Retrofitting towards climate neutrality

D5.3 Report on GDPR and Cybersecurity measures

Program: HORIZON EUROPE

Grant agreement number: 101096522

Project acronym: Green Marine

Project title: Retrofitting towards climate neutrality

Prepared by: PDM

Date: 30/07/2024

Report version: v1.0

Funding acknowledgement
Funded by the European Union; funding from the European Union’s Horizon Europe research and innovation program under grant agreement No. 101096522

UK participation in Green Marine project is co-funded by Innovate UK funding scheme

Disclaimer: The views expressed in this deliverable are those of the authors and are disclosed in a non-reliance basis and for information purposes only. The authors, the **Green Marine** consortium and partner employees and directors do not express or implied representation and/or warranty as to the accuracy and completion of the information set out in this report (including in any opinion, estimate, forecast and/or projection disclosed herein) and shall have no liability to the readers for any reliance placed on this report. The readers will rely solely upon their own independent investigation and evaluation of the information provided herein. Finally, this deliverable is based in information, legislation and data available as at the date of its creation and the authors shall have no responsibility for updating the information contained in this report and for correcting any inaccuracies in it, which may become apparent. The content of this deliverable does not reflect the official opinion of the European Union.

HISTORY OF CHANGES		
Version	Publication Date	Changes
0.0DRAFT	15/05/2024	First working draft
0.6DRAFT	17/07/2024	Internal review
1.0	19/07/2024	Review
1.0	30/07/2024	Published

DETAILS	
Grant Agreement No.	101096522
Project acronym	Green Marine
Project full title	Retrofitting towards climate neutrality
Dissemination level	Public
Due date of deliverable	M18
Actual submission date	M18
Deliverable name	D5.3 Report on GDPR and Cybersecurity measures
Type	Report
Status	Final version; v0.0DRAFT
WP contributing to the deliverable	WP5
Author(s)	Nuno Pedrosa & Carlos Marques (PDM) & João Luís (PDM)
Other Contributor(s)	n/a
Reviewer(s)	George Mallouppas (CMMI)
Keywords	Green Marine, Data Protection, GDPR, Data Processing, Privacy, Compliance, Regulation, Data Management Plan, Project Management Handbook

Acronyms and Abbreviations	
DPIA	Data Protection Impact Assessments
DPO	Data Protection Officer
GDPR	General Data Protection Regulation
EU	European Union
EEA	European Economic Area
LEM	Legal and Ethics Manager (acting as the DPO)

Table of Contents

Document tables

EXECUTIVE SUMMARY

This document is deliverable "D5.3 Report on GDPR and Cybersecurity measures" of the European Union project "Retrofitting towards climate neutrality" (herein referred to as "**Green Marine**"), with **grant agreement No. 101096522**.

The Green Marine project is dedicated to significantly accelerating climate neutrality in waterborne transport through innovative retrofitting solutions. This initiative involves the use of various datasets, predominantly operational data on specific equipment, with a subset containing personal user information. Ensuring robust data protection and cybersecurity is crucial to the project's success, compliance with the General Data Protection Regulation (GDPR), and the maintenance of stakeholder trust.

This report provides a comprehensive overview of the GDPR compliance and cybersecurity measures implemented in the Green Marine project. Key areas addressed include:

- **Overview of GDPR**: An explanation of GDPR's significance, its applicability to the project, and the fundamental principles that guide the processing of personal data.
- **Data Categories and Their Handling**: Classification of datasets into those that do not contain user information and those that do, along with their respective handling procedures to ensure data protection and compliance.
- **GDPR Compliance Measures**: Detailed measures to comply with GDPR, including adherence to data protection principles, lawful basis for data processing, obtaining and managing consent, and upholding data subject rights.
- **Data Subject Rights**: Explanation of the rights granted to data subjects under GDPR and the procedures in place within the project to facilitate the exercise of these rights.
- **Data Protection Impact Assessments (DPIAs)**: The importance and process of conducting DPIAs to identify and mitigate risks associated with data processing activities.
- **Cybersecurity Measures**: Comprehensive technical and organizational measures to protect data, including encryption, access controls, incident response plans, and regular security audits.

To further enhance data protection and privacy, future actions will include the implementation of DPIAs for all high-risk data processing activities. This approach will ensure ongoing compliance, identify potential risks, and improve data protection strategies.

1 INTRODUCTION

Data processing activities performed by members of the consortium (also called the beneficiaries of grant agreement No. 101096522) are required to comply with EU's national and international low, in particular Regulation 2016/679 (of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data) also known as the General Data Protection Regulation (GDPR) regulation.

Data protection and cybersecurity are critical components of any project involving the collection, processing, and storage of data. This includes both operational data related to equipment and datasets containing user information.

1.1 PURPOSE OF THE REPORT

The purpose of this report is to outline the measures taken to ensure compliance with the General Data Protection Regulation (GDPR) and to detail the cybersecurity practices implemented within the Green Marine project. This project involves the use of various datasets, predominantly related to the operation of specific equipment. However, some datasets do contain user information. Ensuring the protection and security of this data is paramount, both to comply with legal requirements and to maintain the trust of stakeholders.

