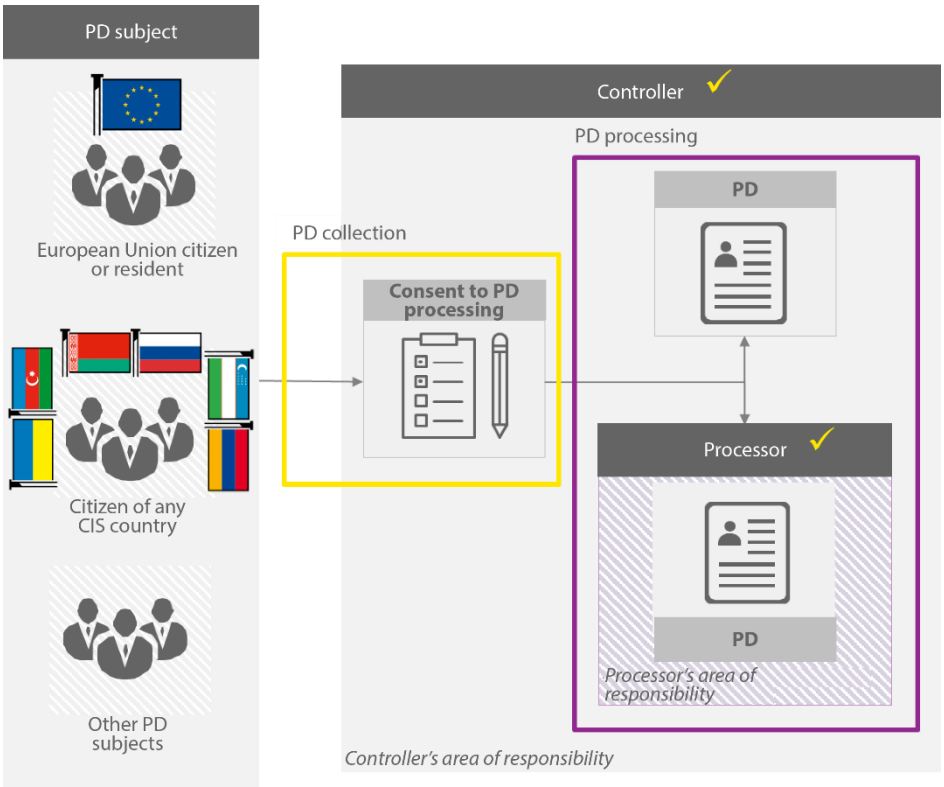
GDPR Impact on the Operation of EU Non-Resident Companies: New Personal Data Handling Procedure

On 25 May 2018, the mandatory EU General Data Protection Regulation (the "Regulation" or "GDPR") was enacted to harmonize the protection of fundamental rights and freedoms of individuals in terms of data processing and free movement of personal data ("PD") between EU member states. The Regulation has completely superseded old Directive 95/46/EC that used to be bedrock of European regulation in the field of personal data for over 20 years.

Considering that the Regulation is a complex regulatory legal act abounding in technical rules and having an extraterritorial effect, EU non-resident companies whose services are nonetheless geared toward the European market are urged to go through the provisions of the Regulation in detail.

BASIC DEFINITIONS OF THE REGULATION

Below you can find a diagram showing the parties involved in PD processing according to the language of the Regulation.



The "controller" determines the objectives and methods of PD processing carried out thereby either by its own means or by involving a third party, while the "processor" processes PD on behalf of the controller and acts strictly in accordance with the controller's instructions.

ANALYSIS

1.1 General Overview of the Regulation Key Requirements

Observance of PD subjects' rights, in particular, notifying the subjects on the details of their PD processing; providing access to these data; correcting and destroying the said data; complying with restrictions on the processing of such data; ensuring data portability (i.e. the rights of a PD subject to obtain PD associated therewith in a structured, universal and machine-readable format, and subsequently transfer them to another controller freely); keeping records of objections against the storage of PD, as well as against any decisions regarding the subject that are solely based on automated PD processing.

Notification of the supervisory authority on PD breach[1]. In the event of PD breach, the controller shall notify the competent supervisory authority within **72 hours** after the controller has become aware of it. Any breach, as well as all related facts, consequences, and corrective measures taken should be documented.

