COUNTDOWN TO THE GDPR & BEYOND

MLEX REPORTS FROM THE IAPP EUROPE DATA PROTECTION CONGRESS 2017
MLex is the leading independent media organization providing insight, commentary and analysis on regulatory risk and opportunity in North America, Europe, Asia and Latin America.

We monitor the activities of governments, agencies and courts and report and analyze the impact of the proposals, decisions and rulings on business.

Our subscription-only services include comprehensive coverage of:

- Antitrust & Competition
- Anti-Bribery & Corruption
- Brexit
- Data, Privacy & Security
- Energy & Climate Change
- Financial Services
- Mergers & Acquisitions
- Telecoms & Media
- Trade

FOR MORE DETAILS
www.mlexmarketinsight.com
US: +1 202 909 2131
UK: +44 (0) 20 3429 5900
EU: +32 (0) 2 300 82 50
HK: +852 2965 1502
LETTER FROM CHIEF TMT CORRESPONDENT MAGNUS FRANKLIN

In six months, the EU will breathe life into arguably the world's strictest privacy law, the General Data Protection Regulation, and companies are not wasting time getting ready. Compliance departments are rushing to prepare their data-handling operations to conform with the new rules, but doing so is time-consuming and costly.

MLex senior correspondent Vesela Gladicheva and I spent two full days drilling into the details of how companies are preparing, and how the thinking of regulators is evolving, at an annual gathering of privacy experts in Brussels, the IAPP Europe Data Protection Congress on Nov. 8-9, 2017.

Proposed new obligations for telecom companies, social networks and a new generation of online communications providers drew particular attention at the event. Regulators shed light on new plans to open up the ability of law enforcement to tap into the databases of these companies, while other regulators and lawmakers suggested privacy obligations could be tightened for these same services.

Two ongoing court cases, testing the EU’s data-transfer agreement with the US – the “Privacy Shield” – and a template for GDPR compliance for international transfers more generally, known as Standard Contractual Clauses, are making companies anxious. But at the same time, some businesses are giving a new lease of life to a third transfer system, previously maligned as being overly burdensome, known as Binding Corporate Rules.

And staying on the subject of international transfers, MLex spoke exclusively to a top EU official seeking to reassure Japan that its membership of a Pacific-Rim privacy agreement doesn't necessarily derail its efforts to get a data-transfer agreement with the EU.

If data is the oil of the digital economy, the price of crude is now going up, and in half a year, regulators will start to demonstrate to companies what risks they face if they fail to comply. MLex will continue to track every step along the way.

If data is the oil of the digital economy, the price of crude is now going up, and in half a year, regulators will start to demonstrate to companies what risks they face if they fail to comply. MLex will continue to track every step along the way.

CONTRIBUTORS

Magnus Franklin
Chief Telecoms, Media and Technology Correspondent

Magnus joined MLex in 2008 and is based in Brussels. He has reported blow-by-blow the end of roaming surcharges, the drafting of the EU’s new privacy regulation GDPR, the race to 5G and the response to services like Spotify and Netflix. He reports on topics including telecom regulation, cybersecurity, privacy and copyright, focusing on EU regulatory and legal risk in the telecoms, media and technology (TMT) sectors. He also helps coordinate global reporting on these topics with other MLex journalists, like the impact on Japan of EU privacy rules. Magnus studied journalism and economics in London, and previously worked at Informa Telecom and Media’s newsletters. Magnus works in English, Spanish, French and Swedish.