1.2 SCOPE OF THE PROJECT AND REPORT

Green Marine aims to significantly accelerate climate neutrality in waterborne transport through the retrofitting of existing fleets with cost-effective emission control solutions. To support decision-makers, retrofitting protocols and a software tool catalogue that gathers knowledge will be developed and validated. The project initial goals include the demonstration of innovative solutions aimed at carbon capture mineralization, energy savings in air quality systems through air reuse, carbon and water capture with membranes, and the use of excess engine heat to produce syngas.

The project aspires to bring the solutions to Technology Readiness Level (TRL) 8, with demonstrations and dissemination activities ensuring global replication of project results.

This report will cover:

- An overview of GDPR and its relevance to the Green Marine project.
- Classification of datasets and the handling procedures for those containing user information.
- Detailed GDPR compliance measures, including data protection principles, consent management, and data subject rights.
- Comprehensive cybersecurity measures to protect all data within the project, focusing on both technical and organizational strategies.
- Methods for continuous compliance monitoring and review, including regular audits and third-party vendor management.

The basis for analysis is **D7.4 Second revision of Data Management Plan (DMP)** submitted on M18**.**

2 Overview of GDPR

The General Data Protection Regulation (GDPR Directive 95/46/EC[1]) is a comprehensive data protection law that governs the processing of personal data within the European Union (EU) and European Economic Area (EEA)[2]. It removed existing fragmentation in different national systems and unnecessary administrative burdens. Enforced since May 25, 2018, GDPR aims to protect the privacy and personal data of individuals, imposing strict requirements on organizations that handle such data. This section provides an overview of GDPR, its relevance to the Green Marine project, and the principles and obligations that must be adhered to when processing personal data.

2.1 What is GDPR?

GDPR is a regulatory framework designed to give individuals control over their personal data and to simplify the regulatory environment for international business by unifying data protection regulations within the EU. The regulation applies to any organization that processes the personal data of individuals within the EU, regardless of where the organization is based. Key objectives of GDPR include enhancing data protection rights for individuals, increasing transparency in data processing activities, and ensuring that organizations implement robust data security measures.

2.2 GDPR Applicability

For the Green Marine project, GDPR is relevant due to the involvement of datasets containing user information. Although the majority of the data relates to the operation of specific equipment and does not include personal data, the handling of any personal information necessitates strict adherence to GDPR guidelines. The regulation mandates that personal data must be processed lawfully, fairly, and transparently, and organizations must implement appropriate technical and organizational measures to protect such data.

2.3 Key Principles of GDPR summarized

GDPR outlines several fundamental principles that guide the processing of personal data. In a nutshell, these include:

- **Lawfulness, Fairness, and Transparency**: Personal data must be processed lawfully, fairly, and in a transparent manner in relation to the data subject.
- **Purpose Limitation**: Personal data should be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
- **Data Minimization**: The collection of personal data should be limited to what is necessary in relation to the purposes for which it is processed.
- **Accuracy**: Personal data must be accurate and, where necessary, kept up to date. Inaccurate data should be corrected or deleted promptly.
- **Storage Limitation**: Personal data should be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed.

[1] Directive 95/46/EC (General Data Protection Regulation). Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504

[2] https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en

- **Integrity and Confidentiality**: Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing, accidental loss, destruction, or damage.
- **Accountability**: Organizations must be able to demonstrate compliance with GDPR principles and are responsible for adhering to them.

2.4 Data Subject Rights

Individuals benefit from several rights concerning their personal data under GDPR:

- **Right of Access**: Individuals have the right to access their personal data and obtain information about how it is being processed.
- **Right to Rectification**: Individuals can request corrections to inaccurate or incomplete personal data.
- **Right to Erasure**: Also known as the ‘right to be forgotten,’ this allows individuals to request the deletion of their personal data under certain circumstances.
- **Right to Restriction of Processing**: Individuals can request the limitation of the processing of their personal data under specific conditions.
- **Right to Data Portability**: Individuals have the right to receive their personal data in a structured, commonly used, and machine-readable format and to transfer that data to another controller.
- **Right to Object**: Individuals can object to the processing of their personal data on grounds relating to their situation.
- **Rights Related to Automated Decision Making and Profiling**: Individuals have the right not to be subject to decisions based solely on automated processing, including profiling.

In the context of the Green Marine project, these principles and rights are crucial for ensuring that any personal data processed is handled responsibly and in compliance with GDPR. The main tool to assess the correct handling information, is the DPIA (refer to §2.5).

2.5 Data Protection Impact Assessments (DPIAs)

For high-risk data processing activities, GDPR mandates the conduction of Data Protection Impact Assessments (DPIAs). DPIAs help to identify and mitigate potential risks to data subjects. They involve a systematic examination of data processing activities and the implementation of measures to safeguard personal data.

By integrating these GDPR principles and obligations, the Green Marine project ensures robust data protection and aligns with legal requirements, thereby maintaining the integrity and confidentiality of personal data.

3 DATA CATEGORIES AND THEIR HANDLING

In the Green Marine project, various datasets are utilized to achieve the project's objectives. These datasets fall into two main categories: those that do not contain user information and those that do. Proper handling of these datasets is crucial to ensure compliance with GDPR and to maintain data integrity and security.

