Bloomberg Law®

Corporate Privacy & Security Challenges

The Countdown Begins:

Perspectives to Help Companies Prepare for the New EU Privacy Regime

Table of Contents

There is no doubt about it – companies doing business with EU countries – and the firms that counsel them – must prepare now to meet complex compliance requirements and avoid costly fines that are scheduled to change the landscape in 2018.

Here, we discuss some of the essential perspectives, cases and developments.

EU Privacy Regime Changes and Data Transfers

Privacy & Security Law Report®

February 20, 2017

Bloomberg BNA

Data Transfers

Onward Transfers of Data Under the Privacy Shield: Keeping the Shield from Becoming a Sword

EU-U.S. Privacy Shield

A central component in the Privacy Shield framework is the concept of "onward transfers"—in which a certified company transfers data onward to another controller or to a third-party agent, such as a service provider. The authors provide tips for companies that are determining whether they are ready to certify with respect to the onward transfer requirements.




By Kendall Burman, Rebecca S. Eisner and Lei Shen

Kendall Burman is cybersecurity & data privacy counsel at Mayer Brown LLP in Washington. Prior to joining Mayer Brown she served in the administration of President Barack Obama, most recently as a deputy general counsel for the U.S. Department of Commerce.

Rebecca Eisner is partner-in-charge of Mayer Brown's Chicago office. One of her main client issues is data privacy and security. She regularly advises clients on global data transfers and privacy issues, privacy assessments and privacy compliance.

Lei Shen is an associate in Mayer Brown's Chicago office and advises clients on a wide range of global data privacy and security issues.

Companies in the U.S. that wish to import personal data from the European Union have a few adequacy options to choose from, including the EU-U.S. Privacy Shield framework. However, companies should know that certification under the Privacy Shield framework requires more than just filling out forms and providing payments. Companies that self-certify to the Privacy Shield must commit to upholding the data protection standards of the Privacy Shield, and that means ensuring that your internal practices and policies are aligned with the principles to which you certify.

The Privacy Shield framework is a successor to the U.S.-EU Safe Harbor framework, which was ruled invalid by the Court of Justice of the EU in October 2015. The invalidation of the Safe Harbor framework meant that for the approximately 4,500 companies that were relying on it for their data transfers, they had to either cease importing personal data into the U.S. or find a legally acceptable alternative mechanism. In the absence of an agreement between the U.S. and the EU, many companies turned to the standard contractual clauses issued by the European Commission for transfers to controllers or to processors,

which were deemed to offer sufficient safeguards with respect to the protection of privacy and fundamental rights under EU law.

The foundation of the Privacy Shield framework, like the U.S.-EU Safe Harbor before it, are the seven core principles of data protection that companies must implement in order to certify for Privacy Shield, and to remain in compliance with it: Notice; Choice; Accountability for Onward Transfer; Security; Data Integrity and Purpose Limitation; Access; and Recourse, Enforcement and Liability. In addition to these core principles, the Privacy Shield adds 16 supplemental principles that strengthen the privacy protections of several of the core principles through heightened protections and stricter language. The Onward Transfer principle is one of the principles that have been further strengthened under the Privacy Shield.

Under the Onward Transfer principle, a Privacy Shield-certified company must ensure that certain rules are followed when transferring data onward to another controller or to a third-party agent, such as a service provider. While companies that certified for Privacy Shield before Sept. 30, 2016 have a nine-month grace period since they certified to bring their existing commercial relationships into compliance with these Onward Transfer rules, companies that are considering certifying now for the first time must be in compliance with such rules prior to certification. Either way, it is critical that these companies take the necessary actions with respect to onward transfers.

Rules for Conducting Onward Transfers

The Onward Transfer principle treats onward transfers of data to data controllers differently from onward transfers of data to a third party acting as an agent, such as a cloud service provider or other data processor. A controller is understood to be a third party who has the authority to use the information for its own purposes, whereas an agent is a third party that is acting under the instructions of the certifying company, such as an information technology service provider. The protections of the Privacy Shield continue applying to any data that were transferred under it, including to any further transfers of such data to another entity. The Privacy Shield ensures the continued protection of such data by mandating specific requirements for onward transfers of data between Privacy Shield-certified companies and third parties acting as controllers, and contracts between certified companies and agents.

The Onward Transfer principle treats onward transfers of data to data controllers differently from onward transfers of data to a third party acting as an agent.

Contracts between a Privacy Shield certified entity and a third-party controller must include the following:

- data can only be processed for limited and specified purposes consistent with the consent provided by the individual;
- the third-party controller must provide the same level of protection as the Privacy Shield principles; and
- if the third-party controller can no longer provide the same level of protection as the Privacy Shield principles, the contract must require that the controller cease processing and or take other reasonable and appropriate steps to remediate.

A Privacy Shield certified company must take the following actions with respect to a third-party agent, and while some of these steps are actions for the certified company to take, it is recommended that all of them be captured in contractual requirements binding the third-party agent:

- transfers of data must be only for limited and specified purposes;
- companies must ascertain that the agent is obligated to provide at least the same level of privacy protection required by the Privacy Shield principles;
- companies must take reasonable and appropriate steps to ensure that the data is processed by third-party agent in a manner consistent with the companies' obligations under the Privacy Shield principles;
- require that companies be notified by third-party agent if they determine they can no longer meet those obligations, and, if so, take steps to stop and remediate; and
- companies must provide a summary or a copy of the relevant privacy provisions of its contract with the Department of Commerce if requested.

To better understand the Onward Transfer principle of the Privacy Shield, it may be useful to compare this new principle with

the corresponding requirements under the two other transfer mechanism with which companies are likely most familiar—the invalidated U.S.-EU Safe Harbor Framework and standard contractual clauses from the EU Commission.

Strengthened Onward Transfer Requirements Under Privacy Shield as Compared to Safe Harbor

The Safe Harbor framework included an Onward Transfer principle that required certified companies to take certain steps with regard to third parties with whom they shared their data. Similar to the Privacy Shield framework, those steps included the application of the Notice and Choice principles to third parties acting as controllers, as well as some process for ensuring that third parties acting as agents take steps to protect the data they receive. Unlike the Privacy Shield, certified companies were free to do this by confirming that the third party subscribes "to the Principles or is subject to the [EU Data Protection] Directive or another adequacy finding or enters into a written agreement… requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles."

The Safe Harbor framework clarified that contracts between data controllers and processors are always required and that the contract must specify the processing to be carried out and any measures necessary to ensure that the data is kept secure. The Onward Transfer principle in the Safe Harbor Framework also made clear that if a third party processes the data in a way that is contrary to the restrictions or representations of the contract, then the certified company will not be held responsible unless they knew or should have known or failed to take reasonable steps to prevent or stop such processing.

In the lead up to the invalidation of the Safe Harbor framework, representatives of the EU data protection authorities as well as the European Commission itself raised concerns over the application of the Safe Harbor principles, and asked whether there was sufficient enforcement of the Safe Harbor principles as applied to third-party agents such as cloud services providers.

The Privacy Shield framework made several changes to address those concerns. Under the Privacy Shield's Onward Transfer principle, certified companies transferring data to third-party agents are required to take reasonable and appropriate steps to ensure that the third party is processing data in a manner consistent with the Privacy Shield principles, and must require that the third party notify them if they determine they can no longer abide by those principles. And, in its principle on Recourse, Enforcement and Liability, the Privacy Shield makes clear that a certifying company has responsibility for and remains liable under the principles for data it transfers to a third-party agent for processing, unless the certifying company can prove that it is not responsible for the event giving rise to the damage. Unlike under the Safe Harbor framework, the Privacy Shield places the burden on the certifying company to prove that they were not liable for any processing of transferred data in violation of the Privacy Shield principles.

The Privacy Shield principles differ from the obligations imposed on data importers under the standard contractual clauses.

Differences Between Standard Contractual Clauses and Privacy Shield

Many companies considering certifying to the Privacy Shield may have standard contractual clauses included in their contracts with third parties for data transfers. Companies should consider carefully whether these clauses are sufficient for the purposes of satisfying the Onward Transfer principle in the Privacy Shield. In many cases, companies will need to negotiate separate and additional requirements into their third-party contracts in order to fully comply with the Privacy Shield. The Privacy Shield requires that third parties provide at least the same level of privacy protection as is required by the Privacy Shield principles, and that the information is processed by the third-party agent in a manner consistent with companies' obligations under the principles.

The Privacy Shield principles differ from the obligations imposed on data importers under the standard contractual clauses so companies certifying to the Privacy Shield may need to include different provisions in their contracts. Specifically, these contracts may need to be amended to add restrictions that are consistent with the Privacy Shield's requirements, including on further onward transfers (subcontracting), the ability to delete personal information after a change in choice by an individual, the requirement to subject the third party to audits and other verifications to ensure compliance with the Privacy Shield, and assistance in providing access to individuals for review and corrections, among others.

