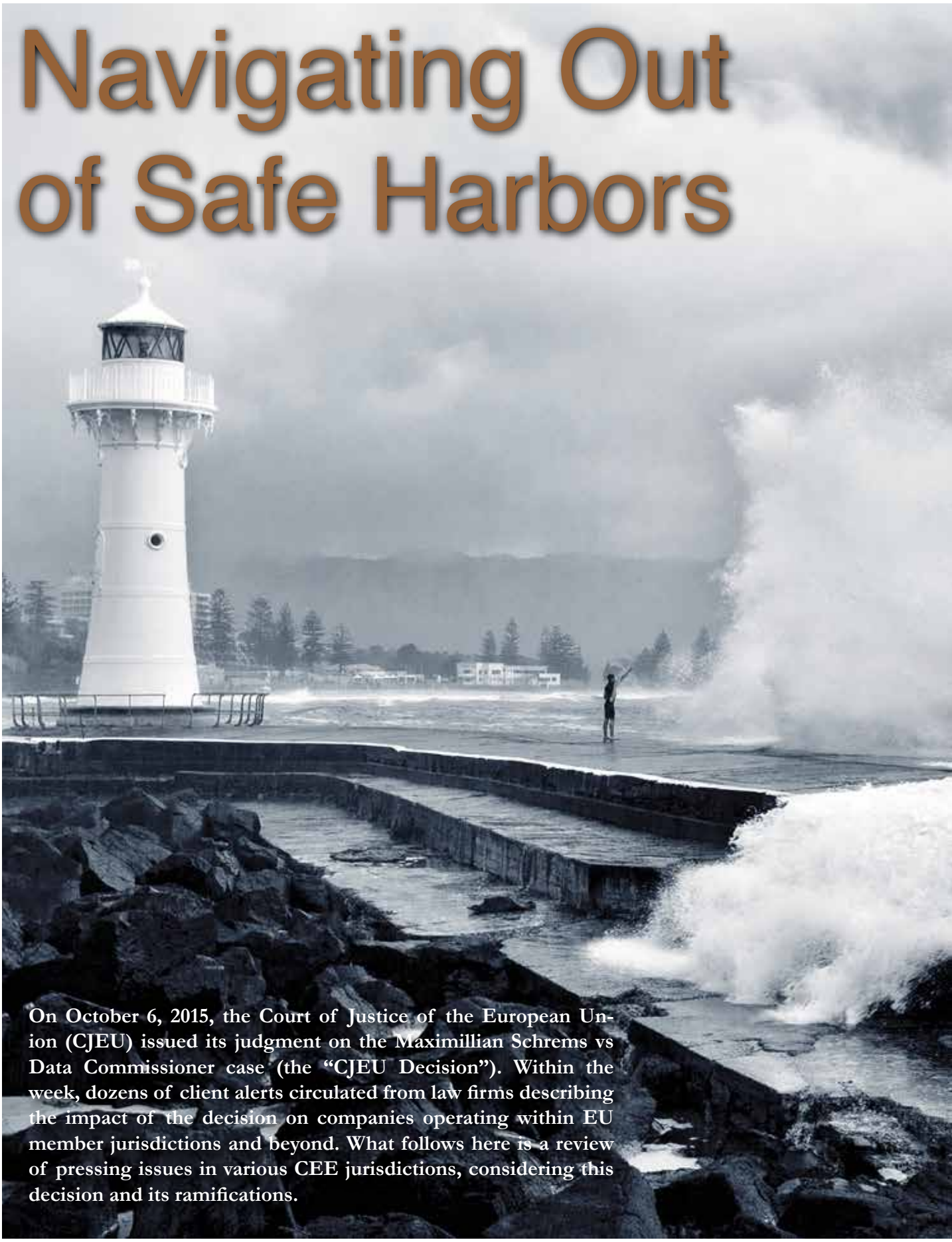
Year 2, Issue 5
October 2015

CEE Legal Matters

In-Depth Analysis of the News and Newsmakers That Shape Europe's Emerging Legal Markets

Navigating Out of Safe Harbors



On October 6, 2015, the Court of Justice of the European Union (CJEU) issued its judgment on the Maximillian Schrems vs Data Commissioner case (the "CJEU Decision"). Within the week, dozens of client alerts circulated from law firms describing the impact of the decision on companies operating within EU member jurisdictions and beyond. What follows here is a review of pressing issues in various CEE jurisdictions, considering this decision and its ramifications.

