

Culture-Minded GDPR Recommendations for an NGO

Noah Page | Rebecca Ramthun | Rayna Sharma | Kaitlyn Smith



WPI

CYCLING
WITHOUT
AGE



Culture-Minded GDPR Recommendations for an NGO

1 May 2022

An Interactive Qualifying Project Proposal

Submitted to the Faculty of

WORCESTER POLYTECHNIC INSTITUTE

In partial fulfillment of the requirements for the

Degree of Bachelor of Science

By Noah Page, Rebecca Ramthun, Rayna Sharma, and Kaitlyn Smith

Report Submitted to:

Advisors Joan Szkutak and Rick Vaz

Sponsors Pernille Bussone and Ole Kassow, Cycling Without Age



This report represents work of WPI undergraduate students submitted to the faculty as evidence of a degree requirement. WPI routinely publishes these reports on its web site without editorial or peer review. For more information about the projects program at WPI, see <http://www.wpi.edu/Academics/Projects>

ABSTRACT

The General Data Protection Regulation (GDPR) is a law designed to protect personal data and privacy, and its complexity has created a market for consulting services to sell compliance solutions to businesses. Our team created compliance recommendations for Cycling Without Age International, a non-profit organization overseeing a global movement that provides bike rides for the elderly community. It was recommended that changes to internal policies, employee practices, and cybersecurity be carried out to improve GDPR compliance. Unlike market solutions, our team considered the organization's unique culture and values. These culture-minded recommendations will be easier to implement and less severely impact the daily practices of the organization.

ACKNOWLEDGEMENTS

Our team appreciates the following individuals who helped us complete this project.

Special thanks to **Ole Kassow** and **Pernille Bussone** for coordinating with WPI to set up the project for our team. Our team felt welcomed right from day one. The family style lunches were amazing, and our team loved the great conversations we had. Working with the two of you was a fantastic experience, and one we will never forget. We'll miss you both!

Thank you to **Christian Persson** for sitting down to do an interview with our team. We really appreciated your time.

Thank you to **Christine Bell** for providing us with information about the CWA Scotland chapter. Our team gained a lot of insight to help us with this project.

Thank you, **Professor Mike Elmes**, for doing a Zoom call with us to gain more insight on evaluating organizational culture! Our team appreciates it.

Thank you to **9 Small Homes** for providing us a warm and welcoming place to stay during our duration in Denmark.

Thank you to our outstanding advisors, **Rick Vaz** and **Joan Szkutak**, who helped us throughout the entire process in making this report. You made our trip so enjoyable, and we really appreciate you both!

EXECUTIVE SUMMARY

INTRODUCTION

The need for privacy, data rights, and cybersecurity has been argued to be critical items necessary for humanity. Out of this need to protect the fundamental human right to privacy, the General Data Protection Regulation, or GDPR, was written by the European Union (EU). This law went into effect on May 25th, 2018, establishing regulations for data protection. Concerns over the difficulty of implementing compliance with GDPR have been expressed both by organizations and scholars alike. The impact specifically on smaller organizations and businesses has been one topic of discussion, with the primary concern being that these organizations may lack the financial resources and manpower to comply with the lengthy regulations.

CYCLING WITHOUT AGE

Cycling Without Age (CWA) is a worldwide non-profit organization focused on giving elderly people bike rides. Ole Kassow, the founder of CWA, was inspired to assist elders with getting back on bikes when he saw an old man sitting on a bench which reminded him of his father (Coulon, 2020). Kassow discovered many people in nursing homes say they want the ability to bike or move the way they were used to before. His solution was to use trishaws, which have three wheels, a seat attached, and are operated by the pilot, so that older people may enjoy their rides without too much movement or discomfort (*Cycling Without Age*). The movement has grown to a global scale and the culture is very pertinent in its operations.



A trishaw

GOALS

CWA attempted to achieve GDPR compliance in the past, but market GDPR solutions were not working for the organization. They were too costly, required too many person-hours to implement, and failed to cater to CWA's unique culture and non-hierarchical organizational structure of a social movement as opposed to a traditional for-profit corporation.

The goal of our project is to recommend lasting changes to adapt Cycling Without Age's data processing procedures such that they meet GDPR regulations while remaining consistent with CWA's mission and values. To achieve this goal, our team identified three research questions that we felt could only be answered through our own field research.

1. What is Cycling Without Age International's culture?
2. How does Cycling Without Age International currently collect, store, and process data?

3. Where are Cycling Without Age International's data processes not GDPR compliant?

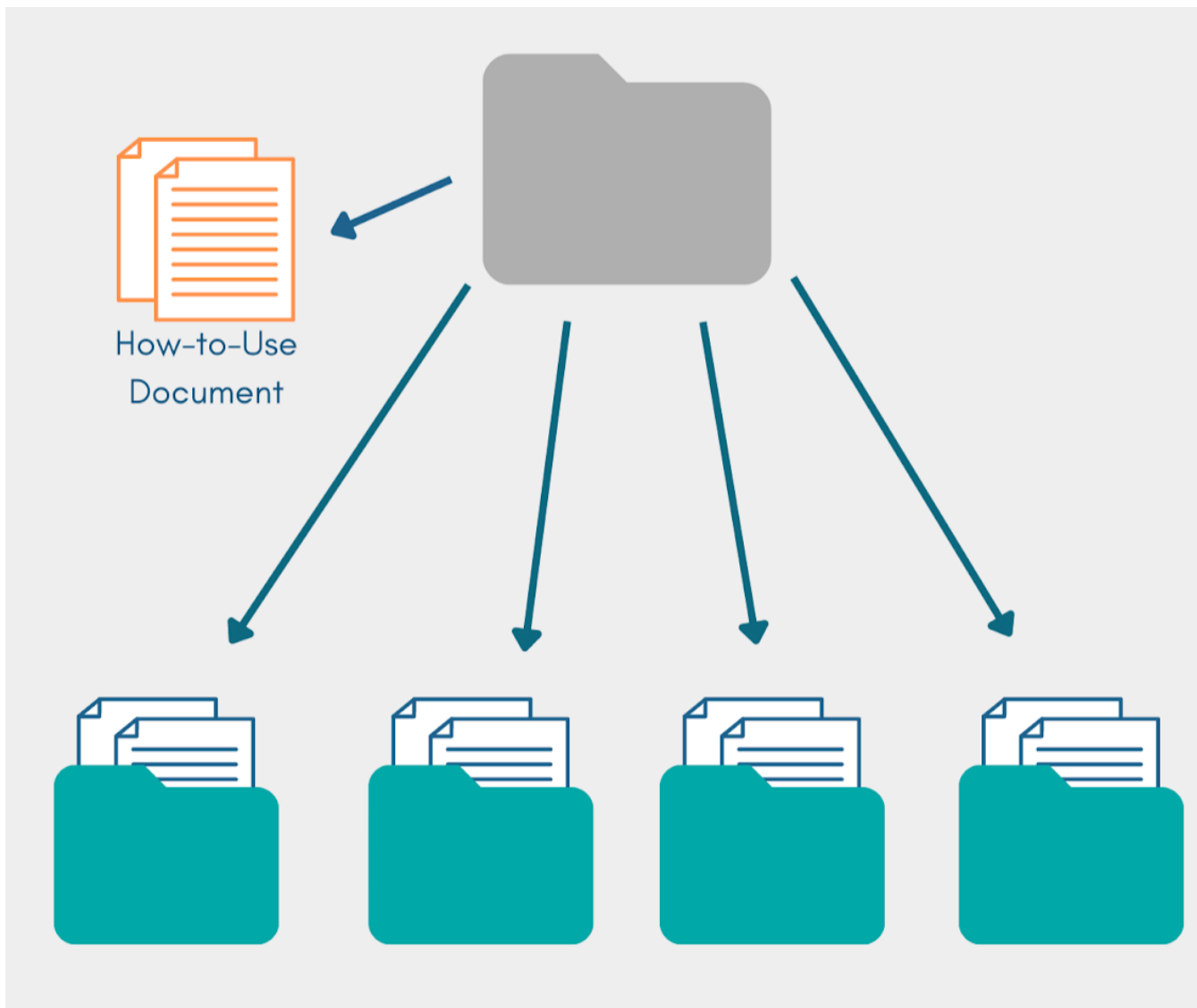
FINDINGS

To understand the culture of CWA International, we recorded observations or thoughts we had while in the workplace. Our integration into the office gave us a clear sense of the organization's structure and what they value. From our observations, we found the following:

1. CWA International values establishing interpersonal relationships and maintaining human connections with its affiliates
2. The employees of CWA International reflect the guiding principles in their daily actions
3. CWA International views GDPR as laborious, but also sees it as an opportunity to improve upon its practices
4. CWA International views itself not at the top of a hierarchical pyramid, but at the center of a web
5. CWA International feels that it has a responsibility to protect what its movement represents

Combined with our background research and our observations, we developed a deliverable that fits CWA International's culture and helps them become and stay GDPR compliant. We chose to create a digital GDPR Knowledge Base. The GDPR Knowledge Base is an interactive and easy-to-navigate alternative to presenting our recommendations in a lengthy PDF format. The Knowledge Base was formatted in a nested folder structure, where the Knowledge Base itself was contained within a single master folder. A single How-To-Use file exists in the master folder. In addition to the How-To-Use document, the Knowledge Base itself has a folder for each topic covered, as shown in the figure below. Within those folders, there is a recommendation document containing details and procedures for implementation and any extra materials, such as graphics or

flowcharts, that users may find helpful. Recommendations will be written as clearly and simply as possible so that anyone who is unfamiliar with GDPR can understand them.



A diagram showing the layout of the GDPR Knowledge Base

Additionally, we evaluated CWA International’s four main systems: Podio, WordPress, The Hood, and MailChimp. We cataloged the data flow throughout these systems to understand how CWA International processes its information.

RECOMMENDATIONS

The four primary systems we evaluated each had recommendations. For Podio, it was recommended that databases with outdated and unnecessary information be deleted and create legal agreements for databases that have administrators from multiple organizations or branches of CWA. For WordPress, the front displayed map should be cleared of any personally identifiable information, there should be WordPress training for new administrators, and old administrators should be deleted. Neither The Hood nor MailChimp had any direct recommendations since they comply with GDPR.

Additionally, recommendations were created for topics that impacted multiple platforms. They are as follows:

1. The New Affiliate form, which is the primary source of new information within CWA's data processing, should be updated so that it only collects necessary data, and we suggested replacing the physical form that collects data with a video recorded response for human connection
2. A privacy policy should be created that lives on the WordPress site and explains how the data is being processed by CWA International and what rights a user has during processing
3. Cookie consent should also be added with the privacy policy so users can manage their experience to their comfort level
4. Implementing both physical and digital security measures such as:
5. Creating password length and variety requirements
6. Requiring Two-Factor-Authentication for administrators
7. Backing up databases frequently
8. Keeping a physical locked filing cabinet for sensitive documents

AUTHORSHIP

<u>Section</u>	<u>Main Author</u>	<u>Main Editor</u>
Acknowledgements	Rayna Sharma	Rayna Sharma
Executive Summary	Rayna Sharma	Kaitlyn Smith
Introduction	Noah Page, Rebecca Ramthun, Rayna Sharma, Kaitlyn Smith	Noah Page, Rebecca Ramthun, Rayna Sharma, Kaitlyn Smith
Background		
Introduction	Kaitlyn Smith	Rebecca Ramthun
2.1 General Data Protection Regulation	Noah Page Rebecca Ramthun	Rebecca Ramthun Rebecca Ramthun
2.2 Becoming GDPR Compliant	Kaitlyn Smith	Noah Page, Rebecca Ramthun, Rayna Sharma
2.3 Workplace Culture and Decision-Making	Rayna Sharma	Noah Page, Rebecca Ramthun, Rayna Sharma
2.4 The Cycling Without Age Organization		
Methodology		
Introduction	Kaitlyn Smith	Noah Page, Rebecca Ramthun, Rayna Sharma, Kaitlyn Smith
3.1 Understanding CWA’s Culture	Rebecca Ramthun, Rayna Sharma	Rayna Sharma, Kaitlyn Smith
3.2 Cataloging CWA’s Current Data Processes	Rayna Sharma, Rebecca Ramthun	(All sections)
3.3 Identifying CWA’s Divergence from GDPR Compliance	Noah Page, Kaitlyn Smith	
Findings		
Introduction	Rebecca Ramthun	Noah Page, Rebecca Ramthun, Rayna Sharma, Kaitlyn Smith
4.1 The Culture of CWA International	Rebecca Ramthun, Rayna Sharma	Rayna Sharma, Kaitlyn Smith
4.2 CWA Specific Deliverables	Kaitlyn Smith	(All Sections)
4.3 The Data Flow through CWA International’s Systems	Kaitlyn Smith, Noah Page	
4.4 Points of Divergence from GDPR within CWA International’s Systems	Noah Page	
Recommendations		
Introduction	Kaitlyn Smith, Noah Page	Noah Page, Rebecca Ramthun, Rayna Sharma, Kaitlyn Smith
5.1 System-Specific Recommendations	Kaitlyn Smith, Noah Page	Smith
5.2 General GDPR Compliance Recommendations	Page	(All sections)

	Kaitlyn Smith, Noah Page	
--	-----------------------------	--

TABLE OF CONTENTS

- Abstract..... i
- Acknowledgements..... ii
- Executive Summary iii
- Authorship viii
- Table of Figures and Tables..... xii
- Introduction 1
- Background..... 2
 - 2.1 General Data Protection Regulation 2
 - 2.1.1 GDPR Terminology 3
 - 2.1.2 The Principles of Data Protection..... 3
 - 2.1.3 Permitted Data Processing and Consent 4
 - 2.1.4 User Rights 5
 - 2.1.5 Physical and Digital Security 7
 - 2.1.6 Joint Controllers..... 7
 - 2.1.7 Proof of Compliance..... 7
 - 2.1.8 Data Breach Response 8
 - 2.2 Becoming GDPR Compliant 8
 - 2.3 Workplace Culture and Decision-Making 9
 - 2.4 The Cycling Without Age Organization 10
- Methodology..... 15

3.1 Understanding CWA International’s Culture.....	15
3.2 Cataloging CWA International’s Current Data Processes	16
3.2.1 Metadata Interviews	16
3.2.2 Data Cataloging.....	16
3.3 Identifying CWA International’s Divergence from GDPR Compliance	19
Findings	22
4.1 The Culture of CWA International.....	22
4.1.1 CWA International Values Human Connection Within Its Organization	22
4.1.2 CWA International’s Upholding of its Guiding Principles	22
4.1.3 CWA International Perceives GDPR as Both an Obstacle and an Opportunity.....	23
4.1.4 CWA International is Equal to its Partners and Affiliates	23
4.1.5 CWA International sees its role as the “Protector of the Values”	24
4.2 CWA Specific Deliverables.....	25
4.3 The Data Flow through CWA International’s Systems.....	29
4.3.1 Podio.....	29
4.3.2 Wordpress	30
4.3.3 MailChimp and The Hood.....	31
4.4 Points of Divergence from GDPR within CWA International’s Systems.....	31
4.4.1 System-Specific GDPR Divergence.....	32
4.4.2 General GDPR Divergence.....	35
Recommendations.....	40
5.1 System-Specific Recommendations	40
5.1.1 Podio.....	40