Transparency of PD processing[2]. Any information about the purposes, methods and amounts of PD processing should be stated as simple as possible.

The Consent to PD processing[3] should be expressed in the form of a statement or in the form of straightforward proactive actions on the part of the subject. The consent to PD processing will be invalid if the subject has had no choice or has not been able to withdraw his/her consent without harming himself/herself.

Data export[4]. In accordance with the Regulation, transferring PD outside the European Union is allowed only to entities within the group, or third-party counterparties outside the European Economic Area, only if the country wherein the recipient of such PD is located ensures an adequate level of PD protection.

Data processing records[5]. Each controller and, if applicable, the controller's representative should keep records of any activity related to PD processing within its area of responsibility.

Appointment of a representative[6]. If the controller or processor based outside the European Union processes PD of subjects located in the European Union, and the PD processing activities of such controller or processor are related to the supply of goods or services, or monitoring of PD subjects' activities in the European Union, then the controller or processor should appoint a representative in writing[7]. However, the appointment of such a representative does not affect the responsibility of the controller or processor in accordance with the Regulation. The designated representative should be subject to enforcement proceedings in the event of non-compliance by the controller or processor.

[1] Article 33 of the Regulation
[2] Articles 5, 6, 9, 10, 85 and 89 of the Regulation
[3] Clause 32 of the Recitals of the Regulation, Article 7 of the Regulation
[4] Articles 44 to 50 of the Regulation
[5] Article 30 of the Regulation
[6] Article 27 of the Regulation
[7] Unless the data processing (i) is occasional; (ii) includes the processing of large amounts of special category PD or PD related to criminal sentences or criminal offenses; (iii) and may put the rights and freedoms of individuals at risk, considering the nature, context, scope, and objectives of data processing, or if the controller is a public agency.

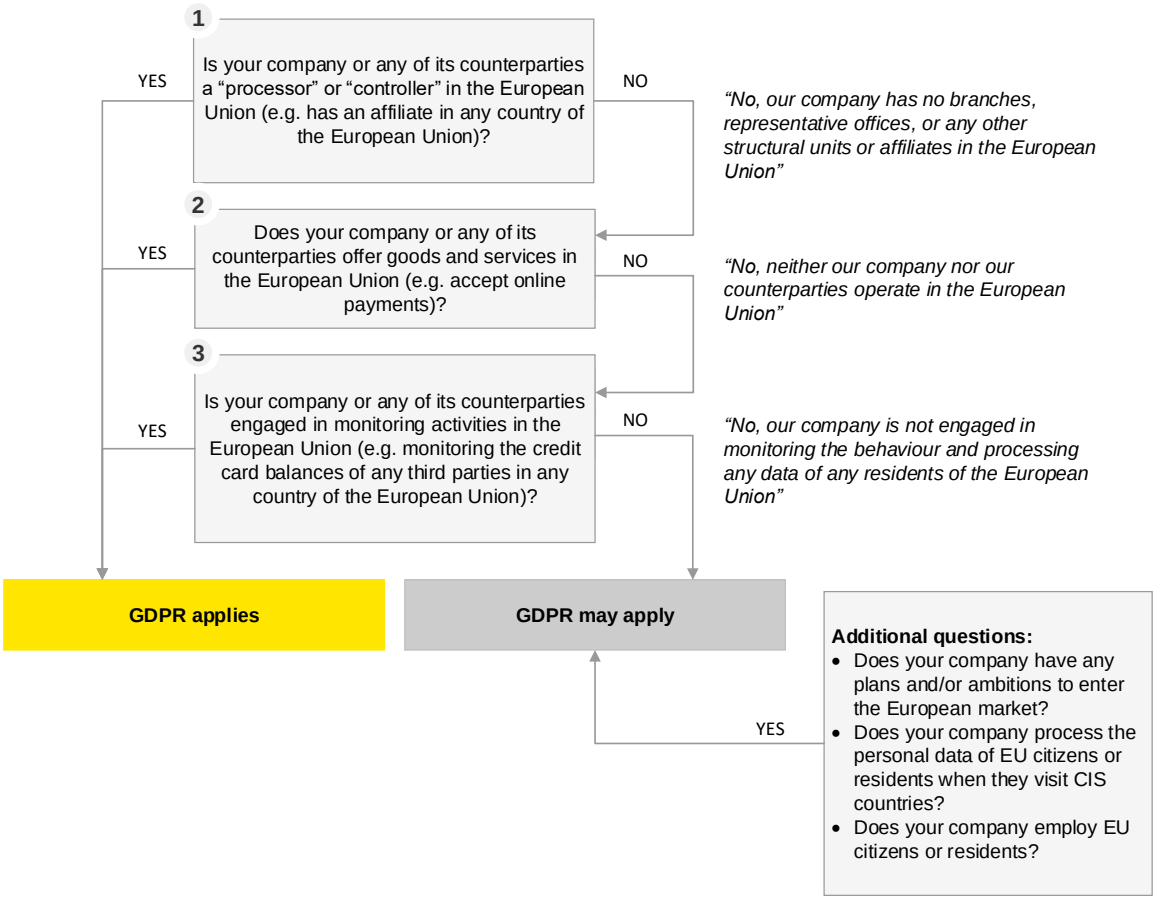
Documentation of data processing. Adoption and execution of PD storage and protection policy (including the data breach response and notification procedure), notification on PD processing (including notification of buyers, customers, employees, etc.), PD subject consent forms. This list is not exhaustive.