An Austrian Against Facebook

In 2000, the European Commission issued Decision 2000/520/EC, outlining a series of Safe Harbor principles involving the protection of data. Based on self-certification that they were ensuring the level of protection required by 2000/520/EC, approximately 4,500 United States companies, including Google and many other IT giants, were allowed to legally transfer user, customer, or employee data.

The CJEU case began when Austrian law student Max Schremps addressed "the state institution of Ireland" – the Data Protection Commissioner, or DPC – "requesting to terminate the routing of his personal data from Facebook Ireland to the servers of Facebook Inc. situated in the US." Schremps claimed that the presumed access of several federal agencies in the United States to his personal data indicated that the country could not adequately ensure its protection. Indeed, as Milan Samardzic, Partner, and Nikola Kasagic, Senior Associate at Samardzic, Oreski & Grbovic noted in an article published in the Thought Leadership section of the CEE Legal Matters website, "in light of Edward Snowden's leaks regarding mass surveillance of personal data by the National Security Agency, it was clear the US is not capable of adhering to the strict requirements set out in European regulations."

No More Safe Harbor

According to Detlev Gabel, Partner at White & Case, the CJEU Decision has two components: First, the court declared the original 2000/520/EC Commission decision invalid. Second, the court ruled that a decision of the EC declaring the protection of personal data provided by a third country adequate cannot "eliminate or even reduce the powers available to the national supervisory authorities under the Charter of Fundamental Rights of the European Union and the Data Protection Directive," meaning that national authorities retain the power to "examine with complete independence" whether data transfer to a third country complies with the Directive.

While Gabel points out that both the EC and national data protection authorities "are expected to issue guidance for businesses affected by the judgment shortly," companies are left in limbo during the interim.

US Reaction

On the day of the ruling, US Secretary of Commerce Penny Pritzker released the following statement in response to the European Court of Justice decision surrounding the Safe Harbor Framework: "Since 2000, the Safe Harbor Framework has proven to be critical to protecting privacy on both sides of the Atlantic and to supporting economic growth in the United States and the EU. We are deeply disappointed in today's decision from the European Court of Justice, which creates significant uncertainty for both US and EU companies and consumers, and puts at risk the thriving transatlantic digital economy. Among other things, the decision does not credit the benefits to privacy and growth that have been afforded by this Framework over the last 15 years.

For the last two years, we have worked closely with the European Commission to strengthen the US-EU Safe Harbor Framework, with robust and transparent protection, including clear oversight by the Department of Commerce and strong enforcement by the US Federal Trade Commission.

The court's decision necessitates release of the updated Safe Harbor Framework as soon as possible.

We are prepared to work with the European Commission to address uncertainty created by the court decision so that the thousands of US and EU businesses that have complied in good faith with the Safe Harbor and provided robust protection of EU citizens' privacy in accordance with the Framework's principles can continue to grow the world's digital economy."

We reached out to several CEE experts for comments about the state of affairs as we went to print in mid-October.

Austria

Axel Anderl, Partner at Dorda Brugger Jordis, explained that, in Austria, the Authority "is working on a solution/proposal [as to] how to cope with the logical consequences of the decision which is that all data transfer to US has to be approved," but that there had been no "official announcement, yet." As to the transition, Anderl said, "although from a strict legal perspective, any data transfer to the US initially based on Safe Harbor has to be stopped immediately, we assume that there will be some kind of regulated approval proceedings to (quickly) legalize the existing transfers. The Authority usually establishes a more pragmatic approach due to the expected heavy workload, as multiple Austrian data controllers currently use US data processors."

Bulgaria

Desislava Krusteva, Senior Associate and Senior Legal Expert at Law and Internet Foundation with Dimitrov, Petrov & Co., explained that the CJEU Decision "does not come as a surprise" in Bulgaria. Krusteva explained that "in its practice the Bulgarian Personal Data Protection Commission (PDPC) has already started to limit the application of the Safe Harbor agreement" and pointed to several instances where "the PDPC has disregarded this EU instrument and has stated in its opinions that in case of data transfers to a Safe Harbor company, prior approval from the PDPC is required in order to ensure an adequate level of protection of the transferred personal data."