3.1 DATASETS WITHOUT USER INFORMATION

The majority of the datasets used in the Green Marine project pertain to the operation of specific equipment and do not contain any personal information. These datasets include:

- **Operational Data**: Data related to the performance, maintenance, and operational parameters of marine equipment and systems.
- **Environmental Data**: Data on environmental conditions, such as temperature, humidity, and air quality, which are relevant for optimizing air quality systems and other operational aspects.

3.1.1 Handling Procedures:

- **Data Collection**: These datasets are collected through sensors, monitoring systems, and manual entries by technicians.
- **Data Storage**: Stored in secure databases with appropriate access controls to prevent unauthorized access and ensure data integrity.
- **Data Processing**: Analyzed using software tools and algorithms to derive insights and optimize equipment performance. The processing is conducted in a controlled environment to maintain data security.
- **Data Sharing**: Shared among project partners and stakeholders as needed, ensuring that no personal data is included.

Since these datasets do not contain personal information, they are not subject to GDPR regulations. However, best practices in data security and management are followed to protect the data from unauthorized access and ensure its reliability.

3.1.2 List of Datasets without User Information

Table 1. Datasets with no user information.

Dataset	Purpose of Data
Dataset 1	Retrofitting a selected air handling unit within the ship to allow suitable demonstration
Dataset 2	Retrofitting an auxiliary engine of a ferry ship targeting either the engine or flue gas.
Dataset 3	The solution can be easily integrated in a piper or inlet/outlet of the HVAC system.
Dataset 4	discontinued
Dataset 5	discontinued
Dataset 6	SepaRaptor with UV as stand-alone devices will be equipped with a wired power connection in selected areas (bridge, crew cabins). Aim is to remove >>90 % of particles <350 nm and utilize UV lighting to kill viruses/bacteria >99.99% within 60 minutes.
Dataset 7	Testing if SepaRaptor pre-treated materials are still suitable for the use of flue gas.

Dataset 8	discontinued
Dataset 9	The TEE system (Patent DE102011056877B4) can be adapted to a variety of circumstances. Depending on which temperature range is used, different "working" liquids can be used, e.g., water in the temperature range of about 170 to 600 K, ammonia in the temperature range of about 150 to 170 K, mercury in the temperature range of 400 to 800 K or lithium or silver in a temperature range above 1000 K. Different types of heat pipes will be explored. If necessary, the heat pipes can be coated after shaping to protect them from mechanical, chemical and / or thermal effects, should those arise especially in the marine environment. As the heat source can be focal or with a broader surface, optimal cross-section of the conductors, and optimal distributions will be investigated. As the output of the TEE is always the same (DC current), this aspect has not to be tailored.
Dataset 11	Dedicated experimental campaign to quantify the performance and emission characteristics of the marine genset with the carbon capture machine and CO_2 absorption performance, syngas re-injection.
Dataset 12	Data gathering to compile task 4.1, task 4.2 and task 4.3 reports. The reports will include proprietary / confidential report of the various technologies.
Dataset 13	To build and evaluate the environmental impact of the critical parts to be retrofitted by the **Green Marine** solutions. Data from sensors and/or experimental results provided by technology providers and/or LCA database (Ecoinvent, Gabi).
Dataset 14	To build and evaluate the technoeconomic impact of the critical parts to be retrofitted by the **Green Marine** solutions that will arise from the LCA assessments.
Dataset 15	Upscaling the membranes in the lab; assessing the membranes performances (permeability, selectivity); designing the membrane separation unit
Dataset 16	Upscaling the membranes; assessing the membranes performances (permeability, selectivity) using the land testing diesel engine; designing the membrane separation unit
Dataset 17	Data collection for correct implementation of Application Program Interface (API), Distributed Service Implementation for task 5.1 Data collection for CFD/HVAC modelling tools and assessments to validate the engineering solutions to achieve GHG emission reductions. For task 5.5 data on GHG emission control technical solutions (open-source literature, suppliers, stakeholders) will be utilised
Dataset 18	To build and evaluate the digital model of the critical parts to be retrofitted by the **Green Marine** solutions. Data from sensors and/or experimental results provided by technology providers and/or simulation results.
Dataset 19	To install and evaluate the performance of the SepaRaptor and UV units using online SMPS/APS monitors and swabs for airborne virus/bacteria characterization by SINTEF/UPM. During operations the ventilation unit will operate under different fresh-air mix, each setting will be tested for prolonged periods of time (depending on ferry ship operation). Other data are related to monitoring airborne aerosols. Here sensors and installed air samplers with SepaRaptor will make the necessary test runs. Also data collected related to the performance of CO_2 removal will be monitored

	using online GC-monitors and other online monitors that help provide a mass/energy balance.
Dataset 20	Data will be used for project communication and dissemination activities, technical / industrial workshops and surveys, participation at workshops and conferences, training and education of students and staff.
Dataset 21	To demonstrate the performance of the air circulation, carbon capture and syngas technologies on board the test vessel(s) compared against reference data using CalMac energy consumption data and data provided by the technology providers and PDM (as per WP5).
Dataset 22	Engineering and preparations for retrofitting on CalMac vessel (MV Coruisk).
Dataset 23	Actual retrofit of the CCM equipment to the CalMac vessel (MV Coruisk).
Dataset 24	Testing and validation of the GHG emission reduction by the CCM equipment.
Dataset 25	Testing and validation of the GHG emission reduction by the CCM equipment.
Dataset 26	A Techno-economic assessment (TEA) will be conducted in relation to CCM's capture modelling tools used prior to and after the Demos in order to validate the tool(s). With these same modelling tools, a conceptual design of the Demos will be made.
Dataset 27	Experimental/raw data to validate /evaluate the models of the software tool catalogue and gamification app.
Dataset 28	Support design for retrofit of Green Marine equipment to CalMac vessel (MV Coruisk).