5.1.2 WordPress.....	41
5.1.3 The Hood.....	42
5.2 General GDPR Compliance Recommendations	42
5.2.1 Lawfulness of Processing & User Consent.....	43
5.2.2 Users’ Rights.....	44
5.2.3 Security Practices	44
5.2.4 Proof of Compliance.....	45
5.2.5 Consent for Cookies.....	46
5.2.6 DPO Requirement & DPIA Procedure	46
Appendices.....	48
Appendix A – Interviews.....	48
A.1: Interview with Cykling Uden Alder IT Director Script	48
A.2: Interview with Cykling Uden Alder IT Director Notes.....	49
A.3: Interview with CWA Scotland CEO Script.....	51
A.4 Interview with CWA Scotland CEO Notes	52
A.5 Interview with Professor Mike Elmes Script.....	56
A.6 Interview with Professor Mike Elmes Notes	58
A.7 Introductory Interview with Global Community Captain	61
A.8 Data Handler Interview with the Global Community Captain Questions .	65
A.10 Data Handler Interview #1 Notes.....	66
A.11 Data Handler Interview #2 Notes.....	67
Appendix B – Information Collected by the New Affiliate Sign-Up Form	71
Appendix C – Information Inputted into the Hood by Users	73
Appendix D – Data Processing Flowchart	74

Appendix E - How to Use the GDPR Knowledge Base.....	75
Appendix F - Cookie Consent Recommendations	76
Appendix G - Security Practice Recommendations	77
G.1 Sample Podio Administrator Agreement.....	77
G.2 Recommendations for Security Practices	78
G.3 Instructions for Backing up Podio Databases	80
G.4 Backing up a Podio Database as an Excel File Walkthrough	81
Appendix H – Lawfulness of Processing and User Consent Recommendations ...	88
Appendix I – Proof of Compliance Recommendations	90
Appendix J – User Rights Recommendations.....	91
J.1– Acknowledging User Rights.....	91
J.2– How to Update the Privacy Policy	94
J.3– Privacy Policy Template.....	95
Appendix K - Data Protection Officer & DPIA Resources.....	102
K.1 Data Protection Officer Resources	102
K.2 Data Protection Impact Assessment Resources	103
References.....	103

TABLE OF FIGURES AND TABLES

Figure 1: The seven principles of GDPR	4
Figure 2: The eight user rights of GDPR.....	6
Figure 3: A trishaw.....	11
Figure 4: Cycling Without Age statistics.....	12
Figure 5: Cycling Without Age's organizational structure	14

Figure 6: Data cataloging spreadsheet template, filled with sample data	18
Figure 7: Divergence Spreadsheet template, filled with sample data	21
Figure 8: How-To-Use document at the top of the GDPR Knowledge Base	26
Figure 9: The layout of the master folder at the top of the GDPR Knowledge Base	27
Figure 10: The layout of one topic's subfolder within the GDPR Knowledge Base..	28
Figure 11: Data flow diagram	29
Figure 12: The CWA global map.....	30

INTRODUCTION

In 1950, 12 member states of the Council of Europe signed the Convention for the Protection of Human Rights and Fundamental Freedoms. This convention established the legally protected fundamental human rights, drawing inspiration from the declaration on universal human rights made by the General Assembly of the United Nations (UN) in 1948. Section 1 of this document sets forth the list of rights every person is entitled to. Article 8 of section 1 is titled “Right to respect for private and family life” and states, “Everyone has the right to respect for his private and family life, his home and his correspondence” (European Convention on Human Rights, 1950).

On January 1st, 2016, the United Nations officially signed the Sustainable Development Goals (SDGs) into action. The SDGs are 17 goals that the world agreed upon to strive to meet for the overall advancement of human society. The UN designed the goals to address global issues, including poverty, global warming, healthcare, equality, and others (United Nations Sustainable Development Agenda, 2016).

The need for privacy, data rights, and cybersecurity has been argued to be critical items necessary for humanity to achieve the SDGs. Scholars have argued that citizens may not be adequately protected from technology misuse, abuse, manipulation, or misapplication without better data privacy laws. The need for regulations to protect citizens from these dangers is crucial for society and the achievement of the SDGs (Michael et al., 2019).

Out of this need to ensure the advancement of the SDGs and to protect the fundamental human right for privacy, the General Data Protection Regulation, or GDPR, was written by the European Union (EU). This law went into effect on May 25th, 2018, establishing regulations for data protection. The law has a widespread scope that applies to organizations in the EU, and any organization that wishes to serve EU residents.

Concerns over the difficulty of implementing compliance with GDPR have been expressed both by organizations and scholars alike. The impact specifically on smaller organizations and businesses has been a major topic of discussion. The primary concern

has been that these organizations may lack the financial resources and labor to comply with the lengthy regulations (McAllister, 2017).

The existing resources for organizations to implement GDPR compliance have flaws. Organizations often hire a cybersecurity consulting firm to audit them and recommend specific changes to achieve compliance. However, this is an expensive process that not everyone may be able to afford. Additionally, these consulting firms frequently apply “one-size-fits-all” recommendations that fail to account for the culture or structure of its client. While open-source tools and resources exist, using and implementing them can be difficult. These tools often have drawbacks similar to those of the consulting firms, as they also may not cater to every organization.

Cycling Without Age (CWA) is a non-profit organization based in Copenhagen, Denmark. CWA had attempted to achieve GDPR compliance in the past, but market GDPR solutions were not working for the organization. The movement ran into many of the problems previously listed, specifically that the tools failed to cater to CWA’s unique culture and non-hierarchical organizational structure.

The goal of our project is to recommend lasting changes to adapt Cycling Without Age’s data processing procedures such that they meet GDPR regulations while remaining consistent with CWA’s mission and values.

BACKGROUND

In this chapter, we begin by discussing the importance of privacy in the era of the internet, introduce General Data Protection Regulation (GDPR), and present a few relevant sections of GDPR. We then overview the impacts of workplace culture on how organizations adjust to change and how to evaluate it. Finally, we discuss the nonprofit organization, Cycling Without Age, as well as its mission, values, unique structure, and its history with GDPR compliance.

2.1 GENERAL DATA PROTECTION REGULATION

Privacy has been established as a human right by the Universal Declaration of Human Rights, the European Convention of Human Rights, and the European Charter of Fundamental Rights (European Data Protection Supervisor, 2019). With the widespread adoption of the internet, increasing amounts of information on individuals are being shared, processed, and stored. *Data protection* is the act of protecting the information that makes up a person's identity (European Data Protection Supervisor, 2019). Proper data protection practices are integral to ensuring the privacy of individuals' information. In 2018, the General Data Protection Regulation (GDPR) was put into effect by the European Union. GDPR defined the principles of data protection, the legal bounds of data processing and consent, the rights of users, and other legislative action relating to how organizations should manage data privacy.

2.1.1 GDPR TERMINOLOGY

General Data Protection Regulation (GDPR) codified data protection as a legal requirement for *data controllers*. Data controllers are entities responsible for deciding the processing performed by *data processors* on the data of *subjects*. Data processors process the data by the data controller's instructions (*What is a data controller or a data processor?*, 2019). Subjects are individuals who provide the data, and often use the services provided by the data processors and controllers. Under GDPR, *data controllers* and *data processors* are responsible for taking actions to protect the personal data of subjects. *Data processing* is any actions performed on data after it has been provided by the subject.

2.1.2 THE PRINCIPLES OF DATA PROTECTION

The General Data Protection Regulation Law was designed to achieve a set of principles of data protection, as seen in Fig. 1 (Regulation 2016/679/EC, Article 5). The first principle of *Lawfulness, fairness, and transparency* states that organizations are not only obligated to comply with the legislation but also that users of their systems must be informed of all actions that an organization performs on their data (*What is GDPR, the EU's new Data Protection Law?*, 2019). *Purpose limitation* defines the responsibility of

organizations to only utilize user data for the explicit purposes that the user consented to. *Data minimization* states that organizations may only collect and store the data necessary to complete their goal. The principle of *Accuracy* requires organizations to keep all records up-to-date, and not store data that is no longer accurate. *Storage limitation* means that data can only be stored for as long as needed to accomplish the goal explained to the user. The principle of *Integrity and confidentiality* requires appropriate security measures to be put in place to protect the data. Lastly, *Accountability* ensures that organizations themselves are responsible for demonstrating and proving they are GDPR compliant (*What is GDPR, the EU's new Data Protection Law?*, 2019).

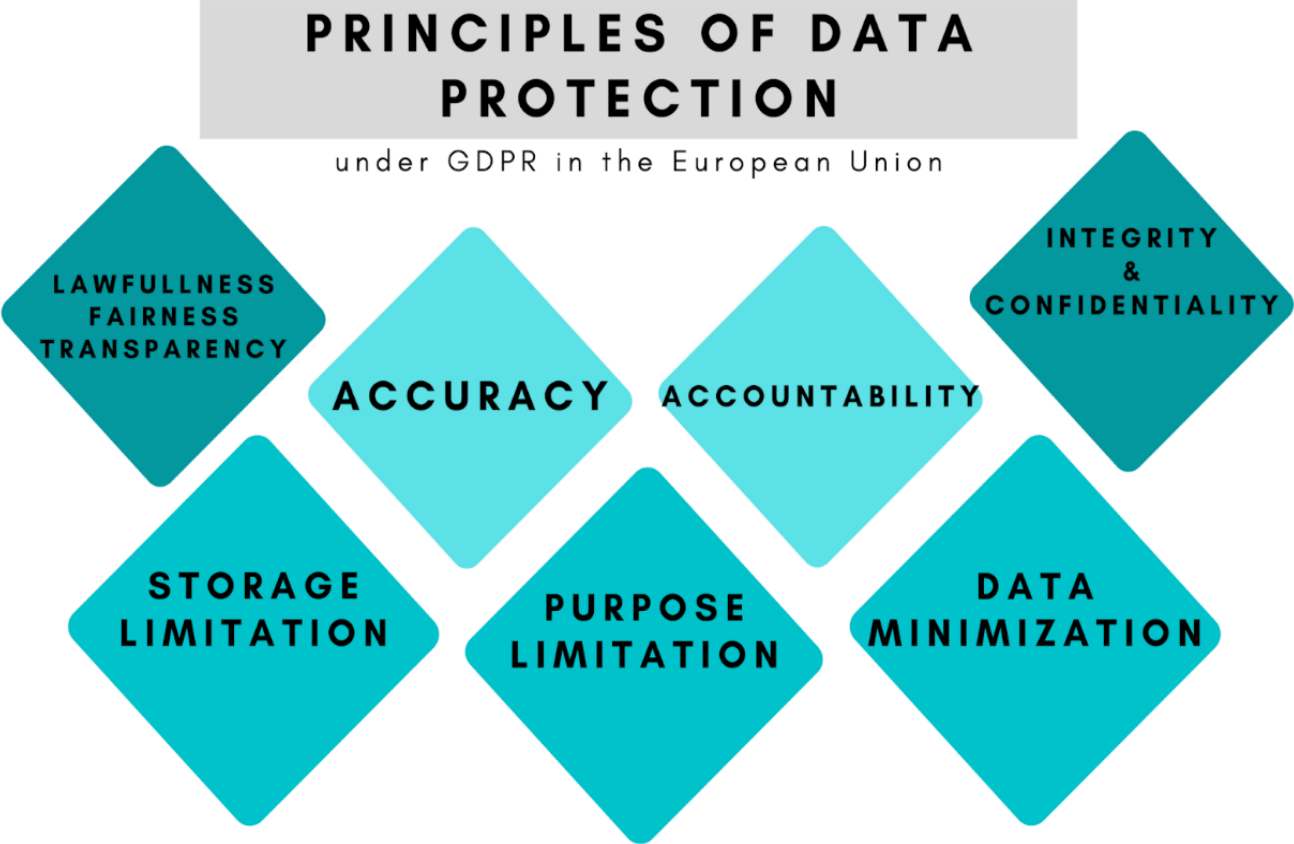


Figure 1: The seven principles of GDPR

2.1.3 PERMITTED DATA PROCESSING AND CONSENT

Under GDPR, there is an exclusive list of six situations in which data processing is allowed (Regulation 2016/679/EC, Article 6). Data processing is only permitted if the controller can prove the existence of one of these six justifications:

1. Receiving unambiguous consent to process
2. Processing in order to prepare to enter into a contract
3. Processing to comply with legal obligations
4. Processing in order to save a life
5. Processing in order to serve the public interest
6. Processing with a legitimate interest to process an individual's data

Additionally, GDPR establishes what user consent looks like for data processing through four conditions (Regulation 2016/679/EC, Article 7):

1. The data processor must store proof that consent was obtained
2. A request for obtaining consent must be presented in a way that is easily distinguishable from any other matters that are compiled with the request. The language used must be clear and plain
3. Consent must be able to be withdrawn, in a method that is equally as easy as it is to give the consent
4. Consent must be freely given, and consent cannot be forced to be a condition for utilizing the service if the lack of consent does not inhibit the operation of the service

2.1.4 USER RIGHTS

In the interest of data protection, and by extension, the protection of privacy, *users* must be guaranteed eight rights by the organization providing services (Regulation 2016/679/EC, Articles 12-23). Organizations have the responsibility to ensure their users retain these rights (Fig. 2).

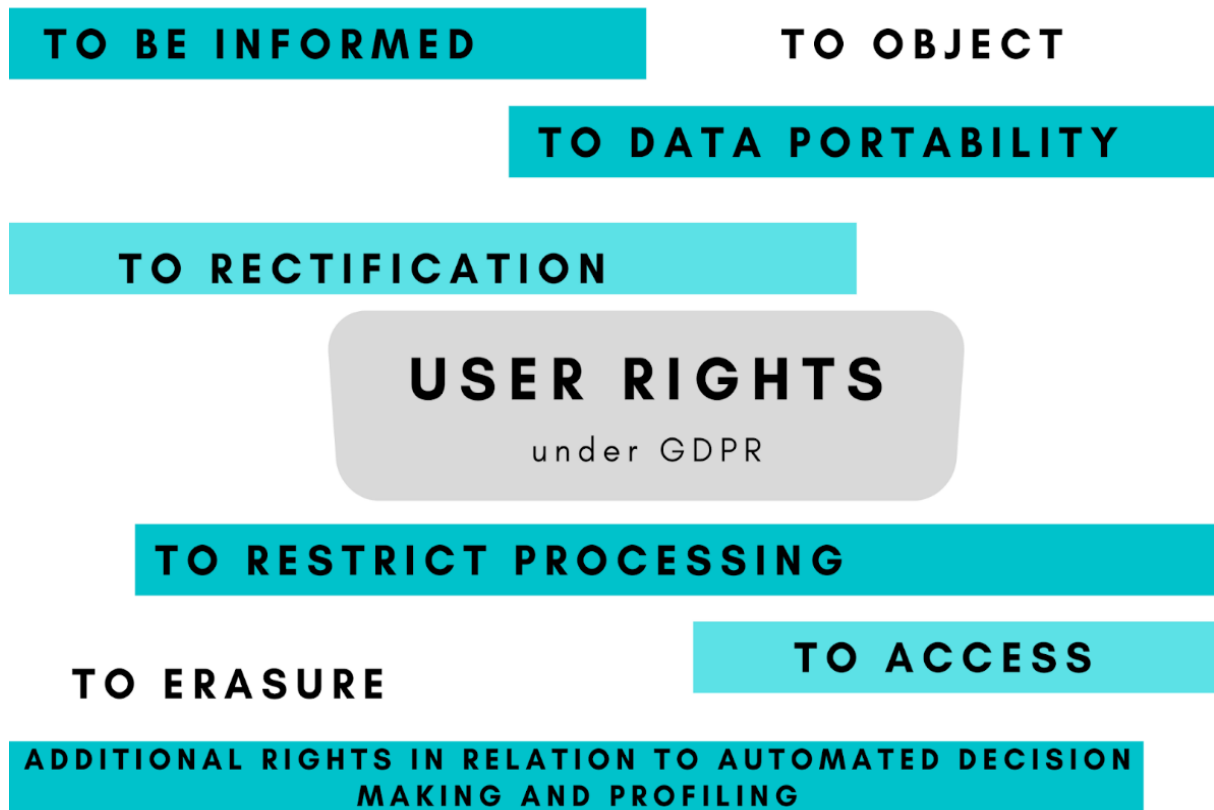


Figure 2: The eight user rights of GDPR

Users have the right *to object*; they can refuse the processing of their data. Users have the right *to data portability*; they can request a copy of all their personal data an organization maintains. Users have the right *to rectification*; they can alter and make their data more up to date or change inaccuracies. Users have the right *to restrict processing*; they can request that only certain processes be performed on their data. Users have the right *to be informed*; organizations must provide simple, comprehensive, and accessible information on how they process data, and inform users of data breaches. Users have the right *to access*; they must be able to access all the data that organizations have on them. Users have the right *to erasure*; they must be able to have all their information erased. Users also have additional rights in relation to automated decision making and profiling. When making changes to data systems, a data processor must remember and prioritize user rights to ensure its processing is GDPR compliant.

