ABA Section of International Law
Your Gateway to International Practice

EUROPE UPDATE

DATA PRIVACY EDITION

Issue 25, February 2018

Message from the Europe Committee

The Europe Committee is happy to present this edition of our Europe Committee newsletter. In this edition of our newsletter we are featuring a series of articles concerning the increasingly important area of data privacy law. The European Union is preparing to implement its General Data Protection Regulation later this spring in an effort to harmonize the protection for individuals throughout the European Union. The co-chairs would like to thank each of the authors for their contribution. We hope that you enjoy reading this edition of our newsletter as much as we have enjoyed preparing it.

We welcome all Europe Committee members who are interested in acting as guest editors to volunteer to organize a future newsletter on a hot topic important to the Europe Committee.

A Note from the Editor

This hot topic issue of EUROPE UPDATE marks my first edition as the Editor in Chief and Vice Chair of Newsletter Publications. This particular newsletter topic is both timely and relevant, and the contributions span a range of topics for all readers with interest in data privacy. I would like to note a special thank you to the former Editor-in-Chief, Michael Balisteri and Jörg Rehder who served as guest editors, and to the committee leadership for their help in soliciting articles for this edition. The contributors to this publication continue to reinforce the role of the Committee in addressing pressing European legal issues, and their pertinence to practitioners in the United States. Thank you to everyone who played a role in getting this issue to publication.

Updates from the Committee

The Section's Annual Conference will be in New York April 17 - 21. We encourage all leadership members to attend one of these upcoming meetings.

This YIR edition discusses select developments in European Law during 2016. Congratulations to Tom Stanton and James Bergeron and all of the other editors for a Year-in-Review well done! The YIR 2018 will be released in the coming months.

Finally, don't forget to join us on our monthly calls, the times and dates of which are distributed through the committee listserv.

Contents

Contributors This Edition

Jorge Alberto Reyes Flores
Founding partner VCR Consultores, S.C.
Laura Butler
Litigation Professional Support Lawyer, Dillon Eustace (Dublin, Ireland)
Vikki Hoyle
Senior Associate, Walker Morris (Leeds, U.K.)
John O'Riordan
Partner, Dillon Eustace (Dublin, Ireland)
Carolien Michielsen
Junior Associate, Stibbe (Brussels, Belgium)
Jörg Rehder
Schiedermair Rechtsanwälte (Frankfurt, Germany)
Daniel Sánchez Cordero Canela
M&A, International Affairs & Regulation, attorney-at-law
Aaron Schildhaus
Counsel, Scharf Banks Marmor LLC (Chicago)
Erik Valgaeren
Partner, Stibbe (Brussels, Belgium)
Mark Weitz
Attorney, Law Offices of Mark Weitz (Los Angeles)

EUROPE UPDATE

About the Europe Committee

The Europe Committee seeks to engage lawyers conducting practices that touch Europe, including the various European countries, the European Union, and the institutions of the Council of Europe. It nurtures a community of lawyers sophisticated in cross-border matters, comparative law, and the continuously emerging transnational law of Europe, public and private. The Europe Committee's activities include the sponsorship of programs at the Section of International Law's seasonal meetings, hot topics teleconferences and newsletter presentations by experts on emerging developments of European law, exploration of legal policy and law reform topics, contribution to the Year in Review issue of The International Lawyer, and co-sponsorship of Section of International Law stand-alone and other programming.

The Europe Committee's membership is its most important asset. We encourage all Committee members to be involved in Committee activities and to communicate freely suggestions and ideas.

Upcoming Events

The following are some of the upcoming Section events:

Employment Law World Tour: Employment Law in France, Switzerland, and the Netherlands
02/21/2018
10:00 AM - 11:00 AM ET
Teleconference
The SIL Employment Committee is embarking on a World Tour of employment law! Our members have volunteered to share their expertise on employment law in their jurisdictions through quick, focused teleconferences that will occur on a regular basis during the 2017/18 season. The teleconferences will follow a uniform format. A presentation of the general principles of employment law will precede brief highlights of hot issues like the gig economy, data security for HR records, discrimination against LGBT workers, and whistleblower protections.

Lifesciences Conference 2018
06/10 - 06/12/2018
Maxwell Chambers
Scandic, Copenhagen
The Section of International Law will host a three-day conference addressing a range of topics touching on lifesciences including European patent package, jurisdiction in life sciences litigation, worldwide clinical trials, artificial intelligence, and ethics.

2018 Section of International Law Annual Conference
04/17 - 04/21/2018
New York, NY
The ABA Section of International Law Fall Conference will feature numerous CLE sessions as well as daily key note luncheon addresses and nightly reception. Attendance is anticipated at over 1,000 individuals. Register before March 2nd to lock in our Early Bird discounts. Hotel reservations must be made before March 24th to be eligible for the reduced bock rates.

German Administrative Court Jumps the Gun in Enforcing the General Data Privacy Regulation

by *Jörg Rehder**

When it comes to data privacy, two of the primary goals for corporations, and their advisors, is arguably to avoid fines and to stay out of the headlines for data privacy violations. From a theoretical perspective, this sounds easy – just observe the data privacy laws. From a practical perspective, however, this is often not as easy as it sounds because, if strictly enforced, it is close to impossible to observe all facets of EU data privacy laws. This may be even more the case when the EU's General Data Privacy Regulation (GDPR) enters into effect later this year. Many hope that last year's words from Germany's Chancellor, Angela Merkel – she hopes that enforcement of the GDPR will be pragmatic – will be heeded.

When compared to the rest of the world, EU data privacy laws have been relatively strict since the mid 1990's. However, not only are the data privacy laws not consistent among the EU member states, their enforcement among the member states has also not been consistent. Some of this undoubtedly stems from significant changes in technology and globalization over the past couple of decades, but much of this inconsistency in enforcement is attributable to different focuses among the EU member states when it comes to data privacy. One primary goal of the GDPR, which will enter into effect on May 25, 2018, is to bring significantly more consistency to data privacy within the European Union.

A fundamental question – and one that cannot be concretely answered until after May, 2018 – is how rigidly the data privacy authorities in any EU Member State will enforce the GDPR. If first indications are a reliable harbinger, corporations will need to pay more attention to data privacy than in the past. Early last year, the Article 29 Working Party, comprised of representatives of the data protection authorities of each EU Member State, contacted each Member State to "remind" them to have sufficient resources on hand once the GDPR enters into force. This is evidence that data privacy authorities will not take a lax attitude towards data privacy enforcement.

In Germany, a recent case before an administrative court in Karslruhe, buttresses the conclusion that data privacy authorities will indeed enforce data privacy laws more rigidly once the GDPR enters into effect. In that case, the data privacy authorities of the German state of Baden-Wuerttemberg sought to enforce the GDPR even before it entered into effect. Specifically, the Baden-Wuerttemberg data privacy authorities issued an order to Infoscore Consumer Data GmbH, a German credit agency, to revise its period for holding personal data. As a credit agency, Infoscore compiled and processed personal

*Schiedermair Rechtsanwälte (Frankfurt, Germany)

data regarding the creditworthiness of individuals. The data privacy authorities issued the respective order on November 25, 2016, exactly one and a half years before the GDPR enters into effect on May 25, 2018.

The pertinent provision of Germany's current data privacy statute sets forth that if personal data is to be processed for commercial purposes, and this personal data is to be transferred, the data must be deleted at the end of the fourth calendar year in which it was first stored. If the personal data is no longer necessary, and the data subject does not object to the deletion of the personal data, it must then be deleted at the end of the third calendar year. Based on this, the Baden-Wuerttemberg data privacy authorities demanded that Infoscore confirm to the authorities that Infoscore intended to comply with this provision even after the GDPR enters into effect. Article 94 of the GDPR states, however, that Directive 95/46/EC, the Directive on which Germany's current data privacy statute is based, will be repealed once the GDPR enters into effect. Infoscore merely responded to the Baden-Wuerttemberg data privacy authorities that it would bring its policy regarding the erasure of personal data in line with the GDPR as soon as it enters into effect.