While this limitation in Bulgaria, had, before the CJEU's decision, been "symptomatic and controversial as contradicting to the provisions of Decision 2000/520/EC," in the aftermath of the CJEU judgment, "it is definitive." As a result of this, Krusteva explained: "Performing data transfers to entities located in the US only on the grounds of the invalidated Safe Harbor scheme bears a high risk of sanctions."

Krusteva emphasized that "for all data controllers in Bulgaria currently it is highly recommended to reconsider the mechanisms used for data transfers to the US in case those transfers are based solely on the fact that the companies-recipients of data are certified under the Safe Harbor scheme. Depending on the structure of the cross-border data transfer, such mechanisms may include: using standard contractual clauses which, according to the European Commission, offer sufficient safeguards to data protection in case of transfers; undergoing an authorization procedure for data transfers to the US; and others."

Croatia

The Croatian Data Protection Authority (AZOP) seems to have acted more quickly than most authorities following the CJEU Decision. Olena Manuilenko, Head of Intellectual Property at Divjak, Topic & Bahtijarevic, pointed out that AZOP immediately issued an initial guidance available on its official website in Croatian. She explained that, according to AZOP, "any transfer of personal data of Croatian data subjects will have to be based either on the data subjects' consent or a data transfer agreement pre-approved by the national DPA, or another available statutory derogation, depending on the circumstances of each case. It is worth mentioning that data transfer agreements based on the EU Standard Contractual Clauses will also have to be submitted to the national DPA for review and approval prior to any data processing or transfer." To add to the challenge, a Croatian translation of the agreements will be required. Manuilenko added: "Companies affected by the ECJ decision may consider adopting the Binding Corporate Rules" – internal rules such as a Code of Conduct – "which would also be considered a sufficient guarantee of the adequate level of personal data protection."

Until approval is obtained, the law does not allow transfers, according to Manuilenko, with potential liability for privacy violations, whether at the misdemeanor level (fines) or criminal level (for directors, managers and the company). She added: "Since the companies who have relied only on Safe Harbor will now have to align their data processing in accordance with the new circumstances, there should be a leniency period, but there is no official guidance about it yet."

Baltic States

"So far Baltic companies, as well as national data protection authorities, all appear to be in a 'wait-and-see' mode," said Pirkko-Liis Harkmaa, Partner at Cobalt, who noted that she had not yet faced many inquiries from clients worried about the CJEU Decision. She reported that "at the moment it seems that none of the Baltic data protection authorities has or is ready to issue their official positions and appear to wait for the Article 29 Working Party uniform guidance."

In Estonia, according to Mihkel Miidla, Senior Associate and Head of Technology & Data Protection at Sorainen, "from now on a prior authorization from the Inspectorate has to be obtained to transfer personal data to the US. The data exporter must demonstrate that it has a valid legal basis to process the personal data and that a sufficient level of data protection is guar-

anteed in the US for that specific case of data transfer." Miidla explained that the exporters of the data can "generally rely on data transfer agreements that are based on EU Model Contracts or Binding Corporate Rules."

There are a few exceptions for which an authorization from the Estonian Inspectorate is not needed, according to Miidla: "(1) If the data subject has provided a valid consent for the specific transfer to take place; (2) Where the transfer is necessary for the protection of the life, health, or freedom of the data subject or another person if obtaining the consent of the data subject is impossible; or (3) If a third person requests information obtained or created in the process of performance of public duties and the data requested do not contain any sensitive personal data and access to it has not been restricted for any other reasons."

"There is a great deal of uncertainty regarding how quickly [companies] should implement new measures and obtain a relevant authorization for transferring personal data to the US," explained Miidla. "On one hand it is clear that the Safe Harbor principles can no longer be relied upon and the data exporters have to implement new measures for the transfers but on the other hand it is also unlikely that the Inspectorate will now direct its resources into active supervision over data controllers who are likely transferring personal data to the US. There is no official guidance available from the Inspectorate on this issue. It is expected that the Inspectorate will soon update their non-binding guidelines on data transfers."