3.2 Datasets with User Information

Some datasets in the Green Marine project contains user information. This personal data is collected, processed, and stored in compliance with GDPR. These datasets include:

- **User Profiles**: Information about public individuals that get involved in the project through the project portal. These can be researchers, technicians, and participants in demonstrations, but also general public that wants to participate in the dissemination activities.
- **Usage Data**: Data on how individuals interact with the project platform, to assess success of dissemination actions and user engagement.

3.2.1 Handling Procedures:

- **Data Collection**: Personal data is collected with explicit consent from the individuals, ensuring transparency about the purpose and scope of data usage.
- **Data Storage**: Stored in databases with stringent access controls to protect against unauthorized access and data breaches. Sensitive information, like passwords, are encrypted.
- **Data Processing**: Processed in accordance with GDPR principles, ensuring that the data is used only for the specified purposes and is kept accurate and up-to-date.
- **Data Sharing**: Shared only with authorized project partners and stakeholders who have a legitimate need to access the data and only the minimum data needed. Data sharing agreements are in place to ensure GDPR compliance.
- **Data Minimization**: Only the minimum amount of personal data necessary for the project is collected and processed.

3.2.2 GDPR Compliance:

- **Lawfulness, Fairness, and Transparency**: Personal data is processed legally, fairly, and in a transparent manner. Individuals are informed about the data processing activities and their rights under GDPR.
- **Purpose Limitation**: Personal data is collected for specific, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
- **Data Minimization**: Only the data that is necessary for the specified purposes is collected and processed.
- **Accuracy**: Personal data is kept accurate and up-to-date. Individuals have the right to request corrections to inaccurate data.
- **Storage Limitation**: Personal data is retained only for as long as necessary for the purposes for which it is processed. Data that is no longer needed is securely deleted.
- **Integrity and Confidentiality**: Appropriate technical and organizational measures are implemented to ensure the security of personal data, protecting it against unauthorized or unlawful processing, accidental loss, destruction, or damage.
- **Accountability**: The project team demonstrates compliance with GDPR through documentation, regular audits, and adherence to data protection policies and procedures.

The Green Marine project ensures that all data is managed in a secure and compliant manner, upholding the principles of data protection and cybersecurity.

3.2.3 List of Datasets with User Information

Table 2. Datasets with user information.

Dataset	Purpose of Data
Dataset 10	Data gathering for the Quality, health, safety, regulatory and environment evaluations, techno-economic assessment, social readiness assessment and exploitation activities. Data will be collected via one-on-one meetings or email with partners, online surveys, and Excel databases.
Dataset 29	To account for user engagement.

4 GDPR Compliance Measures

Ensuring compliance with GDPR is essential for protecting the privacy and rights of individuals whose personal data is processed within the Green Marine project. GDPR outlines stringent requirements for the lawful processing of personal data, emphasizing principles such as lawfulness, fairness, transparency, data minimization, and accountability. This section details the specific measures implemented to achieve GDPR compliance, covering data protection principles, lawful basis for processing, data subject rights, and Data Protection Impact Assessments (DPIAs).

By implementing these measures, the Green Marine project not only adheres to legal obligations but also fosters trust and transparency among stakeholders. The following subsections provide a comprehensive overview of how personal data is protected throughout the project’s lifecycle, from collection and processing to storage and sharing.

4.1 Data Protection Principles

The Green Marine project adheres to the core principles of GDPR to ensure the lawful, fair, and transparent processing of personal data. These principles are foundational to GDPR compliance and guide all data handling activities within the project. The following outlines how each principle is implemented:

4.1.1 Lawfulness, Fairness, and Transparency

Lawfulness: All personal data processing activities within the Green Marine project are based on a lawful basis as stipulated by GDPR. This includes obtaining explicit consent from data subjects, fulfilling contractual obligations, complying with legal requirements, protecting vital interests, performing tasks carried out in the public interest, or pursuing legitimate interests.

Fairness: Personal data is processed in a manner that is fair to the data subjects. This means that individuals are informed about how their data will be used and are not subjected to processing that could unjustly harm them.

Transparency: The Green Marine project maintains transparency with data subjects by clearly communicating the purposes for which their data is collected, how it will be used, who it will be shared with, and the rights they have concerning their data. Privacy notices and consent forms are provided in clear and plain language.