The controller of the data for an organization must also be transparent about how the data subject's information is processed (Regulation 2016/679/EC, Articles 12). A publicly accessible privacy policy detailing the data processing, along with how the organization implements the user's rights must exist on the organization's website. It is also organizations' responsibility to have simple and straightforward methods to allow users to exercise their rights (Regulation 2016/679/EC, Articles 15-22).

2.1.5 PHYSICAL AND DIGITAL SECURITY

GDPR establishes that organizations are responsible for protecting their users through “*Data protection by design and default*”, and “*Security of Processing*” (Regulation 2016/679/EC, Article 25 and 32). Both sections require organizations to have up-to-date physical and digital security systems. These articles are written very broadly so that they do not become outdated as technology advances. They also give the data controllers flexibility in determining how to become compliant. There is no single process for implementing security systems because there are many ways it can be handled that will make a company or organization compliant.

2.1.6 JOINT CONTROLLERS

Organizations must have explicit grounds that define the scope and nature of data processing when two or more organizations have access to the same data (Regulation 2016/679/EC, Article 26). When two organizations are sharing databases, this agreement serves to define the scope of what the *joint controllers* may do with the data, and the grounds for how processing will occur for both.

2.1.7 PROOF OF COMPLIANCE

The section of GDPR, “*Records of processing activities*” states that organizations need to keep records of the type of information, its source, its purpose, the lifespan of its time in storage, and whom it is shared with. It also states that organizations must have documentation showing all the places where data is stored and how data flows between

them. Data flow diagrams identify any privacy risks in processing, and they are usually the first piece of compliance documentation (Regulation 2016/679/EC, Article 30).

2.1.8 DATA BREACH RESPONSE

GDPR also contains articles regarding what must happen when a data breach occurs (Regulation 2016/679/EC, Articles 34 & 35). These state that data breaches must be reported to authorities within 72 hours, along with the type of data that was lost and what the consequences of the breach are. Additionally, if the data was not encrypted, the user must be informed of the breach within the same timeframe.

2.2 BECOMING GDPR COMPLIANT

The process of adapting current data processing systems to become GDPR compliant can be a challenging task for organizations since the law is intentionally broad to leave room for various paths to compliance, there are varying resources as well. However, there are not enough resources to cover every organization's needs. Some resources exist without the need to outsource work to a costly external firm. A small team in Belgium created gdprchecklist.io, a community-run web resource for helping organizations check their current GDPR compliance status. The cybersecurity law compliance firm, IT Governance, created a resource that details the process of meeting this compliance, titled *EU General Data Protection Regulation (GDPR) – An implementation and compliance guide*. The different sections of this book walk through the GDPR laws, explain what they mean, and what a practical application of them would look like (*EU General Data Protection Regulation (GDPR): An implementation and compliance guide*, 2019). Although resources like gdprchecklist.io or GDPR books and guides exist, they still have drawbacks. Tools like these use a plethora of technical jargon that may be difficult for the non-technically proficient to understand, let alone implement within their own organization's internal processes ("Privacy, Data Rights and Cybersecurity: Technology for Good in the Achievement of Sustainable Development Goals", 2019).

In 2019, Henricksen-Bulmer et al. published a case study about implementing GDPR in the charity sector. They observed that GDPR's lengthy requirements and the challenge it places on organizations to "prove" their compliance can be particularly taxing on organizations that do not have the person-power or funding to swiftly enact such broad changes. Additionally, as there is no charity-sector specific guidance under GDPR, organizations that are classified as charities must fulfill GDPR in the same way as large, for-profit companies (Henrikson-Bulmer et. al 2019). The authors summarized the challenges faced by smaller organizations, stating:

"While GDPR affects all organizations, it has particular implications for small to medium enterprises (SMEs) and charities... as these organizations often work within financial and resource restraints and therefore, may lack the expertise to fully understand how best to interpret and implement the changes brought in by GDPR" (Henrikson-Bulmer et. al 2019).

The culture and objectives of an organization are demonstrated by this case study to be important points of reference for potential researchers who are looking especially to provide aid to smaller organizations.

2.3 WORKPLACE CULTURE AND DECISION-MAKING

Workplace culture is part of what shapes an organization and its work environment. There is not a universally agreed-upon way to evaluate the culture and its benefits. However, an understanding of how workplace culture influences decision making can be important to draw from for those proposing recommendations for organizations.

Organizations can be resistant to change at first. A study by Edgar Schein found that companies will not introduce suggestions or changes that may disrupt their traditional flow of work (Schein, 1996). Many operational recommendations don't match the organization that is using it. The author's argument is that time is rarely taken to observe and understand the organization from an internal level (Schein, 1996). Internal workings and culture at companies can drastically affect the result of the suggestions and how well they will catch on internally. Schein argues that to make a good and effective

recommendation, one must combine the viewpoints of employees with various roles within the company. He concludes “When I see my colleagues' inventing questionnaires to ‘measure’ culture, I feel that they are simply not seeing what is there...” (Schein, 1996). His argument is that observation and fieldwork is the best way to do this. These surveys can only cover what is asked, and there will be many loose ends or biases. Journaling and observing will give the truest view of what is occurring within a company. To Schein, observation of all levels of management will give an even better sense of what direction the company should go in.

2.4 THE CYCLING WITHOUT AGE ORGANIZATION

Cycling Without Age (CWA) is a worldwide non-profit organization that brings members of the elderly community on bike rides throughout their cities. Volunteers, known as pilots, pick up elderly riders from their residences and take them on a trip around the city. Ole Kassow, the founder of CWA, was inspired to assist elders with getting back on bikes when he saw an old man sitting on a bench which reminded him of his father (Coulon, 2020). Kassow discovered many elderly people in nursing homes say they long for the ability to bike or move the way they were used to before (*Cycling Without Age*). CWA utilizes trishaws, as shown in Fig. 3, which are bicycle-like structures with a seating area in the front. This is so that elders may enjoy their rides without too much movement or discomfort (*Cycling Without Age*).



Figure 3: A trishaw

CWA has five guiding principles that serve as the framework for its operations: *Generosity*, *Slowness*, *Storytelling*, *Relationships*, and *Without Age* (“Can A Trishaw ride change the world?”, 2019). These principles promote better health and well-being for the elderly community, empower people across age barriers, and implement sustainable and accessible policies that better communities.

Generosity is important to CWA, as the entirety of the organization is based upon the act of kindness. Affiliates that are a part of CWA should show their generosity to those who would like to be a part of the movement. Another is *slowness*, because taking the ride slowly is a tool that allows everyone involved in the rides to be present and in the moment. *Storytelling* is highlighted because on the trishaw rides, elderly passengers can share their life experiences with pilots and riders alike. The next principle, *Relationships*, exists as CWA feels its organization has a role in breaking down intergenerational barriers and connecting across generations on a deeper level. Lastly, the principle of *Without Age* exists as CWA feels its organization has a role in keeping life positive and full of opportunities, no matter what age one may be. (Cycling Without Age, 2012).

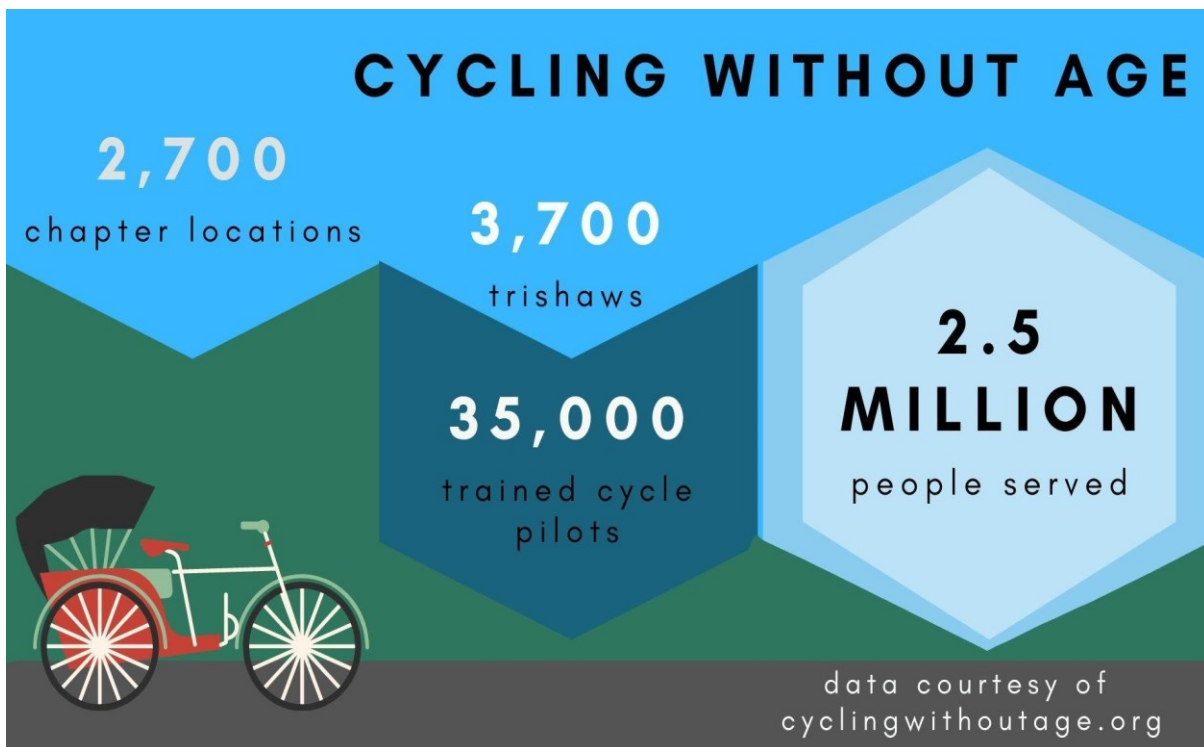


Figure 4: Cycling Without Age statistics

As shown in Fig. 4, CWA is an international movement that spans 52 countries with over 2,700 chapters. CWA considers itself a holacracy, with its organization best characterized as a web rather than the traditional hierarchical pyramid. (“Becoming A Cycling Without Age Affiliate”, 2019). CWA International is the part of the organization located in Copenhagen, Denmark that oversees the movement. CWA International currently has two employees: the Founder and the Global Community Captain.

CWA International has three distinct types of relationships with others within the organization, as seen in Fig. 5. In one instance, it works directly with affiliates, who are the individuals that are running CWA branches or planning to start one within their local communities. The affiliates that work directly with CWA International are often in the initial phases of starting a local chapter in their communities, and CWA International helps provide guidance and support in getting started.

In another type of relationship, CWA International works directly with established local chapters that are headed by an affiliate. A local chapter is a CWA organization that exists within a community and takes care of the planning of coordinating rides and finding

pilots. The logistics of ride coordination, pilot recruitment, and other day-to-day operations stay at the local chapter level and are not passed on to CWA International. CWA International works with local chapters by providing them with its web domain, giving guidance on branding and marketing, as well as providing access to software tools for the local chapters to utilize for themselves.

In the last type of relationship, CWA International works with a country partner. A country partner is an organization that started out as a local chapter but grew to a scale where it now guides the local chapters in its country. These country partners are often registered as charities within the legal authority they are located in. Additionally, country partners have license agreements with CWA International and traditionally refer to themselves as Cycling Without Age in their country's main language. For example, the German country partner is known as Radeln Ohne Alter, and has a contract between itself and CWA International. Local chapters can choose to work with the country partner in their area, or to work directly with CWA International. If a country chapter does not exist, the local chapter will work directly with CWA International.

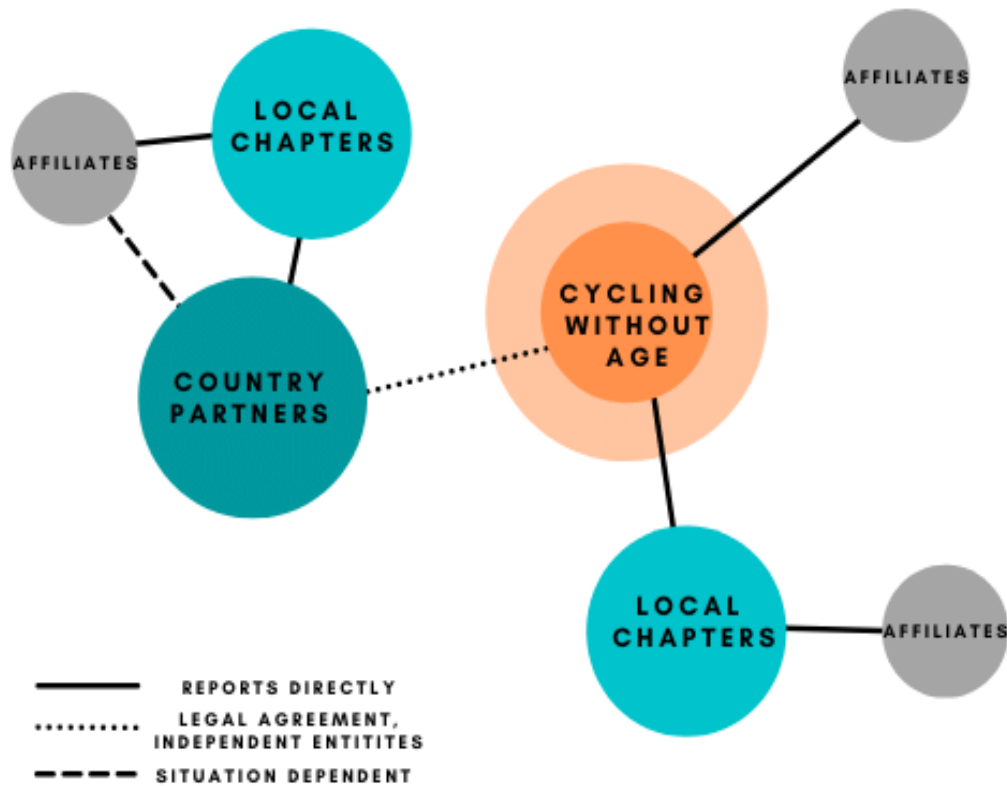


Figure 5: Cycling Without Age's organizational structure

About 90% of CWA International's funding comes from a social enterprise called Copenhagen Cycles, which sells trishaws to fledgling CWA affiliate chapters and donates its profit to CWA. The remaining 10% of its funding comes from donations and grants (P. Bussone, personal communication, March 8, 2022). The non-profit has partnerships with companies around the world to assist in fundraising and spreading CWA's mission and principles.

Previously, CWA International coordinated with a consulting firm to advise them on how to become GDPR compliant. However, the organization ran into some of the issues previously mentioned by Henricksen-Bulmer et al. Additionally, its local-yet-global structure presents challenges that do not fit most market GDPR solutions. To achieve compliance, CWA International will need recommendations that are tailored to fit its unique organization.