At the end of the day, Harkmaa reported out that the Inspectorate "has expressed an opinion that the CJEU Decision does not have a major impact on Estonia and sees that the most probable aftermath of the decision is that the legal costs of companies would rise due to the need to draft model clauses and internal rules. In practice, many companies also have, in parallel to the Safe Harbor exception, relied on model clauses and DPA [Data Privacy Authority] approval or data subject consent, so in most cases the abolishing of the Safe Harbor exception does not affect them."

In Latvia, Harkmaa said, while "companies have started to show interest in how to react to the decision," in fact companies in that country that have transferred data to the US were already going beyond the requirements of the safe harbor exception, so the potential impact on Latvian companies was not particularly large.

In Lithuania as well, according to Harkmaa, "the unofficial Data Protection Authority's opinion appears to be that the CJEU Decision would be relevant for data transfer permit applicants that have based their application on the Safe Harbor exception only, [but] in practice and according to the DPA's knowledge this might have been the case with very few applicants. Others have provided model clauses, etc." Harkmaa added that the unofficial recommendation from the Lithuanian DPA to data controllers, "is to cease transfer as of the CJEU Decision day or to urgently agree on model clauses to ensure the adequate privacy protection." She noted that this is in contrast to the Estonian and Latvian DPAs, which "have expressed no such radical recommendations."

Harmaa said that: "Local companies who belong to multinational groups where certain employee or customer data is being held in centralized databases in servers in US, or local companies who use service providers who retain data in servers in US, are recommended first to inquire how the relevant group company or service provider intends to change its practices in light of the ECJ decision and guarantee adequate safety of data transfers and data processing. If appropriate, EU model clauses should be incorporated into existing agreements, or new appropriate contractual arrangements should be put in place or any other suitable allowed measures guaranteeing the adequate level of data protection should be adopted (such as binding corporate rules). Thereafter the process for applying for DPA approval for the relevant data transfer should be initiated." She clarified that "DPA approval may be skipped if the data subjects give their informed free consent to such data transfers, however from the practical point of view this solution could only work in case of companies who need to approach only a few data subjects (e.g. a few employees whose data is being processed in a centralized US database), but would be complicated and not practical in case of mass data transfers."

Hungary

Marton Domokos, Senior Counsel at CMS, says that: "Hungarian companies who have been relying on the Safe Harbor scheme should seek alternative options of safeguarding the privacy of personal data transferred in the US." He added that "Data transfer to the US is possible on the basis of the prior, express, and informed consent of the relevant person; however, as the result of the CJEU's ruling, Hungary's Authority for Data Protection and Freedom of Information (NAIH) may want to review whether a consent contains adequate information on the level of the data protection in the US. Besides an individual consent or intra-group transfers based on BCRs, the only alternative for Hungarian companies is to conclude the so-called EU Model Clauses (based on Commission Decisions No. 2001/497/EC, and No. 2010/87/EU), provided that there is a legitimate interest for the proposed data transfer. Since January 1, 2012, entering into other individual data transfer agreements is not considered as providing 'adequate protection' for data transfers to the US." Otherwise, the Hungarian Authority is itself analyzing the significance of the CJEU Decision. According to Domokos, "in its communication, the NAIH emphasized that it is currently reviewing the tasks that will arise from the ruling in Hungary and will coordinate with other EU data protection authorities." She suggests that "the NAIH may also want to revise its prior position on data transfers outside the EU; in particular, its Recommendation on Data Transfers Abroad dated November 11, 2013 where Safe Harbor was recognized as adequate protection."

Beyond EU Member States

Of course, the CJEU Decision was significant for non-EU jurisdictions as well, with client alerts appearing from law firms in Montenegro, Serbia, and Turkey appearing soon after the Decision was issued.

Conclusion

While ambiguity hovers over companies in many of the countries affected by the ruling, at the end of the day, Harkmaa's words of guidance – though spoken in the context of the Baltic states in particular – reflect the common theme: "Any recommendations that can be given to clients at this moment have to be based on common sense." She commented: "I do not see any reason for immediate panic, and it is highly unlikely that the DPAs would start to impose sanctions for non-compliance without first issuing official guidance and applying a reasonable grace period for bringing data transfer processes into compliance with such guidance."

Radu Cotarcea