Concluding Tips

Separate addenda or Privacy Shield agreements may offer advantages: Companies will need to review their third-party agreements to determine how to amend them for onward transfer requirements. Unless a company has only a few agreements to review, drafting individual amendments to each third-party contract may be burdensome. You may consider drafting an addendum or Privacy Shield agreement that is intended to apply to all of your onward transfers, without specific

review of each third-party agreement. The addendum or agreement should supersede prior conflicting terms, and should cover all of the onward transfer requirements in one place. For companies that have numerous third-party relationships, one agreement or addendum may be the most practical way to bring the third-party contracts into compliance, versus independent review and amendment of each third-party agreement. The single addendum or agreement has the added benefit of avoiding disclosure of the entirety of your contract with a third party on the non-Privacy Shield terms, in the event that you are required to provide a copy of your third-party contract terms under Privacy Shield to the Department of Commerce.

Retain right to share contract: Certifying companies will want to consider including in their contract with third-party agents specific permissions to allow them to provide a copy of the relevant privacy provisions to the Department of Commerce since this is required of certifying companies if they are asked.

Track EU developments closely: Review of the Privacy Shield framework by the European authorities is baked into the language of the framework itself, allowing for annual review of how the framework's protections are implemented by certifying companies and administrative bodies. There has been much speculation over whether the Privacy Shield framework will survive such review given recent developments in both the EU and the U.S. To almost no one's surprise, the Privacy Shield, like the Safe Harbor framework before it, has been challenged in the European Court of Justice as insufficient to meet the EU's data protection standards. Suffice it to say, predicting the future of the Privacy Shield framework is difficult, and this dynamic area should be tracked closely.

Privacy & Security Law Report®

February 20, 2017

Bloomberg BNA

Data Transfers

The Continuing Impact of the Judgment of the Court of Justice of the European Union Declaring Invalid the European Commission's Decision on U.S.-EU Safe Harbor

EU-U.S. Privacy Shield

The Court of Justice for the European Union began a seismic year for data protection and cross-border data transfers by voiding the legal basis for transatlantic data transfers for the 4,400 companies reliant on U.S.-EU Safe Harbor, the authors write, the aftershocks of which will reverberate throughout 2017 and beyond.

By Cameron F. Kerry and William Long

Cameron F. Kerry is senior counsel at Sidley Austin LLP in Washington and Boston. Kerry is the former general counsel and acting secretary of the Department of Commerce, where he led the Obama administration's work on consumer privacy, including its engagement with the European Union on Safe Harbor and data protection.

William Long is a partner in Sidley's London office working on international privacy issues, was previously in-house counsel to one of the world's largest international financial services groups.

The decision by the Court of Justice of the European Union (the CJEU) on Oct. 6, 2015, invalidating the U.S.-EU Safe Harbor Decision (the Judgment) is a landmark judgment. Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015] ECLI:EU:C:2015:650. By voiding the legal basis for transatlantic data transfers for the 4,400 companies reliant on U.S.-EU Safe Harbor, the Judgment began what has been a seismic year for data protection and cross-border data transfers [1] in the European Union, whose aftershocks will reverberate throughout 2017 and beyond.

[1] Transfers of personal data to countries outside the European Economic Area may not take place under the Directive unless the recipient third country provides an adequate level of protection for the rights and freedoms of data subjects. The Commission under Article 25(6) of the Directive can make a finding of adequacy in respect of a third country by reason of its domestic law or the international commitments it has entered into. In addition, under Article 26(4) the Commission has the power to approve transfers of personal data made on the basis of certain standard contractual clauses which are deemed by the Commission to provide adequate safeguards for the rights and freedoms of data subjects.

The U.S. and EU moved quickly to put in place a new, reinforced data transfer framework in U.S.-EU Privacy Shield that responds to issues in the Judgment, and which was formally adopted by a European Commission adequacy decision on July 12, 2016. Nevertheless, the grounds of the Judgment invited challenges to the Privacy Shield and raised doubts about other existing data transfer mechanisms that could reshape the way in which data is transferred across the Atlantic and globally. Further, by empowering data protection authorities to review adequacy decisions independently of the European Commission, the Judgement has expanded avenues to challenge these mechanisms. At the same time, the passage of the EU's General Data Protection Regulation (GDPR) in May 2016 is requiring companies and DPAs with a great deal of preparation and many questions to answer by May 25, 2018. The only certain thing that one can say is that vast uncertainty is a feature of the EU privacy and data protection landscape in 2017 and, perhaps beyond.

Background

The Judgment was issued following a referral by the Irish High Court in the case of Maximilliam Schrems v Data Protection Commissioner. The case originates from a complaint filed with the Irish DPA against Facebook Inc.'s Irish subsidiary, Facebook Ireland Ltd. in respect of concerns raised by Austrian law student Max Schrems that electronic communications transferred from Facebook Ireland Ltd. to Facebook's servers in the U.S. in reliance on U.S.-EU Safe Harbor could be accessed by the U.S. government's National Security Agency's (NSA) PRISM surveillance program; a program that permits the NSA to target non-U.S. citizens for foreign intelligence purposes. The Irish DPA rejected the complaint as unfounded on the basis that it was obligated to follow the Commission's decision in 2000 on the adequacy of data protection under the Safe Harbor Framework. Mr. Schrems filed an application for judicial review in the Irish High Court. This application was granted but the case was adjourned on June 18, 2014 pending a referral to the CJEU for a preliminary ruling on the question whether the Commission's U.S.-EU Safe Harbor decision precluded a DPA from investigating complaints of inadequate levels of data protection in the U.S.

The only certain thing is that vast uncertainty is a feature of the European Union privacy and data protection landscape in 2017 and, perhaps beyond.

The CJEU Judgment

The Judgment contained two major rulings. Most significantly, the CJEU declared the Commission's U.S.-EU Safe Harbor decision invalid with immediate effect. In addition, the CJEU ruled that DPAs "must be able to examine with complete independence" whether international transfers of personal data from the EU comply with the requirements of the EU Data Protection Directive (the Directive), including adequacy requirements. However, the CJEU also confirmed that DPAs may not adopt measures contrary to a Commission decision of adequacy until such time as the decision is declared invalid by the CJEU and that only the CJEU has jurisdiction to make such a declaration.

Suspension of U.S.-EU Safe Harbor

The CJEU broke its analysis of invalidity of the Commission's U.S.-EU Safe Harbor decision into three parts; first analyzing the Commission's powers under Article 25 of the Directive to approve the Safe Harbor Framework. The CJEU then considered the derogation for national security in Annex 1 of the Commission's decision incorporated by Article 1 of the decision; this derogation parallels the derogation in Article 13 of the Directive. Finally, the CJEU addressed the provision in Article 3 of the Commission's decision that constrained the authority of DPAs to suspend data transfers pursuant to Safe Harbor.

In discussing the Commission's decision-making under Article 25, the CJEU reasoned that both the level of protection required for "adequacy" and the Commission's authority must be "read in light of the Charter of Fundamental Rights of the European Union" (the Charter). While the Charter did not become binding until the entry into force of the Treaty of Lisbon in 2009, the CJEU ruled that "account must also be taken of the circumstances that have arisen after the decision's adoption." As a result, adequacy requires that the level of protection for fundamental rights must be "essentially equivalent to that guaranteed within the European Union […]" and "the Commission's discretion as to the adequacy of the level of protection ensured by a third country is reduced […]" The Commission also must "check periodically" that the basis for adequacy remains justified.

The CJEU then applied these standards in light of the Charter to examine what the Commission's Safe Harbor decision did to ensure a level of protection equivalent to that in the EU. Although the CJEU in many respects followed the advisory Opinion of Advocate General Yves Bot, published shortly before the Judgment on Sept. 23, 2015, it took a different tack in addressing the claims in the case regarding U.S. government surveillance. The CJEU did not attempt to describe the U.S. legal system relating to surveillance. The CJEU instead referred to statements in Commission reports in 2013 that suggested lack of appropriate judicial redress for EU citizens in respect of their data subject rights and broad, undifferentiated access to personal data by U.S. authorities. It also found the Commission's decision on Safe Harbor did not include findings or provisions that address these matters.

The CJEU stated, with reference to the case of Digital Rights Ireland and Others, that in accordance with EU law "derogations and limitations in relation to the protection of personal data [must] apply only in so far as is strictly necessary" and this is not the case if public authorities are granted unfettered access to all personal data. The CJEU confirmed that a finding of adequacy based on a level of "protection essentially equivalent to that guaranteed within the [EU]" or "guaranteed in the EU legal order" requires an assessment of "the content of the applicable rules in that [third] country resulting from its domestic law or international commitments and the practice designed to ensure compliance with those rules …." The benchmark of the

level of protection within the EU logically calls for a similar assessment of the laws in the EU, including those relating to government surveillance by Member States.