4.1.2 Purpose Limitation

Personal data is collected for specific, explicit, and legitimate purposes and is not further processed in a manner that is incompatible with those purposes. Within the Green Marine project, personal data is used solely for activities related to the project’s dissemination objectives, to assess users knowledge of and engagement with the project goals. Any new use of the data is assessed for compatibility with the original purposes and requires new consent if necessary.

4.1.3 Data Minimization

The Green Marine project ensures that personal data collected is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed. Data collection practices are regularly reviewed to ensure that only the minimum amount of personal data required for the project is collected and processed.

4.1.4 Accuracy

Personal data must be accurate and kept up to date. The Green Marine project implements procedures to ensure that inaccurate personal data is corrected or deleted without delay. Data subjects are given the opportunity to review and update their information, ensuring its accuracy over time.

4.1.5 Storage Limitation

Personal data is retained only for as long as necessary to fulfil the purposes for which it was collected. The Green Marine project has defined retention periods for different types of personal data, ensuring that data is securely deleted or anonymized when it is no longer needed. This helps to mitigate the risks associated with prolonged data retention.

4.1.6 Integrity and Confidentiality

Personal data is processed in a manner that ensures its security, including protection against unauthorized or unlawful processing, accidental loss, destruction, or damage. The Green Marine project employs a range of technical and organizational measures to safeguard personal data. These measures include encryption, access controls, regular security audits, and training for staff on data protection practices.

4.1.7 Accountability

The Green Marine project takes responsibility for complying with GDPR principles and is able to demonstrate compliance through documentation and regular audits. Data protection policies and procedures are in place to guide staff in adhering to GDPR requirements. Additionally, the designated Legal and Ethics Manager (LEM) (see D7.2 “Project Handbook including draft Data Management Plan” §2) will also act as the Data Protection Officer (DPO) who will oversee the data protection activities and will ensure ongoing compliance.

4.2 Consent and Lawful Basis

To ensure compliance with the GDPR, the Green Marine project adheres to strict guidelines regarding the lawful basis for processing personal data and the obtaining of consent from data subjects. This section outlines the various lawful bases for processing and the processes in place to ensure informed and explicit consent is obtained where necessary.

4.2.1 Lawful Basis for Processing

Under GDPR, personal data processing must be based on one of the following lawful bases:

Consent: The data subject has given explicit consent to the processing of their personal data for one or more specific purposes. Consent must be freely given, specific, informed, and unambiguous.

Contractual Necessity: Processing is necessary for the performance of a contract to which the data subject is a party, or to take steps at the request of the data subject prior to entering into a contract.
Legal Obligation: Processing is necessary for compliance with a legal obligation to which the controller is subject.
Vital Interests: Processing is necessary to protect the vital interests of the data subject or another natural person.
Public Task: Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
Legitimate Interests: Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

In the Green Marine project, the lawful basis for processing personal data is **Consent**. For personal data to be collected, users must give an informed consent. In its absence, no personal information is collected.

4.2.2 Obtaining and Managing Consent

Informed Consent: Consent is obtained from data subjects in a manner that ensures they are fully informed about the nature, purpose, and scope of the data processing activities. This includes providing clear and concise information about what data is being collected, how it will be used, who it will be shared with, and the rights of the data subject.
Explicit Consent: When processing sensitive personal data or for specific purposes that require a higher level of scrutiny, explicit consent is obtained. This involves an affirmative action by the data subject, such as signing a consent form or selecting an opt-in checkbox.
Freely Given Consent: Consent is given freely and without coercion. Data subjects are informed that they have the right to withdraw their consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.
Recording and Managing Consent: The Green Marine project maintains records of consent obtained from data subjects. These records include the date of consent, the information provided to the data subject at the time of consent, and any changes to the terms of consent.

Children's Consent: When processing personal data of children, additional safeguards should be in place to ensure that consent is obtained from a parent or guardian, and that the information provided is age-appropriate. Users should be over 16 years old, to create a user account, due to legal requirements. All content in the Green Marine project is age safe, even if the technical information may be challenging and require further knowledge.

4.2.3 Withdrawal of Consent

Data subjects have the right to withdraw their consent at any time. The Green Marine project provides simple and accessible mechanisms for withdrawing consent. Upon withdrawal, the processing of the data subject's personal data ceases unless another lawful basis for processing exists. Data subjects are informed about the withdrawal process and the implications of withdrawing consent.

4.2.4 Ensuring Lawful Processing

To ensure that all data processing activities within the Green Marine project are lawful, a thorough assessment is conducted before processing begins. This includes:

- Identifying the specific lawful basis for each processing activity.
- Documenting the justification for choosing that lawful basis.
- Ensuring that data subjects are informed about the lawful basis for processing their data.

4.3 DATA SUBJECT RIGHTS

The GDPR grants several rights to individuals (data subjects) regarding their personal data. These rights are designed to give individuals greater control over their personal information and to ensure transparency and accountability in data processing activities. The Green Marine project is committed to upholding these rights and ensuring that data subjects can exercise them easily. This section outlines each of these rights and the measures in place to support them.

4.3.1 Right of Access

Right of Access: Data subjects have the right to obtain confirmation as to whether their personal data is being processed and, if so, to access that data along with information about the processing activities.

Implementation:

- Personal data is always available in the platform profile page.