METHODOLOGY

The goal of our project is to recommend lasting changes to adapt Cycling Without Age's data processing procedures such that they meet GDPR regulations while remaining consistent with CWA's mission and values. To achieve this goal, our team identified three research questions that we felt could only be answered through our field research:

1. What is Cycling Without Age International's culture?
2. How does Cycling Without Age International collect, store, and process data?
3. Where are Cycling Without Age International's data processes not GDPR compliant?

In this chapter, we describe the methods used to gather the data to answer these questions.

3.1 UNDERSTANDING CWA INTERNATIONAL'S CULTURE

To create recommendations that are tailored to CWA International, our team first evaluated its culture. Although some information about CWA's organization was available in print literature and CWA's own published materials, we needed to conduct our own research to expand upon this information. During our time working at CWA International's office, we recorded our observations about its culture and organizational behavior each day. These records included items such as platform usage preferences, the way the organization utilized its communication systems, and other details that we deemed relevant for documenting CWA International's culture. Additionally, during our data handler interviews, which will be discussed in Section 3.2, we took note of organizational details that shaped how it utilized its data systems.

The primary challenge presented by this method is that it is dependent on our interpretation of CWA International's culture as nonlocal observers. We are unfamiliar with Danish customs, and we may misinterpret the significance of certain actions within the office because of a difference in the meaning of those actions within a Danish office as

compared to an American one. Additionally, we are limited to what we notice CWA International's employees saying in English. Some office communication is conducted in Danish, and the significance of that communication from a cultural perspective will be lost due to our lack of Danish fluency.

3.2 CATALOGING CWA INTERNATIONAL'S CURRENT DATA PROCESSES

To understand where CWA International's data processing fails to comply with GDPR, our team studied the various platforms used by the organization. The overarching question our team answered was: *How does CWA International collect, store, and process its data?* By completing interviews with the employees who work with the data regularly and by developing a comprehensive catalog of the organization's current processes, we were able to assess CWA International's data processing practices.

3.2.1 METADATA INTERVIEWS

To obtain the metadata¹ that our team needed to catalog, we interviewed the CWA's Global Community Captain and the IT director for Cykling Uden Alder about CWA International's data processing practices. We will refer to our interviews with CWA International's Global Community Captain as the data handler interviews. These contained questions designed to understand Cykling Uden Alder, wherein we asked related questions regarding CWA International's collection, storage, and processing of personal data. The Cykling Uden Alder IT director often volunteers their time to CWA International and does much of its IT work. Appendix A.1 contains the interview script that was utilized for this interview. Both interviews gave us the metadata that we needed to organize in our next method, cataloging.

3.2.2 DATA CATALOGING

¹ Metadata is a set of data that gives information about other data. In this case, the answers from the interviews are giving us information about how the data flows through the various CWA systems.

To comprehensively understand the data collection and processing, we cataloged the data CWA International collects, stores, and processes. CWA International utilizes four primary software systems for collecting, storing, and processing: Podio, The Hood, WordPress, and MailChimp. When an individual wants to sign up to become a new CWA affiliate, they answer questions and enter personal data into an application form. The data gets stored in the first software system; a database workspace platform called Podio. The second software system, called The Hood, is a collaborative blog site where CWA members around the world can post about CWA-related topics. The CWA International website runs on WordPress, the third software system, which contains all the public-facing content and posts. Lastly, MailChimp is utilized for sending out CWA newsletters to subscribers. Using our data cataloging spreadsheet, shown in Fig. 6, we recorded what information is kept on which system, who the data belongs to, where the information came from, and what the data is being used for.

By compiling all this information in one place, we were able to see how the data moves through the four primary software systems. The data collected from the metadata interviews were organized into the data cataloging spreadsheet, with each software system having its own category. This approach was selected for its ability to be compiled into a visual flowchart of the data movement through systems, which is a GDPR requirement.

Storage Location							
Podio	The Hood	Wordpress	MailChimp	Information collected	User Type	Origin of data	What is the data used for
X				Database: Example			
x				Data Piece 1	User	Form	As an example
x				Data Piece 2	User	Form	As an example
x				Data Piece 3	User	Form	As an example
x				Data Piece 4	User	Form	As an example
		x		Data Piece 5	User	Form	As an example
		x		Data Piece 6	User	Form	As an example
		x		Data Piece 7	User	Form	As an example
			x	Data Piece 8	User	Form	As an example
	x			Data Piece 9	User	Form	As an example
	x			Data Piece 10	User	Form	As an example
	x			Data Piece 11	User	Form	As an example

Figure 6: Data cataloging spreadsheet template, filled with sample data

3.3 IDENTIFYING CWA INTERNATIONAL'S DIVERGENCE FROM GDPR COMPLIANCE

To meet our goal of creating GDPR compliance recommendations, we sought to answer the question: Where are CWA's data processes not GDPR compliant?

To help us compare CWA International's data processing practices with those of a GDPR-compliant organization, we conducted an interview with the chief executive officer of CWA's Scotland chapter. CWA International had indicated that the Scotland chapter had strong security practices, and we felt it would be beneficial to understand them in detail. The chapter is GDPR compliant due to being supported by the Scottish government since it is a charity. These questions were created to understand how a CWA chapter may go about implementing data security and privacy. This interview taught us how Scotland was succeeding in its compliance and gave us strategies that may transfer well to other CWA organizations. Additionally, this was designed to use Scotland's GDPR compliance as a benchmark for CWA International's compliance. Scotland's particular practices and procedures will not be used as exact recommendations, because its culture is significantly different from CWA International's. Appendix A.3 contains the interview script utilized for this interview.

Not all GDPR compliance issues can be compartmentalized by software systems, as issues may pertain to more general organization procedures that span multiple platforms. To identify GDPR non-compliance across all the different systems CWA International utilizes, our team created the Divergence Spreadsheet. The Divergence Spreadsheet groups together GDPR issues by either system or topic. CWA's four main software systems, WordPress, The Hood, MailChimp, and Podio, all had their individual non-compliance issues grouped by software platform rather than topic. Issues that pertained to multiple of these software systems were grouped by the general topic they belong to. For example, the way CWA International stores physical documents within its office. This issue does not cleanly fit into one of the four main software systems, so it was instead grouped into the "Security Practices" topic. Figure 7 shows the Divergence Spreadsheet's organizational system, with the first set of headers dedicated to the primary software

systems' individual issues and the rest of the headers dedicated to the topic grouped issues.

The first column is labeled as "What is the issue?" and was filled out with a brief description of the non-compliance issue. The second column, "What GDPR Article does it not comply with?" was filled out with the article, section, and if applicable, subsection, that the issue fails to comply with. The third column, "How should we resolve it?" was filled out after our team had produced a culture-minded CWA-specific recommendation to resolve the issue. This spreadsheet allowed us to organize all the GDPR non-compliance of CWA International in one location and identify situations where multiple issues could be resolved efficiently with the same recommendation.

What is the Issue?	What GDPR Article does it not comply	How should we resolve it?
Software System: Podio		
Podio Recommendation 1	Article 0	Fix XYZ
Podio Recommendation 2	Article 200	Implement ABC
Podio Recommendation 3	Article 300	Add LMNOP
Software System: Wordpress		
WordPress Recommendation 1	Article 0	Delete this but download that
WordPress Recommendation 2	Article 0	Download or export ZYX
WordPress Recommendation 3	Article 94	Create BCA
WordPress Recommendation 4	Article 188	Do this
Project: Name of Project Done (Article 10,000)		
Specific Topic Recommendation 1	Article 10,000	In system A, add BBBB
Specific Topic Recommendation 2	Article 10,000	For this, delete YZX and replace it with CBA

Figure 7: Divergence Spreadsheet template, filled with sample data

FINDINGS

In this chapter, we identify the key findings regarding CWA International’s culture. We will then discuss CWA International’s data processing systems, followed by our evaluation of where these systems need adjustments for GDPR compliance.

4.1 THE CULTURE OF CWA INTERNATIONAL

4.1.1 CWA INTERNATIONAL VALUES HUMAN CONNECTION WITHIN ITS ORGANIZATION

CWA International values establishing and maintaining interpersonal relationships with its affiliates, even as its members are spread across the globe and may never meet except through internet exchanges. During interviews, the Global Community Captain of CWA International reported that he believed requesting affiliates to submit pictures of themselves as a part of the affiliate application was important for maintaining a “human connection.” The Global Community Captain expressed that these images made the interaction feel more real and personable. CWA also highly values facilitating interpersonal connections between its affiliates. When new affiliates are approved, the Global Community Captain greets the affiliates via e-mail and encourages them to sign up to The Hood, allowing them to build connections with other affiliates.

Additionally, beyond online interactions, our team observed that the employees of CWA International and Cykling Uden Alder, the Danish branch with whom they share an office, often have family-style smørrebrød lunches together, establishing a sense of community.

4.1.2 CWA INTERNATIONAL’S UPHOLDING OF ITS GUIDING PRINCIPLES

Our experience working within Cycling Without Age International’s office demonstrates a tenet of its organization is its dedication to implementing the guiding principles in its daily decision making. This emphasis on the principles was visible constantly, from the collaborators prioritizing team meals and coffee together

(*Relationships*), to the prioritization of a relaxed-pace office environment (*Slowness*), to the obvious delight in the sharing of stories between the collaborators and the members of the organization (*Storytelling*). The suggestion of using a video format for new affiliates to sign-up immediately sparked interest with the Global Community Captain, specifically in that it would provide an opportunity to increase relationships and better tell stories within the organization at the affiliate's own pace. *Generosity* was present in every aspect of the employee's attitude towards our team, from the sharing of food, space, and knowledge of Danish culture. Finally, the passion for *Without Age*, and unifying people across generations was a frequent topic of conversation, from talk of inclusive cities to finding ways to build connections with conversations over lunch.

4.1.3 CWA INTERNATIONAL PERCEIVES GDPR AS BOTH AN OBSTACLE AND AN OPPORTUNITY

In line with the idea that CWA is a “movement”, the organization's key motivations are to grow and to support its members. CWA International views regulations such as GDPR as laborious and time-consuming, as it does not directly support its mission. While it is perceived as a burden, the organization simultaneously sees it as an opportunity to improve upon its organization practices. This contrast accentuates the balance CWA International's culture strikes between change and tradition, and between flexibility and rigidity.

4.1.4 CWA INTERNATIONAL IS EQUAL TO ITS PARTNERS AND AFFILIATES

A core aspect of Cycling Without Age International is its value of collaboration within its organization and its view of other chapters as equals that are “at its level” and not “below them”. As previously discussed, CWA International views themselves not at the top of a hierarchical pyramid, but at the center of a web, which has distinct impacts on its culture. The metaphor that the employees of the organization used to explain this relationship was that of a family structure. As CWA International was the origin point of the movement, the natural conclusion might be to categorize its relationship to the chapters as a parent-child relationship, where CWA International has authority over the

younger chapters. CWA International views the relationship more like that of an elder sibling and a younger sibling, described by the Global Community Captain as the “sweet older brother” (Appendix A.7) The International organization believes they have a responsibility to protect the movement from external forces, but as each of the partners is legally independent, CWA International has no legal responsibility over its “younger siblings”.

4.1.5 CWA INTERNATIONAL SEES ITS ROLE AS THE “PROTECTOR OF THE VALUES”

A final cultural dynamic we observed was the interplay between CWA International’s view of its role as the “protector of the values” and its respect for the sovereignty of the independent partners. CWA International feels that, although it is not at the top of a hierarchy, it still has a responsibility to protect what its movement represents and ensure that the values that it esteems are also priorities for chapters. At the same time, it does not wish to instruct the other chapters on how to operate outside of necessities. It views this partnership as one based around mutual trust and respect for each other's agency.

The sibling metaphor helps illustrate the culture of this movement. A few country partners previously contacted CWA International seeking guidance on how to become GDPR compliant, and as the “good older sibling”, CWA International wanted to personally demonstrate GDPR compliance, support them, and provide its younger siblings with tools for success. Additionally, as “protectors”, CWA International feels it has a responsibility to protect all members of the movement from the consequences of GDPR non-compliance to the best of its ability.

In hierarchies, making changes such as GDPR compliance comes from the top and then must be instituted by employees at lower levels, or is hired out to consultants. By virtue of its culture, we observed that CWA International cannot– nor would it wish to– approach GDPR that way. Although it would potentially be simpler to assume a more “parental” role and instruct the other organizations to “figure out GDPR”, it would be

counter to the organizational ideal of a collaborating, caring, and mutually supportive global ecosystem.

To protect the image of the entire movement, CWA International has made it a requirement for all affiliates and partners to utilize their WordPress platform, as a way of verifying the legitimacy of the organization. While this policy goes against its desire to not implement rules, this was enacted because site uniformity protected CWA International's values, which was prioritized over giving partners the independence to utilize different website platforms.

4.2 CWA SPECIFIC DELIVERABLES

Our observations on CWA International's culture, combined with our background research, informed us of the design of a deliverable that would meet the organization's needs: a GDPR Knowledge Base. In this section, we will discuss the observations and findings that led to the development of this tool, the considerations our team considered while developing it, and an explanation of the tool itself.

As discussed in section 4.1, CWA International as the "older sibling" seeks to aid the other chapters in any way possible. The employees of CWA International expressed a strong interest in having a tool that was easy to share with its chapters (Appendix A.7). The GDPR Knowledge Base was designed for CWA International to share with the global CWA community, in a format that provides tools and materials and encourages collaboration.

The GDPR Knowledge Base is an interactive and easy-to-navigate alternative to presenting our recommendations in a lengthy PDF format. We chose Google Drive because CWA currently utilizes G Suite for its operations, and it allows for easy sharing of the recommendations and resources with other CWA branches. The GDPR Knowledge Base will be formatted in a nested folder structure, where the Knowledge Base itself is contained within a single master folder. A single How-To-Use file will be contained in the master folder. This file, shown in Fig. 8, contains a disclaimer that the recommendations

are not legal advice and that they were developed specifically for CWA International, along with a table of contents for each of the topics covered in the Knowledge Base.

How To Use the GDPR Knowledge Base

Welcome to Cycling Without Age International’s GDPR Knowledge Base. This Knowledge Base contains a series of folders, each covering a different topic of GDPR. The list of folders should *not* be used as a comprehensive list of all GDPR topics, as the folders represent only topics focused on during an internal CWA International GDPR compliance project. The left column of the chart below contains the list of each topic covered in the GDPR Knowledge Base. Clicking on the topic will reveal a link to the named folder, which contains resources to assist in compliance in that topic. The right column of the chart contains a list of links to the respective documents that list out our recommendations on the topic.

Please note that this is *not* a complete list of every necessary step needed for GDPR compliance, but a collection of resources that were utilized during a CWA International GDPR compliance project. All of the recommendations and resources were created or found by a team of researchers from the Worcester Polytechnic Institute working with CWA International in the Spring of 2022. We hope that these resources can be of use to your organization. **The recommendations and sources provided are not legal advice and are not designed to replace any legal advice.**

Topic	Recommendations / Resources
User Rights (Chapter 3)	See here
Cookie Consent (Articles 6, 7, and 30)	See here
Lawfulness of Processing & User Consent (Article 6 & 7)	See here
Proof of Compliance (Article 30)	See here
Security Practices (Articles 25 and 32)	See here
DPIA Procedure and DPO's (Articles 35, 37, 38, and 39)	See here for DPIA Procedure See here for DPO Information

Figure 8: How-To-Use document at the top of the GDPR Knowledge Base

In addition to the How-To-Use document, the Knowledge Base will have a subfolder for each topic covered, as shown in Fig. 9. These six topics became our focus points because they were identified as areas of non-compliance within CWA’s data processing. The table of contents links directly to the folders on the left column and to the recommendation documents on the right column. Recommendations were written to be as clear and straightforward as possible so that anyone who is unfamiliar with GDPR can understand them. In addition to the recommendation documents, the subfolders also contain useful materials or resources our team found. All of these are free and open-source, and many have already been used by other organizations to become GDPR compliant. Figure 10 shows an example of what a subfolder layout looks like.