The CJEU identified other requirements that must be addressed to establish “essentially equivalent” protections. These include “administrative or judicial means of redress, enabling, in particular, the data relating to [an individual] to be accessed…rectified or erased, which the CJEU considers an absence of respect for the essence of the “fundamental right to effective judicial protection.”

Finally, with regard to Article 3 of the Commission's decision on Safe Harbor, the CJEU held that the constraints on the DPAs' independent powers under Article 25 of the Directive exceeded the Commission's power. Given the procedural context of the case, the CJEU did not consider there to be “any need to examine the content of the Safe Harbor principles” and carry out the essential equivalency test itself.

Building on the decision in Digital Rights Ireland and Others, the CJEU's application of the Charter to the Commission's discretion under Article 25 of the Directive and its requirement that derogations for national security common to the Directive and other EU instruments do not obviate an obligation to ensure that certain fundamental rights are protected affects more than surveillance in the United States. A number of EU governments (including those in France and the U.K.) have had to consider their surveillance provisions in light of the recent attacks in Belgium, Paris and Germany. Although, at least from a U.K. perspective, the recently adopted Investigatory Powers Act 2016, referred to by privacy advocates as the “Snoopers Charter” will likely be subject to further review prior to entering into force as a result of the CJEU's recent ruling in Tele2 Sverige AB, which states that the “general and discriminate” way in which the U.K. government was retaining data for the purposes of criminal investigations was incompatible with EU law and indicates that the CJEU has an expansive view of its competence in the domain of national security and law enforcement. Tele2 Sverige AB v. Post-och telestyrelsen C-203/15, and Secretary of State for Home Department v. Tom Watson and Others C-698/15.

The Birth of the EU-U.S. Privacy Shield

Immediately following the issuance of the Judgment, the Commission stepped up ongoing talks with U.S. authorities to conclude a new framework on transatlantic data flows. Accordingly on Feb. 2, 2016, the Commission announced that a political agreement had been reached on the new framework now known as the EU-U.S. Privacy Shield and the draft documentation was published on Feb. 29, 2016.

According to the Commission, the EU-U.S. Privacy Shield is designed to “[protect] the fundamental rights of Europeans and [ensure] legal certainty for businesses, including European companies, transferring personal data to the U.S.” The framework expands on the principles set out in the Safe Harbor Framework and purports to address the concerns highlighted by the Judgement including in respect of onward transfers, redress mechanisms and the individual rights of data subjects.

As was the case under the Safe Harbor Framework, companies participating in the EU-U.S. Privacy Shield need to certify compliance with a number of Principles and Supplemental Principles. Although the Privacy Shield Principles are incorporated, some have been substantially rewritten, for example, the Accountability for Onward Transfer Principle includes a requirement to notify where a third-party recipient is unable to provide the same level of protection as is required under the Privacy Shield Principles. This is intended to ensure that requirements cannot be circumvented by transferring processing to a third party and that additional assurances in the Privacy Shield regarding access to data by government authorities remain in place where onward transfers take place.

The Article 29 Working Party (the Working Party) published an opinion on the draft documentation on April 13, 2016 (the WP29 Opinion). The WP29 Opinion acknowledged a number of significant improvements as compared to the Safe Harbor Framework with regards to commercial privacy issues but raised concerns including that the data retention principle was not explicitly referenced and that the redress mechanisms were too complex. With regard to access by public authorities, the Working Party expressed concerns regarding the independence of the ombudsperson and its lack of adequate powers to provide satisfactory remedy and the scope of a U.S. Government reservation for bulk surveillance in certain circumstances.

The European Parliament and the European Data Protection Supervisor both issued similar opinions. Both bodies saw a need for a more “user-friendly” redress system and for clarification on the written assurances by the U.S. regarding bulk data collection. Following the reviews, the EU and U.S. officials re-commenced negotiations to finalise the documentation, attempting to address the concerns of the relevant stakeholders.

To date there are over 1,500 self-

The revised Privacy Shield text was sent to the Article 31 Committee for their review and received approval on July 8, 2016. The adequacy decision

certified companies on the EU-U.S. Privacy Shield List.

establishing that the U.S. ensures an adequate level of protection for personal data transferred under the EU-U.S. Privacy Shield from the EU to participating companies in the U.S. was adopted by the Commission on July 12, 2016. From Aug. 1, 2016 companies in the U.S. have been able to self-certify under the Privacy Shield Framework and to date there are over one thousand self-certified companies on the Privacy Shield List.

The key documentation for the Privacy Shield Framework includes:

(i) the Privacy Principles and Supplemental Principles;

(ii) commitments from the heads of the U.S. Department of Commerce, Department of Transportation, Department of State, and Federal Trade Commission (FTC) with regard to enforcement and implementation of the framework; and

(iii) letters from the Office of the Director of National Intelligence (ODNI) and the U.S. Department of Justice to the U.S. Department of Commerce that describe the limitations and safeguards applicable to U.S. government access.

According to the Commission and the Department of Commerce, the Privacy Shield used the CJEU ruling as a "benchmark" to include a number of new elements and materially more stringent and detailed provisions as compared to the Safe Harbour Framework, including:

- Ombudsperson—the Under Secretary of State for Economic Growth, Energy, and the Environment serves as the independent Privacy Shield Ombudsperson with respect to individual complaints regarding possible access by national intelligence authorities. This Under Secretary is also the official vested with presidential authority under President Obama's Presidential Policy Directive 28 to "coordinate" diplomacy on international information technology issues and "to serve as a point of contact for foreign governments who wish to raise concerns regarding [U.S.] signals intelligence activities …" The U.S. government has taken steps to assure the independence of the Ombudsperson via an inter-agency process to review complaints made to the Ombudsperson, filtered through Member State bodies with oversight of national security services. The role of the Privacy Shield Ombudsperson extends beyond the Privacy Shield to encompass complaints relating to other international data transfer frameworks including the proposed EU General Data Protection Regulation (GDPR).

- Annual Joint Review and Enhanced Enforcement—an annual joint review will be conducted by the Commission and the U.S. Department of Commerce, assisted by U.S. security and intelligence agencies, the Ombudsperson, and DPAs to look at all aspects of the Framework, including access by public authorities. The Commission also retains the right to suspend the adequacy decisions of the Privacy Shield Framework if the commitments are not met by the U.S.

- **Access by U.S. Government**—the U.S. government (through the ODNI) has provided written assurances that access to personal data by U.S. public authorities for law enforcement, national security and other public interest purposes will be subject to specific articulated limitations, safeguards, and oversight mechanisms (such as the Ombudsperson mechanism) that safeguard against generalized access. The U.S. further assures that there is no indiscriminate or mass surveillance on the personal data transferred to the U.S. under the Privacy Shield.

- **Avenues of Redress for EU Individuals**—the framework provides a menu of redress options for data subjects. In the first instance, individuals can complain to the U.S. participating company. The company will have to respond to the complaint within 45 days. To the extent U.S. companies are handling human resources data of EU individuals, they will also need to commit to comply with decisions from European DPAs. Other companies may voluntarily commit to submitting complaints to a panel of DPAs. An unresolved complaint can then be dealt with through an alternative dispute resolution procedure, in which all U.S. participating companies must take part, and which will be at no cost to the individual. An EU individual or a DPA can also refer a still-unresolved complaint to a specified team at the U.S. Department of Commerce, which must respond within 90 days, or to the FTC where the Department of Commerce is unable to resolve the matter. In addition, where DPAs have jurisdiction over the transferring company, they can take action. As a last resort, where a DPA does not have jurisdiction, individuals can refer complaints to a binding arbitration panel, the Privacy Shield Panel, which would ensure a binding and enforceable decision subject to judicial enforcement under the U.S. Federal Arbitration Act.

Challenges to Data Transfer Mechanisms

Following the adoption of the EU-U.S. Privacy Shield, the Working Party chairman, Isabelle Falque-Pierrotin, announced that EU DPAs would not launch legal action of their own initiative but would wait until after the first annual review. In assessing the

impact of this statement, it must be noted that neither the Working Party nor its members (the DPAs) can launch direct legal action against the Privacy Shield. Only Member States and EU Institutions (such as the European Parliament) can submit such challenges. DPAs can only ask a national court, in the context of a pending dispute, to refer a question on the validity of the Commission's Privacy Shield Decision to the CJEU.

This one-year hiatus has not prevented others from challenging the validity of both the EU-U.S. Privacy Shield Framework and of other cross-border data transfer mechanisms.

Only Member States and European Union Institutions—not the Article 29 Working Party or national privacy regulators—can launch direct legal action against the EU-U.S. Privacy Shield.

