THE “SCHREMS II” CASE AND WHAT IT MEANS FOR SOUTH AFRICA

Category: Commercial Law,Privacy Law, Infosec, and POPIA,Technology Law
written by Delphine Daversin | October 5, 2020



On the 16th of July 2020, the Court of Justice of the European Union (“**CJEU**”) invalidated the EU-U.S. Privacy Shield. he EU–US Privacy Shield was a framework regulating exchanges of personal data for commercial purposes between the the European Economic Area (“**EEA**“) and the United States. The CJEU further decided that the standard contractual clauses (“**SCC”**) adopted by the European Union Commission are still valid, but there must be protections in place in the third country to which data are transferred, more specifically as far as access by public authorities and judicial redress is concerned. This decision, named the “Schrems II” decision, was long awaited by all privacy professionals and businesses relying on cross border data transfers.

This is a major development for cross-border data transfer and thousands of companies across the globe will be impacted in their daily operations.

SCCs are the most popular data transfer mechanism. SCCs are used as a contractual mechanism by importer and exporter of personal data outside of the EEA, as authorised by article 46 (2) (c) of the General Data Protection Regulation (“**GDPR**”). Though SCCs remain a valid mechanism, the CJEU decided that they are not sufficient *per se* to guarantee that the transfer meets the requirements imposed on the exporter by the GDPR. Additional safeguards, beyond the SCCs, may be required. This is applicable, not only to data export to the US, but to any transfer relying on the SCC mechanism. Therefore, the exporter using SCCs will have to consider the law and practice of each country to which data will be transferred, especially if public authorities may have access to the data. The Schrems II decision requires that the data importer inform the data exporter of any impossibility to comply with the SCCs.

Further to the judgement, the European Data Protection Board provided the following guidance: “*You can contact your data importer to verify the legislation of its country and collaborate for its assessment. Should you or the data importer in the third country determine that the data transferred pursuant to the SCCs or to the BCRs are not afforded a level of protection essentially equivalent to that guaranteed within the EEA, you should immediately suspend the transfers. In case you do not, you must notify your competent supervisory authority*”. The data exporter will have to suspend the transfer of data or to terminate the contract with the data importer if security safeguards as provided

in the SCCs can, in practice, not be enforced.

As far as South Africa is concerned, enactment of the Protection of Personal Information, Act, 4 of 2013 ("**POPIA**") on 1st of July is good news as it reinforces the protections in place for data exported from EEA to South Africa. However, certain legislations, such as the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 ("**RICA**") will have to be carefully assessed in view of the Schrems II case, where transfers of personal information from EU to South Africa are at stake. Indeed RICA regulates, among other things, the interception of communications and the provision of communication-related information in the records of telecommunication services providers. It is worth noting that flaws in the balance between RICA surveillance provisions and the constitutional right to privacy have been brought to Court by the amaBhungane Centre for Investigative Journalism and journalist Sam Sole. The Judge declared RICA invalid on these grounds. The invalidity has however been suspended for two years to allow South Africa's parliament to remedy all defects. Please read Lucien Pierce's article to know more about this case.