INTROSEC HT2020

Problem 2

UrStudent is a software development company based in Stockholm. The company provides software to universities both in Sweden and across Europe that supports activities of students and teachers, including registration of marks, dashboard of individual student's marks and others. The company, to be compliant with GDPR, has started a process of implementing Privacy by Design (PbD) into their software development process. Focus on at least 5 principles of PbD and discuss what implications the integration of PbD will have in their software development process. Provide specific examples to support your discussion.

Solution

GDPR includes regulations that assures the privacy of the data. It is very powerful and has companies complie with it.

I will put my focus in the following principles and analyze each one of them.

a. **Proactive not Reactive:** That means that we are looking for security to be implemented and stop attacks from happening or data stolen. Other than react when something bad has already happened.
   Implications in the development process might be that the company has to be very careful and check against attacks and see how the software operates. A great focus has to be put on that, which might nit have been the case preciously. The data must not be stolen. So test like penetrationtesting and more similar should also be done.

b. **Respect for user Privacy:** The interest of the users should be kept in mind when designing the software. They data should be kept secret at any point. The designshould be user centric.
   Implications for the development prossec is that exept from the security of the data the privacy should also me kept. That means that they should be careful if they also have agreements with 3rd party companies not to give this data away. Sharing user data with other companies if the data remains secure violated the pricavy so they should not have such things integrated into their software and also busines model.

c. **Privacy embeded into design:** That means that it should be embeded into the design. It is one of the very important aspects of when creating and designing the software. Not something that should be as an extra feature. It is something that should be at the core of the designe.

d. **Privacy as the default setting:** It means that the data at any point should be assured to be secure and stay private. The user does not need to do something for it. So basically the pricaxy is built as default into the system.

   Implications for both Privacy as the default setting and privacy embeded into design. What it states is that privacy should be the core of the development and design process. That means that the company now has to base their entire plan on not affecting these two and also implementing them from day one. In some ways it might restrict the company when it comes to their original plan. From day one they will have to comply with the GDPR regulations. Every process that involves data will be carefully managed limited what it can be done by them.

e. **Visibility and transparency:** in other words the others interested into the software/system should be made assured and can be shown to the that the system complies with the rules an the data is secure and private. Basically you get the trust of the users and stakeholders by showing them that the system is secure. The components are visible and transparent.
   In this case implications in the development process of the software might include that every step and every design process is done in a different way that they anticipated and more visible to the user. Also the fact that they have to do with students who have knwledge about regulations and may report them if they do not comply makes them consider these two(vsibility and transparency) more in depth.

Implications in general

The GDPR ristricta a company and many aspects of it. When this company follows PbD policies that automatically translates in more carefull and professional care of the design. That might bring a higher cost also because of new people needed into the team. A higher cost and risk may come if they do not comply with the regulations too. The process of the development too might be slower since there are many things to take into consieration. Also the business may have to recreate their entire system if the precious one was far from the wanted one. Since this company has to apply those regulation into their software they will have to view every aspect of it, since many things are not transparent. Also if they have not followed privacy emebede into design that will come with many implications and a long time to comply with the regulations.