1.2 Extraterritorial Effect of GDPR — Applies Outside the European Union

As a general rule, the Regulation applies to any PD processing operations in the context of their controller's or processor's presence in the European Union, irrespective of the place (country) of actual processing.

However, the Regulation has extraterritorial effect and applies to all companies that process PD of EU residents and citizens, irrespective of the territorial location (registered office) of this company and irrespective of the processing conditions.

The algorithm to determine the applicability of the Regulation requirements to the company's activities is provided below for reference:



One of potential risk scenarios, inter alia, is when a company has a website translated into one or several official languages of the European Union member states, the possibility of accepting payment for services in one of the official currencies of the European Union, a reference to consumers or users located in the European Union.

The Regulation also applies to PD processing by a controller that is based outside the European Union and yet is under the jurisdiction of an EU member state under international law (e.g. diplomatic mission,

consulates), in other words, if the company has assigned PD processing or transferred PD to the territory of EU member states.

Applicability: some cases

In practical terms, the GDPR covers any companies that are "geared" toward the market of EU countries as a potential market for their products or services. For example, a manufacturer is based (registered) in a CIS country, but sells products to EU citizens through a website that has versions in European languages and provides an option to pay for the goods purchased online with credit cards, including in foreign currency.

Another example is a company that is registered in a CIS country and has a subsidiary in an EU country. For example, a Kazakh bank has a subsidiary in the European Union doing business in the EU and involving EU citizens. Obviously, in this case, the Kazakh bank's subsidiary must comply with the requirements of the Regulation. However, if EU citizens' PD are transferred between the Kazakh bank's subsidiary and the Kazakh bank to be ultimately processed and stored in the Kazakh bank, then the Regulation requirements will equally apply to the Kazakh bank.

Another example is monitoring PD subjects' activities in the European Union by tracking the user's geo-location through a mobile app in order to advertise events in the relevant location. The company that owns the mobile app will fall within the Regulation requirements even if it is based (registered) outside the European Union.

1.3 Consequences of Failure to Comply with the Regulation Requirements for EU Non-Resident Companies

Sanctions

The list of sanctions for failure to comply with the provisions of the Regulation provides for penalties and other legal measures that can be applied either individually or cumulatively.

Depending on the type of violation, the Regulation establishes two thresholds for fine amounts:
- A fine up to 20 million euros, or up to 4% of the total annual turnover (whichever is bigger);
- A fine up to 10 million euros, or up to 2% of the total annual turnover (whichever is bigger).

When determining the final fine amount, various factors should be taken into account, including, but not limited to: nature, severity and duration of the offense, measures taken by the controller or processor to mitigate the damage suffered by PD subjects, history of violations on the part of the controller or processor.

It should be noted that any PD subject may file a complaint with the supervisory authority, or seek remedies in court, if the subject considers that his/her rights under the Regulation have been violated during the processing of his/her PD.