Vesela Gladicheva
Senior Correspondent, Telecoms, Media, IT

Vesela covers European regulation in the telecoms, IT and media sectors, and its impact on digital technologies, broadband, spectrum, data protection and copyright. She holds a Master’s degree in journalism from City University London, and works in English, Spanish, French and Bulgarian.
Online-tracking consent will be required from May, EU official says  

Get your EU data-transfer tool approved, BMC Software exec says  

EU’s Privacy Shield concerns likely to be shared by national watchdogs  

Judge data-transfer contracts on their own merits, EU official says  

Privacy Shield will survive legal challenges, EU Commission official says  

E-privacy rules must cover all communication types, leading EU lawmaker says  

Rules to request online evidence should be ‘broad,’ says senior EU aide  

Japan’s part in Apec data-transfer system not a big risk for EU privacy deal, official says  

The belt-and-braces approach to EU data-transfer approval is gaining momentum
Online-tracking consent will be required from May, EU official says

8 November 2017 | Magnus Franklin

The requirement for online advertisers to get consent from web users to deliver targeted advertising will come into force in May 2018, regardless of whether EU legislators have agreed on a new e-Privacy regulation covering such operations, an EU official said today.

Rosa Barcelo, head of unit for digital privacy at the European Commission, told delegates at a conference today that the strict consent requirements in the EU’s General Data Protection Regulation (GDPR) will start applying to the old 2009 e-Privacy law when it comes into force on May 25, 2018.

The comments tap into a debate on whether online marketers will need explicit consent to serve targeted advertising, after the European Parliament proposed tight rules for such activities. Advertisers and publishers have warned that such a rule would pull the plug on the bulk of online business models that offer content for free in exchange for the possibility of building a profile of people as they surf the web, and tailoring adverts to match their browsing patterns.

Barcelo said “the rules have not changed, but something important that has changed is that the definition of consent in the GDPR will start applying in May.”

“Even if the new regulation on e-Privacy is not adopted, the consent rule will apply to the old directive,” she added.

In practice, this means that advertisers placing “cookies”, small files on computers that have an identifier that allows them to track users across the websites they visit, will need to get the freely given consent of users to carry out such tracking.

The stricter consent rule will also have a bearing on a parallel discussion about whether it is legal for websites to introduce “cookie walls.” In other words, whether a website can block a visitor that doesn’t agree to being tracked. The European Parliament has proposed to ban such behavior.

Karolina Mojzesowicz, the commission’s deputy head of unit for data protection, said it didn't want to make a clear-cut rule on whether cookie walls should be banned, saying that this analysis should be done on a case-by-case basis.

CONTINUED NEXT PAGE
“If there is still an option, for example you can have access to the page by paying a not-prohibitive price, there is an alternative to accessing the service without giving consent, you could argue,” she said, suggesting that such a scenario would mean a website could block a visitor that neither paid, nor agreed to be tracked.

Ralf Bendrath — a privacy policy expert working for EU Parliament member Jan Philipp Albrecht, who was responsible for the drafting of the GDPR — said advertisers were wrong to say a ban on cookie walls would break the business models of the Internet.

“You could, as a website operator, count your audience, or where they come from, if you do it only for statistical purposes, and not individual targeting,” Bendrath said, suggesting that the Parliament was only cracking down on the most intimate forms of advert-targeting practices.

But Barcelo warned against introducing an explicit cookie-wall ban: “To say what the parliament has said, that cookie walls are prohibited, you risk creating different treatments for different situations that might be similar.” For example, a website that requires a user to log in before accessing a service, using for example an e-mail, would be allowed to block non-registered visitors, whereas a website that delivered adverts via cookies would not be allowed to block them if they declined to consent to tracking.

Barcelo said that the European Parliament has adopted its proposed amendments to the e-Privacy regulation in a vote last month, but there is no sign when governments, which also have the right to propose changes, will agree a version of the law.

She said the commission is working with Estonia and Bulgaria, which chair EU legislative talks in the remainder of 2017 and first half of 2018, respectively, “to help and assist them so they can reach a position as soon as possible and can sit down with the European Parliament” to hammer out a final compromise text.

“At the moment it is not possible to say when they will reach such a position,” Barcelo added.
Get your EU data-transfer tool approved, BMC Software exec says

8 November 2017 | Vesela Gladicheva

A senior executive at BMC Software has said companies are better off winning regulatory approval for their data-transfer procedures, to ensure they don’t later fall foul of EU data-protection rules.

Elodie Dowling said such approvals, known as binding corporate rules or BCRs, are costly, but that companies gain a competitive edge and can avoid multimillion-euro fines.

