CORPORATE COUNSEL
An ALM Website

Legaltech news ONLINE

MARCH 16, 2017

An ALM Publication

BACK IN THE GDPR

Using Data Mapping to Arrive at a Privacy Impact Assessment

Dan Panitz, Esq.
dan.panitz@unitedlex.com
(212) 226-2928

BY DAN PANITZ, UNITEDLEX,
AND H. BRUCE GORDON,
TEVA PHARMACEUTICALS

In our last article, we introduced practical global corporate data approaches to the EU-U.S. Privacy Shield. In this next part of the series, we dig deeper into what is actually entailed during that process while highlighting key differences between Privacy Shield and the General Data Protection Regulation (GDPR) laws set to be enacted in the EU on May 25, 2018.

With the primary goal of protecting corporate value through exposure containment, this article discusses two major concepts: the basic differences from Privacy Shield to GDPR, and how a global corporation can effectively utilize a corporate data mapping process to arrive at a privacy impact assessment (PIA).

Privacy Shield v. GDPR

To begin, let's recap and expand upon the theme. Privacy Shield is an agreement between the EU and U.S. allowing for the transfer of personal data from the EU to the U.S. This enables U.S. companies, or EU companies working with U.S. companies, to meet the requirements of the GDPR.

In contrast, the GDPR has a legally binding impact on the working of all 28 EU member states with specific requirements regarding the transfer of data out of the EU. By extension, the UK is expected to introduce a revised form of the Data Protection Act

(DPA) to protect consumer data in the same manner as the GDPR.

To avoid ambiguity, GDPR is presently structured (subject to the final determination of the 28 Working Group) including significant teeth, with requirements and repercussions for failing to comply far stricter than those outlined in Privacy Shield. This includes the following key provisions:

• The Right to be Forgotten: An individual has the right to request the erasing of their personal data.

• Increased fines for breaches of the GDPR, up to 4 percent of the infringing party annual revenue (if this doesn't cause you pause, it should).

• A "Privacy by Design" provision requiring data protection measures are designed by the entity from the inception of personally identifiable information (PII) receipt.

• The required appointment of an independent data protection officer (DPO) by multinational companies working across the EU required to manage the legal aspects of the GDPR.

• The prohibition of data being transferred outside the EU without approval from a supervisory body, subject to further definition of the Working Group.

• Mandatory breach notification for certain types of data breach, such as where a breach may impact the rights of the individual (think about developing effective data breach response protocols here).

What now? Wasn't self-certifying under Privacy Shield on or before September 30, 2016 enough? Think again. By the end of 2018, it is estimated that over 50 percent of companies affected by the GDPR will not be in full compliance with its requirements.

Odds are, your business and the data it holds touches somewhere around the world beyond the U.S. It's time to think global compliance versus just in the U.S. The following five elements require primary attention:

• Determine company role under the GDPR;

• Appoint a company data protection officer (DPO);

• Demonstrate accountability in all processing activities;

• Check your cross-border data flows; and

• Prepare for data subjects exercising their rights.

Most importantly, companies need to demonstrate accountability in all data processing activities. This ongoing requirement leads us to an essential activity companies must undergo to prove out GDPR compliance when called upon for the same.

Undertaking an Effective Corporate Data Mapping Exercise/PIA

Not ironically, cybersecurity best practices (which are designed to protect corporate data and PII) are highly instructive in establishing an effective corporate data mapping exercise or privacy impact assessment (PIA). Specifically, we look to what is known as the "Top Down/Bottom Up" method:

Data Transfer Due Diligence

The "top down" portion of the method entails a geographic corporate business analysis, including what respective aspects of company business are done by location. This involves certain data transfer due diligence interview subject matter areas, where those conducting the exercise should focus on operations, privacy, and data protection as applicable:

Business unit/function overview: Where are the operations of your business unit/function, and where it is located?

Processes specific to the business unit/function: Where is collection, use or sharing of personal data in the business? Does the business unit/function have any specific processes related to personal data (e.g., collection, handling, use, or sharing), and how are they documented?

Personal Data

• Describe the individual data subjects for which the organization collects, uses or shares personal data (e.g., human resources, patient, consumer) and the purposes for which the data is collected, used or disclosed.

• Where, geographically, are these individuals located?

• Describe the categories/types of personal data that are collected, used and/or transferred between affiliates or across borders (e.g.,

name, medical history, credit card number, Medicare number, IP addresses).

• In addition to the above, describe any sensitive personal data (e.g., EU definition of sensitive personal data).

• In relation to each category, describe the business units/functions that share personal data. Ask, what groups or organizations are recipients of personal data? Also, what countries are part of the data flows?

