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. Regulatory Comparison

**Eaton Community Bank**- Due to it’s size and local, the privacy policy is based on federal law. Michigan does not have comprehensive consumer rights regulations such as California and Virgina.

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. However, 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 is the most comprehensive privacy agreement of all analyzed. The US agreement, although lengthy, is organized and 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, 4 pages when copied from the website and pasted onto a Word Document. The information provided meets general regulatory requirements such as notice at collection, handling practices, Consumer Rights (exception of discrimination which is specific to CA residents), Opt-Out, and Processing limitations (VCDPA). There is not right to correct or data portability. Limited PII is collected and nothing noted about collection of sensitive data.

The policy also 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. However, US Bank does provide a separate policy to comply with the CCPA but does not list anything in regard to the VDCPA.

Therefore, their general policy does not provide many specific rights to consumers where states do not have specific regulations in place, such as Tennessee.

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.

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 located in mid-Michigan, and Tennessee Performing Arts Center is located in Nashville, TN and does not target citizens of the EU, these entities most likely do not have to adhere to or provide a privacy policy related to the GDPR.

Additionally, these entities do not expressly have privacy policies related to CCPA and VCDPA

Similarities

Differences

* 1. Key Aspects of
     1. GDPR is that businesses are limited in collection and govt. enforces laws
     2. US protections focus on consumer right to litigation. No specific oversight or comprehensive federal law.
  2. Practical Implications
     1. 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 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.

Data Portability is one that is interesting. Outside of Health Care, I can’t think of a time when I requested that my data be transferred to another organization. If this is an option, it would save a lot of time in having to fill out paperwork multiple times. However, a business might still require this as I know my medical provider does. I am not quite sure what day-to-day benefits come out of data portability.

The idea of **restriction of data processing** is complex and a difficult to follow. I don’t see this listed in state laws or in the privacy agreements of the US. It is also unclear why someone might want data kept by an institution but not used?

The US focuses on Opt-out putting more responsibility on the user, however, after looking at examples of opting-in for cookies, it doesn’t appear that there is much difference. I can only assume this is because websites can be accessed from anywhere in the world and therefore have to comply with the highest level of privacy compliance vs. the lowest for when you may actually completing full transactions with an agency.