Once the EU’s General Data Protection Regulation, or GDPR, comes into force next May, “there isn’t much choice any more with regard to whether or not the company is willing to make that investment,” said Dowling, who is general counsel for BMC Software’s operations in Europe, the Middle East and Africa, during a conference in Brussels today.

At least 88 businesses – including General Electric, Hewlett-Packard and Intel – use BCRs to establish internal standards, for example when transferring information to entities in countries that don’t offer a level of data protection that the EU considers adequate. BCRs must be approved by the privacy regulator in the country where the company has its European headquarters.

Houston, Texas-based BMC Software obtained accreditation for using BCRs for data transfers as a controller and processor of personal information from the French data-protection authority in 2015, following a two-year process.

BCRs might be the “best tool” for companies – including smaller organizations such as BMC Software – looking to secure the location of, and access to, personal information they hold, Dowling said.

BMC Software employs 6,000 people in 45 countries.

Dowling also said the mechanism could be useful for companies in the early stages of adopting compliance programs for the new EU rules.

Crucially, BCRs could help companies avoid heavy sanctions for violations, because the instrument is vetted by a data-protection authority and shows the business’s commitment to respect the law, she said.

CONTINUED NEXT PAGE →
“At some point in time, when the regulators will look at potentially fining your organization, I’m sure this will probably be a mitigating factor,” she said. “At least, we are hoping.”

Under the GDPR, BCRs will be available to companies engaged in a joint economic activity. Applications for BCR approval will trigger a detailed cooperation structure among European data-protection authorities.

EU data-protection authorities are currently updating BCRs, and plan to complete their work by end of the year.

“At some point in time, when the regulators will look at potentially fining your organization, I’m sure this will probably be a mitigating factor,” she said. “At least, we are hoping.”
EU’s Privacy Shield concerns likely to be shared by national watchdogs

8 November 2017 | Magnus Franklin and Vesela Gladicheva

European privacy regulators are likely to find flaws in a US-EU data transfer agreement known as Privacy Shield when they finish their evaluation at the end of the month.

But the watchdogs’ concerns will broadly match those already identified by the European Commission, Ireland’s data protection chief Helen Dixon said.

“I think what we are going to see are recommendations and concerns expressed, from the Article 29 Working Party, that to some extent match those of the commission,” Dixon said at a conference today, referring to the umbrella group of national privacy authorities.

“I would anticipate that we will be making recommendations around tightening up the checks that are conducted by the [US] Department of Commerce. In particular, concerns on aspects of onward transfers,” she said.

Dixon said the watchdogs were likely to take issue with FISA 702, a US law that sets the rules for how intelligence agencies carry out surveillance of foreigners, which is due to be renewed by the end of the year.

Watchdogs are also likely to be concerned that “there isn’t a permanent person appointed” to take an ombudsman role under the Privacy Shield to handle complaints about the transfer system.

Privacy Shield survived scrutiny by the European Commission, subject to a number of improvements similar to those outlined by Dixon, in areas including enforcement and the appointment of key oversight roles for the agreement by the US government.

The deal took effect in 2016, and allows companies transferring personal data from Europe to the US to self-certify compliance with EU privacy regulations. In exchange, they don’t have to go through burdensome individual approvals by EU watchdogs. The certification system is policed by the US Federal Trade Commission and Department of Commerce.
Judge data-transfer contracts on their own merits, EU official says

9 November 2017 | Vesela Gladicheva

Facebook’s transatlantic data-transfer contracts don’t need to meet the same high legal bar as EU rulings on foreign privacy regimes, a senior European Commission official has said.

And that’s a message the commission will also be telling EU judges as they handle a new Irish dispute over the social-media company’s handling of users’ data.

Bruno Gencarelli said a variety of ways are available to lawfully move data outside the bloc, and that European judges shouldn’t apply the same test to contractual clauses as to “adequacy” decisions on third countries.

“What for us is very important is that the diversity of [EU] transfer tools ... is fully recognized,” according to Gencarelli, who heads the EU executive’s department for international data flows and protection.

