data protection.

There are exemptions that apply to small businesses including an exemption from the requirement to maintain a record of processing activities under its responsibility[7]. In addition a small business will not need to appoint a Data Protection Officer unless its activities involve (a) 'regular or systematic' monitoring of data subjects on a large scale or (b) processing large volumes of 'special category data' defined in GDPR Article 9.

**Next steps**

Some organisations are yet to assess the impact of the GDPR on their operations or implement the changes that will make them compliant. Urgent attention must now be paid to GDPR.

***What you need to do***

A business will require an investment of time and funds to assess and change systems, processes, policies, and contracts to ensure compliance with GDPR. The business will need to:

1. Establish whether the business has an EU establishment or engages in activities covered by the GDPR. If the business is within the scope of GDPR,
2. Determine whether the business acts as Data Controller or Data Processor. The GDPR establishes different requirements and obligations for data controllers and processors.
3. Conduct an audit. The business will need to conduct a review and an assessment of what types of personal information it collects, how it is collected, what it is used for, who it is shared with, how long they are kept and assess the security of the system for storing the data.

[7] Article 30(5).

4. Review and document the business's legal basis for GDPR-covered processing activities ensuring that each processing activity within the GDPR's scope meets at least one of the GDPR's legal processing grounds
5. Review and update the business' privacy notices or other documentation to ensure they meet or exceed the GDPR's requirements.
6. Review and Update Consent Mechanisms and Language. The business must identify all processing activities that currently rely on the data subject's consent or explicit consent as the legal basis for processing and ensure that the language used meets the GDPR's requirements.
7. Review and revise the business's contract templates for services that involve processing EU personal data to ensure they address all of the GDPR's requirements.
8. Identify and review all profiling activities and automated decisions. Review the identified profiling and automated decisions for alignment with the GDPR's data protection principles, data subject rights, and other requirements.
9. Establish New Corporate Processes including Data Protection Impact Assessments.
10. Prepare for New Documentation (Recordkeeping) Requirements
11. Prepare for New Data Processor Requirements
12. Prepare for New Data Breach Notification Requirements
13. Review Personal Data Protection and Security Measures
14. Review Cross-Border Transfer Mechanisms
15. Prepare for Compliance with New Data Subject Rights
16. Consider Applicable Country- Derogations for specific situations under article 49 GDPR

**Our GDPR Support Services**

We can help by the following:

1. GDPR Privacy Policy –Review and revision of current privacy policy to comply with GDPR. A template privacy policy that contains the updated GDPR prescribed terms.
2. Data Protection Schedule - A data protection schedule to add to contracts with third parties.
3. Review of any cross border transfers –transfer mechanism for Personally Identifiable Information ("**PII**") to ensure they are GDPR compliant
4. GDPR Adequacy Assessment – An offsite review of firms' data protection policies and procedures and an update to them to meet GDPR requirements.
5. GDPR Audit – An offsite adequacy assessment plus an onsite audit of a firm's data protection practices. Carry out a data protection impact assessment for the firm's various processes
6. PII Audit-Review and update of company's consent mechanisms and language

7. GDPR Compliance Manual – Establish new corporate policies. Prepare a manual which contains GDPR compliant data protection policies and associated templates such as a form for recording breaches, information asset register template, data impact assessment review template
8. GDPR Ongoing Compliance Support – Provide telephone and email support in relation to GDPR.
9. Reviewing and updating data protection policies.
10. Identify and review all profiling activities and automated decisions(if applicable)
11. Onsite training designed for management teams and decision makers.


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