"...how rigidly the data privacy authorities in any EU Member State will enforce the GDPR."

The Baden-Wuerttemberg data privacy authorities based their jurisdiction on the authority to pursue breaches of data privacy laws, including if there is sufficient evidence to demonstrate that an entity *will* breach a data privacy provision.

Unlike Germany's current data privacy statute, the GDPR does not set forth a specific period by which credit agencies must erase personal data that is no longer necessary. Instead, Preamble 39 of the GDPR sets forth only that "in order to ensure that personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review." Germany's credit agencies are currently negotiating an agreement with state data privacy authorities that will set forth specific periods by which credit agencies must delete personal data. This will be concluded in accordance with Article 40(2) of the GDPR, which states that "[a]-ssociations and other bodies representing categories of controllers or processors may prepare codes of conduct or amend or extend such codes, for the purpose of specifying the application of the [GDPR]. . . ". The Karlsruhe Administrative Court concluded that there is no evidence that Infoscore breached the data privacy laws currently in effect. What *may* happen in the future cannot be a matter for the courts to resolve now.

The fact that data privacy authorities are already now seeking to enforce the not yet effective GDPR should be an indication as to how serious the data privacy authorities intend to enforce the GDPR. The above-referenced increase in manpower for enforcement of data

privacy laws is a further indication of the anticipated heightened enforcement of the data privacy laws.

Of note is that the Administrative Court in Karslruhe, Germany added the statement that it would be in Infoscore's best interests to observe any future requirements regarding the deletion of personal data. As has been widely reported over the past year, potential fines under the GDPR are significantly higher than potential fines under current data privacy regimes. The European Union followed the path of its anti-trust authorities in that under the GDPR, fines may be as high EUR 20 million or 4% of the worldwide annual revenues of an entity, whichever is *higher*. It would indeed be in Infoscore's best interests – or for that matter, in any corporation's best interests – to avoid such hefty fines.

***

European Courts to Rule on Validity of Data Transfer Instrument Used in EU-US Data Transfers

by John O'Riordan and Laura Butler***

The laws of both the European Union and Ireland specifically prohibit the transfer of personal data to a country outside the European Economic Area (EEA) unless that country provides an adequate level of protection. The Irish High Court recently asked the European Courts to rule on the validity of the legal mechanisms by which most data is transferred between the European Union and the United States in a case referred to as 'Schrems II' – so called after the privacy rights campaigner Max Schrems.

Safe Harbor

Mr. Schrems originally brought a complaint against Facebook's data transfer in the Irish High Courts, which led to the Court of Justice of the European Union (CJEU) striking down Safe Harbor in October, 2015 as a data transfer mechanism between the European Union and the United States. The CJEU held that Safe Harbor failed to afford EU citizens the right to an effective remedy before US courts for breaches of rights guaranteed by the European Union Charter of Fundamental Rights. In the wake of Safe Harbor being struck down, 'Privacy Shield' was designed as an alternative transfer framework to facilitate the transfer of data between the European Union and the United States. It seeks to protect the fundamental rights of any person in the European Union whose personal data is transferred to the United States, as well as bringing legal clarity for businesses relying on transatlantic data transfers. It has been under review since its introduction in July, 2016.

Schrems II

Following the CJEU's decision to invalidate Safe Harbor, Mr. Schrems reformulated his complaint to take account that Safe Harbor had been struck down, which was then investigated by the Irish Data Protection Commissioner (DPC). The DPC's investigation confirmed that Facebook Ireland continued to transfer personal data to the United States in reliance in large part on the use of Standard Contractual Clauses (SCCs).

SCCs, also known as "Model Contracts", are contractual terms approved by the European Commission for validating transfers of personal data to countries outside the EEA region. SCCs are thought to be the most widely used legal instrument supporting EU-US data transfers. They are a highly effective method of lawfully transferring data to the United States or other third countries for many businesses.

High Court Ruling

Before the High Court the DPC asked the Court to refer the matter to the CJEU on the

*Partner, Dillon Eustace (Dublin, Ireland)

*Litigation Professional Support Lawyer, Dillon Eustace (Dublin, Ireland)

basis that the concerns of Mr. Schrems appeared to be well founded. Mr. Schrems himself argued against such a referral in circumstances where he argued that the Commissioner had enough information to finalize his complaint. Facebook also opposed the referral with the assistance of legal representation for the US government, acting as amicus *curiae*. Its argument was that US law and other measures afforded adequate protections for data privacy rights of EU citizens.

Judge Costello of the Irish High Court stated that the DPC *"has raised well-founded concerns that there is an absence of an effective remedy in U.S. law compatible with the requirements of Article 47 of the Charter (of Fundamental Rights)."* She also said that the newly-introduced Privacy Shield Ombudsperson mechanism in the Privacy Shield for dealing with Europeans' complaints about US surveillance did not alleviate those concerns to a sufficient degree.

On the question of SCCs it was held that questions relating to the validity of the European Commission decisions regarding standard contractual clauses should be referred to the CJEU for a preliminary ruling. The specific details of the questions to be referred to the CJEU have yet to be determined and the parties to the proceedings will be given an opportunity to make submissions on the exact order to be made and the form it should take. It may take 18 months for a reference to be finalized before the CJEU, though the court may decide to prioritize the case due to the important legal issues involved.

Impact

SCCs, which are the most commonly relied upon method for providing for data transfers outside the EEA, remain valid for now but could be in danger of offering insufficient safeguards to data transfers when forensically examined by the CJEU. Only time will tell if that is the case and we must wait and see if the current protocols go the same way as Safe Harbor. Binding corporate rules, which are a less-commonly used mechanism used in data transfers, may also be affected by a European ruling in respect of SCCs, though it should be noted that, pending the result of the 'Schrems II' proceedings, businesses can continue to rely on SCCs without fear of illegality.

***

*Schiedermair Rechtsanwälte (Frankfurt, Germany)

European data privacy laws: a survey in the light of recent data scandals

by Erik Valgaeren* and Carolien Michielsen**

The rapidly evolving technological landscape offers many advantages and opportunities to companies. However, new technologies also pose new risks and threats to the security of corporate information technology systems. Data breaches and hacking scandals are continuously occurring and may entail major reputational damage for companies. The awareness of data breaches and hacking is spreading and recent surveys reveal that companies are putting IT security at the top of their priority list.

The increasing awareness on security and cybersecurity has resulted in, or has been advanced by, increasing regulation on IT security. Both at the European and at the national level initiatives are being taken in this respect, both generally – for all companies processing personal data – and sector-specific – e.g. for the telecom industry, the financial sector, etc.

In this article we will discuss some recent regulatory developments on IT security at the European level. We will focus on *ex ante* obligations to protect IT systems against data security breaches and *ex post* obligations on how to remedy any data breaches that may have occurred. At last, we will also briefly discuss the notion of "high risk" data processing activities.

Implementing data security ex ante

European data protection legislation requires companies who are processing personal data to implement "appropriate technical and organizational security measures". This obligation was already in place under the Data Protection Directive 95/46/EC, and has now been further elaborated under the General Data Protection Regulation 2016/679 ("GDPR"). The GDPR has replaced Directive 95/46/EC and will be applicable as of 25 May 2018.

The GDPR requires personal data processing entities to implement appropriate technical and organizational security measures both at the time when the means for processing are determined and at the time of the actual processing. Security becomes a core part of every business from its very beginning and throughout the data processing cycle, requiring data controllers and processors to implement privacy "by default" and "by design".

