# General Data Protection Regulation (GDPR)



**Project purpose**

This project aims to make one platform where journalists can do investigative research with help of multiple AI tools. This means that a journalist creates a story and can add a workflow to a story. This workflow exists out of multiple AI tools where you can put a question, a text or a video based on the use case and can be processed by the tools in the workflow. Note that the output for the first AI tool will be used as input to the next AI tool. This will ease the work of a journalist by time, handlings, maintainability, costs, scalability and reliability.

**Approach**

The approach during this assignment is based on the DOT Framework. The framework defines some strategies that can be used to do some context based research. Also during the research some research questions are formulated, these questions can be answered by using the DOT Framework research methods and strategies.

**During this assignment some questions are formulated:**

* What is GDPR?  
  Library – Literature study
* Which GDPR rules are available and which one did we implement?  
  Library – Literature study
* Are the used AI tools during this project GDPR compliant?  
  Library – Literature study

**What is GDPR?**

GDPR stands for the General Data Protection Regulation. It is a comprehensive data protection law that was introduced by the European Union (EU) and came into effect on May 25, 2018 (GDPR, 2024). The GDPR is designed to strengthen the protection of personal data and give individuals more control over their personal information.

The regulation applies to organizations that process personal data of individuals residing in the EU, regardless of where the organization is located. It establishes a set of rights and principles that organizations must adhere to when handling personal data.

Non-compliance with the GDPR can result in significant fines and penalties. The regulation aims to harmonize data protection laws across the EU member states and strengthen individuals' privacy rights in the digital age.

**Which GDPR rules are available and which one did we implement?**

On the official website of the GDPR, a checklist (GDPR, 2024) of rules is provided and taken into account during this project.

|  |
| --- |
| Lawful basis and transparency |
| 1. Conduct an information audit to determine that information you process and who has access to it. During this project we have two different roles, where the first one is the administrator who manages the users and the AI tools. The second one is the user which has rights to see their own stories, workflows and can make use of AI tools. This means the user has no right to delete or edit a AI tool.  Note that a user has to agree the a privacy policy which has to be created and reviewed yet. The privacy policy has to be created. |
| 1. Have legal justification for your data processing activities. Has to be done. |
| 1. Provide clear information about your data processing and legal justification in your privacy policy. Has to be done. |

|  |
| --- |
| Data security |
| 1. Take data protection into account at all times, from the moment you begin developing a product to each time you process data. Looking in to the microservice architecture we make sure that sensitive data is stored and protected safely. |
| 1. Encrypt, pseudonymize, or anonymize personal data wherever possible. For personal data we make use of key cloak which is an identity provide and handles secure authentication. It has its own database where the users personal info is stored safely. Personal info is only available for the user itself, this can be obtained when the user is authenticated by Keycloak. |
| 1. Create an internal security policy for your team members, and build awareness about data protection. Has to be done. |
| 1. Know when to conduct a data protection impact assessment, and have a process in place to carry it out. Has to be done. |
| 1. Have a process in place to notify the authorities and your data subjects in the event of a data breach. Has to be done. |

|  |
| --- |
| Accountability and governance |
| 1. Designate someone responsible for ensuring GDPR compliance across your organization. Has to be done. |
| 1. Sign a data processing agreement between your organization and any third parties that process personal data on your behalf. |
| 1. If your organization is outside the EU, appoint a representative within one of the EU member states. N/A |
| 1. Appoint a Data Protection Officer (if necessary) The data protection officer will be me, because I am the backend engineer in this project. |

|  |
| --- |
| Privacy rights |
| 1. It’s easy for your customers to request and receive all the information you have about them. The users can make use of the personal info page where they can see the information stored. Also changing their password and device activity. Afbeelding met tekst, schermopname, software, Computerpictogram     Automatisch gegenereerde beschrijving |
| 1. It’s easy for your customers to correct or update inaccurate or incomplete information.  Users can update their information by the personal info page of keycloak. Afbeelding met tekst, schermopname, software, Computerpictogram     Automatisch gegenereerde beschrijving |
| 1. It’s easy for your customers to request to have their personal data deleted. At the moment users can request the admin to delete their account.   There is no functionality build, to delete the users own account and their created stories by their self. This has to be realized. |
| 1. It’s easy for your customers to ask you to stop their processing their data. For this project we are not processing data by ourself, the data that is processed is in hands of the user itself. Using AI tools in their stories can make use of data processing because of the request that is send to the AI tool. Eventually a user needs to see a response based on their request, only this is stored to have an overview of the requests. Technically if users stop doing requests to AI tools no data is processed. |
| 1. 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. This has to be requested to the admin. |
| 1. It’s easy for your customers to object to you processing their data. Has to be done. |
| 1. If you make decisions about people based on automated processes, you have a procedure to protect their rights. Has to be done. |

**Are the used AI tools during this project GDPR compliant?**

In this project only make use of OpenAI tools like ChatGPT and Whisper AI. In the future this could be expanded with AI tools from Hugging Face or some tools from other companies. This still has to be researched.

Afbeelding met tekst, schermopname, Lettertype

Automatisch gegenereerde beschrijving

Open AI has a website (OpenAI, 2015-2024) where they explain that they are GDPR and CCPA compliant and answers the questions right away. A important question is does OpenAI make use of the data and train OpenAI models with? OpenAI answers that with: ”Data submitted through non-API consumer services ChatGPT or DALL·E may be used to improve our models”. If they are making use of data to improve their models, it has to be researched if it is GDPR compliant or not. OpenAI also provides a Security portal (OpenAI, 2023) where they have an overview to their data security, privacy and compliance documentation to answer all the questions.

# Bibliography

GDPR. (2024). *GDPR checklist for data controllers*. Opgehaald van GDPR.EU: https://gdpr.eu/checklist/

GDPR. (2024). *What is GDPR, the EU's new data protection law?* Opgehaald van GDPR.EU: https://gdpr.eu/what-is-gdpr/

OpenAI. (2015-2024). *Security&Privacy*. Opgehaald van OpebAI: https://openai.com/security

OpenAI. (2023, 03 14). *Security Portal*. Opgehaald van OpenAI: https://trust.openai.com/