Some legal precedents when legal entities were held liable for failure to comply with the provisions of the Regulation are as follows:

An audit of a healthcare provider in Portugal revealed unrestricted access of personnel to patients' data. The healthcare provider was ordered to pay a fine for failure of its in-house policy to restrict access to patients' PD adequately. The fine amounted to 400,000 euros, but was challenged later on.

A German company was ordered to pay a fine of 20,000 euros, when an investigation of a data leak caused by a hacker attack established that the company did not use any software facilities to safeguard (encrypt) data.

Another German company was ordered to pay a fine of 50,000 euros for collecting redundant PD that were not required to provide services.

Furthermore, an Austrian company was ordered to pay a fine of 4,800 euros for using video surveillance and inadequate notification of PD subjects thereof.

Reputational Risks

Given the amounts of fines established for failure to observe the requirements of the Regulation, any precedents thereof are highly likely to attract media attention and, therefore, affect the company's reputation and attitude to such company, its products, and services on the part of both existing and potential customers and counterparties. In this context, EU resident companies will obviously be highly motivated to limit their focus to those foreign partners who are ready to ensure compliance of their business processes with GDPR requirements.

In addition, we would like to draw your attention to the fact that any resolutions of the Data Protection and Privacy Commissioner are publicly available on the Commissioner's website in full.

1.4 Possible Impact of GDPR on National PD Laws in CIS Countries

The European Union member states are obliged to "transform" their national laws in line with the Regulation requirements. Given the well-established economic ties with EU business, we assume that PD laws in CIS countries may ultimately be revised so as to eliminate the most critical collisions between the current legal requirements and the provisions of the Regulation. That said, this sort of harmonization may require significant amendments in the national laws of CIS countries.

In practice, the enacted Regulation translates into an additional burden due to the need to take the European regulation into account concurrently with complying with the requirements of national laws for companies in CIS countries whose activities are related to PD processing and focus on the users from and in the European Union.

1.5 Recommended Approach to GDPR for the Company (Involving Interested Parties: Business, IT, Compliance)

The GDPR is a piece of legislation where 75% of the content is accounted for by technical requirements and, therefore, it suggests a comprehensive restructuring, and a major upgrade of all of the company's systems involved in PD handling in one way or another.

A tentative check list of the necessary steps is provided below to assess the effects of the Regulation requirements on the company's activities:

- Identifying the processes and systems that use EU citizens' PD
- Compiling a register of operations and keeping records of all activities related to PD processing (records should include, among other things, the contact details of the controller and processor, categories of PD, PD subjects, processing, information on cross-border transfer, general description of technical and organizational security measures, etc.)
- Assessing the privacy violation risks for critical PD processing operations

- Assessing the non-conformities to the Regulation requirements: identifying the processes and systems requiring changes to comply with the Regulation (GAP analysis/Regulation compliance audit)
- Preparing a program to introduce the Regulation which includes a review of existing procedures and documents concerning the relations with customers, employees, and third parties that can exchange PD with the former and/or be provided with access to PD by the former
- Determining the need to appoint a person responsible for data protection and organizing an in-house PD protection management system

The effort to build a PD protection system that meets all of GDPR requirements independently will require major financial investments and time inputs. In the meantime, these steps can be implemented both through the company's own effort and through the effort of third parties (outsourcing), which may take a part of the load from the company. In order to design and implement technical solutions to comply with the Regulation requirements, it is advisable to use the services of advisors with this sort of experience and international vendors possessing the technologies and services, including information security, data privacy protection, and breach prevention technologies, that meet the Regulation requirements to the fullest extent. Assigning a number of technical PD processing functions to a third party ("processor", as defined in the Regulation) will not indemnify the operator itself ("controller", as defined in the Regulation), but it will reduce the operational risks of the latter and provide an opportunity to comply with the Regulation requirements better.

Restrictions and Use

The findings contained in this document are based on our understanding and interpretation of the provisions of Regulation (EU) 2016/679 of the European Parliament and Council of the European Union, as well as on the published official instructions and recommendations thereto. These instruments can be amended at any time. Obviously, we cannot foresee neither the time nor the essence of such amendments, and yet we have no information at this point indicating that any such amendments that could significantly affect our conclusions are being prepared.

We will not revise the findings presented herein should such amendments be introduced, unless we receive a special offer to do so.

These comments have been prepared for the use by Microsoft Kazakhstan only, and no other individual or legal entity may rely thereon.