The GDPR also contains some new security-related obligations whereby tangible and verifiable functions and steps need to be realized. For example, the GDPR introduces the requirement that Data Protection Impact Assessments ("DPIA") must be conducted for high-risk data processing operations. Furthermore, every data controller and data processor must keep records pertaining to all

*Partner, Stibbe (Brussels, Belgium)

*Junior Associate, Stibbe (Brussels, Belgium)

aspects of the data processing operations carried out under its responsibility or on behalf of the controller.

Additionally, recent sector-specific regulations also require certain actors to implement appropriate technical and organizational security measures. For example, the Directive on Security of Network and Information Systems (NIS) of 6 July 2016 does so for "operators of essential services" and "digital service providers", the Revised Directive on Payment Services (PSD2) of 25 November 2015 for "payment service providers", the eIDAS Regulation of 23 July 2014 for "trust service providers" and the Markets in Financial Instruments Directive (MiFID) for investment firms, APA's, CTP's and ARM's.

To notify or not?

Where this was not the case under the Directive 95/46/EC, the GDPR introduces the mandatory reporting of data breaches to the supervisory authorities and the obligation to notify the data subjects concerned. Such notification obligations make it easier for competent authorities to exercise supervisory tasks, enable the affected data subjects to take mitigating measures and moreover motivate businesses to implement appropriate information security measures.

Under the GDPR, the data controller must notify any data breach likely to result in a risk to the rights and freedoms of natural persons to the supervisory authority without undue delay. Where feasible, this should be done within 72 hours after the controller became aware of the breach. If this timeframe is not met, the untimely notification must be substantiated by reasons justifying the delay. If the data processor becomes aware of a data breach, it must notify the data controller about it. Additionally, if the data controller has determined that the data breach "is likely to result in a high risk to the rights and freedoms of individuals", it must also communicate – without undue delay – the information regarding the data breach to the affected data subjects.

Obligatory notifications in case of data or security breaches are also provided for in various sector-specific regulations, to different authorities and within different timeframes. For example, the eIDAS regulation of 23 July 2014 requires trust service providers to notify "any breach of security or loss of integrity with significant impact on trust service provided or on personal data maintained" to the supervisory body and to the data protection authority within 24 hours and to the natural or legal person concerned without undue delay. Also, the NIS Directive of 6 July 2016 requires a notification to the competent authority and to the CSIRT (Computer Security Incident Response Team) without undue delay, etc.

High-risk processing operations

Introducing the concept of 'high risk processing', the GDPR differentiates between processing operations entailing a different degree of risk for the rights and freedoms of data subjects. As said, DPIA's are only required

in the exceptional category where the processing is likely to result in a "high risk" to the rights and freedoms of natural persons. Also the need for a prior consultation of the data protection authority is reserved for processing operations entailing such a high risk.

Whether the processing entails such a 'high risk' will depend on the presence of one or more of the following factors: automated decision-making, evaluation or scoring, systematic monitoring, sensitive data, scale of processing, vulnerable data subjects, data transfers outside the EU, etc. In particular, a DPIA will be required when the processing entails: (i) any systematic and extensive evaluation of personal aspects of natural persons based on automated processing or profiling upon which decisions are based; (ii) processing the so-called "sensitive" categories of personal data on a large scale; or (iii) a systematic monitoring of a publicly accessible area on a large scale. National supervisory authorities are moreover required to establish a list of the types of processing operations that require a DPIA, as already has occurred in Belgium, for example.

Data protection legislation today already requires implementing appropriate technical and organisational security measures. But compared to the current legal framework, the GDPR contains stricter obligations with regard to data security, data breach notifications, and data subject notifications. On top of that, a multitude of sector-specific regulations impose similar yet sector-adapted obligations on the actors concerned. Adequate and efficient IT security has become a moving target and companies will need to continuously assess and update their security processes according to the "state of the art" and best practices.

Security becomes a core part of every business from its very beginning and throughout the data processing cycle, requiring data controllers and processors to implement privacy "by default" and "by design".

***

When it comes to data privacy, keeping pace with the digital world doesn't have to be complicated – it's about getting the basics right

by Vikki Hoyle*

The world has changed. Rapid advances in technology are revolutionising the way we communicate and do business. Increasingly sophisticated cyberattacks are an ever-present threat. Now, more than ever, people want to take back control over how their data is handled. They want to be able to trust that it will be protected and used appropriately. And businesses need to keep up or else they risk being left behind.

Data privacy is rarely out of the news these days. In Europe, it is practically impossible to escape the build-up to the arrival of the General Data Protection Regulation (or GDPR). Businesses have until 25 May 2018 to prepare themselves for the new regime, which aims to harmonize data protection legislation by the creation of an EU-wide single legal framework, to recognize and embrace technological advances for all businesses (in accordance with the European Union's Digital Single Market Strategy) and to strengthen citizens' fundamental data protection rights. GDPR will not just apply in Europe – data controllers or processors anywhere in the world who offer goods or services to individuals in the European Union, or who monitor the behaviour of individuals in the European Union, will be caught. The digital world is just that – it transcends national boundaries, which brings us to the first cloud on Europe's data protection horizon – the embattled EU-US Privacy Shield.

Cross-border data flows and the openness of the digital economy are essential to the multi-billion dollar trading relationship between Europe and the United States. The Privacy Shield was created to protect the rights of those EU citizens whose personal data is transferred to the United States, and to bring legal clarity to those businesses relying on transatlantic data transfers. On 12 July 2016, the European Commission adopted an adequacy decision that concludes that US organizations registered under the Privacy Shield provide an adequate level of protection for personal data transferred from the European Union to such US organizations. The framework replaces the 'Safe Harbor' regime, which was ruled invalid by the Court of Justice of the European Union (CJEU) in October 2015.

But the Privacy Shield has been dogged by problems. It was criticised even before its launch, and the concerns and challenges have been mounting ever since. Privacy advocacy groups in Ireland and France are seeking to have it annulled in two separate actions before the CJEU, challenging the European Commission's 'finding of adequacy'. Concerns in Europe include US surveillance activities, vacancies at the Federal Trade Commission

*Senior Associate, Walker Morris (Leeds, U.K.)

which enforces the Privacy Shield, and insufficient independence of the Ombudsperson mechanism. The first annual joint review took place in September 2017 and, as the Article 29 Working Party (or WP29) said in a recent press release, the review will be a "key moment" for it to assess the Privacy Shield's robustness and effectiveness.

If the joint review results in the Privacy Shield either being suspended or amended, organizations will need to be prepared to make changes to their policies and procedures accordingly. For now at least, other alternative legal bases for transfers of data include binding corporate rules and standard contractual clauses (but watch this space, because the legal status of data transfers under standard contractual clauses is almost certain to be referred to the CJEU following further litigation in Ireland involving the Austrian privacy activist Max Schrems – the individual behind the Safe Harbor decision). The situation is far from ideal, because businesses like to have certainty, which brings us to Brexit.

On 23 June 2016, the United Kingdom voted to leave the European Union. That is old news by now. What is new, however, is that the UK Government has confirmed once and for all that its upcoming 'Data Protection Bill' will bring GDPR into UK law. According to the Digital Minister, the new Bill will give the UK "*one of the most robust, yet dynamic, set of data laws in the world. It will give people more control over their data, require more consent for its use, and prepare Britain for Brexit*". Indications suggest that the UK could be heading for some kind of 'GDPR-plus' model of data protection legislation which goes beyond EU requirements. And not for the first time. As the Government set out in its recent position paper on the exchange and protection of personal data post-Brexit, when the United Kingdom updated its data protection law to implement the EU Data Protection Directive 1995, it extended the rights and obligations beyond the minimum required by EU law.

