THE EU COURT OF JUSTICE DECLARES THE SAFE HARBOUR DECISION INVALID

Contents

Whilst the Court of Justice alone has jurisdiction to declare an EU act invalid, where a claim is lodged with the national supervisory authorities they may, even where the Commission has adopted a decision finding that a third country affords an adequate level of protection of personal data, examine whether the transfer of a person's data to the third country complies with the requirements of the EU legislation on the protection of that data and, in the same way as the person concerned, bring the matter before the national courts, in order that the national courts make a reference for a preliminary ruling for the purpose of examination of that decision's validity .

T**he Data Protection Directive provides that the transfer of personal data to a third country may, in principle, take place only if that third country ensures an adequate level of protection of the data**. The directive also provides that the Commission may find that a third country ensures an adequate level of protection by reason of its domestic law or its international commitments. Finally, the directive provides that each Member State is to designate one or more public authorities responsible for monitoring the application within its territory of the national provisions adopted on the basis of the directive ('national supervisory authorities').

Maximillian Schrems, an Austrian citizen, has been a Facebook user since 2008. As is the case with other subscribers residing in the EU, some or all of the data provided by Mr Schrems to Facebook is transferred from Facebook's Irish subsidiary to servers located in the United States, where it is processed. Mr Schrems lodged a complaint with the Irish supervisory authority (the Data Protection Commissioner), taking the view that, in the light of the revelations made in 2013 by Edward Snowden concerning the activities of the United States intelligence services (in particular the National Security Agency ('the NSA')), the law and practice of the United States do not offer sufficient

protection against surveillance by the public authorities of the data transferred to that country. The Irish authority rejected the complaint, on the ground, in particular, that in a decision of 26 July 20002 the Commission considered that, under the 'safe harbour' scheme, the United States ensures an adequate level of protection of the personal data transferred (the Safe Harbour Decision). The High Court of Ireland, before which the case has been brought, wishes to ascertain whether that Commission decision has the effect of preventing a national supervisory authority from investigating a complaint alleging that the third country does not ensure an adequate level of protection and, where appropriate, from suspending the contested transfer of data.

In this judgment of 6th October 2015, the Court of Justice holds that the existence of a Commission decision finding that a third country ensures an adequate level of protection of the personal data transferred 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 directive.

The Court stresses in this regard the right, guaranteed by the Charter, to the protection of personal data and the task with which the national supervisory authorities are entrusted under the Charter. **The Court states, first of all, that no provision of the directive prevents oversight by the national supervisory authorities of transfers of personal data to third countries which have been the subject of a Commission decision. Thus, even if the Commission has adopted a decision, the national supervisory authorities, when dealing with a claim, must be able to examine, with complete independence, whether the transfer of a person's data to a third country complies with the requirements laid down by the directive. Nevertheless, the Court points out that it alone has jurisdiction to declare that an EU act, such as a Commission decision, is invalid.**

It is thus ultimately the Court of Justice which has the task of deciding whether or not a Commission decision is valid. The Court then investigates whether the Safe Harbour Decision is invalid. In this connection, the Court states that the Commission was required to find that the United States in fact ensures, by reason of its domestic law or its international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed within the EU under the directive read in the light of the Charter. The Court observes that the Commission did not make such a finding, but merely examined the safe harbour scheme. Without needing to establish whether that scheme ensures a level of protection essentially equivalent to that guaranteed within the EU, the Court observes that the scheme is applicable solely to the United States undertakings which adhere to it, and United States public authorities are not themselves subject to it. Furthermore, national security, public interest and law enforcement requirements of the United States prevail over the safe harbour scheme, so that United States undertakings are bound to disregard, without limitation, the protective rules laid down by that scheme where they conflict with such requirements.

The United States safe harbour scheme thus enables interference, by United States public authorities, with the fundamental rights of persons, and the Commission decision does not refer either to the existence, in the United States, of rules intended to limit any such interference or to the existence of effective legal protection against the interference. The Court considers that that analysis of the scheme is borne out by two Commission communications, according to which the United States authorities were able to access the personal data transferred from the Member States to the United States and process it in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection

of national security. **Also, the Commission noted that the persons concerned had no administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased.**

As regards a level of protection essentially equivalent to the fundamental rights and freedoms guaranteed within the EU, the Court finds that, under EU law, legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data is transferred from the EU to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down for determining the limits of the access of the public authorities to the data and of its subsequent use.

The Court adds that legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life. Likewise, the Court observes that legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, compromises the essence of the fundamental right to effective judicial protection, the existence of such a possibility being inherent in the existence of the rule of law. Finally, the Court finds that the Safe Harbour Decision denies the national supervisory authorities their powers where a person calls into question whether the decision is compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals. The Court holds that the Commission did not have competence to restrict the national supervisory authorities' powers in that way.

For all those reasons, the Court declares the Safe Harbour Decision invalid. This judgment has the consequence that the Irish supervisory authority is required to examine Mr Schrems' complaint with all due diligence and, at the conclusion of its investigation, is to decide whether, pursuant to the directive, ***transfer of the data of Facebook's European subscribers to the United States should be suspended on the ground that that country does not afford an adequate level of protection of personal data***

IRISH COURT ORDERS INVESTIGATION OF FACEBOOK DATA TRASFERS TO THE US

Ireland's High Court on Tuesday (20 October) ordered an investigation into Facebook's transfer of European Union users' data to the United States, to make sure personal privacy was properly protected. The court told the Irish Data Protection Commissioner to investigate following the landmark ruling by the European Court of Justice (ECJ) on 6 October, which struck down the Safe Harbour agreement that had allowed the free transfer of data between the European Union and the United States.

Both the ECJ decision and the 20th October ruling were the result of a challenge by Austrian law student Max Schrems, lodged after revelations in 2013 of the US government's Prism programme, which allowed authorities to harvest private information directly from big tech firms like Facebook and Google. The initial challenge was made in Ireland because Facebook has its European headquarters in Dublin and is regulated by the Irish Data Protection Commissioner. Tuesday's ruling overturns the commissioner's initial refusal to investigate.

Facebook will "constructively engage" with any investigation, its barrister Rossa Fanning told the court.

The ECJ ruling has thousands of US and European companies mired in legal uncertainty over the transfer of personal data from Europe to the United States. That includes payroll and human resources information as well as data used for online advertising, which is of particular importance to tech firms. Under EU data protection law, companies cannot transfer EU citizens' personal data to countries outside the bloc deemed to have insufficient privacy safeguards.

Facebook has repeatedly denied providing the US National Security Agency with 'backdoor' access to its servers, and says its data transfer processes have already been audited by the Irish Data Protection Commissioner.

SAFE HARBOUR RULING FOLLOW-UP: WHAT COULD BE THE NEXT IMPACT? WHAT ARE THE DANGERS OF FORCED DATA LOCALISATION?

Forced data localisation would undermine European fundamental rights as well as damaging the EU's competitiveness. Small ideas sometimes change the world. Russia's forced data localisation is a small idea. Now, with the fall of Safe Harbour, a German data protection agency calls for data localisation. Others will follow. But data localisation is a bad idea – a concept to be quashed in any serious political debate on how to resolve Safe Harbour, and trust in Trans-Atlantic relations.

Russia is a former example. Russia's contentious law requires all legal entities to store and process the personal data of Russian citizens on servers located within Russian territory. Russia's data localisation law is an impressive case of how governments justify legal means by political ends without considering the broader implications for the society as a whole. Officially, Russia wants to safeguard its citizens' privacy rights, as a response to Edward Snowden's revelations of NSA mass surveillance activities. Accordingly, and very much similar to the ECJ, the Russian government officially claims that the security of Russian citizens' personal data is one of the fundamental rights that should be protected, legally and otherwise.

According to Russia's forced data localisation law, **which became effective on 1 September 2015**, not only companies based in Russia are affected, but also all businesses that export to or import from Russia. Every piece of personal information concerning suppliers, business partners and customers (irrespective of whether B2B or B2C) has to be stored and processed on databases within Russia. Ironically and contrary to the initial objectives of the government, Russia's data localisation law does not foresee an export ban for personal data. Personal data can be transferred abroad as long as the primary database used for collection, storage and processing remains in or will be transferred to Russia.

Data localisation is not only a matter concerning Facebook, Twitter and Google. Data localisation rules affect every single business from agriculture to manufacturing and services. In fact, the outcry among companies operating on Russian territory is now particularly strong among retail chains, construction materials and automotive suppliers as well as logistics service providers that are more than overstrained with the re-organisation of databases and global business processes in order to comply with vague and poorly written rules, leaving firms with the substantial risk of being sanctioned for non-compliance.

Personal data is absolutely everywhere. It is often impossible to separate or disentangle personal data from other business-related data. This is not only true for enterprise resource planning (ERP) and customer relationship management (CRM) systems. It is also true for Internet traffic that is regarded as unsuspicious. Given that any transaction on the Internet made while logged in to an online account is effectively personal data, even the most harmless pieces of data will contain personal information about employees, business partners and customers.

Forced data localisation effectively benefits big business. It is a striking feature of the Russian data localisation law that it increases complexity and uncertainty. Complexity is always a subsidy to big businesses to the detriment of micro-, small- and medium-sized enterprises. The wording of the provisions is imprecise and the requirements remain vague. The rules do not clarify how to separate personal data from other business-related data. It is left unclear how to identify the citizenship of 'data subjects' based on digital protocols, leaving considerable room for political manoeuvres and discrimination.

But what about the EU? A series of economic impact assessments conducted by ECIPE points to significant economic costs as a consequence of forced data localisation. For the EU 28, the short-term impact triggered by productivity losses and a less European investment is estimated to be 0.7% of EU GDP (€96bn). European countries should expect a shift in production structures towards less innovative and more volatile sectors such as light manufacturing and agriculture. The numerical results of this analysis do not capture the longer-term adverse effects on technological progress, competitive behaviour and the EU's ability to adopt innovative technologies and 21st century business models. These factors are the main drivers of long term economic output growth. Thus the estimates of economic losses are likely to be are likely to be very conservative.

It is becoming increasingly clear that Safe Harbour is not the only legal instrument that was effectively set on hold by the ECJ. The transfer of personal data based on model contract clauses (MCC) and binding corporate rules also violates EU fundamental rights since these measures do not prevent US intelligence services from accessing data without respecting data subjects' privacy rights and available redress procedures. A German data protection

agency just erased explicit consent from the list of options for customers to send data to the US. The ruling is about fundamental rights rather than just a specific treaty. Therefore, the only legally certain options available to corporations would be to localise data within European borders – or to shut all Europeans off from the bulk of digital services.

It would be foolish to question the ECJ's serious concerns about the US government's mass and indiscriminate surveillance practices. However, we should keep in mind the 28 lax and non-harmonised data privacy laws in 28 sovereign member states that are all running their own intelligence units. Does the ECJ also understand that GCHQ, the UK's Intelligence body, is just as bad as the NSA?

For the Safe Harbour, it is hard to see how the European Commission could negotiate a new agreement that would satisfy all the criteria of the ruling, or how the new mechanisms would be beyond the reach of newly instated powers under the ECJ ruling. Yet, it is high time to speed up talks in order to deliver legal clarification. Any delay would increase the scope of interpretation by national privacy law enforcement bodies, leaving considerable room for political manoeuvres, discrimination of domestic and foreign businesses – potentially costing another great deal of trust and confidence in Trans-Atlantic relations.

DATA PROTECTION: TRILOGUE UPDATE BUT ECJ SAFE HARBOUR RULING PUTS EVERYTHING ON HOLD…

On October 12, Jan Philipp Albrecht (Greens/EFA, DE), rapporteur on the draft General Data Protection Regulation, provided an update to the LIBE Committee about the state of play of the trilogue negotiations. According to him it is realistic to expect the draft Regulation to be adopted before the end of the year, though the ECJ ruling is changing the picture. The participants of the trilogue have managed to reach an agreement on approximately 70-80% of the text of Chapters 2, 3 and 4 (concerning the individual' rights and obligations of companies, profiling, data portability, consent, etc.). However, there are still issues to be agreed, including consent and the rules on a data protection officer, and that following the Court of Justice ruling on Safe Harbour the negotiators will have to look again at the sections dealing with international transfers. If the Regulation is adopted in December 2015, it would enter into force at the beginning of 2018, companies would have two years to bring their data processing into compliance.

CONSULTATIONS

Consultation title	Subject	Deadline	Web site
Public consultation on the evaluation and the review of the regulatory framework for electronic communications networks and services.	Assessing current framework and seek views on possible adaptations to the framework in light of market and technological developments, with the objective of contributing to the Digital Single Market Strategy.	7/12/2015	http://ec.europa.eu/digital-agenda/en/news/public-consultation-evaluation-and-review-regulatory-framework-electronic-communications
Public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy.	input for the analysis of the role of online spaces where providers and users of content, goods and services can meet (such as internet search engines, social media, knowledge and video-sharing websites, news aggregators, app stores and payment systems).	17/12/2015	https://ec.europa.eu/digital-agenda/en/news/public-consultation-regulatory-environment-platforms-online-intermediaries-data-and-cloud
Call for evidence: EU regulatory framework for financial services:	The Commission is looking for empirical evidence and concrete feedback on: • Rules affecting the ability of the economy to finance itself and growth; • Unnecessary regulatory burdens; • Interactions, inconsistencies and gaps; • Rules giving rise to unintended consequences.	06/01/2015	http://ec.europa.eu/finance/consultations/2015/financial-regulatory-framework-review/index_en.htm

THE MEMBER STATES CORNER

This item intends to put in the spotlight some trends/initiatives happening on the regulatory front at national level, so that FEBIS members know better what happens in the other EU countries. Each month a particular item from an EU Member State will be picked up and presented, but we need your input to make it lively and accurate, so please send your national info to Stephanie so it can be put up in next FEBIS newsletters!

German Data Protection authority says Model Clauses are no substitute for "safe harbour" data transfers to the US

Businesses relying on European Commission-approved model contract clauses to transfer personal data from the EU to the US should terminate or suspend those arrangements, a German data protection watchdog has said on 14th October 2015.

The Independent Centre for Privacy Protection in the state of Schleswig-Holstein said it was its view that EU-US data transfers facilitated by the use of model clauses fail to comply with EU law. It outlined its opinion in a new position paper published in light of the ruling k by the Court of Justice of the EU (CJEU) that the 'safe harbour' framework for enabling EU-US data transfers is "invalid".

The Safe Harbour Agreement had meant that US organisations that self-certified compliance with the requirements of the safe harbour regime could transfer personal data from the EU to the US because the arrangements were deemed as meeting data protection standards required under the EU's Data Protection Directive.

That framework was ruled invalid after the CJEU, relying on the European Commission's own assessment of material leaked by whistleblower Edward Snowden regarding US intelligence agency surveillance practices, said that there are insufficient restrictions on how the US authorities can use data transferred to the US from the EU. The Court said that the safe harbour regime did not respect privacy in the way required under EU law, raising additional concern about the fact EU citizens do not have a judicial right to redress in the US if their data is mis-handled by US organisations.

The Schleswig-Holstein authority said that when applying the findings of the CJEU's judgment to data transfers made on the basis of model clauses, such transfers are "no longer permitted". It said there needs to be "comprehensive change" to US law to ensure that there is adequate data protection provided for when personal data is transferred from the EU to the US. **The Schleswig-Holstein authority said it plans to review whether to start scrutinising businesses' EU-US data transfer arrangements and check whether any breaches of data protection laws have been committed.** It explicitly referred to its authority to fine companies up to €300,000 for breaking German data protection rules.

National data protection authorities from across the EU are set to meet to discuss the CJEU's ruling under the auspices of the Article 29 Working Party. The views expressed by the Schleswig-Holstein authority will be of concern to many businesses that have been using model clauses for US data transfers or which are now turning to that mechanism in light of the CJEU's ruling on the safe harbour regime.

"It is as yet unclear whether the Schleswig-Holstein authority speaks for itself only or whether their opinion reflects the result of discussions with other of Germany's data protection authorities on this issue. As we first detailed last week, there were just seven cases between January 2014 and mid-August 2015 that the UK ICO looked into which concerned potential breaches of data transfer rules by organisations. Whether it is initiated by the ICO or other regulators, businesses can expect their data transfer arrangements to come in for greater scrutiny in future in light of the CJEU's judgment," an expert said.

"Even if Europe's data protection authorities agree that model clauses are a suitable mechanism for enabling data transfers, businesses implementing them into their contracts should be aware that the clauses give data subjects certain rights of enforcement of the contractual requirements against data exporters, and in some cases data importers, and they also give data protection authorities certain audit rights,"

The position paper also seems to be extreme in the sense that the Schleswig DPA opines that data subjects are actually not in a position to declare valid consent in data transfers to countries where there is a risk of mass surveillance by intelligence agencies, as this would be contrary to the fundamental personality right enjoyed by people in Germany which, the DPA claims, an individual cannot waive, as a matter of legal principle.

Last week deputy UK information commissioner David Smith said that **the CJEU's judgment meant businesses that have relied on the safe harbour framework "need to review how they ensure that data transferred to the US is transferred in line with the law"**. He said, though, that he recognised that review process would take businesses "some time" and stressed that data transfers can take place on the basis of "different provisions".

Smith said the ICO plans to issue new guidance for businesses on data transfers in the coming weeks after liaising with other data protection authorities in the EU. The European Commission has also said it plans to issue "clear guidance for national data protection authorities on how to deal with data transfer requests to the US, in the light of the ruling

FEBIS– Federation of Business Information Services

Benefiting from the opening of markets within Europe and overseas, world-wide business has experienced substantial growth. As business grows so does the demand for business information, in particular, intelligence for cross-border business activities.

In 1973, leading European credit information agencies joined forces to form the Federation of Business Information Services FEBIS (initially known as FECRO), with its registered office in Frankfurt. Today, FEBIS has developed into a sizable organization comprising more than 60 full Members from all over the world involved in providing Business Information and Debt Collection services of National and International importance.

Supported by a combined workforce of more than 20,000 staff, FEBIS Members generate over 180 million Business Information and Consumer reports annually for over 500,000 organizations, providing these clients with invaluable business support. Aggregate sales turnover of FEBIS Members is in excess of €2.5 Billion.

As the industry association, FEBIS strives to look after common interests of its members. While monitoring new legislation like data protection laws and insolvency laws, FEBIS also oversees and the application of public sources and information.