Following its disposition by the CJEU, Max Schrems' case went back to the Irish High Court, and from there to the Irish Data Protection Commissioner (IDPC), where Schrems added claims relating to Facebook's transfer of data pursuant to Model Contracts. His complaint alleged that Model Contracts suffer from the same defects as the Safe Harbor Framework (i.e. deficiencies in the remedies granted to EU citizens whose data is transferred to the U.S.). In turn, on May 31, 2016, the IDPC issued court proceedings in the Irish High Court to examine the validity of the Model Contracts. The Irish High Court in turn will have to consider whether it is competent to decide the issue or whether it should refer the question to the CJEU. The High Court commenced court proceedings Feb. 7.

In addition, two legal challenges have been filed at the General Court of the CJEU challenging the Commission's adequacy decision on the EU-U.S. Privacy Shield. Individuals and or organizations may challenge EU legislation before the CJEU only if they are “directly concerned” by the legislation, within two months of the legislation coming into force. Digital Rights Ireland, the very same advocacy group referred to in the Judgment, was the first to bring action in the General Court of the CJEU on Sept. 16, 2016, followed by another challenge on Nov. 2, 2016 by French advocacy group La Quadrature du Net. Whether the Privacy Shield is of direct concern to either Digital Rights Ireland or La Quadrature du Net is currently under review, but if the CJEU finds this not to be the case then the relevant action will be declared inadmissible. If deemed admissible, then it will likely take over a year before the CJEU rules on the case.

If any these cases are heard, the CJEU will be presented with a very different view than it was in the original Schrems case, which was decided on the basis of the allegations in Schrems's complaint (in turn based on news stories about the Edward Snowden disclosures). This time, Facebook is appearing in the Irish case, where the U.S. government and a variety of trade associations and civil society organizations have been granted intervention. At least 12 parties including the Commission and U.S. government have requested intervention in the Digital Rights Ireland case; responses have not been filed yet in la Quadrature du Net's case.

Adding to the uncertainly about transatlantic data transfers are questions about what the new U.S. administration will do with regard to international agreements and foreign surveillance that could affect the Privacy Shield. To date, President Trump has not taken any actions to undo Presidential Policy Directive 28 and the safeguards that underlie the European Commission's July 25 adequacy decision. Headlines concerning a provision in a Jan. 25 executive order on immigration suggested that might not be the case, but in fact the provision does not affect either surveillance reforms and the Commission issued a statement confirming it does not affect the Privacy Shield. Nevertheless, there is clearly anxiety in the EU and elsewhere that the new administration might take actions that could cause the Commission to consider suspending the Privacy Shield framework by the time of the first annual review in mid-2017 or provide ammunition for legal challenges.

Investigatory Powers of DPAs

The Judgment on Article 3 flowed logically from its interpretation of the independent powers of DPAs. The CJEU confirmed that irrespective of a Commission decision determining the adequacy of a third country, an individual whose personal data has been or could be transferred to a third country has the right to lodge a complaint with its national DPA concerning the protection of rights and freedoms in respect of the processing of that data. The CJEU further declared that such a Commission decision “cannot eliminate or reduce the powers expressly accorded to the national [DPA]” including investigatory powers, powers of intervention and the power to engage in legal proceedings.

As such, a DPA is entitled to consider the validity of a Commission decision as to adequacy and in particular, whether the “level of protection of fundamental rights and freedoms … is essentially equivalent to that guaranteed within the [EU] by virtue of [the] Directive read in light of the [Charter].” However, DPAs do not have the power to declare such a Commission decision invalid. Instead an individual or DPA should challenge the decision in their national courts from where a referral should be made to the CJEU for a preliminary ruling on validity.

The Judgment arguably opened the flood gates for DPAs to question the legal validity of other Commission decisions of adequacy, for example, those made in respect of EU standard contractual clauses (Model Contracts) which are standard form data transfer agreements between a data exporter in the EU and a data importer outside the EU.

It remains to be seen whether particular DPAs, such as those in Germany, will be more willing to prohibit or suspend international data flows under the Model Contracts Decisions. On Oct 21, 2015, following the Judgement, the German Conference of Data Protection Commissioners (the DPAs responsible at a federal and state level in Germany) released a position paper in which they called into question the validity of Model Contracts and Binding Corporate Rules and affirmed the ability of DPAs to examine the levels of data protection in a third country independently. The group of German DPAs declined to deem existing Model Contracts and Binding Corporate Rules insufficient despite the position of the DPA of Schleswig-Holstein, though they did not approve new applications to use these mechanisms. Moreover, the relevance that these decisions may have on the ongoing litigation in Ireland remains an open question.

In the meanwhile, the Commission adopted two Implementing Decisions (the Model Contract Decisions) as a consequence of the Judgement which would amend the existing adequacy decisions that underpin the Model Contracts for the international transfer of personal data, in particular, amending the power of the DPAs. The Model Contracts Decisions sought to uphold the Judgement to declare that DPAs remain competent to oversee the transfer of personal data to a third country which has been the subject of a Commission adequacy decision and that the Commission has no competence to restrict their powers under Article 28 of the Directive. The Model Contracts Decisions thus stated “in the light of the [Judgment] and pursuant to Article 266 of the Treaty, the provisions in those Decisions limiting the powers of the national supervisory authorities should therefore be replaced.”

Adding to the uncertainly about transatlantic data transfers are questions about what the new U.S. administration will do with regard to international agreements and foreign surveillance.

The Commission has also indicated that it intends to undertake a review of the existing adequacy decision for ten countries other than the United States, recognising that most of the defects the CJEU identified in the Judgment apply to these decisions. This is particularly the case with respect to countries found adequate that also engage in intelligence collection—Argentina, Canada, Israel, and New Zealand (unlike, say, Andorra or the Isle of Man so far as anyone knows).

What Companies Should Do Now

The Commerce Department has reported that some 1,565 companies have subscribed to the Privacy Shield. Many of these are companies that took advantage of the nine-month grace period for reforming contract provisions by subscribing before October, and some are consumer-facing companies for which Model Contracts are a sub-optimal solution and for which the Privacy Shield offers a form of “trust mark” they can offer to customers in Europe.

Now that there is less immediacy, companies that are taking steps to comply with the GDPR may wish to consider combining preparation for the Privacy Shield, which requires some of the same steps. For example:

Data Mapping: in order to determine the types of personal data collected, the purposes for which this is processed and who the recipients of the personal data are (including in respect of international transfers), a form of data mapping exercise should be carried out. The report generated would not only assist in completing a Privacy Shield application but also satisfy the requirement under the GDPR for businesses to maintain a detailed record of their data processing activities.

Notice and Consent: the GDPR introduces new requirements as to the information that should be provided in notices, as well as new consent requirements. Companies can combine their review of existing employee and customer data privacy notices, consents and policies with their review of the same from a Privacy Shield perspective.

Companies that are taking steps to comply with the European Union General Data Protection Regulation may wish to consider combining preparation for the Privacy Shield.

Individual Rights: both the GDPR and the Privacy Shield place great emphasis on data subject rights with, for example, the introduction of an individual's right to have their personal data erased, in certain circumstances and a new right to data portability under the GDPR. Businesses should consider how in practice they will implement the various privacy rights and in particular, the right to erasure which may involve a review of existing data retention policies and procedures.

Information Security: as with the GDPR, the security obligations under the Privacy Shield have been drafted deliberately vague as the level of security required will depend on the activities of the

business and the types and volumes of personal data processed. In addition, under the GDPR, business will be subject to security breach reporting obligations, something many US companies are already familiar with. In readiness, businesses should be reviewing and updating existing information security standards and policies. Businesses should also consider implementing a vendor management program. This would typically address the following: (i) due diligence during the vendor selection process to assess from a data privacy perspective the internal controls and operations of the vendor; (ii) the implementation of appropriate data processing agreements; (iii) the development and implementation of a minimum set of vendor security requirements; and (iv) the carrying out of vendor audits throughout the term of the agreement. This is particularly important as it will assist with the onward transfer requirements under the Privacy Shield and the data processing obligations under the GDPR.

Vendor Contracts and Onward Transfers: from a GDPR perspective, contracts with any service providers involved with the processing of EU personal data should be reviewed (or implemented) to ensure the appropriate data processing and liability wording is in the contract as well as specific timeframes for reporting security breaches. When reviewing these contracts and to the extent necessary, the provisions required in order to comply with the Onward Transfer Principle under the Privacy Shield could also be inserted.

Privacy Law Watch™

February 21, 2017

Bloomberg BNA

Data Transfers

EU Privacy Chiefs Want Trump to Uphold Data Transfer Pact

BNA Snapshot

- EU data protection regulators will question Trump about EU-U.S. data transfer program
- Group also announces delay in guidance on new EU privacy regime

By Stephen Gardner

European Union privacy regulators will soon question President Donald Trump on the U.S. commitment to the EU-U.S. Privacy Shield data transfer pact.

