The Big Pitfalls of GDPR

By Lars Abild
June 14th 2018

Helle Mering, owner of SOSY A/S.

Protect your customers' data. Sounds straight forward, but according to expert it requires a new way of thinking to actually ensure this. Since 1989, Helle Mering has worked with software solutions. Today, she is helping companies pinpoint and solve their challenges based on the new rules for personal data within GDPR. Join us on our journey into the cockpit, and hear the owner of SOSY A/S tell about her simple approach to protection of personal data.

Today, there are much stricter guidelines for developers of digital solutions, in particular in regards to which data you are allowed to use during the development process. The objective is to protect the customers' data so that they – in case of an error - don't end up readily available in cyberspace.

It sounds straight forward, but it requires a new way of thinking, says Helle Mering, who has worked with software solutions since 1989 and who owns the software company SOSY A/S.

The goal – to become data compliant – is a good message to convey these days. But it is quite a journey to get there and to have all processes documented, she says.

In simple terms, what has to be done, when you want to manage your data, and how do you solve some of the obvious challenges which many have taken less serious until now? Areas where you now risk getting huge fines?

Many just copy production data
Helle Mering talks about a known dilemma: Using production data during the development of digital solutions.

”Seen from a compliance perspective, it has never been good practise to take a copy of production data to use for testing, but this has been common practise in many companies. However, the new privacy rules state that this is not allowed when you are working with sensitive data, i.e. data which directly refer to a specific person. And with the big fines that GDPR can impose, this issue is now taken a lot more seriously.”

To be more specific, if you are working in the HR department, you work with wages, statistics for employees etc. That is sensitive data. People working in HR departments of course need access to these sensitive data to do their jobs, but it is not OK to just send a copy of these data to the software development department. They should be working with ‘testdata’, and in order to live up to the requirements of GDPR, testing with data during a development process becomes a true challenge which has to be dealt with.

Data integrity is key
”One of the solutions that we work with offers automatic anonymization of production data when they are to be used for testing. This implies that you have testdata available regarding employees or customers with the same characteristics as the production data, but the developer or the tester cannot see whose data they are working with” says Helle Mering.

The first part of the process is that you have to identify which parts of your data are sensitive.

”Not all of your data is sensitive. It is typically only certain columns or rows in your databases. The next step is to decide, how you want to anonymise or scramble your data. There are multiple ways of scrambling”, she says.

Once this has been taken care of, it is key that you can actually use the testdata that you have produced. That the ‘data integrity’ has been kept.

Mickey Mouse cannot become Donald Duck
”The most difficult part of the process is to ensure that the data integrity is kept when testdata is produced, i.e. that you keep the correct relationship between the different parts of your data. E.g. if you need to test a complete order flow. You cannot scramble your data in the customer database in one way, and your data in the order, invoice or delivery databases in a different way. Then you cannot find sample data which covers a whole flow.”

An easy way of explaining this is that if a customer gets the pseudonym Mickey Mouse in one database, then Mickey Mouse needs to be used in the other databases too. Because then you can test an entire workflow with all its functions and processes. At the same time, anonymization implies that you are compliant with GDPR, in case the the inspectors want to check your procedures.

Helle Mering tells us that historically, there are numerous examples of people just using production data for testing. The stories became horrible when data leaks occur during the testing process. That’s when the problems become serious. Now with GDPR, this area gets even more attention.

”If your testdata are sufficiently scrambled, they are no longer sensitive data. Therefore, it is not as problematic and critical as before, if/when a data leak occurs. And that is precisely one of the main objectives of GDPR: To protect sensitive data.”

Do you have control over your system and users?
Some of the aspects, which is often mentioned in connection with GDPR, is whether you know who has access to your systems and therefore to the databases, and what the users are doing when they are logged on.

”Many companies do not know what people are doing when they are working on their systems. This regards both internal employes and external consultants. Are people actually allowed to do what they are doing – to access the data they are accessing? Often, the data managers think they know what is going on, but we have seen many times that that is not the case,” states Helle Mering.

It may sound very simple, but one of the errors which happens time and time again, is within the area of system access. When a new employee needs access to the system, a copy of an existing user profile is made. That is a quick and easy process. But often quite problematic.

”Because does the new employee really need access to all the same databases and menu options as the person you copied the profile from? This practise, just copying one user profile to the next – and the next … - quickly results in quite a mess in regards to GDPR. Today, companies need to know what each user of the system may and can access, when he/she is logged on,” she says.

Documentation is a huge challenge
The rules also require that you document important work processes within the company to illustrate that you are compliant. This can be just as time consuming and boring as it sounds, if you have to take xx screenshorts of work processes, copy them to Word or PowerPoint and insert the correct comments or instructions. But you need to have this in place to train new colleagues.

”We offer a solution that automatically documents everything you do, and you can insert comments on the fly or afterwards when reviewing your work. Converting the result into Word/PDF or animation are popular features, especially when training materials are to be created.,” says Helle Mering.

The right to be forgotten
One of the rights that a customer has, is the right to be forgotten. This requires that a company knows what data they have about each customer, where such data is stored and well defined procedures for removing the data.

”This part of GDPR implies that it is not only the data protection officer who needs to be in control over the sensitive data. The colleagues who have to perform the processes need to know what to do, and the documentation has to be up-to-date,” says Helle Mering.

Helle Mering
Helle Mering has worked with SOSY’s software solutions and consultancy services since 1989. Originally, the primary focus was systems management, but a number of new business areas have been added over the years. Today, the primary business areas for SOSY A/S are solutions for software test, security and real-time data sharing. Over the years, Helle has spoken many times at conferences in Denmark and abroad about SOSY’s business areas and solutions. Helle took over SOSY in 2003.

Written by

Lars Abild, Journalist

Employed at the Danish newspapers Børsen, Jyllands-Posten and Berlingske. Has also worked as freelance focusing on documentaries for the Danish television channels DR and TV2. Written articles for Information, Weekendavisen and Økonomisk Ugebrev (Financial Weekly Review).