GDPR and Data Complexities

**PREPARED FOR**

Erik van der Schriek

Niko Kuijpers

Gertjan Schouten

**PREPARED BY**

Maarten Blömer

Nick Krijgsman

Faruk Aydin

Jursley Gonzalez

Vincent Andersen

# Table of Contents

[**Table of Contents**](#_z6lhuq9emniv) **1**

[**Case Study**](#_k6jx82pctwds) **2**

[Case goal:](#_bpxkra1gvikb) 2

[Case problems:](#_tz830mgo6nzk) 2

[Case questions:](#_3vn6lbsuph60) 2

[Formulate learning objectives](#_58tw4qf8lsdh) 3

[Brainstorming:](#_llbf4q7qnu37) 4

[**GDPR Discussion**](#_zc6h8lveooxw) **5**

[Scenario 3rd party database (Maarten)](#_505gm0evad4t) 5

[How will GDPR affect it?](#_lzsb6znd569l) 5

[Steps to take](#_da1cbfh7lzqb) 5

[Scenario right to be forgotten (Vincent)](#_5fg2hbyyn53s) 5

[How will GDPR affect it?](#_tqvqtmf0o1p9) 5

[Steps to take](#_p6hckykplgel) 5

[Scenario security breach (Nick)](#_5fg2hbyyn53s) 5

[How will GDPR affect it?](#_69r4dx9vtcxo) 5

[Steps to take](#_ejpofzfu1qle) 5

[**Ethics Essay**](#_cg2taz46zkvz) **6**

[Thought process](#_izlssr2i4wll) 6

[Ethical considerations](#_lxax4x9e3fji) 6

[Conclusion](#_lxax4x9e3fji) 6

[How GDPR affected us and steps to take (Jursley)](#_13g2s5t5mszj) 7

[How reusing existing technology helps with this](#_h8j2gsiirrsp) 7

[Ethical considerations that are relevant for us](#_y1eflhav3wg1) 7

[**Sources**](#_qwibiw7iqp2l) **8**

# Case Study

## Case goal:

Get yourself familiar with the fundamental concepts of GDPR, so that you can help the CTO with the three scenarios. For each of the scenarios, describing how GDPR will affect it and what concrete steps the CTO should take to be GDPR proof. When doing this, make sure you investigate and define clear procedures and advise on how to provide technical support to execute these.

## Case problems:

1. Client's Project X is hosted by the company partly on premise at the client and partly in a 3rd party cloud platform. In the cloud, a managed scalable distributed database is being used.
2. Project X had major database revisions and necessary migrations. To avoid data loss a data backup is in place, also for older versions of the database. The company does not know what CRM data is stored in the database as it is encrypted for security reasons. The client who is the owner of Project X had a private data leak that was reported to the authorities and made public. As a result, some of the end-users decided to use their privacy as an argument to cancel subscription to Project X. The end-users claim their right to be forgotten, but if their private data can be removed from the database is unclear.
3. Recently, an employee of the company (a software engineer) has lost his laptop. That laptop was used to work on Project X and contains Git branches and VPN access to cloud where Project X is deployed.

## Case questions:

* What to do to become GDPR compliant?
* What would you do when you can’t guarantee privacy or if there is a privacy breach?

## Formulate learning objectives

• Think about how GDPR will affect your group project and what needs to be done to become GDPR-proof (you may need to consult your PO and update your project backlog after this)

• From a technical point of view, think about how GDPR will affect the design and implementation of your group project. How can reusing existing technology help with this?

• Discuss what ethical considerations are relevant to your group project and how this may affect the product backlog and/or implementation of your group project (you may also want to discuss this with your PO).

## Brainstorming:



# GDPR Discussion

## Scenario 3rd party database (Maarten)

### How will GDPR affect it?

Depending on where the data is stored, the company has to make sure that the host does not sell the data to others. Cloud computing always presents a risk of leakage. It is challenging for enterprises to determine the applicable laws when it comes to cloud computing, currently the laws are blurry due to geographical locations being attached to these laws. Within the EU the physical location of where the data is stored determines which privacy rules apply.

### Steps to take

Make sure that ahead of time that there is a clear contract and clause written to make sure that the private data can adhere to the country of origin’s laws. Otherwise a person’s data cannot be fully removed if it’s backed up somewhere else where it does not need to adhere to certain laws. Breach notification obligations and protocols must be included in data processing agreements. Even if the cloud provider experiences a data breach that impacts multiple customers, the controller should own external communications and manage the overall breach with their support. ISO 27001, 27018.

## Scenario right to be forgotten (Vincent)

### How will GDPR affect it?

According to the official GDPR ruling of “Right to be forgotten” which the end-users are basing their claim on, they can withdraw their consent for processing of their data. This means that with this request the data should be deleted to the best of the controllers’ possibilities, assuming that the identity of the user can be proven in a suitable way. In which case the controller can request for additional information or refuse to erase the data.

The law does not however state in what form the data has to be erased, it should however have the result that the data should no longer be discernible without disproportionate effort. This gives the opportunity for the controller to do things such as physically destroying data or overwriting the requested data using software.

### Steps to take

Consider the following texts in the scenario of the case:

1. *“To avoid data loss a data backup is in place, also for older versions of the database.”*
2. *“The company does not know what CRM data is stored in the database as it is encrypted for security reasons. “*
3. *“The end-users claim their right to be forgotten, but if their private data can be removed from the database is unclear.”*

In **sentence 1** they claim that multiple data backups are in place, this means that with an erasure request, the user’s data should be deleted from all forms of backups since they requested so on ground of consent and where data is no longer needed for their original processing purpose.