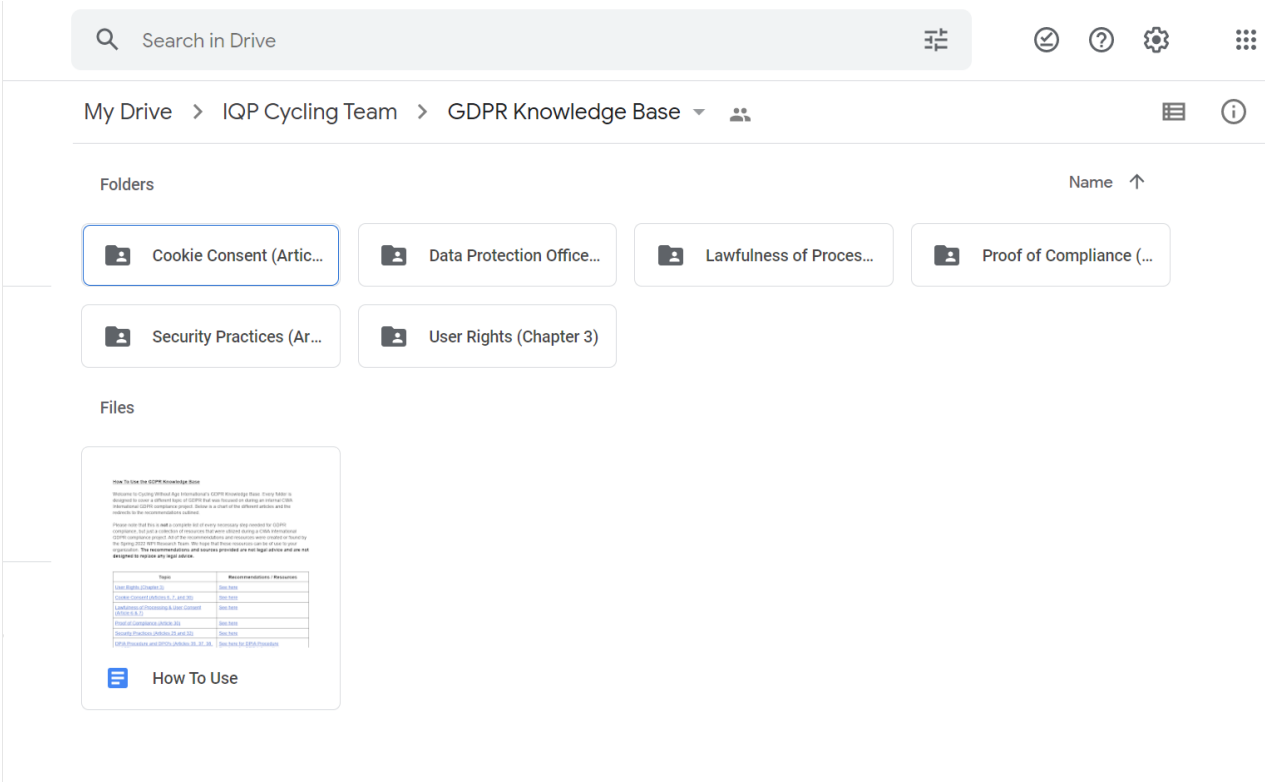


Figure 9: The layout of the master folder at the top of the GDPR Knowledge Base

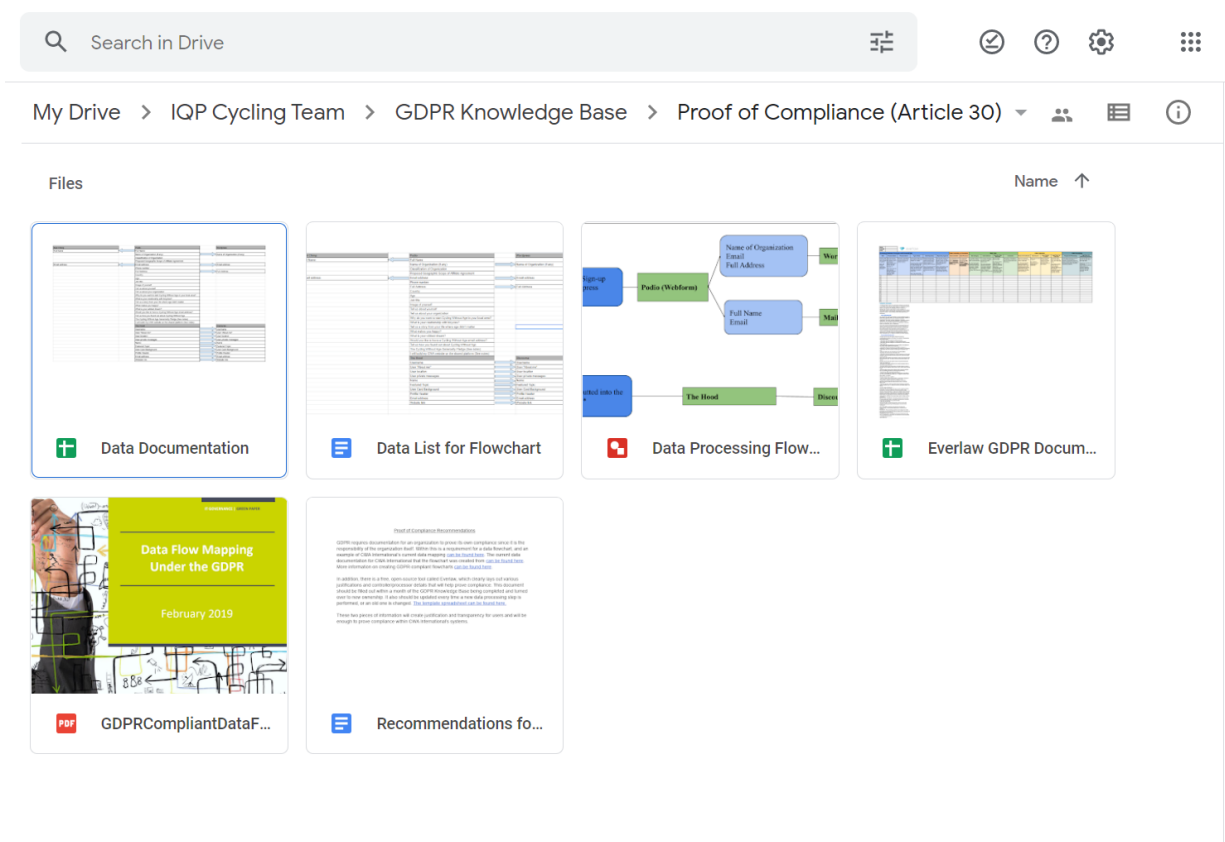
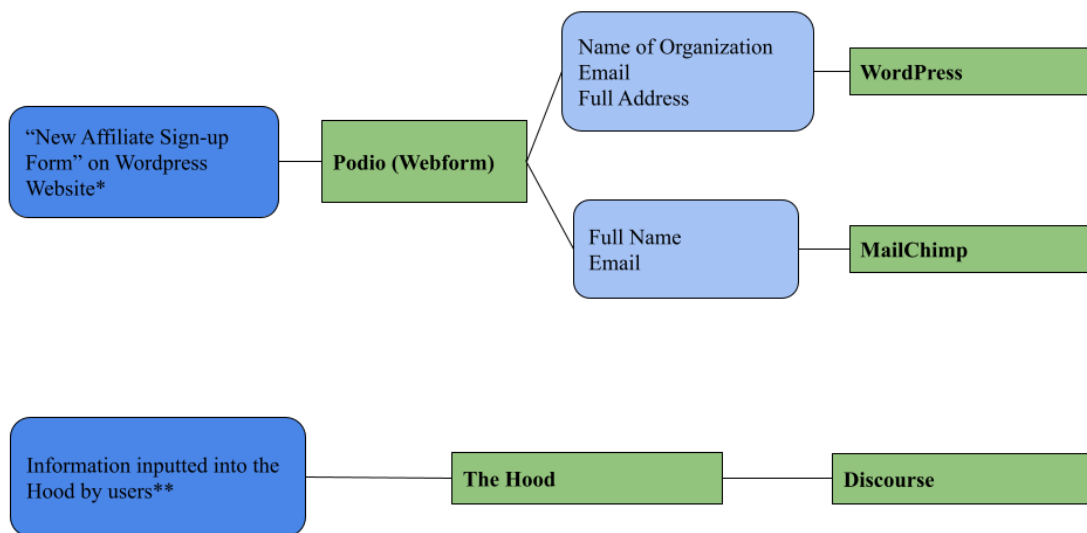


Figure 10: The layout of one topic's subfolder within the GDPR Knowledge Base

4.3 THE DATA FLOW THROUGH CWA INTERNATIONAL'S SYSTEMS

From our cataloging methods described in section 3.2, we were able to create a data flow diagram of the way data moves through CWA International's systems. As seen in Fig. 11, we will explain the data flow through each system in the subsections below.



*See Appendix C for list of all information on the New Affiliate Sign-Up Form

** See Appendix D for list of all information inputted into the Hood by users

Figure 11: Data flow diagram

4.3.1 PODIO

The majority of the currently utilized data that moves throughout CWA International's data systems comes from the New Affiliate Sign-Up Form. The sign-up form is located on CWA International's main website, underneath the "Getting Started" tab, on a page titled "Becoming an Affiliate". This form collects a variety of items, such as names, full addresses, and some personality questions.

When the user submits the new affiliate sign-up form on the CWA International website, the information gets stored in CWA International's primary database software, Podio. CWA International's Podio platform is cloud-hosted, yet CWA International does

not pay for the software access. The company that owns Podio, Citrix, allows CWA to have access for free.

4.3.2 WORDPRESS

CWA International’s website runs on a WordPress framework. The main part of the data collection and storage on WordPress comes from GravityForms, a plug-in installed on the site. GravityForms maintains any forms and submissions that an administrator would create and post. The data stays in the plug-in and is not encrypted and is private to everyone but the editors, who can edit anything on the site, or administrators, who can not only edit but also have access to the back end of the site.

Another aspect of the WordPress site that the CWA International team has stated they value highly is the CWA global map, shown in Fig. 12.

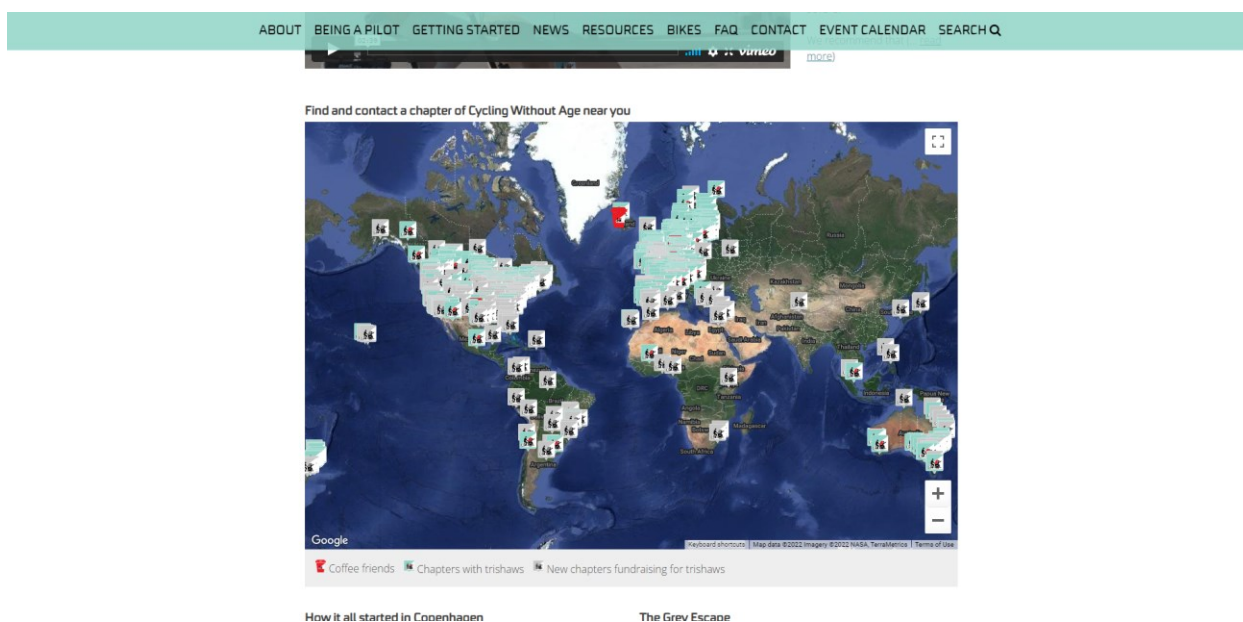


Figure 12: The CWA global map

The CWA global map is an interactive feature of CWA International’s website where users can explore the map and find local chapters of CWA all over the globe. Clicking on one of the pins allows a visitor to see details about the CWA chapter, including the name of the organization, the email address of the affiliate who leads the chapter, and the full address of the organization. These three pieces of user data from the global map are manually copied by the Global Community Captain from the Podio database that

stores the results of the new affiliate sign-up form.

4.3.3 MAILCHIMP AND THE HOOD

In addition to the data that is copied from Podio into WordPress, CWA International has another system that stores personal data copied from the Podio database. The platform utilized for managing the CWA newsletter, Mailchimp, also stores the full names and email addresses of affiliates. These two pieces of information are also manually copied by the Global Community Captain.

The secondary source of user data originates when affiliates create accounts on CWA International's global information sharing platform called The Hood. Personal information, such as the user's name, email address, and more are collected in the sign-up process and stored in the Hood itself (See Appendix C) The personal data stored in The Hood is also shared with Discourse, the platform that The Hood runs on.

4.4 POINTS OF DIVERGENCE FROM GDPR WITHIN CWA INTERNATIONAL'S SYSTEMS

Using the divergence spreadsheet described in Section 3.3, we identified areas of non-compliance in CWA International's systems. Similar to the Divergence Spreadsheet, this section groups together GDPR issues by either system or topic. The four main systems all had their individual non-compliance issues grouped by software platform rather than topic. Issues that pertained to multiple of these software systems were grouped by the general topic they belong to. Each section also includes how the area of non-compliance relates to CWA and how the recommendation fits CWA.

4.4.1 SYSTEM-SPECIFIC GDPR DIVERGENCE

4.4.1.A PODIO

The main area of noncompliance within Podio was the databases. These databases store personal information from various origins, the main one being the New Affiliate Form. First, we identified that one of CWA International databases was a residual workspace from when CWA was formed. It held information pertaining to a separate organization from a time -it was less clearly independent from CWA International. GDPR article 32 section 2 states that steps need to be taken to reduce the risk of unauthorized access to personal data. CWA International Podio administrators can access personal user data from another organization that they are not authorized to view.

The CWA International Podio workspace has several databases other than the “New Affiliates” database which contain user data with no plans for further utilization. These databases were created for temporary projects, such as when Cycling Without Age was accepting orders for a book, they had published in 2017. Personal data including names, email addresses, and full addresses were collected and stored. GDPR article 5, section 1, subsection e, states that data should not be stored for longer than is needed to complete the task outlined to the user.

Some of the Podio workspace administrators are employed by other CWA partners, which are legally distinct entities from CWA International. Currently, no legal document dictates how the Podio administrators from other CWA partner chapters are allowed to utilize the data. GDPR article 26, section 1 states that in instances where two or more legally separate entities jointly control data, there needs to exist a contract that defines the parameters by which they are allowed to utilize the data.