Although Trump's Jan. 25 immigration executive order limiting extension of the Privacy Act to non-U.S. citizens doesn't have a direct legal effect on the Privacy Shield, it has raised concerns over U.S. intentions. The Article 29 Working Party of data protection officials from the 28 EU countries said in a Feb. 16 statement that it would write to the Trump administration "pointing out concerns and asking for clarifications on the possible impact" the order may have on the Privacy Shield.

The Privacy Shield allows U.S. companies that self-certify with the Commerce Department their compliance with EU-approved privacy and security principles to legally transfer personal data from the EU to the U.S. The Privacy Shield is relied upon by over 1,000 U.S. companies, including Alphabet Inc.'s Google, Microsoft Corp. and Facebook Inc., as well as thousands more EU companies that send data to those U.S. companies.

An Art. 29 Party spokeswoman told Bloomberg BNA Feb. 17 that the group would publish a letter to the Trump administration on the Privacy Shield within the next 10 days.

The executive order at issue has been stayed by the U.S. Court of Appeals for the Ninth Circuit. However, the Trump administration has vowed to issue a new immigration executive order.

A White House official familiar with the matter told Bloomberg BNA Feb. 17 on background that the executive order applies to agencies only "to the extent within applicable law" and that the "Trump administration will ensure that no privacy laws are violated." It is too early to speculate on whether there would be similar language in upcoming executive orders, the official said.

The regulators also said, in the statement, that it is delaying its next round of guidance on the EU's new privacy regime until at least April.

Daniel Fesler, a partner with Baker McKenzie in Brussels, told Bloomberg BNA Feb. 17 that the late delivery of guidance could mean that companies will need to review their data protection compliance programs late in 2017 or in 2018, shortly before the EU General Data Protection Regulation (GDPR) takes effect in May 2018. That could be "extremely cumbersome" and "a challenge for organizations trying to prepare themselves," Fesler said.

Redress Concerns

Privacy advocates raised concerns over Trump's executive order when it was issued. But attorneys and political leaders on both sides of the Atlantic tried to quell the storm, saying the order was aimed at immigration and national security concerns rather than commercial data transfer arrangements. The order is also limited to actions that aren't already authorized by law. The Redress Act authorizes EU citizens to utilize the Privacy Act to complain about alleged government misuse of personal

data transferred under the Privacy Shield. The Obama administration's Department of Justice specifically included EU countries as being covered by the Redress Act.

European Commission spokesman Christian Wigand told Bloomberg BNA Feb. 17 that the commission, the EU's executive arm, had already contacted U.S. officials “to ask for some clarifications on the U.S. Judicial Redress Act.” Wigand didn't give details of the commission's specific concerns.

EU privacy regulators are authorized to “enforce and uphold individual rights. They do this independently and are therefore free to raise questions with U.S. counterparts,” Wigand said.

Mauricio Paez, a privacy and data protection partner with Jones Day in New York, told Bloomberg BNA Feb. 17 that the EU privacy regulators weren't being unreasonable in asking the Trump administration about the Privacy Shield. EU data privacy regulators have a “great interest in understanding these questions and the administration's views,” he said.

Slow Progress on GDPR Guidance

The privacy regulators also are moving forward with guidance on the GDPR. Parts of the guidance are expected in April, while others won't be available until the later part of 2017.

Guidance on data protection impact assessments that must be carried out under the GDPR for high-risk processing would be provisionally adopted in April, the Art. 29 statement said.

The working party indicated that new guidance on consent, profiling and notification of data breaches, which is prioritized for 2017, would likely appear later in the year. A workshop on those issues is slated for April, they said.

To contact the reporter on this story: Stephen Gardner in Brussels at correspondents@bna.com

To contact the editor responsible for this story: Donald Aplin at daplin@bna.com

Privacy Law Watch™

January 12, 2017

Bloomberg BNA

Data Protection

What Should a Company's 2017 EU General Data Protection Regulation Budget Look Like?

EU Privacy Compliance

The author provides advice on how companies should set up a budget in preparation for compliance obligations under the European Union's new privacy regime—the General Data Protection Regulation—which will take effect in May 2018.

By Chiara Rustici

Chiara Rustici advises businesses as an independent European Union General Data Protection Regulation analyst and implementation consultant. Rustici was formerly an Italian National Research Centre research fellow and a business director with strategy and profit and loss responsibility for the City of London. She is the author of the forthcoming book GDPR: The functional specifications of EU-grade privacy, published by O'Reilly.

Postponing a budget exercise until after the Article 29 Working Party (WP29)—the European Union's 28 privacy commissioners— released their official EU General Data Protection Regulation guidelines in English risked leaving businesses short of time. The EU privacy commissioners and the European Data Protection Supervisor have, so far, published sufficient indications and guidelines for businesses to know what is expected of them in preparing for the GDPR, albeit not all in the same place or in the same language. It is highly unlikely that the WP29 guidelines, due out in stages between the end of December and the first few months in the new year, will radically depart from what has been issued by other EU institutions or the national privacy commissioners themselves so far. There are no excuses for not having a GDPR budget in place before the end of 2016.

Another common misperception is that businesses should wait until a data protection officer (DPO) has been hired and leave the GDPR budget up to them.

In fact, a lot needs to be in place—and can be put in place—in an organisation before a DPO is hired. The role of the DPO is crucial in navigating data protection issues, but there is a very early role for the enterprise data architect in making an organisation's information technology (IT) infrastructure GDPR-ready. Think of a DPO as a ship's captain and of a GDPR architect as the naval engineer: to set sail to the seas you rely on a good captain, who can chart a course and avoid thirty-foot waves; but to build or make a ship sea-worthy, and ensure that it can withstand even thirty-foot waves, you first rely on a good naval engineer. They perform different functions.

We know that an IT director has already been fined by one the German privacy commissioners for taking on the data protection officer role: the arrangement was deemed a conflict of interest under the current directive. Seeing this as a precedent for the GDPR's required independence of the DPO role from an IT director role, understandably, chief information officers (CIOs) are reluctant to take the lead and display apprehension in owning the GDPR implementation budget if a DPO is not yet in place.

In this case, too, the best business advice is not to procrastinate. That the DPO roles should be kept separate and

independent because a conflict of interest might arise between the DPO function and all the other business functions in the day-to-day operations of the business once the GDPR is enforceable, is no reason for IT and other C-suite leaders to skirt their current responsibilities in building a GDPR-ready organisation. That does not appear to me to be the message of this fine. Additionally, there are ten key data architecture reasons why CIOs and other IT leaders should be involved in GDPR preparations right from the start. See Chiara Rustici, GDPR, The functional specifications of EU-grade privacy, Chapter 1, O'Reilly, early release edition.

A 2017 GDPR Budget Should Be a Federated Budget Exercise

As the regulation impacts, horizontally, all business functions, the total must include both front-end and back-end functions. In other words, the budget is there to ensure that any interaction of EU-based individuals with a brand's real and digital estate follows the EU data protection principles: that will mean product design, user experience, distribution and after sales support, HR, marketing, legal, risk and compliance, storage and security should all own a share of the corporate GDPR budget.

It is very dangerous to think in terms of key, “personal data”- centric business functions and those that can worry about the impact of the GDPR later or not at all.

2017 is the year to become 100 percent compliant with the new EU privacy regime. The first five months of 2018 should be set aside as contingency remediation time for minor glitches, not for major changes.

There is also a very dangerous temptation for businesses to allocate their entire GDPR implementation budget to external advisors. Anecdotal evidence suggests consulting firms are selling compliance services by relying on an unquantifiable army of GDPR implementation contractors they expect to hire once the market “revs up.” The trouble is, this army does not yet exist and the few GDPR architects I am aware of—professionals capable of translating the regulation's functional requirements into technical requirements—are four times oversubscribed. For businesses that want to minimise risks, allocating budget to train their own employees to grasp GDPR requirements and empower them to actively find their own solutions is the safest bet.

How much should businesses allocate to GDPR implementation?

Businesses should take no risks on this count, either. A good starting point is to presume one is far from being GDPR-ready and will be fined. I advise businesses to ring fence 4 percent of the 2016 global turnover and earmark it as budget for the 2017 compliance exercise: one way to look at it is that if it doesn't get used in 2017 for GDPR preparations, it'll have to be used in 2018 to settle the fine. A business may achieve compliance with less, of course, and carry any excess over to the following years, but it would be hard to argue to a regulator that the business was serious about data protection if it can't even point to a budget that is at least commensurate with the fine. The fact that technology solutions are not yet available or are far from being perfect, and one cannot precisely quantify the cost for implementing each GDPR obligation yet, shouldn't be an excuse not to have a figure earmarked for each issue. Below I share my own ten bullet point memo-to-self: if a business has nothing else to go by, the total budget allocated may be divided in equal parts. As the year progresses, and one's GDPR compliance journey becomes more specific, amounts can be refined and re-allocated from one heading to another.