• Are there other groups that access or wish to access the business unit's/function's personal data?

Third-party relationships (third parties are more than just vendors—this could include customers, consumers, CROs, etc.)

• Does the group share or receive personal data with third-parties? Who are they, and where are they located?

• In what jurisdictions are the third parties located? Where do they store the data?

• For what purpose is the personal data shared with each third-party?

• Describe the process the group follows when it vets a third-party. Is there a privacy and/or security assessment of the third party or vendor conducted prior to drafting or negotiating a contract?

• Does that third party share the data with a further third party for any reason, e.g. sub-processing?

• Does the group have joint responsibility for any personal data with any other organization (either within or outside the group), e.g. collaborative research projects?

Secondary data uses: Does the group engage in any secondary uses of personal data such as analytics or market research? Are there secondary uses that are currently not used that could benefit the business unit/function?

Notice and consent practices: Does the business unit/function collect consent from individuals? If so, who is responsible for providing notice and obtaining consent (as applicable)?

Training and awareness: Has the business unit/function received privacy and/or information security training within the past 12 months? Do individuals in the business unit/function who regularly work with personal data receive any additional training regarding privacy and/or information security?

Complaints process: What mechanisms exist which enable individuals to submit complaints regarding the handling of their personal data?

Incident response: Is there general awareness within the business unit/function about how to respond to a privacy or security incident? Within the last 12 months, has the business unit participated in any simulated incident response activities?

Near-term data use plans or needs: Within the next 18 months, does the business unit/function have any plans that implicate a new use of personal data?

Privacy and information security interactions: Describe the business unit's/function's level of engagement with the privacy and information security functions. Who is responsible for privacy compliance within the business unit/function? Who is the contact person for privacy-related questions? How is privacy considered when planning a new project/activity?

Resource needs: Are any additional resources needed to enhance your business unit's/function's privacy posture?

Additional Opportunities: Are there any opportunities to enhance privacy and/or information security not covered?

The Bottom Up Process

Next, we must assign PII risk levels based upon results of geographic analysis and data transfer due diligence. Top risk level items should be regularly reviewed, with periodic review for other items and upon change in business practices. Ask, where is the origin of PII per risk level assignment?

The company may now also reduce the overall data universe/custodian locations based upon PII risk level priorities, enabling it to work within a more manageable/cost-effective range of data.

The "bottom up" process identifies computer/technology systems (cloud based or

otherwise), processes, platforms, applications, software and methodologies which collect, assemble, replicate, share, backup, transfer and/or otherwise hold PII data in any way. A few questions can help in this identification:

• What systems interact with data related to classifications within PII risk levels?

• What tools/processes can be utilized to located PII within systems? We recommend consultation with company RIM, IT, technology and other process owners to create the map for the company data.

• What rules apply to the above? State, federal, foreign and by treaty?

• What processes can the company use to segregate PII? What are the pros/cons of each method? Are there practical considerations, such as data category maximums, to identify, locate and segregate PII?

The Next Steps

An effective corporate data mapping exercise/PIA is a crucial process to demonstrate accountability in all data processing activities subject to both GDPR and Privacy Shield liability. Although a moving target by the inherent nature of exponential data growth, top priority PII items can be isolated for "mini" review at reasonable intervals or upon material changes to systems, data sources and business protocols.

Remember the new maxim: *The corporation may keep personal data only for as long as this serves the lawful purpose for which the data was collected*. This begets ongoing analysis to isolate and dispose of PII when outside of legitimate or required data retention periods.

Simple tips to lessen exposure may include online retailers offering users drive-by purchases (the ability to order items without creating an account). The key here is individuals must know exactly the terms to which they agree in providing a company use of their data. A company needs to be clear on the data it holds/transfers and be accountable for the data it processes.

We leave you with the conclusion that any company operating globally should protect their value through exposure containment under both Privacy Shield and the forthcoming GDPR by undertaking an effective corporate data mapping exercise and PIA with subsequent updates based upon determined risk levels and corporate changes.

Dan Panitz, UnitedLex VP Global Legal Solutions, is an experienced attorney based in New York with more than 20 years of combined legal, technology and corporate advisory experience. Having worked with SEC enforcement and NASD (now FINRA) arbitration, Dan also holds Anti-Bribery & Corruption specialty certifications for the PRC, UK and the US.

H. Bruce (HB) Gordon currently works for Teva Pharmaceuticals located in Horsham, Pennsylvania as their Manager, ESI Response Management. Prior to Teva, HB worked for AmerisourceBergen Corporation as the IT Liaison to the Legal Department, and Rohm and Haas Company as the IT Manager for the Legal Department.