Another area of GDPR noncompliance we found within the Podio platform was the number of workspace administrators. The Podio workspace for CWA International has seven administrators; CWA International only has two employees. The remaining five individuals are people who work for other CWA partner chapters. Article 32, section 2 states that systems need to be designed to reduce the risk of unauthorized access to stored

personal data. Having so many administrator accounts that can access the stored personal data, especially when the administrators do not work for CWA International, qualifies as a data risk. If one of the administrator's accounts became compromised, the data would be as well.

Additionally, there is data stored within the “New Affiliates” database in the Podio workspace with no current or future plans to use this information. The personal stories and photos, contributed by affiliates when filling out the New Affiliate Sign-Up Form (Appendix B), were initially utilized by Cycling Without Age International to help approve affiliate applications. This information is not utilized after the affiliate is approved to start a chapter, yet it is still stored in its databases. GDPR article 5, section 1, subsection e, states that data should not be stored for longer than is needed to complete the task outlined to the user.

Lastly, the CWA International Podio administrators have access to the Podio workspaces of other CWA chapters. Article 26, section 1 states that in instances where two or more legally separate entities jointly control data, there needs to exist a contract that defines the parameters by which they are allowed to utilize the data.

4.4.1.B WORDPRESS

Cycling Without Age International stores personal data in two places on the main WordPress site: the world map (Fig. 10) and the various forms in GravityForms². The map displays personally identifiable information, such as addresses and emails, that is accessible from the main website. Article 6 states that users must give consent for their information to be managed or used in specific ways. Chapter 3 describes user rights and discusses how data subjects need to be aware of how their data is processed early in the procedure.

² GravityForms is a WordPress plug-in that makes using forms on the site easier. It assists in building and implementing the forms in an easy understandable way.

The GravityForms plug-in collects submissions posted on their site. These forms are outdated, as all of them were created between 2015 and 2019, and most do not have any submissions more recent than 2020. Article 5, section 1, subsection e, states that data should not be stored for longer than is needed to complete the task outlined to the user.

CWA International does not currently have a protocol for granting WordPress administrator accounts, criteria for user addition, or rules for the level of access users have. If an individual wants to create a post, they ask CWA International, and will typically be granted permission without any formal process. In some cases, individuals were granted several levels of access higher than necessary for the tasks they performed on the site. In addition, users that no longer need access or are not with the organization have retained administrative privileges. As a result, the website has almost 50 administrators with editing/creating access. Personal information stored on the map and in the forms can be viewed by anyone with access. Under article 32, data handlers are responsible for ensuring the confidentiality and protection of their system and steps should be taken to reduce the risk of unauthorized administrators.

4.4.1.C THE HOOD

The amount of information collected by CWA International's current use of The Hood is minimal. There are administrator accounts that belong to individuals no longer associated with CWA International. This is not in compliance with article 32 section 2, which states that steps need to be taken to reduce the risk of unauthorized access to stored personal data. The Hood's privacy policy and cookie consent policy are up to date, transparent, and GDPR compliant by Discourse and site design.

4.4.1.D MAILCHIMP

While MailChimp does store some personal data, the website itself has layers of data protection already embedded. There are 9 legal documents that outline the security measures taken by the site, including privacy policy, terms of use, and cookie statements. Each of these documents outlines how the data that CWA International adds is protected, and therefore we do not have any recommendations for compliance with this system.

4.4.2 GENERAL GDPR DIVERGENCE

4.4.2.A LAWFULNESS OF PROCESSING & USER CONSENT

Article 6 of GDPR outlines the six conditions in which data processing is legally permitted. One of the commonly utilized legal data processing conditions is the sixth condition, found in section 1, subsection f, of article 6. This condition states that processing is legal if the processing is necessary for the “legitimate interests pursued by the controller”, and that the processing is the minimal amount that can be conducted in order to achieve the given goal. CWA International’s new affiliate sign-up form currently collects and stores several pieces of personal data, such as the photos of the affiliates, that is not necessary for CWA International to perform its functions. This is not in compliance with article 6, as CWA International is collecting and storing photos without any justification.

Article 7 of GDPR explains how users must give consent for the processing of their personal data to be legal. Article 7 section 1 states how it is the data processor’s responsibility to demonstrate that the user gave consent for their data to be processed. CWA International does not currently ask for or keep records of users’ consent for their data to be processed. Additionally, article 7 section 3 states that users must be able to withdraw their consent at any time, which is not a service that CWA International currently provides.

4.4.2.B USERS’ RIGHTS

Chapter 3 of GDPR (articles 12-23) covers the different rights that a user has over their personal data³. CWA International’s data processing practices currently do not have systems in place to ensure the protection of these rights. Article 12 states that users have a right to transparent communication from the controllers and processors.

³ See Fig. 2 in Section 2.1

Article 13 states that when personal data is collected, the data controller must provide the data subject with contact information for the controller, legal justification for collecting and processing the data, information on who, if any, the collected information will be shared with, the period for how long the data will be stored for, as well as the way that the user can revoke or modify their consent in the future. Article 15 outlines that data subjects have the right to confirm the processing of their own data and access to the data. In addition, it also outlines the rights that are listed in the other articles to ensure all of chapter 3 is complying.

Articles 16, 17, and 18 all cover the rights that the subject has towards the processing and information. Article 16 states that users have the right to fix any issues with the processing, including correcting information. Article 17 states that the user has the right to request any erasure of the information that exists. Article 18 discusses that the user can restrict or object to the processing at any point. Article 19 covers the three articles previously discussed, emphasizing again the user's rights and the communication that follows. The controller must effectively communicate any changes to the recipients of the information, and to the data subject if they request it, which is currently not possible on CWA International's systems.

Article 20 states that when distributing personal data to the data subject or other controllers, it must be in a clear, machine-readable fashion. Article 21 outlines the right to object by the data subject so that the processing is suspended unless the controller can provide sufficient need to continue processing. Finally, article 22 says that users cannot be subject to solely automated decision making or profiling, meaning that there must be some human interaction involved in the decision-making process. Articles 14 and 23 do not apply to what CWA does in its organization.

4.4.2.C SECURITY PRACTICES

Article 32 of GDPR covers general cybersecurity practices, and states that care needs to be taken to ensure the “ongoing confidentiality, integrity, availability, and resilience of processing systems”. There are some areas in which CWA International's systems and practices could be updated to align with article 32. CWA International does

not currently take routine backups of its systems. This increases the impact that ransomware and malicious software could have on CWA International systems and could make its stored user data a bigger target for attackers.

Currently, administrators are not required to have two-factor authentication on their accounts. Given the access that these platform administrators must store personal data, this increases the likelihood that administrator accounts could be compromised and jeopardize the stored personal user data.

Additionally, there is not an internal password policy for CWA International employees. No procedure exists that mandates a minimum password length, dictates whether employee passwords are allowed to be reused on different platforms, or how often passwords should be changed. This places CWA International employees at higher risk for account compromise. There is also not a procedure within CWA International for keeping IT systems up to date. No policy exists for requiring that personal computers receive the latest operating system updates or that software tools utilized by CWA International are kept up to date. This is a security vulnerability, as a malicious actor may target CWA International's personal data, and without updated security patches, systems can be attacked easier.

Article 25 covers the general security procedures of an organization. CWA International employees lack formal cybersecurity awareness training, which means they may be more vulnerable to social engineering attacks such as phishing⁴. CWA International does not require that employees enable encryption on the hard drives of personal laptops. If an employee laptop were stolen, it would be easier for an attacker to extract personal user data from the employee's laptop. CWA International employees are also not required to have up-to-date antivirus software installed on personal devices. Without antivirus software, these devices have a greater likelihood of getting infected with

⁴ Phishing is a technique attackers may use to gain access to someone's passwords, by using social engineering techniques to trick a target into entering their password in a malicious website

malicious software that, if gone unnoticed, could compromise sensitive user information or steal passwords to administrator accounts with access to personal data.

Finally, CWA International does not currently have a secure location in its office for physical documents with personal information on it. In the event of an office break-in, an intruder would be able to steal documents with user data on them, which can be considered a data protection threat under article 25.

4.4.2.D PROOF OF COMPLIANCE

GDPR article 30 states that organizations must have documentation to prove their compliance with the GDPR law to provide to regulators if requested. CWA International does not currently have documentation to prove its compliance.

4.4.2.E CONSENT FOR COOKIES

Various GDPR articles dictate that users need to have the ability to accept, decline, or manage the permissions for cookies they want for the website⁵. Article 6 states that data should be processed with integrity and confidentiality, and by not having a consent option for users it is not compliant with GDPR. ⁶ in a visitor's browser without first asking for consent from the users. Under article 7, organizations need proof of consent for data they are processing; cookies also require written consent. Article 30 states that data being processed should be recorded for the regulators to check compliance.

4.4.2.F DPO REQUIREMENT & DPIA PROCEDURE

Per article 37 of GDPR, certain conditions exist in which an organization must appoint a Data Protection Officer (DPO). CWA International is not a public authority, does

⁵ A cookie is a cache of information placed in a user's browser that websites use to retain user preferences and former actions on the site.

not process data in a scope that requires regular and systematic monitoring of users on a large scale, and does not process data relating to criminal offenses or other protected data types. Therefore, CWA does not need to appoint a DPO.

Per article 35 of GDPR, Data Protection Impact Assessments (DPIAs) must be performed when organizations are processing data that is considered under GDPR to be “high risk.”⁷ At the time of this report, we determined that CWA International does not collect or store high-risk data, does not need to conduct a DPIA, and is not in violation of article 35. However, Appendix K goes over the process for DPIA and needing a DPO.

⁷ For more a list of the kinds of processing defined as “high-risk”, consult “Examples of processing 'likely to result in high risk'. ICO. (n.d).”, found in References

RECOMMENDATIONS

5.1 SYSTEM-SPECIFIC RECOMMENDATIONS

Combining our cultural findings with our data processing and divergence findings was the last step in creating our recommendations for CWA International. Our recommendations were compiled in this section in the same format as above: first by the primary systems, then by topics that span multiple platforms.

5.1.1 PODIO

Move non-CWA databases out of the CWA International Podio workspace and delete databases that do not have current or future to be utilized. The database belonging to the CWA founder's other organization should not be located within the CWA International Podio workspace. We believe this recommendation will not only support GDPR compliance, but also support CWA International's desire to make their processes more efficient overall by acting as a type of "Spring Cleaning".

Remove workspace administrators that are not employed by CWA International where possible and create "Joint Controller Agreements" for administrators that cannot be removed without negative impacts. This recommendation is based on our finding that CWA International values their personal relationships with their partners and affiliates. In instances where sharing the same Podio workspace is a part of this personal relationship, the Joint Controller Agreement may be the GDPR-compliant solution. This draws on our finding that CWA International values its non-hierarchical structure, and in some cases the removal of another CWA partner from the Podio workspace may be perceived by some partners as CWA International overstepping their power.

Delete pieces of information within the "New Affiliates" database that have no current or planned use. This recommendation draws from the fifth cultural finding, as it allows CWA International to "clean up" their Podio workspace and improve their efficiency.

CWA International employees should leave the Podio workspaces of other legally distinct chapters where possible and create “Joint Controller Agreements” for accounts that cannot leave without negative impacts. Employees should only leave if it will not have a negative impact on their relationship or the performance of their duties. This recommendation achieves GDPR compliance, while minimizing the impact on the core aspects of the CWA International culture.

5.1.2 WORDPRESS

Remove affiliates’ personally identifiable information from the map. We suggest that the home addresses be completely removed from the map, and that a chapter-specific CWA email replace any personal emails listed. The recommendation to modify the map, instead of deleting it, was advised by the Global Community Captain; they emphasized the value of the map as a tool that helps connect people who are interested in getting involved with CWA to contacts within their community (Appendix A.7). This decision was also supported by our cultural finding that CWA International takes action to reinforce its guiding principles; we wanted to keep the guiding principle of *Relationship* in mind when recommending that GDPR compliant.

Routinely delete WordPress forms that contain personal data with no current or future plans for utilization, and periodically remove the personal data from utilized forms. The team recommends CWA International adopts a policy of checking active Gravity Forms for new entries once every six months. If there are any entries during this check, it is recommended to move the entry off WordPress, where many administrators exist, to a more secure platform such as Podio or Google Drive. Additionally, it is recommended that forms that have not received entries in two and a half years or more should be deleted from the website entirely. These recommendations draw from the finding of the way CWA International views themselves at the same level as other partners and chapters. Giving forms a two-and-a-half-year grace period before they are deleted minimizes the chance that partners and chapters with editing access who may have made forms on the website will feel that CWA International is overstepping their boundaries by deleting their content. This presents CWA International another opportunity for GDPR to improve and

simplify their systems, as recommending a routine “six-month cleaning” of Gravity Form entries not only helps GDPR compliance, but also reduces clutter and unnecessary data on WordPress.

Implement a procedure for determining the access level of new WordPress accounts, train new editors in good WordPress practices, and routinely remove unneeded administrators. This procedure should contain a list of criteria that an individual must meet in order to be promoted to the next level of access. For example, if an individual reaches out to CWA International requesting WordPress access to make a blog post, CWA International should be able to refer to their procedure as to what level of access this user will be granted. The user would then be granted the lowest level of access that allows them to achieve their objective. The training for new WordPress accounts should outline how to use the platform, as well as what rules to follow to prevent accidental content deletion or erasure. The periodic review of the WordPress accounts should feature the removal of any accounts whose WordPress access is no longer necessary. This review should be carried out once every six months. These recommendations are based on CWA International’s excitement towards GDPR being an opportunity to make their practices more efficient and more effective and having formal procedures in place should save CWA International employees time when providing access.

5.1.3 THE HOOD

Remove unnecessary administrator and residual test accounts. The accounts of the original creators of The Hood, members who are no longer a part of CWA, and several other unnecessary administrator accounts exist, as outlined in the Divergence Spreadsheet. Test accounts were utilized during the initial creation of The Hood, but no longer serve any purpose. Deleting these users will minimize the chance that one of these accounts becomes compromised. This is also recommended because of the finding that CWA International views GDPR compliance as an opportunity to make processes more effective and efficient.

5.2 GENERAL GDPR COMPLIANCE RECOMMENDATIONS

This section details our recommendations for areas of GDPR compliance that are not tied to specific databases but are more general GDPR recommendations. Each section is divided into subcategories, some spanning multiple articles. Below, we state the key recommendations, as well as our reasoning for choosing these recommendations.

5.2.1 LAWFULNESS OF PROCESSING & USER CONSENT

Change the process for new affiliate applicants to store fewer personal data and be more personable. The current new affiliate signs up form posted on the CWA website should be edited such that it only collects the full name and email address of the applicant. The form should also have an area where the new affiliate can consent to their data being collected through the form and can agree to the CWA Generosity Pledge. Each of these selectors should include both a “Yes” and a “No” button, in order to properly constitute consent. Additionally, this form should have a “file upload” button, where an applicant can submit a 3–5-minute video of themselves answering a series of personal interview questions. A reformatted proposal of the questions can be found as part of Appendix H. The Global Community Captain can then review the uploaded video and decide whether to approve the new applicant to start a CWA chapter. In the event of rejection, the Global Community Captain should notify the applicant over email. The applicant’s name and email address should then be stored for a period of no more than 3 years, to minimize the risk of repetitive spamming of applications. In the event of approval, the Global Community Captain should notify the applicant over email and send along a second form that would then collect the personal information that CWA needs from that applicant, such as the name of the organization the affiliate represents (if any), the city that the affiliate is operating out of, and the phone number of the affiliate. Regardless of whether the applicant is approved or rejected, the video of the applicant will be deleted out of the database immediately after the decision has been made. This new video application process was recommended because it is in line with CWA International’s belief that they are the “protectors of the values” regarding the rest of the CWA movement. Implementing a video application allows the Global Community Captain to have a more personable evaluation of the applicant and can decide based on the video

whether the applicant is a good fit for CWA and if they represent the values that CWA International holds in such high regard. Additionally, the video application provides an opportunity for CWA International to start off their relationship with this new chapter in a way that favors the personal relationship between them.