The comments came a month after the Irish High Court decided to seek guidance on the case from the EU Court of Justice in Luxembourg. The referral could cause uncertainty for companies handling personal information in the EU, which commonly shift data from the bloc to other countries under the terms of these contracts.

“We will certainly be active on that case,” Gencarelli told a conference in Brussels, confirming that the commission would formally “intervene” to offer its views before the EU court.

An adequacy decision issued by the commission ranks highest of all data-transfer methods in terms of robustness, Gencarelli said.

“It cannot be that the same test is applied across the board to all EU transfer tools,” he said.

“The practice shows these tools have been considered to be subject to different tests and conditions,” the official said.

In 2015, the EU court invalidated the EU-US Safe Harbor data-transfer accord, which had been used by thousands of companies since 2000. The instrument — which had confirmed that the American legal system ensures a level of data protection similar to that of the EU — failed to provide sufficient safeguards to European residents, the court ruled.
Privacy Shield will survive legal challenges, EU Commission official says

9 November 2017 | Vesela Gladicheva

The Privacy Shield data-transfer accord between the EU and US should ride out court challenges over its lawfulness, the deputy head of the European Commission’s international data flows department said today.

The deal, which allows more than 2,500 companies to transfer personal information across the Atlantic, meets the requirements set out by the bloc’s highest court, Ralf Sauer told privacy experts at a conference in Brussels.

“I’m confident that we’ll still see Privacy Shield in two years,” Sauer said, referring to how long it might take to resolve pending challenges if accepted by the EU courts. “We think it’s lawful.”

Privacy Shield was drawn up to replace the Safe Harbor agreement, annulled in 2015 by Europe’s highest court for failing to safeguard EU citizens’ personal data. Sauer said its replacement fulfils the EU Court of Justice’s criteria for improvements.

Last autumn, however, civil-rights organizations in France and Ireland brought separate cases to the EU’s lower-tier General Court seeking to annul the Privacy Shield accord. They say it fails to protect Europeans from mass surveillance by US intelligence services.

EU judges have yet to decide whether to review the lawsuits. The EU executive has lodged an “application for inadmissibility” against Digital Rights Ireland’s case in a bid to dismiss it early on.

The US government has asked to intervene in both court actions.

Speaking at the same conference today, a senior US Department of Commerce official said the government was closely monitoring the lawsuits.

“Privacy Shield was designed specifically to withstand new challenges,” said James Sullivan, who is deputy assistant secretary for services and international trade.
E-privacy rules must cover all communication types, leading EU lawmaker says

9 November 2017 | Vesela Gladicheva

All companies providing electronic communications – from the likes of Skype, WhatsApp and Instagram to dating apps, online games and Internet-connected devices – should fall under revised EU telecom-privacy rules, a leading European lawmaker said today.

That was the view of the lawmaker leading the European Parliament’s work on the e-Privacy Regulation today, suggesting a step up in lobbying efforts by technology companies and advertisers could follow.

Speaking at a conference in Brussels, Birgit Sippel, a German Socialist, also said the EU should force companies to seek permission from users before they handle personal data, rejecting concerns by businesses that the move would give individuals “consent fatigue” and endanger media pluralism.

“Confidentiality of communications is essential for the respect for other fundamental rights and freedoms,” such as freedoms of expression and of information, said Sippel, who was recently appointed to lead the assembly’s negotiations on the bill.

Sippel’s remarks come weeks after the parliament agreed on a common position on the bill. Lawmakers are now waiting for national governments to adopt a position so that negotiations can begin on a final consensus text for the regulation. Sippel said those talks should start early next year.

She called it “absurd” that telecom operators enabling subscribers to send text messages are subject to the EU’s existing e-privacy rules while so-called over-the-top services such as WhatsApp and Skype aren’t covered.

The lawmaker also stressed that machine-to-machine communications should be covered by the updated rules whenever they carry users’ personal information. “As the Internet of Things and connected devices gain momentum, we have to find ways to protect their communication data too,” Sippel said.

CONTINUED NEXT PAGE
Here, she said, legislators will need to define in more detail the cases that the rules should cover.

