GDPR

COMPLIANCE & AUDITS

The European Union has updated its data protection laws which will have a significant direct or indirect impact on most businesses operating all over the world. Whether your business is based in Europe or further afield, you need to know what is happening on the GDPR front and then determine what this means for your organisation's compliance efforts. The good news is that the GDPR only becomes effective on 25th May 2018, though we recommend that preparation is commenced without delay.

What is the GDPR?
The GDPR is the General Data Protection Regulation (Regulation (EU) 2016/679). The GDPR comes into force **on 25 May 2018** and will repeal Directive 95/46/EC, implemented in UK law by the Data Protection Act 1998 (the "**DPA**").

The GDPR is a European Regulation and has direct effect in all the European Member States including the UK. The Information Commissioner's Office (the "**ICO**") will be responsible for enforcing the GDPR in the UK.

What is the New Data Protection Bill
The Data Protection Bill is intended to ensure that the UK and EU data protection regimes are aligned post Brexit. Therefore, if you are GDPR compliant you will most certainly be compliant under the new UK Data Protection Act.

Why is the GDPR relevant to most businesses?
Save for very limited exceptions, the GDPR applies not only to every UK business, but also to any business across the globe that is processing personal data of European subjects.

Why do I need to be GDPR compliant?
The GDPR breaches could attract significant financial penalties (up to €20m or 4% of global revenue, whichever is higher) and reputational damage.

What is new under the GDPR?
The GDPR marks a step-change to the previous data protection regime. The GDPR tightens the data protection regime imposing, among other things, stricter controls in certain areas and enhancing the rights of data subjects (the owners of the personal data). The GDPR, amongst other things:

- contains obligations for controllers and also for processors (the DPA only applies to controllers);
- adds new rights for individuals and strengthens some of the rights that exist under the current regime (e.g. enhancement of the right to object – so called right to be forgotten -, a new right to data portability);
- makes explicit and tightens requirements around accountability and governance: the GDPR expects organisations to implement comprehensive but proportionate governance measures, such us:

    - privacy by design (consider privacy and data protection in the early stages of any project);
    - privacy impact assessments - to identify and reduce the privacy risks and to design more efficient and effective processes (this assessments are only compulsory for high risk processing operations);
    - accountability: requires organisations to demonstrate that they comply with the GDPR.

- includes a new obligation to notify:

    - the national data protection regulator, (which in the UK is the ICO) of breaches that are likely to result in a risk to rights & freedoms of individuals (e.g. financial loss, loss of confidentiality) - within 72 hours of becoming aware; and
    - the individuals, if a breach is likely to result in a high risk to the rights & freedoms of individuals (e.g. identify theft) – without undue delay.

- significantly increases the penalties for noncompliance:

    - Under the current DPA the maximum monetary penalty could be £500,000;
    - Under the GDPR, the maximum monetary fine could be up to 20 million Euros or 4% per cent of global turnover, whichever is higher.

- Increases its territorial scope. The GDPR applies to:

    - processing carried out by controllers or processors operating within the EU (regardless of whether the processing takes place in the EU or not);
    - the processing of personal data of EU individuals by organisations established outside of the EU (when offering their goods or services to EU individuals or monitoring their behaviour).

PREISKEL & CO LLP

4 King's Bench Walk, Temple,
London, EC4Y 7DL
United Kingdom

Tel: +44 (0)20 7332 5640
Fax: +44 (0)20 7332 5641
Email: info@preiskel.com

www.preiskel.com

How can I achieve compliance?
The starting point to achieve GDPR compliance for any organisation would be to review the personal data it holds, the justification for holding the data, its data processing activities and the data flows involved. Some of the steps that an organisation could take might be to:

- verify if its policies, codes of practice, guidelines (the **"Privacy Compliance Documentation"**) and procedures meet the requirements of data protection laws relevant to its data processing activities (**"Adequacy Audit"**);
- verify if such organisation is in fact operating in accordance with its Privacy Compliance Documentation and procedures;
- gain an overview of how the organisation shares personal data with other organisations (such as other companies of a group, suppliers, sub-contractors etc.);
- identify potential data protection and privacy compliance gaps and weaknesses (**"Compliance Audit")**;
- increase the level of data protection awareness amongst management and staff;
- implement a security breach notification procedure;
- assess its ability to comply with main data protection principles (e.g. minimisation, accuracy, retention); and
- implement procedures to comply with data subject requests.

Once the above steps are completed, then the organisation would need to update its Privacy Compliance Documentation and procedures to bridge any gaps detected during the audit (i.e. to correct any data compliance issues and gaps).

Why Preiskel & Co?
Given our firm's expertise in telecoms and technology, it may come as no surprise that we have been advising clients on data protection matters for many years and are well aware of the compliance (including technical) challenges national and international organisations face.

The firm is playing an active role in how those selling goods and services through mobile devices are to best address the GDPR and indeed to thereby gain consumer trust. Daniel Preiskel is on the EMEA Board of the Mobile Ecosystem Forum (www.mobileecosystemforum.com) working alongside major multi-nationals as well as some early stage companies in addressing consumer trust. Digital consent is going to be a key area and Preiskel & Co contributed to MEF's Consumer Trust Guide to Digital Consent.

PREISKEL & CO LLP

4 King's Bench Walk, Temple,
London, EC4Y 7DL
United Kingdom

Tel: +44 (0)20 7332 5640
Fax: +44 (0)20 7332 5641
Email: info@preiskel.com

www.preiskel.com

Furthermore, the firm has been independently ranked by the prestigious WhoswhoLegal guide 2018, as a leader in data privacy law.

We offer a partner-led, tailored service and have a well-balanced, commercial approach to legal work, including where multiple jurisdictions are involved.

Do you want a quote?
We would be delighted to have a discussion with your organisation to understand your privacy compliance requirements.

Daniel Preiskel
Partner
PREISKEL & CO LLP
dpreiskel@preiskel.com

Jose Saras
Partner
PREISKEL & CO LLP
jsaras@preiskel.com

PREISKEL & CO LLP

4 King's Bench Walk, Temple,
London, EC4Y 7DL
United Kingdom

Tel: +44 (0)20 7332 5640
Fax: +44 (0)20 7332 5641
Email: info@preiskel.com

www.preiskel.com

w.preiskel.com