5.2.2 USERS' RIGHTS

[Creating a public Privacy Policy on the CWA International website that follows the 11 articles of Chapter 3 of GDPR.](#) The Privacy Policy should serve as a transparent way to show users what exactly is being done to their data and what rights they have regarding the processing. We recommend utilizing the Privacy Policy template that we created (Appendix J). This template was adopted from an open-source Privacy Policy template and edited so that the policy was relevant to the data processing practices of CWA International. In addition, the CWA-specific version has green highlighted sections where we recommend CWA International employees fill out the information specific to their organization. There are also yellow highlighted sections that are for areas that must be added or written by CWA International. All of these items will be added by CWA International's team with specific regards for how they use their data processing. This recommendation was selected because while it is slightly tedious, it is a comprehensive aspect of compliance. This was also recommended to support the fourth cultural finding, CWA being the protector of values. The organization cares about protecting the image of other branches and themselves, and by adding a transparent privacy policy, it will present as more forthcoming and trustworthy to those it collaborates with.

5.2.3 SECURITY PRACTICES

[Back up Podio databases regularly.](#) This protects against breaches and accidental deletion because the data will be stored in a secondary location elsewhere. step-by-step procedure we created that explains how to single out a database on Podio and back it up to Excel while making sure it is password protected (See Appendix G.3 & G.4). Alternatively, there is another option, which is to use an automated backup tool called Momentum Tools.

This is a more automatic way to accomplish the same process as above, but it is a paid software.

Podio administrators should read and sign a statement highlighting the importance of protecting their account and the data they have access to. It should outline the responsibilities and privileges that an administrator account has (see Appendix G.1). This falls into our cultural finding of CWA protecting their values so that they are protecting their image by having all of the administrators on the same page.

Administrators should be required to change passwords every 90 days (about 3 months) and to enable Two-Factor Authentication (2FA). Podio itself has a help page that can be utilized to set up 2FA on CWA's Podio, and it requires a smartphone app. Google Authenticator is the recommended platform, although others can be used.

Personal devices should have their hard drives encrypted and run antivirus software and the most up-to-date firmware. This protects any personal information stored on the device in the event it is stolen, as well as reduce the likelihood of a malicious actor utilizing technical exploits to steal personal data. Malwarebytes is antivirus software that should be utilized across personal devices. It is recommended that the help articles linked in the Knowledge Base document for this are followed (See Appendix G.2).

Podio, WordPress, and The Hood administrators should go through annual cybersecurity training. The recommended platform is to use Wizer training, which has a free awareness course that covers a broad range of topics in a short amount of time.

All sensitive documents should be secured inside a locked filing cabinet on the office premises. The cabinet should be locked with a single key that a single individual has access to. This will keep all physical documents containing personal data as safe from theft as possible.

5.2.4 PROOF OF COMPLIANCE

After implementing all other recommendations, the open source GDPR proof of compliance spreadsheet published by Everlaw should be filled out. This spreadsheet can

be found in the Knowledge Database. Our team's recommendation for CWA International to utilize Everlaw's spreadsheet as opposed to using a more traditional proof of compliance tool such as Lexoforms, is due to the resource being free and open source, which allows CWA International to share the tool with their other chapters and partners. The recommendation to do this draws heavily from our finding regarding CWA International's valuing of their non-hierarchical structure, and their valuing of being able to share materials and resources with their chapters.

[Maintain an up-to-date data cataloging spreadsheet and data processing flow chart.](#)

These recommendations will help CWA International present their data processing practices to GDPR auditors if needed. The recommendation to maintain an updated version of these documents is based on our team's cultural findings regarding CWA International's views towards GDPR compliance as an opportunity to make their practices more organized and effective.

5.2.5 CONSENT FOR COOKIES

[Add the Cookie Notice plug-in to WordPress.](#) This plug-in can easily be installed to the WordPress site so that a pop-up will appear on the page allowing users to consent, decline, or manage the cookies that the site uses. This is a straightforward way to meet compliance since the WordPress site already has plug-ins installed and administrators are familiar with them. Settings can also be customized after they have been set, which makes it quite simple to use or edit. This procedure has been documented in our Knowledge Base (see Appendix E).

5.2.6 DPO REQUIREMENT & DPIA PROCEDURE

[Review requirements for needing to appoint DPO and having DPIA procedures.](#)

While CWA International currently does not need any DPIA procedures or Data Protection Officers, we still compiled information and recommendations for their organization (see Appendix K) if there comes a time when the organization will need this procedure or a DPO. We created these recommendations and compiled resources because although the international chapter does not immediately have a use for them, other

branches of CWA likely will. Once the Knowledge Base is sent out, other branches can utilize the shared resources within it. This recommendation fits well with our third cultural finding in which CWA International has an “older sibling” mentality for the other chapters worldwide, where they strive to help other chapters wherever possible.

APPENDICES

APPENDIX A – INTERVIEWS

A.1: INTERVIEW WITH CYKLING UDEN ALDER IT DIRECTOR SCRIPT

The following interview script was utilized to interview the IT Director for CWA Denmark. This interview will be conducted over Zoom.

We are a team from WPI working with CWA International to recommend lasting changes to adapt CWA's data processing procedures such that they meet GDPR regulations, while still remaining consistent with CWA's mission and values. We are attempting to analyze CWA's organizational structure and culture in order to ensure that our recommendations are easy to implement and do not strip away any of the unique human connection that CWA uniquely develops.

We had some questions for the Global Community Captain about CWA's current GDPR compliance situation, and they recommended that we speak to you with some of these questions as well.

Firstly, would you mind sharing with us what your role is at CWA and what types of work you do on a day-to-day basis?

Would you mind giving us a walkthrough of how you feel CWA stands in terms of GDPR compliance and cybersecurity? Can you elaborate on what work has been done to develop this field in the past and how involved you have been?

What do you believe are the primary obstacles in CWA's path to GDPR compliance?

Were you involved with CWA working with Sixtus in 2020 to achieve GDPR compliance? If so, can you comment a bit about what your involvement was?

Pernille mentioned you had some ideas towards overhauling the map on the website. Could you talk a bit about that? What issues do you see with the current map, and what places for improvement can you identify?

Can you discuss your work with Book2Go?

Do you have anything else to add that may not have touched on relevant to GDPR compliance that you believe could be valuable to our team?

Thank you so much for your time, this has been a really valuable interview for us, and we are looking forward to utilizing the information you have shared.

A.2: INTERVIEW WITH CYKLING UDEN ALDER IT DIRECTOR NOTES

Christian's role within CWA/CUA

Hired by CUA for 10 hrs a week + volunteering hours (8 hrs a week)

Volunteering with CWA, Not many people qualified to work with IT

Creates user accounts, G Suite access, administrators on The Hood

IT questions, WordPress, Book2Go– (Denmark, Sweden & in the States, changing)

Managing domains

Thoughts on GDPR compliance and cybersecurity? Has there been work to develop that in the past?

GDPR in the Danish organization

Hasn't been considered before

Not structured, moving towards them

People can see what is written in groups, which should only be visible to the people in those groups

→Compartmentalizing the data

What are, in your opinion, the biggest obstacles to CWA's GDPR compliance?

How GDPR runs presents challenges for volunteer based organizations

All about people volunteering, people giving free hours whenever they have them

→ Hard to have strict control of what they do and when they do it

→ Lots of access but not on how they manage that data, do they still need access?

→ People spread out globally no direct responsibility

(Can't disable people if they don't know people are still working on items)

How systems are being introduced into CWA

→ "Someone gets a good idea and then they just start doing it, no control on how it's set up, Who has access? How can we integrate?"

→ Lot of systems that people don't know about/have control of

→ Lack of overview, no direct way to set items up

→ The Hood, no documentation on how to see who has access to what

Christian has limited amount of time

Were you involved with Sixtus, CWA compliance

(No)

Website global & in Denmark

According to Christian, website needs to be remade

Access, data presented, functionality is old

Security-wise

Contact details on people who have/were active

Needs to be cleared out

More control over that data

Bike story, still there

Last date and after that stories disappear, archived etc

Maybe we can make a book? (Consent?)

All the websites are Wordpress

Hosted by company called Symbiotic

Anything else that would be valuable to know on helping CWA towards
GDPR compliance

Lot of systems

Lot of admin

Lot of people with access that they don't need

Consent that if you have admin rights you treat it as any other login

You should active 2FA as a default as an admin

No rules for sizes of passwords

A.3: INTERVIEW WITH CWA SCOTLAND CEO SCRIPT

Hello, we are a team of WPI students working with CWA International to make recommendations about their GDPR compliance. We had heard from the Global Community Captain that your chapter may have some experience with GDPR compliance, and we were wondering if you might have a few minutes to answer some questions about your experience that might help us in our work. If you have some time to meet in the near future we would love to speak with you.

Questions

What is your primary type of data collected (new affiliates, is it information about local chapters, pilot stuff, etc)

What work, if any, have you performed towards being GDPR compliant?

Dynamically ask questions to probe further into how their GDPR compliance is implemented

What is the procedure for when a new chapter in Scotland wants to startup?

a. Is there a form? If so, what is on the form?

What software / platforms do you use to manage, store, and access data?

Who has access to collected data? A set group of people or anyone?

b. How do you determine who receives access?

What limitations are there for data collection in order to be GDPR compliant?

Did you get to this point just through internal means or did you have assistance from an external consulting firm or auditor?

Do you have any additional ideas, comments, or suggestions that you believe may be relevant to our work that you wish to share?

Thank you so much for your time, this has been a really valuable interview for us, and we are looking forward to utilizing the information you have shared

A.4 INTERVIEW WITH CWA SCOTLAND CEO NOTES

Scotland is the only international chapter that is supported directly by their own government

a. Launched it as a small community group in Scotland

b. Would not operate in a normal way

i. To have access to any care facility, Scotland has a lot of rules and regulations

- ii. Would need to comply with Scotland laws before they could have any riders
 - c. All the chapters operate directly under the country chapter
 - i. Fully support them
 - ii. Organize all regulations for the smaller chapters
 - iii. They just need to comply
- 2. Government pays the headquarters
 - a. Every chapter is started by HQ and then becomes their own
 - i. Annual license
- 3. Collect a ton of data from the individual chapters
 - a. Name, personal address, etc.
 - b. Thousands of people's data
 - i. Volunteers go through a disclosure process
 - ii. No criminal or at-risk background
 - c. Very private, secure facility to store
 - i. All stored in head office (physical copies)
 - ii. Only the Scotland CWA CEO has access to it
 - iii. IT Specialist who ensures the cybersecurity is secure online (Paid monthly fee)
- 4. When Pilots join, fill out various different forms
 - a. Application
 - i. Work history
 - ii. Age
 - iii. Gender
 - iv. Address

- b. Signed declaration of health status
 - c. Photograph endorsement/permissions
 - i. Photographic ID
 - ii. Everyone has a fully trained volunteer
 - iii. Carry it around to endorse training is done
 - d. Insurance policy comes from government funds and the forms being signed
5. Works very well
- a. Enables all the chapters to feel local support
6. CWA Denmark
- a. Couldn't do it like them because UK has different restrictions
7. Scotland uses their own database (Not Podio)
- a. Use a CWA email for regular dialogues
 - b. But there's another database for confidentiality
 - c. Only paid staff
 - i. There's only 5 people on payroll but there are different levels
 - ii. CEO has most access, and others have some access but not as much
 - d. Mentioned microsoft database?
8. Public website
- a. Part of CWA International, want a presence there (pay for it)
 - b. Update their own pages
 - c. No individual data on the map
 - i. Organization data only

- d. Single person running the updates, others have some access but limited

9. Individuals reach out for starting chapters

- a. There are judgment calls made
- b. Don't support chapter started by an individual, only by groups
- c. People should want to help
- d. Can recognize there are people who aren't the right type of person to run it or shouldn't

10. Types of Questions asked on Form

- a. Application form is kept
- b. Meet personally with every chapter and the group that is coordinating
 - i. Could be Zoom
 - ii. Could be 2 people to 30 people
 - iii. Chatting with them, data isn't recorded
 - iv. Don't let chapters start without riding/driving the trishaw themselves
- c. Won't totally say no, but they'll discourage people from being the lead person
- d. A lot of the data in the application process isn't recorded, you're gaining personal perception
- e. "It's a lifestyle not a job"

11. Communication with CWA International

- a. Tension because Scotland is structured and CWA-I is less so
- b. Teams are widespread

12. Did interview for a US person

- a. Had interest in country chapters and discussed with them

13. Because Scotland chapter is a charity, they register charity reports and are audited annually (every new financial year)

A.5 INTERVIEW WITH PROFESSOR MIKE ELMES SCRIPT

We are working with a nonprofit organization named Cycling Without Age based out of Copenhagen, Denmark, which is looking to become GDPR compliant. GDPR, or the General Data Protection Regulation, is a law passed in the EU in May of 2018 that sets strict requirements for how data privacy and cybersecurity must be implemented in an organization. The organization has taken some steps to getting started on proving their compliance, but have hit roadblocks. Many of the attempts they've made to adjust their data collection methodology haven't stuck because consultants' recommendations have been more geared towards a traditional corporate organization, and haven't catered to their unique structure and culture. The organization defines their structure as a holacracy (feels loosely used), which has made it extra difficult to unify the organization in making changes towards GDPR compliance. The international office is very hesitant towards requiring changes from the smaller chapters, that they view as more independent organizations than an extension of themselves. Our team is trying to make recommendations for CWA to be more GDPR compliant, while ensuring recommendations account for their structure and culture. In order to accomplish this, we need to first evaluate their organizational culture in order to make recommendations that cater to it. We were hoping you could speak to us on things that are valuable to know when assessing an organization's culture, items to look for, and a few other questions. **We are looking for tools/ways of thinking for assessing their culture that can aid us in making choices for our recommendations that are more likely to stick because we understand how their organization "thinks" at a deeper level.**

What are important things to keep in mind when evaluating an organization's culture?

If you were working on this task, what approaches would you take?

Are you familiar with the OCAI assessment? If so, what are your thoughts on its effectiveness and its validity?

We are looking to use the information we gather on their culture to help advise us make these changes; when evaluating culture to create organization-specific recommendations, what would you keep in mind?

Do you have any experience with non-profits or charities?

Do you have any experience with holocracies? If so, do you mind talking to us about how to work with policy for holocracies that are looking to not be hierarchical but still enact change.

Do you have any other people we could speak to who might have some more insight on tackling problems like this?

A.6 INTERVIEW WITH PROFESSOR MIKE ELMES NOTES

Authority structure, units

CWA has a global spread

How many work directly with the core organization?

As a nonprofit in Copenhagen

It has to comply with the data policies

All the data they collect from the various organizations

Defined as a social movement

To fill a need, sense of passion

Compliance with GDPR seems trivial in comparison

Getting in the way of the movement

How difficult is it going to be for it to become compliant?

How do you describe the culture

Loosely coupled organization

In different countries, different laws

Organizational Culture

Values, rituals, symbols, ways in which they operate

What assumptions are they operating under?

(It's a complicated idea)

Not monolithic

Many cultures potentially in tension

Social Movement v. Culture of Regulation, protecting privacy rights

Similar organizations, decentered, social movements, holacracy

Regulatory agency

How do you deal with charities, what recommendations do you make for dealing with

these kinds of challenges?

