Olga N. Tsiptse
25-05-2021

Personal Data transfer in the era of EU General Regulation for Data protection and the new EU-China Comprehensive Agreement on Investment

CAI (Comprehensive Agreement on Investment) is one of the most important Agreements of the last years, in reference to economy of both EU and China and is considered as the most ambitious Agreement that China ever has signed.
As it is already said, examples of market access by China are
-manufacturing,
-automotive sector,
-financial services,
-health,
-maritime exports etc
but some of the fields also are computer science, telecommunication and cloud services
https://ec.europa.eu/commission/presscorner/detail/el/ip_20_2542

All these actions, fields of economy and decisions include data transfer from and towards EU, decision making, profiling and monitoring. That means that many data of EU citizens are going to be processed outside EU, no matter their role as data subjects, employees, client, vendors etc
That further means that any of the participants in that Agreement in any way shall be well aware and have the knowledge -or at least have team of specialist with them, lawyers / ITs etc - of the most severe, difficult and highly effective to economy EU GENERAL REGULATION for data protection, in short GDPR!!! (EU Regulation 2016/679).
So we have article 44, GDPR

The above mentioned Regulation with the high fines of article 83, GDPR for non compliance towards it, is something that will bother strongly all of the CAI participants in any way, because as is mentioned in article 3, GDPR :

"Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

a.the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

b.the monitoring of their behaviour as far as their behaviour takes place within the Union.

3.This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law."

We could say many things about all Regulation but that would take 80 hrs of non-stop speaking so we will focus on the issues that we shall have in mind and start with them.
As I mentioned the sever administrative (and not only administrative) fines that GDPR threatens in article 83, we shall focus on that:

“Infringements of some of the GDPR provisions shall, …, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher or for some other provisions of GDPR will be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher”

BUT GDPR Is not only THREAT OF FINES!
Is something more wide and more deep!
Is about PROTECTION OF PRIVACY AND PERSONAL DATA PROTECTION!!! Which are fundamental Human Rights for all EU CITIZENS (article 7-8 EU Charter of Fundamental Rights & Convention 108 +)

Unfortunately I can not further analyze the definitions, that anyone who processes data shall be aware, even the data controllers and processors outside EU, that processes personal data but in article 4, GDPR are these Definitions mentioned.

GDPR was set into force EXACTLY 3 years ago in 25th of May, 2018, though it was issued in 2016. These 2 years of adjustment shows to all that it is a really very strict Regulation that applies homogeneously in all EU Member States. Each country has its Data Protection Authority but there is the European Data Protection Board in Brussels, that set all the Guidelines.

And now we leave all these general provisions and references, because the provisions that shall play huge role in CAI, are those of Chapter 5 GDPR articles 44-50.
Transfers of personal data to third countries or international organisations

In General after all, we live in a global environment and data transfers outside EU is a very often situation.
All these actions and transfers, though SHALL BE LAWFUL and the data processing shall take place only if there is one of the LEGAL BASIS Gdpr provides and in the protection frame that is referred to GDPR, meaning:

-either Adequacy Decision, like the one that used to be between EU and US Privacy Shield This is a decision that the legal framework in a particular country or territory provides 'adequate' protection for individuals' rights and freedoms for their personal data. So far, the Commission has recognised Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay as providing adequate protection. Adequacy talks are ongoing with South Korea.,

-or Binding corporate rules,

-or Standard Contractual Clauses that are edited by DPAs or EDPB, this moment we are waiting the new SCCs from EDPB that were a few months ago in public consultation,

-or Code of Conducts/ Ethics,

-or certification mechanisms

As we said above, the strong financial, trade and other relationship between EU and US, lead to the creation of PRIVACY SHIELD, for safe transfer of data EU citizens towards US. Unfortunately, SHREMS Decision (C-311/2018 DATA PROTECTION COMMISSIONER vs Facebook Ireland & Schrems) invalidated that Privacy Shield decision 2016/1250, for the reasons mentioned in Schrems Decision. So any data transfer towards US from EU is NOT lawful! And until now the issue is not resolved.

The second problem was SCHREMS II decision that hit again in 16th July, 2020:
Two popular data processes were ruled illegal by the Court of Justice of the European Union (CJEU). This case is known as "Schrems II", and the ruling is not appealable. The two data processing activities are:
• Processing EU data by cloud service providers or other processors
• Providing non-EU companies access to EU data for business-related processing

The Risks from that Decision for the Businesses, Executives, and Boards are Disruption, Losses and Liability:
- penalty for non-compliance with Schrems II is immediate termination of access to data, not fines.
- disruption to operations from terminated access to data
- revenue, and stock value.

The burden of proof for compliance is on an organisation in order to regain access and use their data.

Of course, all the above are not effective only to data transfers between EU and US but it is a good example to see the practical apply and the consequences of GDPR and non compliance to that especially when the data transfer in 3rd to EU countries is not LAWFUL!!!

The European Data Protection Board (EDPB) has published some recommendations for complying with Schrems II: eg. The EDPB recommends transforming data into a new protected format called "GDPR Pseudonymization". Also, the EU Cybersecurity Agency (ENISA) has established best practices for GDPR Pseudonymization.

I would like to make a reference to the second protection frame that I mentioned above the SCCs.

On 12 November 2020, the European Commission published a draft Implementing Decision on standard contractual clauses for the transfer of personal data to third countries, along with its draft set of new standard contractual clauses.

The draft Implementing Decision explains that the SCCs previously adopted by the Commission needed to be updated due to new requirements in the GDPR and developments in the digital economy.

The New SCCs combine general clauses with a modular approach.

Controllers and processors should use the general clauses and, in addition, select the modules applicable to their situations. The modules vary based on the transfer scenario and designation of the parties under the GDPR and distinguish (1) controller-to-controller transfers; (2) controller-to-processor transfers; (3) processor-to-processor transfers; and (4) processor-to-controller transfers. This approach tailor the obligations and responsibilities.

And of course, The New SCCs may be used for transfer of personal data to a sub-processor in a non-EEA country.

These points, were my contribution to that new Agreement that shall be subject of interest of the Agreement players

THANK YOU VERY MUCH Olga N. Tsiptse