According to the Government's position paper, the Untied Kingdom is "*considering an ambitious model for the protection and exchange of personal data with the EU that reflects the unprecedented alignment between British and European law and recognises the high data protection standards that will be in place at the point of exit*". It wants to explore a UK-EU model which could build on the existing adequacy model in two ways. Firstly, by enabling an ongoing role for the Information Commissioner's Office (ICO) in EU regulatory fora. Secondly, by the United Kingdom and the European Union agreeing to mutually recognise each other's data protection frameworks as a basis for the continued free flows of data between the European Union and other EU adequate countries, and the United Kingdom, from the point of exit (until longer-term arrangements come into force). This would be to avoid regulatory uncertainty for businesses and public authorities in the United Kingdom, EEA, and EU adequate countries. Where we go from here depends on the outcome of the negotiations between the UK and the EU27.

What is clear from the position paper is that the government's focus extends beyond Europe, to the rest of the world. It sees the United Kingdom as one of the leading drivers of high data protection standards across the globe, and stresses that "*global leadership and standards are needed to ensure that individuals can have confidence that their data is being appropriately protected wherever they choose to access goods or services, but not in such a way as to undermine the provision of those goods or services, including on a cross-border basis*". That is really what it comes down to. It is about businesses having arrangements in place which customers can trust and have confidence in. And that does not have to be complicated. In fact, these are standards that every business should adhere to, wherever they are, and whatever regime they are subject to (be that GDPR, 'GDPR-plus', or something else).

Going back to GDPR, there is a certain sense of fear surrounding the implementation of this enhanced regime and what it means for businesses. In the United Kingdom, the Information Commissioner has recently sought to address this in a series of 'myth-busting' blogs. She notes that, if misinformation goes unchecked, "*we risk losing sight of what this new law is about - greater transparency, enhanced rights for citizens and increased accountability*". The new regime is described as "*an evolution in data protection, not a total revolution*" and the message for businesses is that "*if you are already complying with the terms of the* [UK] *Data Protection Act, and have an effective data governance programme in place, then you are already well on the way to being ready for GDPR*".

In the end, it's about accountability, transparency, and fairness. It's about responsible data management and handling information correctly – understanding what personal data is collected and why, how it is processed, where it is stored, the security measures in place to protect it, how long it is retained for, and why. It's about giving individuals greater choice and control over how their personal data is used. It's about building a culture of privacy and integrating data protection into the heart of the business. Quite simply it's about good business practice.

The businesses that have the potential to thrive in our ever more connected world are those that look beyond compliance and embrace data protection as an opportunity, not a threat. Legislation such as GDPR encourages innovation and provides businesses with the perfect opportunity to review and improve the way they manage data whilst ensuring that they maximize the potential of their data assets. Strengthening customer relationships by developing customer trust can only be a good thing in a world where reputation matters.

***

The Right to be Forgotten in Europe: Current Legal Status and Future Challenges

by Marc Weitz*

Under EU law, the "Right to Be Forgotten" is a protection of the private internet user's ability to request and have removed links to public information about the individual. In other words, they have the right to request to be forgotten by the internet. This article will briefly describe the law, the process to make such a request, the effects of the law, problems with the law, and the current state of the law with updates on pending legal action.

Background

The Right to be Forgotten is an extension of the idea of individual internet privacy but is distinguished from the right to privacy in that it seeks to allow individuals to remove once public information rather than keep private information private.[1] Along with the benefits of having an enormous, widely available resource of information, the Internet has also become a permanent store of information. Criminal records, ill-advised posts and photos, or simply information that the user no longer wants shared remain available on the Internet to be found by search engines.[2] The Right to be Forgotten gives the internet user the right to control such information by requesting its removal entirely or from search engine results, in essence making the internet forget them.[3] The law is an attempt to control a side effect of the information age and return to the pre-internet days where most things in people's lives went unrecorded and thus naturally disappeared into the past.

In the European Union, the Right to be Forgotten is codified first in Article 12 of the Directive 95/46/EC[4] and was clarified in 2012 in a draft proposal, which summarized the objective:

> Article 17 provides the data subject's right to be forgotten and to erasure. It further elaborates and specifies the right of erasure provided for in Article 12(b) of Directive 95/46/EC and provides the conditions of the right to be forgotten, including the obligation of the controller which has made the personal data public to inform third parties on the data subject's request to erase any links to, or copy or replication of that personal data. It also integrates the right to have the processing restricted in certain cases, avoiding the ambiguous terminology "blocking."[5]

The Court of Justice of the European Union further clarified the law in a ruling issued in

*Attorney, Law Offices of Mark Weitz (Los Angeles)

May 2014 in the case of *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*.[6] The *Gonzalez* case found that controllers are responsible for removing links to third-party websites, which contain information subject to removal through approved right to be forgotten requests.[7] "[C]ontroller shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data[,]"[8] [9] and includes search engines such as Google, Yahoo!, and Bing, as well as social networks like Facebook." The case further stated that "every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified[.]"[10]

The Process of Requesting Removal

According to Google's online form, a user seeking to remove information from search results under the Right to be Forgotten must input the EU country under which the law applies, their name, email, verify their identity, and then list the URL and reason for removal.[11] After submitting the form, Google explains its process as follows:

> "When you make such a request, we will balance the privacy rights of the individual with the public's interest to know and the right to distribute information. When evaluating your request, we will look at whether the results include outdated information about you, as well as whether there's a public interest in the information - for example, we may decline to remove certain information about financial scams, professional malpractice, criminal convictions, or public conduct of government officials."[12]

Google itself provides updated statistics in its Transparency Report on the number of requests it receives, along with examples of those that are granted and those that it does not grant, as well as an updated description of the criteria it uses.[13] Google has removed 43.2% of requests from the implementation of the law till September 3, 2017.[14]

Balancing the public benefit against the Right to be Forgotten is controversial though, as it is a subjective standard.[15] Common examples of abuse of the Right to be Forgotten are the removal of information about people who have committed fraud, doctors with multiple cases of malpractice, and sex offenders.[16] These individuals clearly want this information removed from search results under the Right to be Forgotten, but at the same time this information provides a public benefit in that it informs and potentially warns the public about interacting with such individuals. Some examples are clear, but the world is full of nuance, and it is up to humans reviewing these applications for removal to decide.

The intent of the law, in its most perfect form,

seems to be to remove the stigma of innocent and embarrassing mistakes from one's past, or to remove more serious mistakes from one's past in proportion to their severity, the amount of time that has passed, and their behavior since, rather than be haunted until eternity. Suzanne Moore of The Guardian called it the right to have an imperfect past.[17] Of course, some things need to remain discoverable. Indeed, the theory is similar to the criminal justice system in which the record keeping of crimes is treated with different levels of severity. Those who have served out their punishment for a crime are in principle said to have paid their debt to society. In most cases, severe crimes remain part of an individual's permanent record, such as murder or sex offenses, and continue to have consequences even after the punishment is served. However, minor crimes are often expunged after a certain amount of time or at reaching a certain age. The intent behind the Right to be Forgotten seems to follow that thinking.

The Right to be Forgotten gives the internet user the right to control such information by requesting its removal entirely or from search engine results, in essence making the internet forget them.

Ultimately, further laws or case precedent is needed to clarify where that line is drawn.

Application of the Law Geographically

Last year the Court of Justice of the European Union (ECJ) accepted an appeal to rule on whether the Right to be Forgotten applies outside the European Union.[18] The internet is worldwide, and the Right to be Forgotten is an EU law applicable only within the European Union.[19] However, the Right to be Forgotten is rendered useless if it is not applied outside of EU borders.[20] Those outside of the European Union could still find "removed" information or by Europeans simply using a free and readily available VPN, which allows users within the European Union to appear that they are outside and thus able to access content not available within the European Union.

The showdown over the geographic reach of the Right to be Forgotten is related to a fine imposed in by the CNIL ("Commission Nationale de l'Informatique et des Libertés"), the French government agency regulating personal online data, and thus in many ways, Google.[21] [22] In March 2016, the CNIL fined Google 100,000 Euro for not delisting information under the Right to be Forgotten over all its sites around the world. [23] As could be expected, Google appealed France's administrative course, who passed it on to the Court of Justice of the European Union ("CJEU") in July 2017.