The scope of the bill should be extended also to cover ancillary online services with communication features, including dating applications and messaging within apps such as online games, because communications might be sensitive, Sippel said.

**Consent**

The German lawmaker said the EU should oblige companies by default to obtain permission from users before collecting and handling their data.

She rejected arguments made by tech industry companies, including advertising businesses, that repeatedly asking users for consent will lead to “consent fatigue” and endanger media pluralism.

“What we are aiming at is to abolish the current practice of surveillance-driven advertising,” Sippel said.

She also addressed the question of companies using “legitimate interest” to collect and process personal data, saying this legal basis can’t be used for sensitive information such as health data, regardless of whether it is content data or metadata.

“What we are aiming at is to abolish the current practice of surveillance-driven advertising,” Sippel said.
Rules to request online evidence should be ‘broad,’ says senior EU aide

9 November 2017 | Vesela Gladicheva and Magnus Franklin

A regime to let law-enforcement officers request online evidence should be as broad as possible, according to Renate Nikolay, chief of staff of EU justice commissioner Věra Jourová.

The European Commission is working on a “European production order system” to manage law-enforcement requests for “e-evidence” from cloud-computing providers, messaging and voice-chat platforms, and other online services, Nikolay said at a conference today.

There is a “lack of clarity on the legal obligations” online companies face when they are approached by law enforcement, Nikolay said. “We want to go a step further.”

The new proposal could be broader, and encompass more categories of data that companies would need to make available, as compared with previous EU laws drafted in the wake of major terrorist incidents, she said.

“Is it content data, is it metadata, is it subscription data?” said Nikolay. “We want to be as broad as possible.”

EU justice ministers are set to debate a report on the retention of communications data at a meeting in December, which has been circulated internally among governments but not made public. The report analyzes the effects of EU Court of Justice rulings in this area on domestic laws.

The commission has run into trouble with previous legislative attempts in this area. A data-retention law that obliged telecom providers to give up call locations and other data was struck down by the EU Court of Justice in 2014 – and that only applied to serious crime. Nikolay said today that the commission wants the new proposal to apply to less-serious crimes too.

Still, EU justice ministers are set to endorse a memo that broadly supports the idea to develop EU legislation in this field, with a view to combating cybercrime.

The Council of Europe, a non-EU body that includes countries bordering the bloc, also adopted guidance on production orders in March 2017, setting out an extensive analysis of the problems the commission is trying to solve.
Japan’s part in Apec data-transfer system not a big risk for EU privacy deal, official says

10 November 2017 | Vesela Gladicheva and Magnus Franklin

Japan’s chances of reaching a deal with Europe on data-privacy standards is unlikely to suffer from its entry into an Asia-Pacific data-transfer deal, according to a senior EU official.

Bruno Gencarelli told MLex in the sidelines of a conference that “Japan’s compliance with privacy law is not simply, or not mainly, to do with its adherence to the Apec [Cross Border Privacy Rules] system. It has a much harder law.”

Gencarelli, who heads the European Commission’s international data flows and protection unit, was referring to Japan becoming the first fully functional member – besides the US – of the Asia-Pacific Economic Cooperation forum’s CBPR.

The US-based system is intended to build international digital commerce and data transfers between economies in Asia and in North and South America.

Gencarelli’s comments come at a time when Japan is racing to win a finding of “adequacy” status from the EU by next May, when Europe’s sweeping new privacy law, the General Data Protection Regulation, or GDPR, takes effect.

Proponents of the CBPR say they see no conflict between the two, and the secretary general of Japan’s Personal Information Protection Commission, Mari Sonoda, has said Japan’s membership has not been a significant topic of interest for EU officials as the two sides work on the mutual adequacy finding.

Gencarelli’s comments will discomfit experts who have predicted that the CBPR agreement could prove a headache for Japan in its EU adequacy push.