How much should businesses aim to accomplish in 2017?

A tall order, but 2017 is the year to become 100 percent compliant. The first five months of 2018 should be set aside as contingency remediation time for minor glitches, not for major changes.

There are three phases to taking an enterprise to GDPR compliance and they need not be in sequence but can take place in parallel: (i) a fact-finding phase, where personal data flows created by the different business processes are mapped; (ii) a boardroom phase, where the corporate privacy posture and the business model around personal data is revised and agreed; and (iii) an internal crowdsourcing phase, where all the business functions are empowered to find, test or co-create the technology solution to meet their GDPR obligations. I refer to crowdsourcing for good reason: nobody gets personal data better than the people who use personal data. Top-down GDPR compliance by committee alone will fail: while central ownership of the compliance journey is crucial, evidence suggest bottom-up involvement of front-line employees in finding solutions yields the best results.

What Headings Should a 2017 GDPR Budget Itemise?

Of course, no single template will suit all businesses. Larger corporations, especially those in regulated industries, tend to centralise shared functions and may have a “compliance management system” already in place to deal with large scale

regulatory changes, involving a multi-stakeholder compliance committee, codes of practice to cascade Do's and Don'ts down the organisation and whistle-blowing procedures for reporting non-compliance. Smaller businesses and start-ups may function as a network of de-centralised self-contained businesses with their own marketing team, their own databases, and may never have had to deal with anything quite so demanding before. Ultimately, it will be the structure of each business to dictate the specifics. However, these are the headings I rely upon for my own use:

• **Budget for data inventory and mapping**. But, note that automated solutions promising file autoclassification or algorithmic recognition of personal data require a lot of fine-tuning: until machine learning “has cracked” the broad GDPR definition of personal data, Art. 30 still requires complex human judgment.

• **Budget for privacy and state-of-the-art safety by design and by default**. But, note that neither privacy by design or state-of-the-art safety are achieved through single software solutions but involve two distinct processes - one for future data collection and one for “sanitising” legacy data sets that a business wants to hold on to or for erasing datasets it no longer wishes or has reason to rely upon.

• **Budget for solutions to enable the exercise of Art. 15-22 data subject rights**. This part of the budget should be owned by IT, especially as Art. 17 right to erasure, Art. 20 right to portability, Art. 21(1) right to object to processing and Art. 18 right to restriction of processing are not achievable through ad hoc intervention alone but involve core and very demanding IT architecture changes. Note that reliance on legitimate business interest as a lawful basis for processing is no easier on the IT architecture than reliance on consent.

• **Budget to train employees to recognise GDPR personal data flows**. A business' first and best line of defence, they will contribute to filling the inevitable gaps in a data map.

• **Budget for incentives for hunting down “rogue or non-obvious” personal data records**. If, on budget day, anyone laughs this off, refer them to the extensive Bug Bounty literature in IT security and Microsoft Corp.'s well known six-figure vulnerability rewards for ethical hackers.

• **Budget to train employees**. Existing employees should be trained to understand the functional specifications of the GDPR in their own role and business function.

• **Budget to train employees to negotiate with sector-specific vendors and co-design GDPR solutions for their role and business function**. If they have not helped design these solutions, they will not use them. Central ownership of the compliance programme is key, but delegating/decentralising the research of potential solutions multiplies chances of success.

• **Budget for stress-testing GDPR resilience of the solutions proposed**. Seek inspiration from the “Hack the Pentagon” initiative and the EU's own Bug Bounty funding. Keep the two budgets separate: one to support identification of personal data potential leaks, and a different one to stress-test the solutions found to prevent personal data leaks, including access control layers, encryption and de-identification of the data sets themselves.

• **Budget to co-ordinate and integrate the solutions crowdsourced from the business units/functions**. Set up single accountability/demonstrability framework. The different solutions need to integrate with each other and central project management is key.

• **Budget to hire both a GDPR architect and a GDPR DPO**. There will be collaboration first and then a handover between the first and the second, but a single professional profile with both sets of skills does not yet exist or is extremely rare.

Professional membership associations should help produce standards and vet Regulation Technology vendors but, at this writing, no EU certifications or trust marks have yet been approved: ultimate responsibility for vetting vendors offering solutions, and verifying that these reliably address GDPR obligations, rests entirely with the buyer.

World Data Protection Report™

December 29, 2016

Bloomberg BNA

European Union

EU Privacy Upheaval Demands Urgent U.S. Corporate Game Plan

BNA Snapshot

- EU privacy regime preparation overshadows other international data privacy issues in 2017
- U.S. companies must use 2017 to get compliance programs in place to sync with new privacy regime

By George R. Lynch

Dec. 2 — Seismic changes taking effect in 2018 for European Union privacy law will make the scramble for compliance a top 2017 priority for U.S. companies that use EU data.

Gearing up for the EU General Data Protection Regulation (GDPR) "is everything. It's hard to overstate that," Lisa Sotto, who chairs Hunton & Williams LLP's privacy and cybersecurity practice in New York, said. It is "an extraordinary shift" that requires serious and sustained attention from U.S. companies, she told Bloomberg BNA.

Thousands of companies face a new legal scheme that is full of ambiguities. They need to prep for the GDPR now to have even a chance of being ready by the May 2018 deadline, Sotto said.

The stakes are high. The EU and U.S. are each others' largest trading partners, with combined trade reaching $700 billion in 2015, according to the U.S. Census Bureau.

Meanwhile, there is uncertainty in the EU wherever you look, Cam Kerry, senior counsel at Sidley Austin LLP's Privacy, Data

Security and Information Law group in Washington, told Bloomberg BNA. “There are tons of questions facing companies as they put compliance programs in place,” Kerry said.

Personal data is the currency of international commerce.

U.S. multinational companies doing business in Europe will have to spend 2017 figuring out how to implement new requirements for the handling of EU citizens' personal data, such as names, financial and location information and health records.

> *Very few people know how to interpret the EU privacy regulation, let alone comply with it.*
>
> *Lisa Sotto, Chairman Privacy and Cybersecurity*
> *Hunton & Williams, New York*

The GDPR is the first major overhaul of EU data privacy law in over two decades. It includes huge maximum fines and requires organizations to notify privacy regulators of data breaches within 72 hours.

Fines for violating the GDPR can reach 20 million euros ($22.5 million), or up to 4 percent of a company's global revenue, whichever is higher, for violations of data processing consent, individual privacy rights or international data transfer rules, or for ignoring orders from privacy regulators.

To illustrate, Alphabet Inc.'s Google had $60.6 billion in revenues in fiscal year 2015, Bloomberg data show. A fine of 4 percent means Google could get a bill from the EU exceeding $2.4 billion for a single infraction.

Because the GDPR is completely new, “very few people know how to interpret it, let alone comply with it,” Eduardo Ustaran, European head of Privacy and Cyber Security at Hogan Lovells LLP in London, told Bloomberg BNA.

Divide and Conquer

Companies should invest in 2017 in readiness exercises that include finding holes in compliance programs and identifying the data flows around their business, Andrew Dyson, head of the global data protection and privacy group at DLA Piper LLP in London, said.

Some companies already are reviewing their existing EU privacy compliance program and benchmarking it to GDPR standards to see what's missing and what policies and procedures they will need to put in place, Ustaran said. Benchmarking is the most important action a company can take, he told Bloomberg BNA.

Companies also should assign GDPR compliance responsibilities to different divisions within companies, Monika Kuschewsky, European data protection partner at Squire Patton Boggs LLP in Brussels, said.

For example, legal divisions will need to take stock of existing contracts to determine what needs to be changed in data processor and data controller agreements, she said. Other departments could set up privacy offices.

Sotto said companies should consider the GDPR in small chunks, creating a road map of “module-based” piece-by-piece issues to tackle before the effective date.

U.S. companies that seek compliance protection for data transfers from the EU through the new EU-U.S. Privacy Shield program also need to contemplate GDPR compliance, Kerry told Bloomberg BNA.

Guidance Can't Come Fast Enough

The text of GDPR is full of ambiguities and new requirements, and companies will be looking to upcoming guidance for clues on how to best position themselves for the GDPR.

Isabelle Falque-Pierrotin, chairwoman of the Article 29 Working Party and president of the French privacy office, told Bloomberg BNA that the working party plans to release guidance on the data protection officer requirement, enforcement issues and data portability by the end of 2016. Further GDPR guidance on consent and other issues will be released in 2017.

