GDPR WITH ITS HIGH PENALTIES IS ALMOST HERE. MAY 25, 2018. LESS THAN 125 DAYS TO GO.

It is the biggest shift in data protection and privacy legislation in Europe for a generation, with extra-territorial effect, so a US company may have to comply even if it is not based in Europe.

Failure to comply exposes a company to unprecedented regulatory risk, and huge penalties for serious breaches - up to 20 million Euro or 4% of global turnover - whichever is higher!

- Many organizations based outside the EU will find themselves caught by the GDPR, given that it significantly expands the territorial reach of European data protection and privacy rules.
- It applies to non-EU companies where services are provided into the EU or where personal data is obtained in the EU and transferred outside.
- The GDPR substantially increase the risks associated with a failure to comply with the new European data privacy regime. With stepped fines - of up to 4% of annual global turnover - organizations should determine whether they are in scope and, if so, the steps necessary to achieve compliance before May 25, 2018.
- A 72 hour mandatory breach notification to the data protection regulator and possible notification to the at risk data subjects also raises the financial and reputational risk for non-compliance.
- The direct regulation of data processors is new and will add unprecedented weight to the compliance burden.
- With corresponding exposure to regulatory investigations, sanctions, claims from individuals and class actions, with the possibility of criminal offences being added to this - already unnerving - list as well, now is not the time to be caught unprepared.

KEY ISSUES

- The GDPR, and why it may be a game-changer for a US organization (even if it is not in Europe).
- The General Data Protection Regulation (the GDPR) becomes effective on May 25, 2018.

KEY ISSUES FOR CONSIDERATION:

Extraterritoriality

US companies with no presence in the EU will be caught by the GDPR if they either target offers of goods or services to, or monitor the behavior of, individuals in the EU.

Action:

- Assess whether your online activities result in you processing EU personal data for the purposes of the GDPR. This could include situations where your websites and apps directly offer goods or services to individuals within the EU, or where cookies and tracking activities on your websites and apps monitor the behaviour of individuals within the EU.

Processors are directly regulated

Currently only data controllers (the organization deciding on the purpose and means of the processing) are subject to EU data protection law.

The GDPR changes this. Processors (third party service providers that process personal data on behalf of the controller customer) are regulated in some key respects, for example in relation to information security measures and record- keeping requirements.

Importantly, for the first time processors have liability under the new law and can be subject to fines.

Action:

- Determine whether your business (irrespective of location(s)) is a data processor in respect of EU personal data. If so, you are caught by the GDPR.
- Ensure you fully understand the new legal obligations on processors, and their application to your business, under the GDPR. Adopt a comprehensive program to implement any changes to ensure compliance.
- Processors that can demonstrate robust compliance to controller customers, both ahead of May 2018 and subsequently, are highly likely to gain a competitive advantage.

Cybersecurity - increased regulatory risk and scrutiny

After May 25, 2018, data breaches involving EU personal data can attract substantial fines. The GDPR also requires data processors to accept more onerous cyber and data security contractual provisions.

Action:

- As the risk profile of security breaches increases to high, review and assess your security measures. Put in place any necessary additional measures to support GDPR-standard compliance.

Mandatory breach notification

Personal data breaches must be reported to the data protection regulator without undue delay, and in any event within 72 hours.

All high risk breaches also require notification to the data subjects concerned.

In addition, processors must inform their controller customers when they become aware of any personal data breach.

Action:

- Evaluate your processes, procedures and systems, and if necessary develop a security breach readiness strategy, to meet the 72 hour breach notification requirement.

IT systems: capability and design

GDPR requires organizations to build privacy by design into their systems and processing activities. Data protection impact assessments will be required before carrying out processing involving new technology.

IT systems must be technically capable of supporting GDPR compliance, for example in relation to the rights of individuals to access, rectify, and/or erase their personal data.

Action:

- Engage your IT team now. Review all existing systems to identify any gaps in current capability against the new requirements of the GDPR. This is likely to be a very significant workstream within any GDPR compliance program. In some instances, systems may need to be (re)designed to meet the new GDPR obligations.

Data transfers from Europe to anywhere else

Restrictions remain, and under the GDPR data controllers will no longer be able to reach their own view on whether a country outside the EEA is adequate. Assurances must be given that adequate safeguards are in place.

There is a new obligation on data processors to comply with the data transfer regime.

Action:

- Consider how cross border transfers are currently structured, either as controller or processor. Changes to processes and contracts may be required.

Reputational impact

The financial price and reputational impact of getting GDPR wrong would undoubtedly be a board-level issue.

Mandatory reporting requirements for breach both to regulators and in some cases affected data subjects also adds a new element of reputational risk.

Action:

- A company will need to ensure it has the resources to both assess whether a breach has occurred, and then report it within the 72 hour window to the regulator once this has been established. Delay in reporting and notice has created the most significant negative publicity in recent breaches.

CONTACTS

US

Megan Gordon
Partner

T +1 202 912 5021
E megan.gordon@cliffordchance.com

Daniel Silver
Partner

T +1 212 878 4919
E daniel.silver@cliffordchance.com

Alice Kane
Counsel

T +1 212 878 8110
E alice.kane@cliffordchance.com

UK

Jonathan Kewley
Partner

T +44 20 7006 3629
E jonathan.kewley@cliffordchance.com

Richard Jones
Director of Data Privacy

T +44 20 7006 8238
E richard.jones@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 31 West 52nd Street, New York, NY 10019-6131, USA

Clifford Chance US LLP

Abu Dhabi • Amsterdam • Bangkok • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Moscow • Munich • New York • Paris • Perth • Prague • Rome • São Paulo • Seoul • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.