“What we are assessing is the level of protection ensured by the new Japanese law, which entered into force last May, and the creation of an independent supervisor,” Gencarelli said. A new Japanese privacy law was implemented in May, following the establishment last year of the Personal Information Protection Commission.
Japan’s CBPR membership is just “part of the context,” said Gencarelli, referring to concerns over whether companies handling EU citizens’ personal data can transfer them to countries where privacy systems do qualify for the Asia-Pacific rules, but not for the higher EU standards.

“Japan has a law and a data-protection authority,” said Gencarelli, adding that the country “doesn’t only rely on a certification” to ensure high standards of privacy, suggesting robust underlying structures for protecting privacy.

“Japan’s compliance with privacy law is not simply, or not mainly, to do with its adherence to the Apec [Cross Border Privacy Rules] system. It has a much harder law.”
The belt-and-braces approach to EU data-transfer approval is gaining momentum

10 November 2017 | Vesela Gladicheva and Magnus Franklin

They may be seen as cumbersome, slow and often costly, but binding corporate rules are beginning to look very attractive to multinationals with big data-crunching operations looking to secure EU regulatory approval for data-transfers abroad.

The increasing appeal of BCRs lies primarily in uncertainty surrounding the legality of other simpler transfer methods: specifically fears that the EU-US Privacy Shield and so-called standard contractual clauses could be declared void by the EU courts.

Standard contractual clauses are templates pre-approved by watchdogs for use in contracts, while “adequacy” agreements such as Privacy Shield let companies self-certify compliance.

By contrast, BCRs have been seen as overly complicated and drawn out. They are internal procedures governing how multinationals make intra-company transfers from country to country. They must be approved by the data-protection authority in each EU country the data will touch, and getting approval typically takes between one and two years.

But BCRs are gaining a new lease of life as companies worry about the future of overarching agreements such as Privacy Shield – and realize that complying with EU data-privacy rules entails much of the same work as getting certified for international data transfers, so it is efficient to do both at the same time.

“I would encourage companies to look at binding corporate rules, where they can be applicable,” said Helen Dixon, the Irish Data Protection Commissioner, recently.

“A lot of the bigger companies we talk to that implement binding corporate tools have said to us that they have proved to be hugely useful accountability tools within [their] organizations,” she said, adding that each company should look at the various mechanisms available and see which is most appropriate for it.

Negotiations on BCRs happen on two levels. First, the company needs to justify its legitimate interest for transferring data; that is normally easy. Second, the extent of the company’s adequacy will be scrutinized; that means a lot of preparatory work.

CONTINUED NEXT PAGE
But many of the things that companies will need to demonstrate for BCR compliance are the same as the ones they need to show if the data protection authority comes knocking after EU data-protection rules enter into force on May 25, 2018.

**Precautions**

Privacy experts at a conference this week said that companies with BCRs will be in an enviable position if the EU courts invalidate the use of standard contractual clauses or knock down the fledgling the EU-US Privacy Shield, both of which are being contested before the EU’s Court of Justice.

While EU officials say this is unlikely to happen, the court over past years has had a track record of ruling in favor of strong privacy protections – including the EU Court of Justice declaring Safe Harbor, the predecessor EU-US agreement to Privacy Shield, invalid in October 2015.

MLex has learned that a key trigger for a wider use of BCRs will be an upcoming set of guidelines from European data-privacy regulators to clarify when companies that team up are considered to be “joint controllers” of the use of a person’s data, and what measures should apply in such cases.

If the implementation of rules around joint controllers is done strictly, BCRs may be a tool to divide liability in case of a violation, which under current rules could amount to 4 percent of global turnover for each of the companies involved.

And it is the compliance risk that is the principal reason for companies to opt for the resource-intensive route of getting BCRs approved. “I’m sure at some point in time, when the regulators will look at potentially fining your organization, I’m sure that this will probably be a mitigating factor. At least, we are hoping,” BMC Software’s Elodie Dowling told the conference.
MLex’s unique insight, analysis and commentary delivers investigative and forensic coverage of cases working their way through decision-making bodies and regulatory agencies around the world.

Regulatory change is coming. Be ready. Be the first to understand how regulatory change impacts your clients. Request a free trial.