As of now, no one knows what the process will be for resolving issues when the GDPR takes effect, Kerry said. The working party needs to set time tables and get broad input from all parties.

EU-U.S. Privacy Shield: Tool for 2017 and

Pragmatic guidance that is technology-neutral, and in some cases possibly tailored to specific industries, will serve companies best, Kuschewsky said. The guidance should also help companies cut compliance with the regulation into different phases and sizable chunks, because coming to grips with the GDPR in one fell swoop is not an effective way to prepare, she said.

Official guidance is particularly needed in areas where new obligations are introduced by the GDPR, Ustaran said.

New Rules Added, Old Rules Expanded

One of the biggest compliance demands raised by the GDPR is that it expands existing privacy requirements, Ustaran said. Companies that were in full compliance with previous rules must rethink how to comply with new requirements in the same subject area.

Companies already are required to disclose in a privacy notice how they will use customer data, for instance. The GDPR adds to this obligation, Ustaran said. It will also require vendors that contract with companies to secure personal data, a huge, additional obligation and change from current practice. Multinationals routinely work with hundreds, and perhaps even thousands, of vendors and services handling personal data of employees and customers.

Perhaps even more challenging than meeting expanded requirements will be addressing wholly new privacy obligations, Ustaran said.

Some of the requirements introduced by the GDPR include:

- privacy impact assessments for major projects;
- data breach notification to national privacy regulators within 72 hours of discovery of a breach;
- implementation of privacy by design principles in new projects;
- individuals control portability of personal data from one company to another; and
- pseudonymization of personal information used in big data applications.

Some companies will have to designate a data protection officer (DPO). DPOs will serve as in-house privacy officers for data controllers and data processors that meet certain requirements. Having a DPO in place won't provide a safe harbor from the GDPR, but would be viewed as a plus for privacy regulators undertaking or considering enforcement actions.

These “brand new issues require a lot of thinking about what's actually involved,” Ustaran said.

To contact the reporter on this story: George R. Lynch in Washington at glynch@bna.com

How Does Brexit Impact GDPR Compliance?

Brexit adds a wrinkle to the challenges some multinational companies face in their 2017 efforts to gear up for compliance with the EU's new privacy regime.

The U.K.'s planned departure from the EU doesn't directly impact U.S. companies preparing for the GDPR, and it appears U.K. companies will be applying similar rules to the GDPR regardless of the country's impending exit from the bloc, privacy pros say.

As long as the U.K. remains consistent with GDPR, it should be able to retain its access to the EU Digital Single Market.

Companies based in the U.K. should remain focused on getting ready for the GDPR,

Beyond

The Privacy Shield replaces the invalidated U.S.-EU Safe Harbor program, which was relied on by over 4,400 U.S. companies and tens of thousands of EU companies to legally transfer personal data of individuals in the EU to the U.S. for 15 years.

The Safe Harbor was certified by the EU as adequate to protect the privacy of personal data sent to the U.S.

The new Privacy Shield replacement—which adds additional privacy promises that U.S. companies must self-certify compliance to the U.S. Department of Commerce—was also found adequate by the EU.

But like the old Safe Harbor, the Privacy Shield faces a challenge in the EU's highest court over whether it will adequately protect the personal data of EU citizens from U.S. government reach.

Despite uncertainty

To contact the editor responsible for this story: Donald G. Aplin at daplin@bna.com

privacy professionals and the U.K. Information Commissioner's Office said.

The GDPR will take effect before the official Brexit date, and the U.K. will want to continue to transfer data freely with the EU.

The effective date of Brexit is more unclear than ever after the U.K. High Court ruled that the U.K. Parliament must approve the formal move to exit the EU.

Multinational companies may need to decide whether it is more sensible to move headquarters from the U.K. to an EU jurisdiction so they don't have to answer to multiple regulators, Ustaran told Bloomberg BNA.

over the stability of the Privacy Shield raised by the court proceeding, many privacy pros support the certification process. They say it gives companies the opportunity to meet the standards of basic EU-centered compliance evaluation and, for now, an added layer of legal protection.

• The Department of Commerce began accepting Privacy Shield applications Aug. 1, and more than 1,500 companies, including Microsoft Corp., Facebook Inc. and Salesforce Inc., have applied to join.

• Commerce provides information on how to join the Privacy Shield and its benefits for U.S. companies. It also provides information to EU companies about how to verify an organization's commitments on its Privacy Shield website.

• The website has a directory of Privacy-Shield approved companies.

International Trade Reporter™

March 09, 2017

Bloomberg BNA

Data Privacy

Commerce's Ross May Face EU-U.S. Data Transfer Pact Tests

BNA Snapshot

- Commerce's Ross not expected to upend EU-U.S. Privacy Shield data transfer program
- But he may be called upon to calm EU privacy concerns, privacy attorneys say

By Daniel R. Stoller

Recently confirmed U.S. Commerce Secretary Wilbur Ross may be faced with the task of bolstering confidence in an important European Union-U.S. cross border data transfer program, privacy attorneys told Bloomberg BNA March 1.

Although Ross has other priorities on his plate, including North American Free Trade Agreement (NAFTA) reform, he can expect, at some point this year, to deal with EU-U.S. Privacy Shield data transfer program issues. Over a thousand U.S. companies certified in the program, as well as tens of thousands of EU companies that work with them, rely on the program to legally transfer personal data out of the EU. Some in the EU are concerned that President Donald Trump may take action to undercut the program's privacy guarantees, and it may fall to Ross to calm those fears.

Ross should be up to the task, Brian Hengesbaugh, former special counsel to the general counsel at Commerce and part of the core team that negotiated the U.S.-EU Safe Harbor data transfer pact that preceded the Privacy Shield, told Bloomberg BNA March 1. He “will have a strong grasp of the importance of Privacy Shield for the U.S. and the global digital economy,” Hengesbaugh, now a privacy and data protection partner at Baker McKenzie in Chicago, said.

Jeewon Kim Serrato, counsel at Shearman & Sterling LLP and co-head of the firm's global privacy and data protection group, told Bloomberg BNA March 1 that Ross and the Trump administration will need to balance U.S. national security interests with EU citizens’ “rights to privacy and data protection” to make sure the Privacy Shield remains intact.

Hengesbaugh said Ross’ background as “a successful investor and business leader” will invariably lead him to start with trade reforms such as NAFTA, but he will inevitably have to face Privacy Shield issues head-on. Ross, a private equity investor, is worth $3 billion, Bloomberg data show.

Companies shouldn't worry that a lack of completed, lower-level political appointments may negatively affect Commerce's administration of the Privacy Shield, Hengesbaugh said. The Privacy Shield process predates Ross at Commerce, so there won't be “much differentiation” in how different staffs handle the data transfer program, he said.

Commerce didn't immediately respond to Bloomberg BNA's email request for comment.

Privacy Shield

The Privacy Shield allows U.S. companies that self-certify their compliance with EU-approved privacy and security principles with Commerce to legally transfer personal data from the EU to the U.S. It provides critical support for the more than $260 billion in trade in services between the U.S. and EU, according to the Obama administration's Jan. 4 exit memo on Commerce. The Privacy Shield replaced the Safe Harbor framework, which was invalidated, in part, due to fears that it was inadequate to protect EU personal data sent to the U.S. from widespread government access.

Ross said during a Jan. 18 confirmation hearing that he remains committed to the Privacy Shield, but “there will be a tension

between privacy on one hand and problems of localization and data and the implications that they have for the internet as we go forward."

The Privacy Shield's first annual review set for this summer will be an early test for Ross to see how "businesses, the U.S. Department of Commerce and the European data protection authorities" have lived up to expectations under the cross-border data transfer program, Serrato said. Ross will need to reach out to EU privacy regulators to ensure "that the data collection practices by U.S. intelligence agencies and businesses meet the requirements for providing adequate protections" for EU citizens, she said.

EU Privacy Shield Concerns

Earlier, Trump's immigration executive order asserted limitations on the ability to extend the Privacy Act, which allows individuals to sue the government over alleged misuse of their personal data, to non-U.S. citizens. The Privacy Shield depends, in part, on amendments to the Privacy Act that allow the Department of Justice to designate that citizens from countries or groups of countries, such as the EU, may also sue under the law.

The immigration order has been stayed by federal courts, and officials on both sides of the Atlantic have promised that it doesn't affect the Privacy Shield. Trump is expected to release a new version of the immigration order soon, but it is unknown if it will include language similar to the initial order.

In the meantime, the U.S. Department of Justice has assured the European Commission, the EU's executive arm, that Trump's executive orders won't affect EU citizen redress rights under U.S. laws, Hengesbaugh said. That should signal to companies that the "Privacy Shield will remain in place and operating as currently structured for the foreseeable future," he said.