In **sentence 2** however, they claim to now know what CRM data is stored and that it’s encrypted. Encrypted data must mean that they have a key and are able to restore the data to their original and readable format. If this is not the case, it would be a form of irresponsible encryption in which case they would be better off hashing and salting the data. This could, however, give some ground that the data is incomprehensible and unusable for the company if they wouldn’t use it for any other processing of it.   
  
In the last **sentence 3**, they give a vague reason as to if their private data can be removed from the database. This could have to do with anything; due to the encryption, identity verification issues in the database etc. as no further information is given.

The next best steps for the CTO would be to look at the following:

1. Verify the identities of the data subjects
2. Check if the data is accessible for deletion in their databases
3. If possible, delete all records of data from the users in every database backup including the currently used one

## Scenario security breach (Nick)

### How will GDPR affect it?

The risk of leaving your laptop unattended is that a data thief can steal data. This can result in a massive GDPR fine. If there is any chance there is personal data stolen, the GDPR states that the supervisory authority has to be notified within 72 hours. In addition the individuals also have to be notified their data could have been stolen.

### Steps to take

When you recognize that your security has been breached you have to notify the supervisory authority within 72 hours. The notification should at least have:

* A description of the breach including, the categories and approximate number of data subjects and an approximate number of personal data records.
* Contact details of the data protection officer for more information.
* The likely consequences of the breach.
* Measures taken or proposed to be taken to address the data breach, including, where appropriate, measures to mitigate possible effects.

After the notification the controller has to document the personal data breaches and monitor the actions taken.

So specifically for this scenario my cousin, the CTO of Project X, has to notify the supervisory authority. The measures he can take are setting stricter rules about the use of your company laptop and giving all employees a course in how to use your laptop safely.

### 

# 

# Ethics Essay

## 

## Thought process & Ethical considerations

## Conclusion

***What would you do in his place?***

First of all I doubt if the same incident will happen to me. The CTO made some questionable decisions before the data got stolen. The first one being giving someone else access to your work laptop which has a lot of sensitive data. The second mistake is leaving your laptop unattended and even worse unlocked. So if I somehow get in the same situation as this CTO did, I would check the logs and see if there was any access during the presentation, if so telling the CEO can still prevent the product being lost by releasing it as soon as possible to have the rights. Not the most ideal solution but it is one I could live with and maybe save the company from losing the project.

***Is there an ethical border you would never cross?***

After discussion, we agreed that lying about the situation to cover for your own mistakes is for the worse, having to live with the guilt and ultimately firing people for your own mistakes. This can lead to more problems; not only for oneself but for others too.

***Would you come clean to the founder of the company or choose another solution?***

Check the log records of the databases if there was any acces from the laptop during the time period that the laptop was unattended. Check if there are camera’s around, so yes there is a possibility to request access to the footage. From there you could check if anyone other than you and your cousin was around the laptop.

And to prevent further implications it would be best to just come clean right away. Then there is a possibility that immediate action can be taken and even legal precautions like taking a patent on the software system and processes.

***Have a group discussion about this. Remember there is no right or wrong answer, however you need to think deeply about this:***

***How can your own moral compass guide you in this situation? What steps would you take, and why?***

We had some conflicting discussions in the group as there were multiple ways “out” of this situation. It depends on the moral compass of each person which is different but we for example, discussed some of the things that the CTO could’ve done to get out of it “mostly” scot free. We went through the examples in the case by blaming others which would eventually still put the company at harm and only save ourselves.   
Others had some thoughts about coming out cleanly in which case we assumed that we would get fired from the CTO position. Then we thought about starting anew somewhere else even though we have some reputation issues but we still had to pay the bills somehow.

Overall it depends on the person and how honest one is. It also matters how much we’re willing to deal with it on a personal level.

***What would the perceived impact of your decision be on your personal situation and those of involved stakeholders?***

Maybe by reporting this incident in time, there would still be enough time to block/recover some data. By doing this, you will of course deal with the consequences, but it’ll be worth it if the important data is saved. It’s also better than being recognized as a liar (if/when they find out that it was your fault).

**Advice**

## How GDPR affected us and steps to take (Jursley)

Currently the GDPR did not have affect on our implementations. We are only saving a username and password.  
In the future we will be adding more fields to the user database. The possibility to modify or remove the datasets that we have now is implemented. With the use of a event bus we will be able to delete, modify or add data with unique identifiers to link all datasets to a single user or service. This will guarantee that all data concerning a specific user will be accessible.

All sources will need validation with a jwt token preventing from unauthorized sources/users to access data that they aren’t supposed to have access to.

## How reusing existing technology helps with this (Faruk)

Using existing technologies can help get projects up and running faster and safer. Obviously, this requires a prior investigation into possible risks. Not only the risks are something to think about. It’s also important to know which information the technologies are requiring. It can be handy to create a data classification. All types of data and their priorities and risks are described in a data classification.

The nice thing about existing technologies is that there is often already a study to read. However, if it turns out to be a reliable technology, collaboration between the current and researched technologies should also be considered. It could just be that the collaboration could lead to new risks. It is recommended to make a risk analysis beforehand.

# Sources

|  |  |
| --- | --- |
| **Researcher** | **Source** |
| Nick | <https://gdpr-info.eu/art-33-gdpr/> |
| Nick | <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_en> |
| Vincent | <https://gdpr-info.eu/issues/right-to-be-forgotten/> |
| Maarten | <https://www2.deloitte.com/nl/nl/pages/risk/articles/cyber-security-privacy-gdpr-update-the-impact-on-cloud-computing.html> |
| Vincent | <https://www.thesslstore.com/blog/deleting-data-for-gdpr-could-encryption-do-the-trick/> |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |