Niels Roefs

Abstract

Document containing what I did for the project regarding the GDPR.

GDPR

Individual Project

# Introduction

This document outlines how MyWatchlist complies with the General Data Protection Regulation (GDPR) and the necessary requirements. As our application is intended for use within the European Union, adherence to GDPR is essential. The GDPR, established by the European Union in May 2018, provides a comprehensive legal framework for data privacy and security. It applies to any organization worldwide that targets or collects data from EU residents. The regulation enforces strict privacy and security measures, with severe penalties for non-compliance, including fines that can reach millions of euros.

# GDPR Compliance

## Conduct an information audit to determine what information you process and who has access to it.

**Implementation:**

Not needed, this is only needed for a company that has at least 250 employees.

## Have a legal justification for your data processing activities.

**How to implement it:**

I should identify the legal bases for each type of data processing, such as consent, contract, or legitimate interests. I should document these justifications clearly, ensuring they are reflected in my privacy policy and terms & conditions. I should ensure that anyone involved in data processing understands these legal justifications and regularly review data processing activities to ensure the legal bases remain valid.

**Implementation:**

Reasons for processing data have been mentioned in the privacy policy and terms & conditions.

## Provide clear information about your data processing and legal justification in your privacy policy.

**How to implement it:**

I should use simple and straightforward language in the privacy policy to explain data processing. I should clearly state why and how data is processed, and make sure that users are required to accept the privacy policy and terms & conditions when they create an account. I should ensure that the privacy policy is easily accessible to users at all times.

**Implementation:**

It is all mentioned in the privacy policy and terms and conditions. When people create an account, they need to accept the privacy policy and terms and conditions.

## Take data protection into account at all times, from the moment you begin developing a product to each time you process data.

**How to implement it:**

I should collect and use only the data necessary for my purposes. I should integrate data protection measures into the design of my systems and processes from the beginning. I should continuously evaluate and improve my data protection measures to ensure ongoing compliance with GDPR requirements.

**Implementation:**

From the moment I started developing MyWatchList, I took into account using as minimal personal data as possible.

## Encrypt, pseudonymize, or anonymize personal data wherever possible.

**How to implement it:**

I should use tools to encrypt data both during storage and transmission. I should replace identifiable data with pseudonyms where possible and remove identifying information to anonymize data. I should implement policies to manage these techniques effectively and ensure ongoing compliance.

**Implementation:**

No implementation due to time constraints.

## Create an internal security policy for your team members, and build awareness about data protection.

**How to implement it:**

I should develop clear guidelines for data handling and ensure all team members are regularly trained on these practices. I should conduct regular awareness programs to keep team members informed about data protection requirements and best practices.

**Implementation:**

No implementation due to time constraints.

## Know when to conduct a data protection impact assessment, and have a process in place to carry it out.

**How to implement it:**

I should recognize when a data protection impact assessment (DPIA) is necessary, such as when introducing new data processing activities that could impact privacy. I should develop a process for conducting DPIAs, identifying potential risks, and implementing measures to mitigate those risks. I should document the findings and actions taken as a result of the DPIA.

**Implementation:**

No implementation due to time constraints.

## Have a process in place to notify the authorities and your data subjects in the event of a data breach.

**How to implement it:**

I should implement systems to detect breaches quickly and create a notification plan to inform authorities and affected individuals promptly. I should document all breaches and the responses to them, and establish a team responsible for managing breach incidents to ensure swift and effective responses.

**Implementation:**

No implementation due to time constraints.

## Designate someone responsible for ensuring GDPR compliance across your organization.

**Implementation:**

Since there is only one developer, this is not necessary.

## Sign a data processing agreement between your organization and any third parties that process personal data on your behalf.

**Implementation:**

Data does not get shared with third parties.

## If your organization is outside the EU, appoint a representative within one of the EU member states.

**Implementation:**

MyWatchList is based in The Netherlands, so this is not necessary.

## Appoint a Data Protection Officer (if necessary)

**Implementation:**

Not necessary because there is only a single developer.

## It's easy for your customers to request and receive all the information you have about them.

**How to implement it:**

I should set up a simple process for data requests. I should verify the identity of the requester to ensure data security, and provide the requested data in an easily readable format. I should create a profile information page where users can manage their data requests.

**Implementation:**

No implementation due to time constraints.

## It's easy for your customers to correct or update inaccurate or incomplete information.

**How to implement it:**

I should provide an easy-to-use feature for updates. I should verify these updates to ensure data accuracy and create a profile information page where users can manage their information.

**Implementation:**

No implementation due to time constraints.

## It's easy for your customers to request to have their personal data deleted.

**How to implement it:**

I should set up a straightforward process for users to request data deletion. I should verify the identity of the requester and confirm the deletion with the user. I should create a profile information page where users can delete their accounts.

**Implementation:**

Users are allowed to delete their own personal data. It deletes their accounts and any reviews placed on movies.

A screenshot of a computer

Description automatically generated

## It's easy for your customers to ask you to stop processing their data.

**How to implement it:**

I should provide a clear mechanism for users to opt out of data processing. I should verify the identity of the requester and confirm the cessation of data processing. I should create a profile settings page to manage opt-out requests, making the process easy for users.

**Implementation:**

No implementation due to time constraints.

## It's easy for your customers to receive a copy of their personal data in a format that can be easily transferred to another company.

**How to implement it:**

I should implement a process to export data in a commonly used format. I should verify the identity of the requester and confirm the data transfer with the user. I should create a profile settings page where customers can request and manage data transfers.

**Implementation:**

No implementation due to time constraints.

## It's easy for your customers to object to you processing their data.

**How to implement it:**

I should provide a simple process for users to submit objections. I should verify the identity of the requester and confirm the objection. I should create a profile settings page to manage objections, ensuring the process is straightforward for users.

**Implementation:**

No implementation due to time constraints.

## If you make decisions about people based on automated processes, you have a procedure to protect their rights.

**Implementation:**

There are no automated processes so there is no implementation necessary.