To contact the reporter on this story: Daniel R. Stoller in Washington at dStoller@bna.com

To contact the editor responsible for this story: Donald Aplin at daplin@bna.com

Privacy Law Watch™

February 28, 2017

Bloomberg BNA

Data Breaches

When a Breach Strikes, You Have 72 Hours to Act: How to Respond Under GDPR

Data Breach Notification

The tight deadlines for reporting a data breach under the European Union General Data Protection Regulation make it important for companies to have robust breach detection, investigation and internal reporting procedures in place, the author writes.

By Joke Bodewits

Joke Bodewits is a senior associate in Hogan Lovells' Amsterdam office where she is a member of the Privacy and Cybersecurity Practice Group.

Security Obligations, Breach Notifications… the GDPR is Coming

At the moment, hacks are world news and examples of data breaches are making daily headlines. Daily headlines can be good, but no one wants to have his company featuring headlines as a result of data breaches or security incidents.

Ironing out the security obligations and data breach notification requirements will help your company prepare for the unhappy moment you are informed of a potential data breach, and may prevent your company from being a headline for the wrong reason. This article aims to getting you started and includes some practical recommendations in preparing for and dealing with data breaches.

Security Obligations

Security plays a prominent role in the European Union's new General Data Protection Regulation (GDPR). With rules applying directly to both controllers and processors, any company processing personal data should have an idea of the security obligations applicable to it.

Both controllers and processors are obliged to “implement appropriate technical and organizational measures” taking into account “the state of the art and the costs of implementation” and “the nature, scope, context, and purpose of the processing as well as the risk or varying likelihood and severity for the rights and freedoms of natural persons.” Moreover, the GDPR requires controllers to only engage processors that provide “sufficient guarantees to implement appropriate technical and organization measures” in order to meet the GDPR's requirements and protect data subjects' rights.

The GDPR provides specific suggestions for what kinds of security actions might be considered “appropriate to the risk,” including:

- the pseudonymization and encryption of personal data (which could result in an exemption to notify data breaches, see below);

- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, such as a data breach;

- a process for regular testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

Controllers and processors that adhere to either an approved code of conduct or certification mechanism may use these tools to demonstrate compliance with the GDPR's security standards.

Breach Notification Obligations

The GDPR includes specific breach notification guidelines. Under the GDPR so-called “personal data breaches” should be notified to supervisory authorities.

A “personal data breach” is defined as “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.” This broad definition differs from most U.S. data breach laws, for example from laws under which data breaches only have to be notified in the event of potential fraud or identity theft.

In the event of a personal data breach, controllers must notify the competent supervisory authority (which is most likely the supervisory authority in the member state where the controller has its main establishment). Notice to supervisory authorities must be provided “without undue delay and, where feasible, not later than 72 hours after having become aware of it.” If notification is not made within 72 hours, the controller must provide a “reasoned justification” for the delay. Notice to affected individuals should be done “without undue delay”.

Notice is not required if “the personal data breach is unlikely to result in a risk for the rights and freedoms of natural persons” which leaves room for discussion to argue that in certain cases no notification obligations apply.

Security Breaches: Hope for the Best and Prepare for the Worst

Although personal data breaches always come as a surprise and the timing could not be worse, reasonable preparations could prevent a personal data breach ending in a company catastrophe. However, valuable preparations can only start once you have a clear and complete picture of all data flows within and from you organization.

With a picture of the data flows in mind, it can be assessed where your company is most vulnerable. Please consider that you most valuable assets could be your weakest link when it comes to personal data breaches. Therefore, it is recommended reviewing all vendor agreements on security obligations and data breach notification requirements (although the GDPR includes an obligation for processors to “notify the controller without undue delay after becoming aware of a personal data breach”). Furthermore, it is also recommended implementing an internal security incident response plan and to train employees on data confidentiality and on notification and handling of security incidents. You should make sure that employees understand what constitutes a personal data breach, and that this is more than a loss of personal data.

Preparations for data breaches can only start once you have a clear and complete picture of all data flows within and from you organization.

In light of the tight timescales for reporting a breach, it is important to have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether you need to notify the relevant supervisory authority or the affected individuals.

When a security incident happens, my practical recommendation is to take the following steps.

Step 1: Investigate Whether the Incident is a Personal Data Breach

A personal data breach may involve loss of personal data or the unlawful processing of personal data. Only if an incident actually resulted in a breach of personal data the mandatory notification obligation applies. For instance, lost USB sticks, stolen laptops, malware infections or hacked databases containing personal data are considered personal data breaches.

A threat or a shortcoming in security measures, such as weak passwords or outdated firewalls, are not considered a personal data breach as long as no personal data has been leaked. Therefore, these issues in security measures do not fall within the

mandatory notification obligation.

Step 2: Investigate the Personal Data Breach

As a second step, the nature, scope and possible consequences of the personal data breach should be investigated. For this investigation the answers to the following questions can be relevant:

- **What is the source of the personal data breach?** For instance, is it a stolen device or is it an internal security measure which has been hacked?

- **How many individuals are affected by the personal data breach and is the data breach likely to result in a risk to the rights and freedoms of the individuals affected?** For instance, a hack of a customer database could most likely have a severe impact on private lives of many people. On the other hand, a breach concerning only business contact details of one customer may have minimal impact only.

- **Does the personal data compromised include sensitive data?**For instance, credit card details, passport numbers or health data.

- **Was the personal data compromised encrypted or secured in a manner which makes it impossible for a third party to assess?** For instance, if adequate encryption is used or the data is adequately hashed and salted it can be assumed that third parties will not be able to access the personal data.

- **Which steps are taken to mitigate (further) loss of personal data?** For instance, if it is possible to wipe all personal data remotely so that loss of personal data can be prevented or if access to hacked database could be regained, it is possible to mitigate further loss.

- **Which parties are involved in the data breach?** For instance, if a shared database is hacked, it cannot be excluded that several parties will be involved and/or affected by the data breach.

Step 3: Notify the Supervisory Authority—if Needed

The supervisory authority should be notified by the controller of any personal data breach that results in or is likely to result in "a risk to the rights and freedoms of natural persons." This has to be assessed on a case by case basis. For example, you will need to notify the relevant supervisory authority about a loss of customer details where the breach leaves individuals open to identity theft. On the other hand, the loss or inappropriate alteration of an internal telephone list, for example, would not normally meet this threshold.

In this respect it is relevant to know the answers to the above questions and have an idea of the reasonable consequences the breach may have (for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage). If not yet all information is available, the controller should still notify the supervisory authority. If needed, the notification may be amended at a later stage when the full details are known or the notification could be withdrawn if not needed after all.

Step 4: Notify the Affected Individuals—if Needed

Where a personal data breach is likely to result in a "high risk" to the rights and freedoms of individuals, you must notify those concerned directly. A "high risk" means the threshold for notifying individuals is higher than for notifying the relevant supervisory authority.

If affected individuals must be informed, you should provide at least the following information:

- the scope and nature of the personal data breach;

- the name and contact details of the data protection officer (if your organization has one) or other contact point where more information can be obtained;

- a description of the recommended measures to mitigate any possible adverse effects (e.g. contact your credit card provider, change your password, etc.).

Notification to individuals shall not be necessary if the controller can demonstrate that "appropriate technological protection

measures" were applied to the data concerned by the personal data breach, which "shall render the data unintelligible to any person who is not authorised to access it."

Step 5: Create and Maintain an Internal Data Breach Register

Controllers are obliged to document any personal data breaches, which shall at least include information on the facts relating to the personal data breach, the efforts and remedial actions taken. It is recommended also documenting any communication with supervisory authorities and affected individuals. Moreover, in the event a decision was made not to notify supervisory authorities and/or affected individuals, it is recommended to keep a record of the facts and the reasons why such decision was made as a supervisory authority may initiate an audit or request for information at any time.

Step 6: Evaluate the Personal Data Breach and Update Technology and Policies

The new principle of accountability requires controllers to be responsible for and to be able to "demonstrate" and "evidence" compliance with the data protection principles, which include security obligations. In view of the accountability requirement, it is recommended documenting what your organization has done to prevent future personal data breaches originating from the same source as well as updating your breach detection, investigation and internal reporting procedures.

Let's hope that whenever you get the call about a potential data breach, the steps set out above make you feel comfortable handling the breach in a compliant and effective manner. If not, feel free to get in touch. After all, it takes years to build a good reputation and seconds to destroy it.

IT MATTERED AFTER THE DATA BREACH.

When our client was hacked, we had to react swiftly and with precision. And this is exactly why we rely on *Bloomberg Law*. Its news and unique analytics keep us ahead of fluid domestic and global privacy and data security laws, as well as the latest trends in managing breaches. We were able to quickly advise on how to respond, report and comply. *Bloomberg Law*. Because reaction time matters.
www.bna.com/bloomberglaw

Bloomberg Law®

When It Matters.