Unit 1 Collaborative Discussion 1

Peer Responses

Contents

Response to Kikelomo Obayemia

Hi Kike,

In your opinion, do you think that decision-making concerning data privacy is something that should be made at the team lead / development team level or higher-up, say management level? I ask because, in terms of a code of conduct, Data Privacy is definitely a topic each employee must be aware of -- regular training sessions should certainly be held to maintain awareness -- however, decision-making powers surely must rest with management who bear the burden of responsibility.

So, for example, based on one's role, yes one may work with this or that data, and certainly, as IT professionals, if we feel the data should be treated in a sensitive manner, we ought to flag it so.

Response to Taylor Edgell, Kikelomo Obaymei

Hi Taylor,

I do not think there would be any conflict in non-EU companies being forced to adopt EU GDPR standards; it comes with the requirement of doing business in the EU. We can test this thought by looking at the financial rules around the globe within each country (specifically the tax rates). Here each country is free to determine their own financial regulations, however, all must abide by common laws when dealing together on the world stage -- sovereignty is never relinquished.

In this regard, doing business in EU requires non-EU businesses to comply with EU requirements, and interestingly enough, there indeed are several countries signing up to adopt GDPR principles (EU_1, ND.) though, since the GDPR framework is flexible, not all business are required to implement the same stringent requirements and various parts of the framework permit modification (ICS, ND.)

References

EU_1, (ND.) Adequacy Decisions. Available from https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en [Accessed 02 February 2021]

ICS, (ND). Irish Computer Society: Harmonisation and Flexibility within the GDPR. Available from https://www.ics.ie/news/harmonisation-and-flexibility-within-the-gdpr [Access 02 February 2021]

Response to Suresh Sigera

Hi Suresh,

In your Software Requirements Specification (SRS), who is responsible to determine what *is* or *is not* sensitive data? In terms of the GDPR regulation, there are three main roles, each with distinct responsibilities (Metric, 2017):

1. Data Controller
2. Data Processor
3. Data Protection Officer

References

Metric. (2017) Decoding GDPR Roles and Responsibilities [pdf] Available from https://www.linq.it/wp-content/uploads/Decoding_GDPR_Roles_and_Responsibilities.pdf [Access 02 February 2021]

Response to Solomon Kanihiro

Hi Solomon,

I can empathise with your situation. You mentioned in your opening statement "there is no telling what this data is going to be used for and what impact it will have on our lives". My experience is that individuals who steal such data use it for their own personal gain.

For example, identity fraud in South Africa is a massive plague: people end up with court fines and demands to pay accounts they did not open. To tackle this issue, the private sector have come together to establish a Fraud Prevention company (which major banks and retailers have joined). The company enables citizens to protect their national identity number by making a sworn statement of truth about their ownership. If a fraudster then uses a citizen's data without consent to open false accounts, the retailers and banks are aware and will take steps to prevent such fraud. In a way, this is similar in spirit to GDPR, but it is not the same.

For this reason, your idea to raise awareness of the value of data we submit (within Uganda) is a tremendously good suggestion. But the challenge is how to raise awareness.

The governments have Data Protection policies, but still, people fall prey to providing data they should not. So Data Protection policies, it seems, are good to enact jurisdiction or legal concerns, but ultimately it is the citizens who must act responsibly. Surely awareness is a two-pronged approach: government and citizens working together?

Response to Taylor Edgell

Hi Shan, Taylor,

Openness is possible among companies, but it takes agreed-upon standards to work effectively. GDPR is having a positive impact in the area of data privacy in more countries that merely the EU. Your view is towards openness among companies, the EU has a bigger picture in mind. With reference to EU_1 (2019), Japan has formally recognised EU GDPR standards. This implies that businesses within Japan will now provide a similar level of data privacy afforded to EU citizens. In this regard, openness is defined by the GDPR standard. Not only has Japan signed onto GDPR standards, but so has Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man Jersey, New Zealand, Switzerland and Uruguay, according to EU_2 (ND.).

References

EU_1. (2019) What happens to personal data transferred from EU to Japan. [pdf] Available from https://ec.europa.eu/info/sites/info/files/research_and_innovation/law_and_regulations/documents/adequacy-japan-factsheet_en.pdf [Accessed on 02 February 2021]

EU_2 (ND.) Adequacy decisions Available from https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en [Accessed on 02 February 2021]

Response to Rachel Doherty

Hi Dr Nawaz, Rachel, Kike,

If each functional unit defined their own policies and guidelines, while still aligning to policies defined at corporate or global level, would this not be slightly redundant; redefining the same policy in each functional unit?