4.3.2 Right to Rectification

Right to Rectification: Data subjects have the right to have inaccurate personal data corrected and incomplete data completed.

Implementation:

- Users can access their personal data and edit the details in the platform.

4.3.3 Right to Erasure

Right to Erasure: Also known as the "right to be forgotten," this allows data subjects to request the deletion of their personal data under certain circumstances, such as when the data is no longer needed for the original purpose, or if they withdraw their consent.

Implementation:

- Users can request that their account is deleted, in the platform

4.3.4 Right to Restriction of Processing

Right to Restriction of Processing: Data subjects have the right to request the restriction of their personal data processing in specific situations, such as when they contest the accuracy of the data or object to the processing.

Implementation:

- Data is used to track overall user engagement. Restricting access is akin to ask for the account deletion, which can be requested in the platform.

4.3.5 Right to Data Portability

Right to Data Portability: Data subjects have the right to receive their personal data in a structured, commonly used, and machine-readable format and to transfer that data to another controller.

Implementation:

- Data subjects can request data portability by submitting a written request to the DPO.
- The project team provides the data in a portable format within one month, ensuring it can be easily transferred to another controller.

4.3.6 Right to Object

Right to Object: Data subjects have the right to object to the processing of their personal data based on certain grounds, such as direct marketing or processing based on legitimate interests.

Implementation:

- Data is used to track overall user engagement. Restricting access is akin to ask for the account deletion, which can be requested in the platform.

4.3.7 Rights Related to Automated Decision Making and Profiling

Rights Related to Automated Decision Making and Profiling: Data subjects have the right not to be subject to decisions based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

Implementation:

- Users are not individually profiled or otherwise subject to decisions based on their overall engagement or use, so this does not apply.

4.3.8 Procedures for Exercising Rights

Exercising Rights: Data subjects can exercise their rights by using the platform or submitting requests to the DPO. The project ensures that these requests are handled promptly and transparently.

Implementation:

- The user can make all the changes directly in the platform.
- The user can make requests to the DPO who is responsible for managing and responding to all data subject requests.
- Clear procedures and forms are provided to facilitate the submission of requests.
- The project team maintains records of all requests and their outcomes to demonstrate compliance with GDPR.

4.4 Data Protection Impact Assessments (DPIAs)

Data Protection Impact Assessments (DPIAs) are a critical component of the GDPR compliance framework, particularly for processing activities that are likely to result in high risks to the rights and freedoms of individuals. DPIAs help to systematically identify and mitigate potential risks associated with data processing activities. This section outlines the purpose of DPIAs, the circumstances under which they are conducted, and the procedures followed within the Green Marine project to ensure compliance with GDPR requirements.

4.4.1 Purpose of DPIAs

The primary purpose of a DPIA is to ensure data processing activities comply with GDPR by:

- Identifying potential risks to data subjects' privacy and security.
- Evaluating the need and proportionality of the processing activities.
- Implementing measures to mitigate identified risks.
- Demonstrating accountability and transparency in data processing practices.

4.4.2 When to Conduct a DPIA

A DPIA is required for any processing activity that is likely to result in a high risk to the rights and freedoms of individuals. This includes, but is not limited to:

- Processing of sensitive personal data on a large scale.
- Systematic monitoring of publicly accessible areas on a large scale.
- Processing involving new technologies or innovative approaches.
- Data processing that could significantly affect individuals.

Within the Green Marine project, a DPIA is conducted in the following scenarios:

- Introduction of new data processing activities involving personal data.
- Significant changes to existing processing activities.
- Deployment of new technologies or methods for data collection and analysis.

4.4.3 DPIA Process

The DPIA process within the Green Marine project is carried out in several stages, ensuring a thorough evaluation and mitigation of risks:

1. **Identifying the Need for a DPIA**:

- A preliminary assessment is conducted to determine if a DPIA is required for a specific processing activity.
- The DPO collaborates with project teams to identify processing activities that warrant a DPIA.

2. **Describing the Processing**:

- The processing activity is documented, including the nature, scope, context, and purposes of the processing.
- Information about the types of personal data involved, the data subjects, and any data transfers is included.

3. **Assessing Necessity and Proportionality**:

- Evaluation of the need and proportionality of the processing activity in relation to its purposes
- Alternatives to achieve the same purpose with less risk to data subjects are considered.

4. **Identifying and Assessing Risks**:

- Potential risks to data subjects' rights and freedoms are identified and assessed.
- Evaluating risks related to data security, privacy, and potential impacts on individuals.

5. **Identifying Measures to Mitigate Risks**:

- Measures to mitigate identified risks are proposed and implemented.
- These measures may include technical controls (e.g., encryption, access controls) and organizational measures (e.g., policies, training).

6. **Documentation and Reporting**:

- The DPIA findings and the measures implemented are documented in a comprehensive report (this report).
- The report includes a summary of the processing activity, identified risks, mitigation measures, and any residual risks.

7. **Reviewing and Updating the DPIA**:

- DPIAs are reviewed periodically and updated when there are significant changes to the processing activity or when new risks are identified.
- Continuous monitoring ensures that the measures remain effective and that new risks are promptly addressed.

