Autumn Noblit

Group 6

Data Privacy Project Individual Analysis

1. Apps Selected
   1. **Eaton Community Bank** (Local Credit Union serving residents of Mid-Michigan)
   2. **Sandals Resorts** (International Company headquartered in Jamaica serving clients worldwide)
   3. **Tennessee Performing Arts Center (TPAC**) (Non-profit, theater in Nashville, TN with services available on-site only)
   4. **US Bank** (International Financial Institution offering global services and headquartered in Minneapolis, MN)
2. Individual Analysis

**Eaton Community Bank**

The privacy policy is approximately 3 pages easy to understand. ECB serves community members in Mid-Michigan and Michigan does not have a comprehensive consumer rights law, such as those in California and Virgina, the privacy policy is written to align with US Federal Regulations

The policy is limited in its consumer rights but does provide information on how, why and for what purpose the information is collected. Additionally, there is a limited opt-out policy, however, the provisions don’t apply for two reasons, 1) You can’t opt out of sharing for everyday purposes, internal, joint or affiliate marketing. 2) The company doesn’t share information with affiliates or non-affiliates.

There is no reference to CCPA, VCDPA or GDPR. While the policy is not required to contain elements of the GDPR, the privacy policy appears to align with the GDPR Principles relating to processing of personal data in the fact that Eaton Community Bank collects limited personal information which is only necessary for the purpose of its processing (except for internal marketing).

**Sandals**

This privacy policy is the most comprehensive privacy agreement of all analyzed. The US agreement, although lengthy at approximately 28 pages when copied from the web and pasted on a Word Document, is organized and fairly easy to understand. The policy even provides a specific breakdown of how categorical data is collected and used in a matrix format on their website.

Although this is the most comprehensive agreement, there is nothing specific in the US agreement regarding rights to correct data or data portability. However, as an international resort that keeps track of clients’ flights and booking reservations, I cannot see why they would not correct most, if not all personal data. I have personally never had an issue calling in to make a change or updating my information online.

The US agreement also provided links that are specific to residents of California (CCPA) and Virgina (VDPCA) along with links to multiple other US state laws. Sandals also provides a separate EU privacy agreement.

Because this corporation has such a comprehensive privacy agreement, it is a bit lengthy and laborious to read. Therefore, it may be easy for a consumer to overlook important information.

**Tennessee Performing Arts (TPAC)**

This privacy policy is similar to that of Eaton Community Bank in that it is relatively short equaling approximately 4 pages when copied from the website and pasted onto a Word Document.

Although TPAC doesn’t do business in California or Virgina, the policy includes many components of the regulations outlined in both the CCPA and VCDPA. Those components include, notice at collection, handling practices, right to know, opt-out processes, right to delete and data minimization. There is not information on rights to access or correct data nor on data portability. Limited PII is collected and nothing noted about collection of sensitive data.

Additionally, although TPAC doesn’t target EU citizens, the policy contains components of Data Subject Rights as listed in GDPR. Such as explicit consent to opt-in for promotional items marketing.

**US Bank:**

Overall, their general privacy policy is very similar to the policy of Eaton Community Bank and aligns privacy policies to US Federal Law. The general consumer privacy policy is short, being approximately 3 pages. The general policy does not provide many specific rights to consumers where states do not have specific regulations in place, such as Tennessee. However, US Bank does provide a separate policy to comply with the CCPA but does not list anything in regard to the VDCPA.

Like ECB’s privacy policy, the US Bank does provide information on what personal information is collected, how it’s collected and used, and how to limit sharing/opt-out of affiliate sharing and direct marketing.

Additionally, there is a privacy policy in alignment with the GDRP for those using US Banks Global Funds Services. According to their website, U.S. Bank Global Corporate Trust Europe, U.S. Bank Global Fund Services Ireland and U.S. Bank Global Fund Services (Luxembourg) S.à.r.l established this policy.

1. **Assumptions and Limitations**

After completing some research, I found that the GDPR does not necessarily apply to EU residents living or visiting the US or other countries. Because Eaton Community Bank is in mid-Michigan, and Tennessee Performing Arts Center is located in Nashville, TN and neither institution targets citizens of the EU, it is assumed these entities do not have to adhere to or provide a privacy policy related to the GDPR. Additionally, since these entities do not do business in California or Virginia, they do not have to explicitly provide policies that align with the CCPA and VCDPA.

Limitations for US Residents are that the oversight and accountability for these regulations is left in the hands of the consumers hands. This is unlike the GDRP where enforcement of privacy protections is the responsibility of national data protection authorities in each EU state. These limitations leave individuals with the burden of both identifying policy breaches and then taking actions against companies. This is an overwhelming if not almost impossible task for an individual consumer to take on. Therefore, many breaches of compliance may go undetected or unenforceable due to the resource disparity between individuals and corporations. In the EU, citizens may have a fair fight against corporate breaches of privacy policies due to having the backing of their governments.

1. **Practical Implications**

In the US, consumers are left to navigate the complexities of data privacy and proper adherence to laws by institutions. This makes it almost impossible to know if laws are being followed unless something like a data breach happens or one finds themselves in a situation of stolen identity. Even then, a consumer can’t necessarily trace their identity breach of information back to one single source.

How quickly businesses reply to requests depends on the capacity and ethical principles of the organization and the people they have working with them. It seems plausible that a large company could be unresponsive or work on a timeline that is best for them since the fear of any type of penalty from an individual would be minimal.

1. **Conclusion**

All of the agreements have the same general framework in place explaining data collection, sharing and opt-out policies. TPAC and Sandals provided information on deletion rights and more in-depth information on the use of cookies on their websites. None of the websites specifically addressed data portability.

Additionally, the entities serving local consumers (TPAC and ECB) did not have any references to CCPA, VCDPA or the GDPR. Although US Bank has policies that align with regulations of the CCPA and GDPR, it does not mention VCDPA. Sandals Resorts is the only agency in my analysis that includes information related to CCPA, GDPR, and VCDPA. Additionally, Sandals provides separate policies in alignment with multiple US state laws and Canadian laws.

Overall, these privacy agreements were generally well-organized and relatively easy to read and understand. However, the Sandals Resorts policy was lengthy, which made it more difficult to finish reading. While each organization appears to meet the minimum legal requirements in their written policies, this analysis didn’t explore the real-world implementation or ease of consumer use.

This is where the real challenge arises, when individuals must navigate these policies in response to a privacy concern. In this way, the GDPR stands out, offering clearer, more enforceable protections. As the U.S. continues to develop its privacy policies, it should consider adopting a more comprehensive approach -one that includes a single-entry access point for consumers to report and resolve corporate privacy policy violations.