**Case Study 2 – GDPR Analysis**

**Media storage service**



Project Members & Student Numbers:

* Francisco Marcó (4467752)
* Sava Vasilev (4663438)
* Kaloyan Andreev (4408020)

Elaboration Date: 08/06/2022

Group 10

Table of content

[1. Introduction 2](#_Toc105750865)

[2. Security measures 2](#_Toc105750866)

[3. Data processing 3](#_Toc105750867)

[4. Individual rights of concerned persons 4](#_Toc105750868)

[5. Data Protection Impact Assessment 5](#_Toc105750869)

[Sources 5](#_Toc105750870)

# Introduction

In our solution, we deal with personal data that has to be subjected to scrutiny to protect our users. Therefore, the following document aims to provide records and statements regarding the management of personal data by our company. We serve

The objective is to prove that our solution is GDPR compliant, and to provide details and context into how we process the data, what are the user’s rights, and more.

# Security measures

A paramount aspect of our solution, security is one of the most important points to consider when developing the system architecture and application development.

Because of the security concern, we devised a secure and well-planned architecture. Firstly we’ve configured an IDS/IPS system in our network. This will keep us alert in case our network is penetrated and the data is compromised, a major concern. Secondly, our architecture is built with redundance in mind. In case of failure or malfunctioning, we have in place a second firewall and domain controller. These standby designs allow us to restore functionality on a secondary resource using a failover. Finally, we’ve devised and structured VLANs, so that each resource works and communicates only with the necessary resources and components.

To further ensure security, we’ve taken the following actions towards protecting the user personal data:

* **All passwords are stored in hashed form**
* **Directories containing user data are encrypted**

Furthermore, we’ve determined that our solution is CIA compliant:

|  |  |  |
| --- | --- | --- |
| **Concept** | **Implemented** | **Details** |
| Confidentiality | YES | Personal data is protected from unauthorized access attempts (via user authentication, encryption, intrusion prevention/detection, etc.) |
| Integrity | YES | Personal data can only be changed by authorized administrators. |
| Availability | YES | Systems hold and display the user’s own personal data when requested. |

In case of a data breach or major security concern, we assure to document all, providing fixes and letting the users know if their personal data was compromised.

As a note, the solution could be even more secure by implementing cryptography. Stored data could be encrypted by using a cypher, but because of time constraints we were unable to implement this.

# Data processing

By agreeing to our Terms and Conditions, the user gives ‘Group 10’ (referred to as the company — or ‘we’, ‘us’, etc.) access to the given data in the registration form. This data is used and processed for authentication and file tracking purposes.

The given data in the registration form provides us access to:

* **User-generated username**
* **User’s name**
* **User-generated password**
* **User’s email address**
* **User’s phone number**

Because these items can contain sensitive information, we assure that these are managed and processed with security as the biggest concern. For example, all directories owned by users are encrypted using BitLocker and all passwords are stored in hash form in the database.

As mentioned, this data is mandatory for authentication and user profile creation. As such, only users who have their login credentials can access their own files, which likewise are securely stored in our File Server. Out of the box, the user has no way of accessing other user’s files without their credentials.

Furthermore, we also store data regarding the files uploaded onto our server. These are:

* **Assigned file ID**
* **File owner (username)**
* **File name (given by user)**
* **File type (extension)**
* **Directory the uploaded file is in**
* **Directory the synchronized file is in**

This data does not prove to be sensitive enough to consider implementing any further security measures. In case of a data breach, an attacker would not prioritize this information. However, encryption of the directories where the files are stored could be considered, considering that if it was breached it could pose as a security threat. Despite that, all the mentioned data is stored in a secure, enclosed VLAN.

# Individual rights of concerned persons

According to GDPR, a set of guidelines regarding individual’s rights have to be taken. As so, we will define these and provide proof of implementation.

* **Right to be informed including privacy information: In the repository’s ReadMe file and the User Registration page, we let know the user that they should read this document to know more about how their data is managed and processed before registering.**
* **Right to request personal data: At all times, the user is allowed to retrieve their personal data. To do so, there is a drop down menu located in the top left of the web-application, which will display the user’s username, first and last name, email address and phone number. Otherwise, in case any info needs to be changed, the user can contact us.**
* **Right to rectification and data quality: User credentials are only updated after the user contacts us in case it needs changing. And while not personal, all uploaded files data is constant but synchronized files data is not. In case a file name’s changes In one directory, it will be updated in the database, which in turn will update the change in the other synchronized directory.**
* **Right to erasure including retention and disposal: The user is free to request the deletion of any of our data which contains what is deemed as personal data. Likewise, files previously owned by this user would be deleted as well**
* **Right to restrict processing: Unfortunately, the personal data we collect has to be processed to validate and authenticate users. Any user who desires to restrict the processing, would be unable to access their account**
* **Right to object: Again, the personal data collected by us is processed to authenticate users. While the user can object to the collection of their data, we would not be able to provide an alternative means of authentication. If needed, the company might request the user’s firstborn child as a means of validation of your identity (with no returns accepted).**

# Sources

(n.d.). Retrieved from Business.gov.nl: [10 steps to comply with the GDPR in the Netherlands | Business.gov.nl](https://business.gov.nl/running-your-business/business-management/administration/how-to-make-your-business-gdpr-compliant/)

*ico.* (n.d.). Retrieved from Information Commissioner's Office: [Controllers checklist | ICO](https://ico.org.uk/for-organisations/sme-web-hub/checklists/data-protection-self-assessment/controllers-checklist/)

*ico.* (n.d.). Retrieved from Information Commissioner's Office: [Data protection self assessment | ICO](https://ico.org.uk/for-organisations/sme-web-hub/checklists/data-protection-self-assessment/)

*ico.* (n.d.). Retrieved from Information Commissioner's Office: [Data protection impact assessments | ICO](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/)

*ico.* (n.d.). Retrieved from Information Commissioner's Office: [Microsoft Word - dpia-template-v1.docx (gdpr.eu)](https://gdpr.eu/wp-content/uploads/2019/03/dpia-template-v1.pdf)

Watson, M. (2018, July 12). Retrieved from governance: [How to create GDPR-compliant documentation - IT Governance USA Blog](https://www.itgovernanceusa.com/blog/how-to-create-gdpr-compliant-documentation)

Wolford, B. (n.d.). Retrieved from GDPR.EU: [Data Protection Impact Assessment (DPIA) - GDPR.eu](https://gdpr.eu/data-protection-impact-assessment-template/)