The implications for a country's sovereignty of law are immense. The Right to be Forgotten is unlikely to be implemented in the United States because of the right to free speech under the first amendment to its constitution.[24] Thus, if the CJEU rules that the Right to be Forgotten must be applied across EU borders, then information, even that deemed to be protected free speech by the

United States, would need to be deleted. Google and other controllers, such as Facebook, Yahoo!, and Bing, would be caught somewhere in the middle.

Like many things in life, this issue hinges on power and money. Google and other controllers comply with French and EU law in large part because France has the seventh largest economy in the world and the European Union has the second largest economy in the world. [25] Google profits from its access to these markets and therefore must follow each jurisdiction's laws and pay fines as the case may be. Of course, the United States is the largest economy in the world, so controllers must also follow their law as well. This web of relationships creates a conflict.

A solution to this problem could come in a few forms. One such solution could be an international convention on how the right to be forgotten could be uniformly treated, similar to how copyrights and trademarks laws are handled internationally. However, before the United States could subscribe to such a convention, it would still need to overcome its freedom of speech rules. More importantly, there may not be the will amongst the world community to pursue such a convention as a matter of politics, returning back to objectives of money and power, mentioned earlier. Relatedly, copyright and trademark conventions exist because they are a huge part of the world economy with trillions at stake. Such conventions facilitate international business. Indeed, companies spend a lot of money pushing governments to create such uniformity.

However, when it comes to the Right to be Forgotten, there is little money to be made in its protection. It is considered an ethical issue – a human right. [26] As such, the political will is not as strong as an economic issue. And while this may be an important issue to EU citizens, most people are likely not bothered enough to pursue such a convention. Others may have the attitude that having potentially embarrassing information on the web is a reality of the modern age with which one must live.

The reality of this issue may lead to a "Balkanization" of the web, in which the Right to be Forgotten information is available in some countries and not available in others. However, there may still be a benefit in making the information less easy to find. Criminal records, birth records, addresses, and telephone numbers are examples of information that is available if one looks hard enough. "Balkanization" and the availability of information in some places and not others is something that exists already. For instance, censorship of the internet in places such as China, which in itself is controversial, but is an existing reality. [28]

For those individuals living in the European Union who have been granted requests to have information removed, it becomes more difficult for those in the European Union to find it. Extra effort would be required for those seeking such information by searching the internet outside the territory protected by

the Right to be Forgotten. Many seekers would need to know that such information exists in the first place to find it.

Further, compliance with the law is frustrating for controllers such as Google, as the standards are unclear. Controllers are likely to be hit with lawsuits from individuals whose removal they have denied. Equally, regulatory agencies may fine controllers for not complying with the law properly, leaving controllers open to being blindsided for thinking they are doing the right thing under the law when someone else may think differently. The creation of safe harbors within the law would be beneficial to data controllers and help them do their job of compliance without fear. In other words, the law should designate that if controllers are following a certain set of criteria they would be protected from certain lawsuits and fines retroactively. And any revealed loopholes within the law could be addressed and implemented without the data controller being unfairly punished for something they did not justifiably know about.

The Future, Key Things to Watch Out For, and Conclusion

The next thing to watch out for is the upcoming ruling by the CJEU on whether the Right to be Forgotten applies outside the European Union, and how the United States and other countries in turn react to EU law being imposed on their own system if that happens. Watch for any move toward an international convention on a uniform standard. Also look for clarification on standards for what content is eligible for removal under the law, an important specification that would increase legal certainty but could equally chip away at the rights of EU citizens entailed by the Right to Be Forgotten. With data controllers stuck in the middle, it would be fair to create safe harbors under the law, so that they are not continually blindsided by lawsuits from individuals or fines imposed by regulatory agencies.

The evolution of this law in the European Union will be fascinating to watch. In the meantime, the advice for lawyers and their clients who may need to comply with the law is to stay diligent on the current state of the law but to make sure that clients are advised that the law is changing and is rather unclear, resulting in unforeseen fines or lawsuits. Such warnings put clients on notice and protect the attorney.

***

[1] Weber RH (2011). The Right to Be Forgotten More Than a Pandora's Box?. jipitec, Vol. 2, https://www.jipitec.eu/issues/jipitec-2-2-2011/3084.

[2] *Id.*

[3] *Id.*

[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 P. 0031 – 0050, article 12. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046

[5] European Commission. Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal

Data and On the Free Movement of Such Data (General Data Protection Regulation). 2012/0011 (COD). Article 17. Right to be forgotten and To Erasure, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

[6] Judgment of May 13,2014, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, Case C-131/12, [2014] E.C.R. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0131&from=EN

[7] *Id.*

[8] *Id.*

[9] Charles Arthur, *Explaining the 'right to be forgotten' – the newest cultural shibboleth,* May 14, 2014, The Guardian, https://www.theguardian.com/technology/2014/may/14/explainer-right-to-be-forgotten-the-newest-cultural-shibboleth

[10] Judgment of May 13,2014, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, Case C-131/12, [2014] E.C.R. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0131&from=EN

[11] Google Removal Request. https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=0-636394172048522278-945396792&rd=1

[12] *Id.*

[13] Google Transparency Report, https://transparencyreport.google.com/eu-privacy/overview

[14] *Id.*

[15] Sophie Curtis, *EU 'right to be forgotten': one year on.*, The Telegraph, May 13, 2015, http://www.telegraph.co.uk/technology/google/11599909/EU-right-to-be-forgotten-one-year-on.html

[16] *Id.*

[17] Suzanne Moore, *The right to be forgotten is the right to have an imperfect past*, August 7, 2017, https://www.theguardian.com/commentisfree/2017/aug/07/right-to-be-forgotten-data-protection-bill-ownership-identity-facebook-google

[18] Reuters, *France's Fight Over Google Search Results Was Kicked to Europe's Top Court*, Fortune, July 19, 2017, http://fortune.com/2017/07/19/france-google-right-forgotten-eu-court/

[19] Victor Luckerson, Americans Will Never Have the Right to Be Forgotten, Time Magazine, May 14, 2014, http://time.com/98554/right-to-be-forgotten/

[20] Reuters, *France's Fight Over Google Search Results Was Kicked to Europe's Top Court*, Fortune, July 19, 2017, http://fortune.com/2017/07/19/france-google-right-forgotten-eu-court/

[21] Victor Luckerson, Americans Will Never Have the Right to Be Forgotten, Time Magazine, May 14, 2014, http://time.com/98554/right-to-be-forgotten/

[22] France, *la Commission Nationale de l'Informatique et des Libertés*, https://www.cnil.fr/fr/la-cnil-en-france

[23] Victor Luckerson, Americans Will Never Have the Right to Be Forgotten, Time Magazine, May 14, 2014, http://time.com/98554/right-to-be-forgotten/

[24] U.S. Const. amend I

[25] "World Economic Outlook Database". International Monetary Fund. 18 April 2017.

[26] Judgment of May 13,2014, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, Case C-131/12, [2014] E.C.R. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0131&from=EN

[27] Victor Luckerson, Americans Will Never Have the Right to Be Forgotten, Time Magazine, May 14, 2014, http://time.com/98554/right-to-be-forgotten/

[28] Paul Mozur, *China's Internet Censors Play a Tougher Game of Cat and Mouse,* The New York Times, August 3, 2017, https://www.nytimes.com/2017/08/03/business/china-internet-censorship.html?_r=0

Privacy Law: Europe's Impact on US Business

EU-US Privacy Shield: Will it shield you from the General Data Protection Regulation (GDPR)?

by Aaron Schildhaus*

Part I: Privacy Shield Replaces Safe Harbor

Many US businesses are familiar with the EU-US Privacy Shield and its analogue, the Switzerland-US Privacy Shield (jointly referred to as the "Shield"), which was agreed to by the U.S. Department of Commerce (DOC), the European Commission (Commission), and Switzerland. The Shield is the latest mechanism now validly in force to enable US entities to be in compliance with personal data transfer requirements in Europe. It is based upon EU Member State implementation of the 1995 European Data Protection Directive (95/46/EC), which is, and will continue to be, the law in effect for the next half-year until the 1995 Directive is superseded by the GDPR (see below).