4.4.4 Accountability and Transparency

To demonstrate accountability and transparency, the Green Marine project maintains detailed records of all DPIAs conducted.

4.4.5 Roles and Responsibilities

Data Protection Officer (DPO): The DPO is responsible for overseeing the DPIA process, providing guidance to project teams, and ensuring compliance with GDPR requirements.

Project Teams: Project teams collaborate with the DPO to identify processing activities that require a DPIA, participate in the risk assessment process, and implement mitigation measures.

Supervisory Authorities: If a DPIA identifies high residual risks that cannot be mitigated, the project team consults with the relevant supervisory authority before proceeding with the processing activity.

5 Cybersecurity Measures

Cybersecurity measures are implemented to protect both operational data and personal information from unauthorized access, breaches, and other security threats. This section outlines the comprehensive cybersecurity strategy adopted in the project, detailing technical and organizational measures, access controls, data breach response, and ongoing monitoring and review processes.

5.1 Overview of Cybersecurity Strategy

The cybersecurity strategy in the Green Marine project is designed to protect data against a wide range of threats. The main tool is minimization of information, requiring the least possible information to achieve the project goals. From this strategy, it encompasses preventive, detective, and responsive measures to ensure that data is secure throughout its lifecycle. The strategy is aligned with industry best practices and standards, such as ISO/IEC 27001, and complies with GDPR requirements.

5.2 Technical Measures

5.2.1 Encryption

- Sensitive data, at rest and in transit, is encrypted using strong encryption protocols (e.g., AES-256, TLS).
- Encryption keys are managed securely, with access restricted to authorized personnel.

5.2.2 Pseudonymization

- Personal data is pseudonymized[3] where possible to minimize the risk of reidentification in the event of a breach.
- Pseudonymization techniques are applied to datasets containing sensitive information.

5.2.3 Access Controls

- Role-based access controls (RBAC) ensure that only authorized personnel can access sensitive data.
- Multi-factor authentication (MFA) is implemented to add an extra layer of security for accessing critical systems and data.

5.2.4 Firewalls and Intrusion Detection Systems

- Firewalls are configured to protect the network perimeter and segment internal networks.
- Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) monitor network traffic for suspicious activity and potential threats.

5.3 Organizational Measures

5.3.1 Data Protection Policies

- Comprehensive data protection and cybersecurity policies are established, outlining roles, responsibilities, and procedures for safeguarding data.

[3] **Pseudonymization** is a data processing technique in which personally identifiable information within a dataset is replaced with artificial identifiers (pseudonyms), to protect the privacy of data by making it more difficult to attribute data to specific individuals without additional information. This technique is particularly significant in the context of GDPR, as it helps to mitigate privacy risks while still allowing data to be useful for analysis.

- Policies are reviewed and updated when necessary to reflect evolving threats and regulatory requirements.

5.3.2 Employee Training and Awareness

- Training sessions are conducted to educate employees about data protection principles, cybersecurity best practices, and their role in maintaining security.
- Staff is informed about the latest security threats and prevention strategies.

5.4 Access Controls

- **Role-Based Access Controls (RBAC):** Access to data and systems is granted based on the principle of least privilege, ensuring that individuals have the minimum level of access required to perform their duties. Access rights are reviewed regularly and adjusted as necessary to reflect changes in roles or responsibilities.
- **Audit Logs and Monitoring**: Detailed audit logs are maintained to record access to data and systems, providing a trail for forensic analysis in the event of a security incident. Continuous monitoring of systems and networks is conducted to detect and respond to suspicious activity in real-time.

5.5 Data Breach Response

- **Detection and Reporting**: Systems are in place to detect data breaches promptly, including alerts for anomalous activity. In the event of a data breach, the incident response team is activated, and the breach is reported to the relevant authorities and affected data subjects within the required timeframe.
- **Containment and Eradication**: Immediate steps are taken to contain the breach and prevent further unauthorized access or data loss, while the source of the breach is identified and eradicated, with remedial actions implemented to prevent recurrence.
- **Recovery and Post-Incident Analysis**: Data and systems are restored to normal operations as quickly as possible following a breach. A post-incident analysis is conducted to understand the root cause of the breach and to improve security measures.

6 COMPLIANCE MONITORING AND REVIEW

6.1 AUDITS AND ASSESSMENTS

Audits and assessments are conducted periodically to evaluate the effectiveness of cybersecurity measures and to ensure compliance with GDPR and other relevant regulations. Findings from audits and assessments are used to continuously improve security practices.

6.2 THIRD-PARTY VENDOR MANAGEMENT

Third-party vendors are assessed for their cybersecurity practices and compliance with data protection requirements. When applicable, data protection agreements are in place with all third-party vendors to ensure they adhere to the same security standards as the Green Marine project.

Regarding third parties, it is important to state that no user information will be provided to participants outside the Green Marine consortium. Even within the consortium, user information will be provided only if necessary and justified. All information regarding user participation will be available in aggregated form, without any individual identification, totally anonymized.

7 CONCLUSION

The Green Marine project is committed to advancing climate neutrality in waterborne transport through innovative retrofitting solutions while ensuring the highest standards of data protection and cybersecurity. This report has detailed the measures taken to comply with the General Data Protection Regulation (GDPR) and to safeguard all data handled within the project.

