Deloitte.
Legal

Special Legal Alert

March 2018

Issue № 03/SLA

EU General Data Protection Regulation (GDPR)

Dear friends,

With the General Data Protection Regulation (Regulation (EU) 2016/679) (the "GDPR" or the "Regulation") coming into effect in May 2018, companies with operations outside of the European Union ("EU") are already beginning to ask how it will affect them.

GDPR may have consequences for companies outside of the EU

When might overseas companies be caught by the GDPR?

Firstly, the Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or processor[1] in the EU, regardless of whether the processing actually takes place in the EU or not[2]. This is likely to capture, for example, when third country headquarters process the data of employees working for an EU branch, and could include technical processing located outside of the EU.

Secondly, it applies to the processing of personal data of data subjects who are in the EU ("Data Subjects") by a controller or processor not established in the EU where the processing activities relate to:

1. offering goods or services to Data Subjects (both paid and free of charge) ("Criterion 1"); or

2. monitoring Data Subject behaviour as far as their behaviour takes places in the EU ("Criterion 2")[3].

In the event of violations, the GDPR stipulates fines even on companies registered outside the EU of up to 4% of the offender's total annual worldwide turnover or Euro 20 million, depending on which is higher

Which actions may qualify as "the offering of goods or services" to Data Subjects?

If a personal data controller/ processor and Data Subject are in different locations, goods and services are likely to be offered electronically.

A key aspect in establishing whether Criterion 1 applies, is **intention** i.e. whether the controller/processor intended to offer the goods/services to a Data Subject. The recitals talk about whether it is "apparent" that the controller/processor envisages offering goods or services to Data Subjects in one or more Member States in the EU. Intention is unlikely to be established, for example, if the website of the controller/processor is merely accessible in the EU**.**

However, Criterion 1 is likely to be met if:

- the company's official website is available in one of the official EU languages, which is not the official language in the company's country of incorporation, and goods/services can be ordered in that language;
- prices for goods/services on the website are in the national currency of an EU country; or
- the website explicitly mentions customers or users who are in the EU.

How is "monitoring behaviour" defined?

The recitals note that in order to determine whether a processing activity can be considered to monitor behaviour of Data Subjects, it should be ascertained whether natural persons are tracked on the

---

[1] GDPR define the terms "data controllers" and "data processors." The former are entities (including state bodies) independently or together with other entities defining the purpose and means of processing personal data; the latter – entities (including state bodies) handling personal data on behalf of controllers
[2] Article 3.1 of the GDPR
[3] Article 3.2 of the GDPR

internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analyzing or predicting her or his personal preferences, behaviours and attitudes.

It is assumed that the following behaviour would be caught:

- using cookies to track online EU user activity on an official website[4]; and
- collecting data on the IP addresses of users visiting an official website, particularly if combined with other data which, together with the user's IP address, can identify the user.

Again, in light of the recital noted above which introduces an element of positive decision taking, it is clear that an intentional element to the monitoring is required for the GDPR to apply to non-EU businesses. Unintentional collecting without further profiling is unlikely to be caught.

Personal data protection representatives

In many cases, companies established outside the EU to whom the Regulation applies, will be required to designate a representative in the EU. However, the representative only needs to be established in one of the Member States where the Data Subjects whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are.

Sanctions

Significant fines of up to 4% of annual worldwide turnover or Euro 20 million, depending on which is higher, can be imposed on companies.

However, despite the significant fines and cross-territorial application of the GDPR, the Regulation does not list specific mechanisms for bringing entities registered outside the EU and violating GDPR rules to account. What is clear is that the enforceability of the GDPR outside of the EU can only operate successfully with international cooperation.

In 2015, Kazakhstan and the EU entered into an Expanded Partnership and Interaction Treaty, pursuant to which the parties are responsible for ensuring a high level of security of personal data through the exchange of experience and practices.[5] Combined with Kazakhstan's accession to the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data[6] and an Additional Protocol to it, we would expect these instruments to be able to work together to provide a framework for cooperation between authorities, and ultimately enforcement.