The Shield was developed to replace the formerly utilized Safe Harbor (Commission Decision 2000/520/EC of 26 July 2000), which was invalidated by the European Court of Justice (ECJ) in the case of Maximilian Schrems v. Supervisory Authority. Consequently, as of October 31, 2016, the DOC stopped accepting all US-EU Safe Harbor certifications. The Safe Harbor was held by the ECJ to be insufficiently safe to protect the personal data of EU citizens and residents, thus paving the way for the Shield.

On August 1, 2016 after the Commission had deemed the Shield adequate to enable data transfers under current EU law, the DOC began accepting certifications from U.S. companies to join the program (81 FR 47752; July 22, 2016). The Shield provides for self-certification from US companies that have privacy policies and practices in place that comply with the provisions of the Shield. Although over 2400 entities have already self-certified, there is a real possibility that legal challenges to the efficacy of the Shield will eventually prevail. This could result in a holding that the Shield, like the Safe Harbor before it, does not adequately protect the personal data of EU citizens.

Actually, the Shield is only one of several mechanisms enabling US and European companies to be in compliance with data protection requirements when transferring personal data from the European Union (and/or Switzerland) to the United States. For example, other approved means for cross-border data transfers are Standard Contractual Clauses ("SCC") and Binding Corporate Rules ("BCR"), although the latter method is much more difficult to adopt and generally has much less flexibility, and consequently is likely not to be the mechanism of choice for most US companies. Most organizations have been

*Counsel, Scharf Banks Marmor LLC (Chicago)

opting for the more flexible and more simply implemented Shield or SCCs.

The Shield provides for a joint annual review, the first of which took place in September, 2017. The joint press release following the review was not particularly substantive: "The United States and the European Union share an interest in the Framework's success and remain committed to continued collaboration to ensure it functions as intended."

Self-certification for the Shield by US organizations is easy to do online. However, self-certifying and then not adhering to the Shield's compliance requirements would likely be costly in the long term. Under the Federal Trade Commission (FTC) Act, US entities' failures to implement business practices that comply with the Shield can be deemed as deceptive trade practices and the US can enforce adherence through administrative orders or court orders. Violations of those orders can result in civil penalties of up to $40,000 per day or per violation. In a similar way, failure of implementation by air carriers or ticket agents could be held in violation of 49 USC 41712 and also result in fines and penalties in similar amounts. Persistent failure to comply can result in an organization's removal from the Shield and thus also its inability to transact further business with EU Member States and Switzerland.

The Shield principles include the "Notice Principle," which requires informing individuals about the organization's participation in the Privacy Shield and providing a link to, or the web address for, the Privacy Shield List. Organizations must identify the types of personal data collected, committing that the Privacy Shield requirements will be followed relative thereto, and they must disclose to the data subject the purposes for which they collect and use that person's personal data. It also requires listing information regarding how to contact the organization for any inquiries or complaints, including how to contact any relevant establishment in the EU and/or Switzerland that can respond to such inquiries or complaints. Organizations must: (i) identify the type or identity of third parties to which it discloses personal data, and the purposes for which it does so; (ii) clearly state the right of individuals to access their personal data, and how individuals can limit the use and disclosure of their personal data; and (iii) identify the independent dispute resolution body designated to address complaints and provide appropriate recourse free of charge to the individual. Finally, under the Notice Principle, the organization must state that it is required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements, and it must explain its liability in cases of onward transfers to third parties.

Importantly, the notice must be provided in clear and conspicuous language when individuals are first asked to provide personal data to the organization, or as soon thereafter as is practicable, but in any event before the

organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization, or when it discloses it for the first time to a third party.

Between the United States and Europe, proper data treatment is essential. Since the European data protection requirements are arguably more stringent than data protection requirements in the United States, noncompliance with them could mean not doing business in or with Europe. The penalties and consequences are too heavy. But, getting the Commission to agree with the United States on a mechanism for US corporate compliance with European data protection laws has not been easy, nor has it been noncontroversial. Many Europeans remain skeptical about the ultimate efficacy of the Shield, particularly in the wake of the Edward Snowden affair, which showed, *inter alia*, that the US Government was violating the spirit of the Safe Harbor with the cooperation of a number of US technology companies.

Despite this, many on both sides of the Atlantic have been optimistic that the Shield constitutes an effective solution to the limitations of the Safe Harbor; others, however, continue to doubt that it will solve the concerns of privacy groups. In any event, it's arguably the best game in town for the moment to legally transfer personal data from the European Union to the United States.

A cautionary note to US companies providing self-certification: it is not enough to certify that you are in compliance. Your compliance programs must be designed not only in accordance with the Shield provisions but they must also be implemented and properly monitored to avoid serious legal consequences.

Accordingly, US businesses and other entities processing personal data should be adopting policies that take into consideration the provisions of the EU General Data Protection Regulation that will come into force in May, 2018, and they should anticipate that the Shield could eventually succumb to legal challenges a la Safe Harbor. Indeed, challenges are already afoot.

Part II: EU General Data Protection Regulation 2016/679 (GDPR) Replaces EU Data Protection Directive 95/46/EC

During the same time frame that the Shield was being designed and implemented, the EU was engaged in a project to update and replace its existing data protection provisions (the ones for which the Shield is intended to provide compliance). The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize privacy and data security laws across Europe and to reshape the way organizations across the region approach data protection. Because it is a Regulation, and not a Directive, it will be directly applicable in all EU Member States in May, 2018. By comparison, a Directive would instead only require that each state enact its

own national law that satisfies the directive's requirements.

Article 1 of the GDPR "lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data (and it) protects fundamental rights and freedoms of natural person and in particular their right to the protection of personal data..."

The GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the European Union, regardless of whether the processing of personal data takes place therein, and it could apply to the processing of personal data in the European Union by a controller or processor not established in the European Union.

After four years of planning and work, the GDPR was approved by the EU Parliament on April 14, 2016, and therefore entered into force 20 days after its publication in the EU Official Journal; it will be directly applicable in all members states two years after this date. Its official starting date, therefore, is May 25, 2018. Organizations not in compliance at that date may be subject to heavy fines.

This leads to a practical query: Would organizations participating in the Shield be considered to be in compliance with the GDPR? With regard to processing personal data transferred under and in accordance with the Shield, it would appear that they would be in compliance; however, any processing of EU personal data outside of the Shield does not necessarily mean that there is GDPR compliance. And, as stated earlier, the mere fact of self-certifying, but not meeting the underlying criteria as set forth above, would expose organizations nominally protected under the Shield, to serious consequences in terms of their ability to conduct operations with Europe, not to mention liability to pay fines of up to twenty million Euros or 4% of their worldwide turnover, whichever is greater.

Again, it should also be kept in mind that potential challenges to the Shield now under way in Europe could invalidate it, in which case, US entities must have robust and actively monitored procedures and policies in place that meet all the requirements of the GDPR. Mere reliance on self-certification will not be sufficient going forward. It is a wise, if not essential, practice for clients to be prepared for the GDPR in all respects, even if already "protected" by the Shield.

Therefore, organizations must have in place procedures and policies that will be adequate to satisfy the inevitable, future challenges by persons claiming they are inadequately protected by the Shield.

***

The Territorial Scope of the GDPR

by Daniel Sánchez Cordero Canela** and Jorge Alberto Reyes Flores**

Introduction

There are two main legal systems of data protection in the world: the American model and the European model.