Key areas covered in the report include:

- **Overview of GDPR**: A comprehensive explanation of GDPR, its relevance to the Green Marine project, and the key principles guiding data processing activities.
- **Data Categories and Their Handling**: Differentiation between datasets that do not contain user information and those that do, along with the specific handling procedures for each category to ensure data protection and compliance.
- **GDPR Compliance Measures**: Detailed compliance strategies, including adherence to data protection principles, lawful basis for data processing, and mechanisms for obtaining and managing consent.
- **Data Subject Rights**: Explanation of the rights granted to data subjects under GDPR and the procedures in place within the project to uphold these rights.
- **Data Protection Impact Assessments (DPIAs)**: The process and importance of DPIAs in identifying and mitigating risks associated with data processing activities.
- **Cybersecurity Measures**: Comprehensive technical and organizational measures to protect data, including encryption, access controls, incident response plans, and regular security audits.

7.1 FUTURE ACTIONS

Moving forward, the Green Marine project will implement Data Protection Impact Assessments (DPIAs) for all high-risk data processing activities. This approach will further enhance the project's ability to identify and mitigate potential risks to data subjects' privacy and security. The DPIA implementation will involve:

- Conducting thorough risk assessments for new and existing data processing activities.
- Engaging with stakeholders to understand and address their data protection concerns.
- Documenting and reviewing DPIAs regularly to ensure ongoing compliance and improvement of data protection measures.

8 APPENDIXES

Example for User data collected in the project platform:

Data Protection Impact Assessment (DPIA) for Platform User Database

1. Introduction

Project Name: Green Marine Platform User Database
Purpose of DPIA: To assess and mitigate the risks associated with the processing of personal data in the Green Marine platform user database, ensuring compliance with the General Data Protection Regulation (GDPR).
Date of DPIA: [Date]
DPIA Conducted By: [Name], Data Protection Officer (DPO)

2. Description of Processing

Nature of Processing:

- Collection, storage, and management of personal data related to users of the Green Marine platform.
- Data includes user profiles, contact information, usage data, and communication logs.

Scope of Processing:

- The user database contains personal data of platform users including employees, researchers, partners, and participants in the project.
- The database is used for user authentication, access control, communication, and project management.

Context of Processing:

- The data is processed within the Green Marine project to support decision-making, project coordination, and user engagement.
- The platform is accessible to authorized personnel and users from partner organizations.

Purposes of Processing:

- To manage user accounts and access permissions.
- To facilitate communication and collaboration among project participants.
- To monitor and analyze platform usage and engagement on content

3. Assessment of Necessity and Proportionality

Lawful Basis for Processing:

- User data is processed based on consent obtained during user registration.

Data Minimization:

- Only essential personal data is collected during user registration.
- Regular reviews are conducted to ensure that no unnecessary data is retained.

Proportionality:

- The processing activities are proportionate to the purposes of user management and project coordination.
- Data protection measures are in place to mitigate any adverse impact on data subjects.

4. Risk Assessment

Identification of Risks:

- Unauthorized access to user data.
- Data breaches leading to the exposure of personal data.
- Inaccurate or outdated user information.
- Insufficient user consent management.

Assessment of Risks:
- **Unauthorized Access**: High risk due to potential impact on user privacy and project integrity.
- **Data Breach**: High risk considering the volume and sensitivity of personal data.
- **Inaccurate Data**: Medium risk as it could affect project decisions and user communication.
- **Consent Management**: Medium risk due to the need for clear and revocable consent procedures.

5. Mitigation Measures

Technical Measures:
- **Encryption**: All personal data is encrypted at rest and in transit.
- **Access Controls**: Role-based access controls (RBAC) are implemented to restrict data access to authorized personnel.
- **Audits**: Security audits and vulnerability assessments are conducted regularly to identify and address potential threats.

Organizational Measures:
- **Data Protection Policies**: Comprehensive data protection policies are established and regularly updated.
- **Employee Training**: Regular training sessions are conducted to educate employees about data protection practices and GDPR compliance.
- **Incident Response Plan**: A detailed incident response plan is in place to manage data breaches and notify affected parties promptly.

Data Accuracy Measures:
- **Data Validation**: Automated checks are in place to validate the accuracy of user data during input.
- **User Reviews**: Users are periodically prompted to review and update their personal information.

Consent Management:
- **Clear Consent Forms**: Consent forms are designed to be clear and informative, ensuring users understand what they are consenting to.
- **Easy Withdrawal**: Users can easily withdraw their consent through the platform settings.

6. Documentation and Reporting

DPIA Documentation:
- This DPIA report is documented and stored securely.
- The report is reviewed and updated annually or when significant changes to the processing activities occur.

Reporting to Supervisory Authorities:
- In the event of high residual risks, the DPIA findings will be reported to the relevant supervisory authority.

7. Conclusion

The DPIA for the Green Marine platform user database identifies potential risks associated with the processing of personal data and outlines measures to mitigate these risks. By implementing the recommended technical and organizational measures, the project ensures compliance with GDPR and protects the privacy and security of platform users.

DPIA Review Date: [Next Review Date]
Approved By: [Name],