Author: Bartosz

Your cousin graduated in ICT & Software Engineering 10 years ago and is still working happily at an ICT agency called 'Make more money with IT!'. He was promoted to the CTO role and leads a high-profile project with many stakeholders and possibly large amounts of end-users.

Recently a legislation was passed on GDPR making each company responsible for privacy aware data handling. Company does not have a separate privacy officer and decided to make CTO the end responsible for GDPR-proofing the company.

Your cousin has read that GDPR compliance is mandatory and needs to address it as soon as possible to avoid company image damage and potential financial fines. In concrete work it means he will need clear procedures on how to handle GDPR.

In collaboration with his team he came up with following scenarios that need to be tackled first:

1. Customer’s project X is hosted by our company partly on premise of X and partly in a 3rd party cloud. Project is a CRM system and uses a scalable distributed database.
2. Employee of our company – a SW engineer - has lost his laptop. That laptop was used to work on project X, contains Git branches and VPN access to cloud where project X is deployed.
3. Project X had major DB revisions and necessary migrations. To avoid data loss a data backup is in place, also for older versions of DB. The company does not know what CRM data is stored in DB as it is encrypted for security reasons. Customer who is the owner of the project X had a private data leak that was communicated to the authorities and made public. As a result, some of the clients decided to use their privacy as an argument to cancel subscription to project X. How to remove their private data is not clear.

While working on the scenario 2 your cousin recollected an incident he was involved in:

As a fresh CTO, your cousin was asked to be a part of a delegation to represent the company at yearly consortium of best practices in ICT in Shanghai. Just before his company was to present, the laptop of his colleague malfunctioned. As a quick fix your cousin lend his laptop to give the presentation from it.

After presentation there were many questions from the audience and your cousin went to lunch with some of the interested parties. He forgot his laptop completely and left it unattended at the presentation hall. When he came back from lunch laptop was unlocked (probably to make sure presentation will not be disturbed by an automated screen lock).

Your cousin is nervous. Clearly, he cannot be 100% sure that no one accessed company sensitive data or even the project X data containing huge DB of private customers. After he got his CTO role, he took mortgage for a large villa. He can lose the villa and his CTO role for what he did. His reputation will be stained for a long time as well, he may even be fired. He has much to lose. His wife thinks he should not speak about it especially because there is no proof something happened. However, observability feature in project X was partly implemented. He can remove log records himself, pretend like if he was testing if anyone would notice suspicious access, destroy his laptop and pretend it was stolen, use account of the intern to update the log or ….

Half year later an almost clone of Project X is promoted by another company at half the price. Various companies are buying it like crazy. The founder of 'Make more money with IT!' is furious and demands heads to fall for not launching the project X earlier.

**Assignment**

Help with the 3 scenarios by describing how GDPR affect these and what concrete steps should be taken to be GDPR proof. Make sure you investigate and define clear procedures and advise on how to provide technical support to execute these.

You meet your cousin at the family evening. He was a bit drunk and nervous. He told you the part of the ‘laptop story’ starring ‘his colleague’ and consequences of a ‘fast competitor company’. You are smart and you connect the dots.

You could not stop yourself from thinking how it would affect you. What would you do in cousin’s place? What would you do in his ‘colleague’ place? Where is the ethical border you would never cross? What would force you to come clean? You are also not sure how to judge your cousin, he is not good at lying and you suspect ‘colleague’ does not exist. Will you look differently at him the next time you meet?

Choose either CTO standpoint, your own (as his cousin) or an IT-internship student who noticed suspicious log entries in project’s X log. Write an essay, look from at least 2 perspectives on the problem and finalize it by taking clear stance yourself including the perceived impact of your decisions on identified stakeholders.