The American model system of data protection is closely aligned with property rights. The inception of the American model began with the work of Thomas M. Cooley and what he called "the right to be let alone." [1] Samuel D. Warren and Louis D. Brandeis retook Cooley's work on torts and modified it to more closely resemble the modern American legal system. They established that recent inventions and business methods call attention to the next step that must be taken for the protection of the person, and for securing to the individual what is *the right to be let alone*. The American legal system has expanded that idea and is currently composed of a mosaic of federal and state laws [2] that protect the right of privacy in specific areas. [3]

The European model is based on the fundamental right of the protection of natural persons in relation to the processing of personal data. [4] In this article, we will focus on the European model. Two regulations within the European model stand out: (i) the Directive 95/46/EC [5] (the "Directive") and (ii) the Regulation (EU) 2016/679 [6] (the "GDPR"). The Directive is the rule governing present cases; however, it will be repealed by the GDPR starting from May 25, 2018.

We will proceed to analyze and compare the territorial scope of the Directive and the GDPR.

Territorial Scope of the Directive and the GDPR

The Directive applies where processing of personal data is carried out *in the context of the activities* of an *establishment* of the controller on the territory of the Member State. [7] The controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community. [8]

The GDPR copies a substantial part of the territorial scope of the Directive. The concepts of *establishment* and *in the context of the activities* are reflected in both statutes. However, there are new additions in the territorial scope of the GDPR. [9]

Since the territorial scope of the GDPR copies, in most parts, the Directive, we will analyze below the two main situations in which it applies.

*M&A, International Affairs & Regulation, attorney-at-law

**Founding partner VCR Consultores, S.C.

a. EU "established" controllers or processors [10]

The GDPR will apply to organizations that have EU "establishments" where personal data are processed "in the "context of the activities" of such an establishment by a controller or a processor. [11] Even though the GDPR defines the term of main establishment, it leaves the definition of an "establishment" open to interpretations, just like the Directive did. Furthermore, the GDPR, as well as the Directive, also fail to define the concept of "in context of the activities." Both concepts, as we will see below, have already been defined by the Court of Justice of the European Union ("CJEU"). [12] Even though the CJEU defined such concepts based on the Directive, we believe that such definitions will still apply to the GDPR.

With regards to the concept of "establishment," the CJEU has noted that to determine whether the data controller has an establishment in a Member State, other than the Member State or third country where it is registered, both the degree of stability of the arrangements and the effective of activities in that other Member State must be interpreted in the light of the specific nature of the economic activities and the provision of services concerned. [13] This broad and flexible construction is particularly true for undertakings offering services exclusively over the Internet. [14] An effective activity exercised through stable arrangements can even be a minimal one. [15] The legal form of the data controller, whether simply a branch or a subsidiary with a legal personality, is not a determining factor. Even though the concept is broad, there are also limits that do not fall within the term "establishment." For example, there will not be an establishment merely because the undertaking's website is accessible in such Member State. [17]

With regards to the concept of "in the context of the activities," the CJEU has determined that such term cannot be interpreted restrictively. [18] However, the Court has pointed out that it is for the national courts to determine whether the company carries out the data processing in question in the context of the activities of an establishment situated in the Member State in question. [19] Furthermore, the CJEU has established that the directive does not require the processing of personal data in question to be carried out "by" the establishment concerned itself, but only that it be carried out "in the context of the activities" of the establishment. [20] In other words, the CJEU has set forth a floor and a ceiling to the definition of such concept. The term "in the context of the activities" cannot be transposed and defined by Member State law restrictively, as well as broadly enough to include every processing of personal data carried out by the establishment. The consequence of this decision allows for flexibility by Member States, but it also harms the principle of harmonization that underlies the goals of the European Union. It is important to note, however, that the CJEU has provided several examples as to what is "in the context of the activities." As an example, the CJEU has

determined that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State when the operator of a search engine sets up in a Member State a branch or subsidiary that is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State. [21]

b. Non-EU "established" organizations who target [22] *or monitor* [23] *EU data subjects* [24]

Non-EU established organizations will be subject to the GDPR where they process personal data about EU data subjects in connection with

(i) the "offering of goods or services" (payment is not required); or

(ii) "monitoring" their behavior within the EU.

The GDPR added a new concept, which was not part of the Directive, consisting of "offering of goods or services." However, the GDPR failed to define what would be considered to be "offering of" goods or services within the EU. The term "offering" implies intent of the offeror to offer the offeree goods or services within the EU. The GDPR has already analyzed:

(i) what could be considered evidence of intent; and

(ii) what will not be considered intent.

The CJEU has also analyzed:

(i) what activities should be considered to be enough for intent;

(ii) what activities should be considered to be enough to form evidence of intent; and

(iii) what activities should not be considered to be intent in a consumer protection case in which the concept of "directed to" was the one being disputed (as opposed to "offering of"). [25]

We believe that, based on the similar policies pursued in consumer cases and data protection cases, as well as the similar functions [26] that consumer protection directives and regulations have with the Directive and the GDPR, the consumer protection case of the CJEU will shed light on the intent of the "offering of" goods or services within the European Union set forth into the GDPR.

i. What will be considered intent under "offering of" goods or services within the EU

The CJEU noted that sufficient intent is found with the classic forms of advertising to constitute "directed to" consumers domiciled in a Member State. [27] Such classic forms of advertising cover all forms of advertising carried out in the contracting state in which the consumer is domiciled, whether disseminated generally by the press, radio, television, cinema, or any other medium, or addressed directly, for example by means of catalogues sent specifically to that state, as well

as commercial offers made to the consumer in person, in particular by an agent or door-to-door salesman. [28] This intention is not always present in the case of advertising by means of the Internet. [29]

ii. What could be considered evidence of intent under "offering of" goods or services within the EU

The preamble of the GDPR establishes that factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the European Union, may make it apparent that the controller envisages offering goods or services to data subjects in the European Union. [30]

The CJEU established that evidence of intent may be found in the following additional scenarios:

1. When the company mentions that it is offering its services or its goods in one or more Member State designated by name. [31]

2. Where there is disbursement of expenditure on an internet referencing service to the operator of a search engine in order to facilitate access to the company's site by consumers domiciled in various Member States. [32]

Items of evidence of intent are as follows:

1. The international nature of the activity at issue, such as certain tourist activities; mention of telephone numbers with the international code;

2. Use of a top-level domain name other than that of the Member State in which the trader is established, for example '.de', or use of neutral top-level domain names such as '.com' or '.eu'; the description of itineraries from one or more other Member States to the place where the service is provided; and

3. Mention of an international clientele composed of customers domiciled in various Member States, in particular by presentation of accounts written by such customers. [33]

It is important to highlight that it's not the CJEU, but the national court that ascertains whether there is enough evidence for there to be intent. [34]

iii. What will not be considered evidence of intent under "offering of" goods or services within the EU

The preamble of the GDPR establishes that the mere accessibility of the controller's, processor's or an intermediary's website in the EU, of an email address or of other contract details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention. [35]

Furthermore, the CJEU has established that evidence of intent does not include mention on a website of the trader's email address or geographical address, or of its telephone number without an international code. [36]

***

[1] WARREN, SAMUEL AND BRANDEIS, LOUIS, THE RIGTH TO PRIVACY, Harvard Law Review.Vol.IV, Nº. 5., December 15, 1890.

[2] See HUTCHINS, J.; U.S. Data Breach Notification Law: State by State. Ed. ABA Section of Science & Technology Law. 2007.

[3] For example: (i) the Electronic Communications Privacy Act, (ii) the Fair Credit Reporting Act, (iii) the Cable Communications Policy Act, (iv) the Omnibus Safe Streets and Crime Control Act, (v) the Telephone Consumer Privacy Act and (vi) the Bank Secrecy Act.