Also, who is responsible for governing the policies of each functional unit? The assumption is that this responsibility lies at the corporate level. If true, why would corporate not, therefore, make all policy decisions? Considering this question, I think of the U.S.A and the separation between federal and state law; it is like an order of precedence.

Response to Sergio Caldera

Hi Sergio, Kieron,

Sergio, you mentioned that you think data collection techniques will improve so that businesses do not fall foul of fines. With the emergence of Big Data and Cloud computing, data collection indeed has become easier for companies, and in this regard, I would argue that companies collecting such data do so ultimately to make money; they worry about potential fines later on. Do you think this would be so? For Big Data to be useful, I think companies need more data points to relate to disparate data sets, not less. I believe Cloud Computing and the exponential explosion of more data poses massive challenges to the idea of data privacy. Eventually, an assumption is that the laws may become overwhelmed and likely will fail society, resulting in Big Tech having greater access to more data without their consent.

Response to Kieron Holmes

Hi Kieron,

When considering your question to Nawaz, I think the lack of adequate finances is the number one barrier to compliance followed by a lack of knowledge.

Rosenzweig (2013) notes that when crimes are committed, judges consider intention and culpability. He summarises that "Americans are therefore asked to undertake an impossible task—knowing what conduct is allowed and what prohibited—and then punished when they

fail. That is simply unjust." I think the same thought can be applied to businesses and GDPR policy. The law exists, businesses cannot claim ignorance. However, conduct (or intention) must surely come into play when meeting out potential fines. In this regard, GDPR (2021) in the section How much is a GDPR fine, layout the steps used to determine the severity of a fine and here again we can observe the ideas of intention and culpability.

Therefore, while finances can be deemed the most significant hindrance -- people and tools cost money -- lack of knowledgable (ignorance) can pose a greater threat. To resolve this, it is therefore imperative for IT professionals to bring such knowledge to their employers or even other businesses. For example, when providing contact details to a business, one can query their data privacy policies and engage them in helpful conversation.

References

GDPR (2021) What are the GDPR fines? Available from https://gdpr.eu/fines/ [Accessed on 11 February 2021]

Rosenzweig, P. (2013) Ignorance of the Law Is No Excuse, But It Is Reality Available from https://www.heritage.org/crime-and-justice/report/ignorance-the-law-no-excuse-it-reality [Accessed on 11 February 2021]

Response to Suresh Sigera, Dr Nawaz Khan

Hi Nawaz, Suresh,

According to Felz (2018), Data Protection Impact Assessments (DPIA) is one way to identify risks (and fines) related data privacy. DPIAs are necessary every time businesses adopt technology that handles automated processing of data. Article 35 of the GDPR regulation goes into detailed about DPIAs (EU_1, 2021)

With regards to frameworks to support businesses, the following standards can help:

BS 10012 2017 + A1 2018 Standard (data protection of personal information) and

ISO 27701 (privacy extension for security management)

References

EU_1. (2021) General Data Protection Regulation: Data Protection Impact Assessment. Available at https://gdpr.eu/article-35-impact-assessment/ [Accessed on 02 February 2021]

Felz, D. (2018) German DPAs Issue DPIA Blacklists -Many Companies Likely to be Affected. Available at https://www.alstonprivacy.com/german-dpas-issue-dpia-blacklists-many-companies-likely-to-be-affected/ [Accessed 02 February 2021]

Bibliography

Std_BS, (2018) BS 10012 2017 + A1 2018 Standard. Available from https://www.itgovernance.co.uk/shop/product/bs-10012-2017-a1-2018-standard [Accessed on 02 February 2021]

Std_Iso, (2021) The international standard for privacy information management. Available from https://www.itgovernance.co.uk/iso-27701 [Access on 02 February 2021]

Response to Andrey Smirnov

Hi Andrey,

Could you expound a little more on your statement regarding the slowdown of velocity due to GDPR regulations? I'm assuming the following:

1. Data Architects and Business Analysts should be well-versed in sensitive data
2. The company has a GDPR-related code of conduct in place to guide decisions

So if the points above hold true, surely velocity should *not* slow down because each team member understands the impact of their tasks and also the sensitive nature of customer data they're working with.

However, I would like to raise one more point: if the development teams worked with *obfuscated/anonymised* data, velocity would again not be impeded because according to directive 2016/80 (point 21) GDPR does not apply to anonymised data (EU_1)

References

EU_1, (2016) Directive (EU) 2016/680. Available from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG&toc=OJ%3AL%3A2016%3A119%3ATOC [Accessed 02 February 2021]

Bibliography

R26, (2020) Not applicable to anonymous data. Available from https://gdpr.eu/recital-26-not-applicable-to-anonymous-data/ [Accessed 02 February 2021]