Importance of reviewing compliance programmes

While the currently in effect Data protection Law in Kazakhstan pursues many of the common GDRP principles for ensuring the protection of personal data, the processes for the latter, are less regulated and defined (in terms of the obligation to appoint a data protection officer,

---

[4] *EU case law has previously found that information about a user's browsing and internet use can be classified as personal data*
[5] *Article 237 Treaty on Expanded Partnership and Cooperation between the European Union and its Member States, on the one hand, and the Republic of Kazakhstan, on the other (Astana, 21 December 2015)*
[6] *Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Strasbourg, 28 January 1981; CETS # 108)*

anonymizing/encrypting or otherwise protecting data when transferring data (across borders) etc.).

In light of the GDPR, if a firm has any European customers, it would need either to become compliant for its entire user base, or become capable of identifying EU residents within its user base and adhering to GDPR rules for that group only. It will depend on the scale of the mix but it is likely to be expensive and impractical to build and maintain two parallel systems and policies for EU residents and non-EU residents and an incorrect classification could lead to penalties. A GDPR-compliant system, which incorporates local legal requirements, could be the optimal solution. Companies should ensure that the relevant decision makers understand the implications of the GDPR and that all standard agreements and internal policies and procedures that cover data protection issues—including HR policies, IT policies, and any policies affecting individual customers, are reviewed to ensure that they are compliant with both local Data protection law and the GDPR.

Does your company meet personal data security requirements?

B

- What types of personal data does your company collect? In what jurisdiction are the subjects of personal data?
- Are company documents checked internally and independently for compliance with personal data protection legislation?

D

- Have employee personal data protection roles been clearly defined in your company? Has
- Has a legal analysis of the risks related to your company's compliance with GDPR been performed?

- Do your company's internal processes enable it to react quickly and effectively to violations of personal data security comply with applicable law?

C

- Does your company monitor legislation for important changes in personal data security?

How Deloitte can help

The Deloitte Legal team will be pleased to provide you with more detailed advice on any issues that arise after reading this alert. You can find the contact details of our main team members below.

The Deloitte Legal team members will be pleased to provide you with legal advice on personal data security, including:

01 Legal overview of the Company's compliance with personal data protection standards

02 Preparation of a road map to meet personal data protection standards

03 Drafting of legislative compliance policies with respect to personal data protection

04 Legal consulting on personal data protection issues

- The Special Legal Alert provides an in-depth analysis of the most significant amendments and changes planned to be introduced into legislative acts regulating business across a wide range of sectors. Our main objective is to inform our active and potential clients of the new developments in various areas of law.
- Deloitte is not responsible or liable for the use of the information contained in the Special Legal Alert.
- The information contained in the Special Legal Alert contains comments and conclusions based exclusively on information received from open sources.
- Even though the Special Legal Alert covers topics of a legal nature, it is not a legal conclusion on any of the issues discussed in it.
- The aim of the Special Legal Alert is to provide information of a general nature. Deloitte does not accept management decisions for anyone having read the Special Legal Alert, and also does not take responsibility for any decisions taken based on the details provided in the Special Legal Alert. Our conclusions are of an exclusively informative nature. Anyone having read the Special Legal Alert will be responsible for any decisions taken to implement or refuse to implement recommendations and advice, if contained in the Special Legal Alert.

Contact Us:

Almaty/Astana

Agaisha Ibrasheva
Tel.: +7(727) 258 13 40
Fax: +7(727) 258 13 41
Email: aibrasheva@deloitte.kz

Viktoriya Tyan
Tel.: +7 (717) 258 03 90
Fax: +7 (717) 259 14 09
Email: vtyan@deloitte.kz

Caroline Armitage
Tel.: +7 (717) 258 03 90
Fax: +7 (717) 259 14 09
Email: carmitage@deloitte.kz

deloitte.kz