[4] Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty on the Functioning of the European Union provide that everyone has the right to the protection of personal data concerning him or her.

[5] A directive is a norm that shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods. In other words, the EU specifies certain legislative objectives in a directive, which would then be up to the Member States to transpose the directive by enacting legislation that would accomplish the relevant objectives. One of the consequences of providing this much leeway to Member States is that harmonization suffers between each Member State. Furthermore, as a general rule, directives have to be transposed in order to gain relevance within the Member State.

[6] A regulation is a norm that shall have general application. It shall be binding in its entirety and directly applicable in all Member States. No action on the part of the Member States is necessary in order for the regulations to become binding within the EU.

[7] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 P. 0031 – 0050, article 4. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046

[8] *Id*

[9] 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 the monitoring of their behavior as far as their behavior takes place within the Union.

[10] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 96/46/EC, Official journal L 119, 4/5/2016 P. 0001 – 0080, article 3.1 [GDPR] : "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."

[11] *Id.*

[12] It is important to note that the CJEU does not have the same function as to what a traditional court would have. The TFEU defines the CJEU's jurisdiction in connection with the various types of proceedings before the CJEU. The most important proceedings is the preliminary ruling procedure. When a Member State court confronted with a novel question regarding the interpretation or validity of EU law, such court may (and, in some particularly cases, must) refer that question to the CJEU. The CJEU doesn't decide the case or even how EU law is to be applied to the facts of the case. The CJEU is only concerned with the validity or interpretation of EU law. Therefore, one should not look at whether certain segments of the CJEU are holding or dicta (binding or non-binding) but whether such question referred to the CJEU has been already asked and resolved, as well as whether the statute that such question derived from has not materially changed in the new statute.

[13] Judgment of 1 October 2015, *Weltimmo*, C-230/14, EU:C:2015:639, paragraph 29. [*Weltimmo*] Facts of the case: A company which has its registered office in Slovakia, runs one or several property dealing websites concerning properties situated in Hungary, which are written in Hungarian and whose advertisements are subject to a fee after a period of one month. A Hungarian regulatory agency imposed a fine for infringement of an Hungarian

statute which was transposed from the Directive. Question asked to the CJEU: Whether the Directive must be interpreted as permitting the data protection authority of a Member State to apply its national law on data protection with regard to a data controller whose company is registered in another Member State and who runs a property dealing website concerning properties situated in the territory of the first of those two States.

[14] *Id.*

[15] *Id,* at 31.

[15] Judgment of 13 May 2014, *Google Spain,* C-131/12, EU:C:2014:317, paragraph 45. [*Google Spain*] Facts of the case: An EU citizen sued Google Spain and Google Inc. requesting Google Spain and Google Inc. the removal or concealment of personal data relating to him so that certain information ceased to be included in search results. The regulatory agency considered that operators of search engines are subject to data protection legislation given that they carry out data processing for which they are responsible and act as intermediaries in the information society. Question asked to the CJEU: Whether the Directive is to be interpreted as meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State when 1 or more of the following 3 conditions are met: (i) the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State, or (ii) the parent company designates a subsidiary located in that Member State as its representative and controller for two specific filing systems which relate to the data of customers who have contracted for advertising with that undertaking, or (iii) the branch or subsidiary established in a Member State forwards to the parent company, located outside the EU, requests and requirements addressed to it both by data subjects and by the authorities with responsibility for ensuring observation on the right to protection of personal data, even where such collaboration is engaged in voluntary.

[16] Judgment of 28 July 2016, *Verein Fur Konsumenteninformation*, C-191/15, EU:C:2016:612, paragraph 76. [*Verein Fur Konsumenteninformation*] Facts of the case: Amazon EU (established in Luxembourg) has a website with a domain name ".de" and addresses consumers in Austria, with whom it concludes electronic sales contracts. The regulatory agency brought an injunction to prohibit the use of the terms of the contracts since they were contrary to legal prohibitions. Question asked to the CJEU: Whether the Directive must be interpreted as meaning that the treatment of personal data by an undertaking engaged in electronic commerce is governed by the law of the Member State to which that undertaking directs its activities.

[18] *Weltimmo*, paragraph 25.

[19] *Verein Fur Konsumenteninformation*, paragraph 79.

[20] *Google Spain,* paragraph 52.

[21] *Id.* at 60.

[22] Known as the "marketplace principle" or "service-oriented approach." This principle has been brought up by Article 29 Working Group in the Working Paper 179 as a suggestion for the Directive. However, we believe that the GDPR has taken such principle since it has included the concept of "offering" which implies intent. The marketplace principle consists that the activity involving the processing of personal data is targeted at individuals in the EU. This would need to consist of substantial targeting based on or taking into account the effective link between the individual and a specific EU country. The Working Party notes that this criterion is already used in the field of consumer protection: applying it in a data protection context would bring additional legal certainty to controllers as they would have to apply the same criterion for activities which often trigger the application of both consumer and data protection rules.

[23] This is a new addition, which was not in the Directive, of the territorial scope of the GDPR to protect private date within the EU.

[24] GDPR, article 3.2.

[25] Judgment of 7 December 2010, *Pammer Hotel Alpenhof*, C-585/08 and C-144/09, EU:C:2010:740. Facts of the case (*Pammer v Reederei*) [*Pammer Hotel Alpenhof*]: A consumer who resided in a different Member State from that of the company, concerns a voyage by freighter from Italy to the Far East organized by that company, though an intermediary company, which gave rise to a contract

between it and the consumer. The voyage turned out not to be like the voyage described and the consumer sued seeking reimbursement. Facts of the case (*Hotel Alpenhof v Heller*): A consumer who resided in a different Member State from that of the company, reserves rooms from the company's website. His reservation and confirmation were effected by email, the company's website referring to an address for that purpose. The consumer found fault in the company's services and left without payment. The company sued the consumer. Question that both cases asked to the CJEU: on the basis of what criteria a trader whose activity is presented on its website or on that of an intermediary can be considered to be 'directing' its activity to the Member State of the consumer's domicile, within the meaning of Article 15(1)(c) of Regulation No 44/2001, and, whether the fact that those sites can be consulted on the internet is sufficient for that activity to be regarded as such.

[26] Case C-96/00 *Gabriel* [2002] ECR I-6367, paragraph 37

[27] *Pammer Hotel Alpenhof,* paragraph 67.

[28] *Id,* paragraph 66.

[29] *Id,* paragraph 68.

[30] GDPR Preamble paragraph 23.

[31] *Pammer Hotel Alpenhof,* paragraph 81.

[32] *Id.*

[33] *Id.* paragraph 83.

[34] *Id,* paragraph 85.

[35] GDPR, Preamble paragraph 23.

[36] *Pammer Hotel Alpenhof,* paragraph 77.

ABA Section of International Law
Your Gateway to International Practice

EUROPE UPDATE

ABA ● Section of International Law ● Europe Committee

EUROPE UPDATE

American Bar Association

Section of International Law,
Europe Committee©

Europe Committee Website:

http://apps.americanbar.org/dch/committee.cfm?com=IC825000

Read all our newsletters on the website and LinkedIn!

Europe Committee **LinkedIn Group** - ABA International II:Europe:

http://www.linkedin.com/groups/ABA-International-II-Europe-4378315/about

The Europe Committee continuously seeks qualified professionals prepared to contribute their time and talents to continue developing a more active Committee. This is a prime opportunity to become involved with a community of lawyers that share an interest in Europe and European law, who are fellow American Bar Association members.

The Europe Committee welcomes any suggestions, ideas or contributions to enhance this occasional publication.

If you are interested in participating actively with the Committee, please contact any member of the Committee Leadership.

EUROPE UPDATE CURRENT ISSUE: DATA PRIVACY EDITION

GUEST EDITORS

Michael L. Balistreri and Jörg Rehder