Sometimes bureaucracies can be very helpful

How can we do this without drawing attention, the regulators

Not wanting to tell them what to do

Prof. Elmes has never used an organization survey

Culture analysis can be highly qualitative

Can talk about culture in terms of its uniformity and strength

Weak culture, subcultures, all do and believe their own thing

Strong culture

Structure & Culture

Structure is fragmented and loose, not strong ties between components

Is there a structure?

Sometimes culture fills in for that

Ex: Bureaucracy- structure rules the roost

Shared mission statement, vision for the future

Informal cultural things, rituals

Events/rituals they ignore?

Comparing structure

Different cultures versus different components

Will culture lead you to the promised land?

Do you have enough time to get everything you need?

Is culture the wrong focus?

If you have a fragmented organization, loose ties

Differentiation versus Integration

How do they tie together, connect?

Different groups different places

Sometimes they don't need to be connected...

For GDPR they do

There isn't a need for a lot of connection

Don't need to review each other

Decentralized organization

GDPR: Problem that requires some degree of centralization

Policies and practices

Move in a direction that protects us, you

We have some ideas on what to do, but we can't make this happen unless you are also involved

Crowdsourcing

Solution can only come from everybody talking to each other

Can't do it top-down

Highly decentralized structure, not in the interest of the organization

Can't just say we don't know what to do

Hey, we're serious about this but we know we need your help to make this viable

May be pride associated with this

Opening up channels of communication

We can't do this alone, everyone has to buy in

Come up with solutions, implement them

Can't work if it comes from the top down

Need everyone together in the problem-solving arena

Need everyone to feel as though it's important

→ We know a lot more about culture than we realize

Involving other people on The Hood, involving them to talk about the issue

Why this is so hard given the structure of the organization and the values held, why we need to involve others

If done well, end up with better solutions, the unifying factor of the voices

A.7 INTRODUCTORY INTERVIEW WITH GLOBAL COMMUNITY CAPTAIN

1. Sign-ups
 - a. Creating Relationships
 - b. Getting set-up
 - c. Can join as affiliates and then change your mind
 - d. Charity registrations

- e. Formal agreements
- 2. Partners/Country
 - a. Things are complicated, not strict rules
 - b. No exclusivity mindset
 - i. In theory, someone could say “we want to start our own thing” CWA couldn’t stop them
 - ii. There’s no exclusivity– but it’s hard to compete with an existing organization
 - iii. German organization– v. someone who wants to do something simple
 - iv. Sometimes these individuals don’t seem welcome
 - c. Chapters v. partners
 - i. Diplomatic problem– chain of command cutting
 - d. Partners don’t have their own link for signup
 - i. Need a partner agreement
 - ii. Need a map of some degree
 - iii. (Most) partners have signed the affiliate agreement
 - iv. Encourage all of the partners to send in for accounting
 - v. via Discourse platform the Hood
 - vi. The partners (10 total)-- they don’t always like to be frequently reminded
 - vii. Putting a link on the Hood where they ask the partners to send the info had a high degree of success (lots & lots of people sent in info, including affiliates!)
 - 1. Were not obliged to send in info, but had a large turnout, Get a lot more impact reports
 - 2. Don’t always have to differ between smaller and larger setups
 - 3. Formal contract is for risk with fraud with more people
 - viii. Info in the reports
 - 1. Financial
 - 2. Data– how many rides how many pilots
 - 3. What do we really want with these numbers?
 - a. Made it a little more philosophical (need a justification)
 - b. Demographics- what communities are you impacting?
How do you even begin to ask that?

- c. Don't want to impose things on anyone?
 - e. Lots of diplomacy necessary
 - f. Contract with partners
 - i. Want to see this as a global community
 - g. Discussions on Scotland
 - i. Supported by govt
 - 1. NGO v govt funding??
 - 2. Partnering with state or individual
 - 3. If you receive state funding– censorship
 - 4. The govt can decide- govt owned nursing homes
 - ii. Communication with the Scotland group
 - 1. Concerns on losing state support
 - 2. They have to send in a report to the government of Scotland
 - 3. They said they'd send impact report to CWA in April after they had done their own filing, when requested by CWA-I in for February
 - 4. Contract said– want to know who's on the board, etc., chain of communication, (just one person) no email address
 - 5. Concern from Scottish group head of passing along PII
 - 6. Is the Scotland chapter already GDPR compliant?
3. GDPR
- a. Perspective that as long as there are large corporations not complying, CWA is “small-time”
 - b. Showing that CWA-I can protect the movement
 - Need to reduce contact details available on the website
4. Other observations
- i. Terms of the contract need clarification
 - ii. On podio, on the hood
 - iii. Protection of the organization from the up-top
 - iv. Things are very delocalized by design, but how do you keep communication channels open?
5. *“Guardians of the principles”* Sweet older brother, but maybe we need to protect the younger sibling.

- a. What is need to know for CWA international, for communication?
 - i. How can we reduce the data that gets “upstairs?”
 - ii. Use this as an oppurtunity to express desired culture, could be a way to be open and follow the rules at the same time
 - iii. 4+ platforms, but everyone is able to use all the platforms for free
 - iv. It would mean that all the affiliates are required to be in the same universe, and nobody can be hid (fraud protection) (this protects everybody, social contract)
- b. Social contract
 - 1. Still want people to be able to use the name– but maybe flexibility isn’t always what ensures endurance
 - 2. Affiliates sign the form (CA, US, Germany, UK)
 - 3. A degree of protection
- c. Finding how people save data right now
 - i. Google drive/ personal v public
 - ii. A lot of people don’t know Podio exists
 - iii. Grown very quickly with varying information given
- d. Agreements
 - i. GCC will be sending us agreements from other groups

A.8 DATA HANDLER INTERVIEW WITH THE GLOBAL COMMUNITY CAPTAIN QUESTIONS

Questions 1-5 were asked during Data Handler Interview #1, and all else were resolved through other discussions or addressed in Data Handler Interview #2

1. What kinds of information collection do you perform? Are any of these data collection correspondances performed on a repeating basis?
2. What forms of contact information do you collect / store? What is this contact information used for? How often is it actually utilized?
3. What data from partners / affiliates do you need to collect / store in order to perform your operations?
4. What data from partners / affiliates is collected? Is any of the collected data not strictly necessary to perform your operations?
5. Is there a master list of all types of data that CWA collects / stores?
6. When data is collected from affiliates on the key platforms, is there anyone else the data is shared with?
7. When chapters sign up, what types of disclosure or checks for consent are in place (if any) before they enter in data? If so, is there a way for users to withdraw consent?
8. How is the access to these software / platforms distributed and managed?
9. How long does CWA keep the data in the system that is used? Is there a way for users to request their data to be deleted? If so, is this procedure documented?
10. Do you have an up-to-date privacy policy that your website visitors can view? If so, what is contained within it? If so, is there a process for notifying users when it is updated?
11. Does CWA have a Data Protection Officer? (DPO)
12. Is there any data protection training for CWA employees?
13. Is there a protocol in place for ensuring that technical cybersecurity is up to date?

14. Is there a protocol in place in the event of a data breach/all data is gone?

15. Do you have any additional ideas, comments, or suggestions that you believe may be relevant to our work that you wish to share?

A.10 DATA HANDLER INTERVIEW #1 NOTES

Question 1: What kinds of information collection do you perform? Are any of these data collection correspondances performed on a repeating basis?

Affiliate Sign up Sheet (daily/weekly basis), e-mail(daily), any poll or survey results

(rarer), financial package info that's collected in April

The affiliate information from the sign-up sheet is manually moved over to the proper Country Podio by Pernille in the event that the person filled it out on the main website and not on the location where there's a country partner. This excludes places that don't have their own country chapters (US, CA, etc)

Question 2: What forms of contact information do you collect / store? What is this contact information used for? How often is it actually utilized?

The information from the affiliate sign up

Question 3: What data from partners / affiliates do you need to collect / store in order to perform your operations?

Receiving information from Partners etc: Just the report in April

Question 4: What data from partners / affiliates is collected? Is any of the collected data not strictly necessary to perform your operations?

Photograph requested of members

Question 5: Is there a master list of all types of data that CWA collects / stores?

No

A.11 DATA HANDLER INTERVIEW #2 NOTES

Question 6: When data is collected from affiliates on the key platforms, is there anyone else the data is shared with?

Yes, Data is shared with others within ecosystem

Wordpress– Founder's daughters have been assisting with WordPress

(What kind of access do they have? Assess.)

Chapters can get sub-pages

Symbiotisk told them they could be added to their own groups

Explains why there are a couple of Americans randomly places

Divert them to Wordpress groups individually

For our investigation, every time there is a new affiliate, it is shared with people who are not in the organization

Besides the Podio administrators, is there anyone else

Podio table is the mothertable

GCC fills the info that they shared there into other organizations

Data source, just Podio admin that has access to that

Then goes to Wordpress, admin have access to limited subset

(1) Update map

(2) If they want to edit a wordpress site (name chapter name email address as an account).

From the main affiliate form, is there any other place

Mailchimp

Newsletter

Invitation link to the Hood

Generate a link

The Hood

Once people are signed into the Hood, can admin see any other information on users?

-Last IP address

-username, name (can edit)

-primary and secondary email

-can see if they have 2fa

-activity, posting,

May not be personal

Administrator view of Discourse

Using the discourse form

Consent to allowing the collection of the IP address

Article 19/Chapter 3 Overhauling consent checks

When you fill out the new affiliate form

Yes I give consent to be added to Mailchimp etc

Email, added to map, added to mailchimp, they are added to g suite

Christian will generate

There are other people on the platforms that have access

Is there a way we can subcategorize somehow

Can see who they are

Mailchimp is not public

Brief assessment of Mailchimp

Question 7: When chapters sign up, what types of disclosure or checks for consent are in place (if any) before they enter in data? If so, is there a way for users to withdraw consent?

System in place for withdrawing consent :

Email to Pernille says (remove from map, etc)) requires contact to Pernille

Informal, No way to revoke consent

Newsletter for different groups (affiliates, partners, specific areas)

Sent out every 3 mo.

Who created the website on wordpress, are they still a manager?

(Symbiotisk)

Gravity forms plug-in with wordpress

All admin and editors can see everything

Confident this data was exported somewhere else

8. How is the access to these software / platforms distributed and managed?

Provided when tasks need to be completed

9. How long does CWA keep the data in the system that is used? Is there a way for users to request their data to be deleted? If so, is this procedure documented?

Forever unless asked

10 Do you have an up-to-date privacy policy that your website visitors can view? If so, what is contained within it? If so, is there a process for notifying users when it is updated?

No, nothing on data processing

11. Does CWA have a Data Protection Officer? (DPO)

No

12. Is there any data protection training for CWA employees?

No

Having a resource that you can recommend, that exists

Chapters with people on payroll read through powerpoint and take the quiz

Self administered

Virtual calls with people from all over the world (newsletter)

Give them the training resources

Cybersecurity workshop

13. Is there a protocol in place for ensuring that technical cybersecurity is up to date?

Documented or undocumented protocol for cybersecurity

Office policy

Laptop updates

Bring laptop everywhere

(No)

14. Is there a protocol in place in the event of a data breach/all data is gone?

(No)

15. Do you have any additional ideas, comments, or suggestions that you believe may be relevant to our work that you wish to share?

APPENDIX B – INFORMATION COLLECTED BY THE NEW AFFILIATE SIGN-UP FORM

Full Name

Name of Organization (if any)

Classification of Organization

Proposed Geographic Scope of Affiliate Agreement

Email address

Phone number

Full Address

Country

Age

Job title

Image of yourself

Tell us about yourself

Tell us about your organization

Why do you want to start Cycling Without Age
in your local area?

What is your relationship with bicycles?

Tell us a story from your life where age didn't
matter

What makes you happy?

What is your wildest dream?

Would you like to have a Cycling Without Age
email address?

Tell us how you found out about Cycling
Without Age

The Cycling Without Age Generosity Pledge

I will build my CWA website on the shared
platform

APPENDIX C – INFORMATION INPUTTED INTO THE HOOD BY USERS

Username

User "About me"

User location

User private messages

Name

Featured Topic

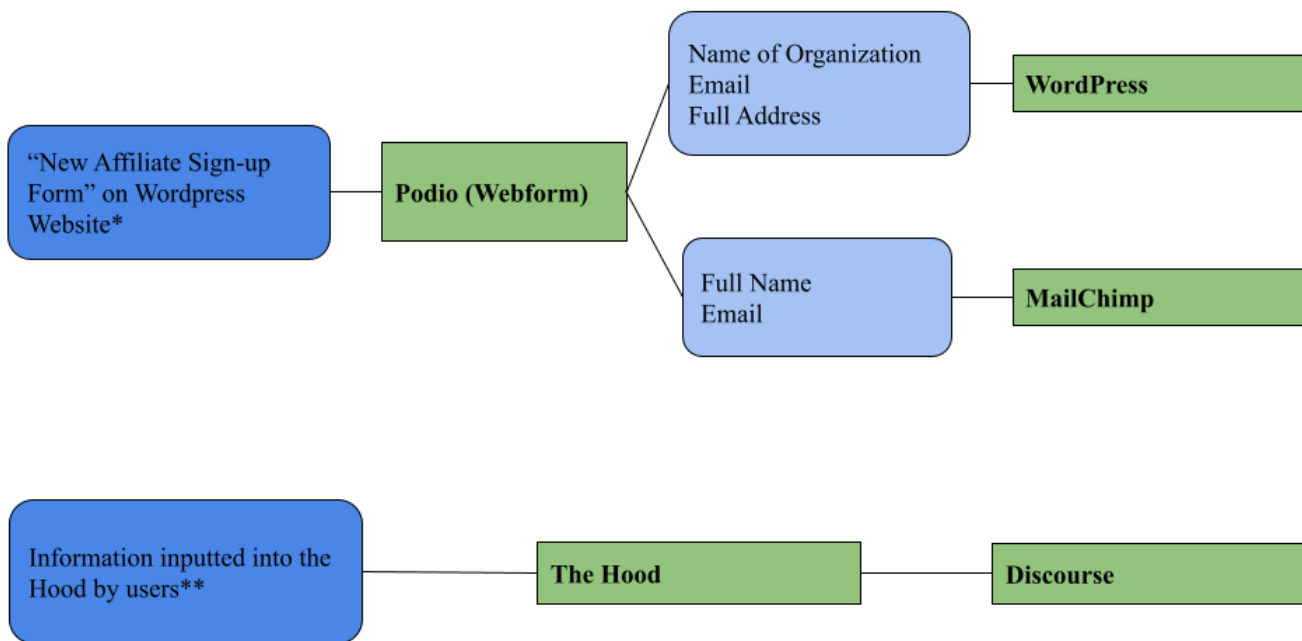
User Card Background

Profile Header

Email address

Website link

APPENDIX D – DATA PROCESSING FLOWCHART



*See Appendix C for list of all information on the New Affiliate Sign-Up Form
** See Appendix D for list of all information inputted into the Hood by users

APPENDIX E - HOW TO USE THE GDPR KNOWLEDGE BASE

How To Use the GDPR Knowledge Base

Welcome to Cycling Without Age International's GDPR Knowledge Base. Every folder is designed to cover a different topic of GDPR that was focused on during an internal CWA International GDPR compliance project. Below is a chart of the different articles and the redirects to the recommendations outlined.

Please note that this is **not** a complete list of every necessary step needed for GDPR compliance, but just a collection of resources that were utilized during a CWA International GDPR compliance project. All of the recommendations and resources were created or found by the Spring 2022 WPI Research Team. We hope that these resources can be of use to your organization. **The recommendations and sources provided are not legal advice and are not designed to replace any legal advice.**

Topic	Recommendations / Resources 
User Rights (Chapter 3)	See here
Cookie Consent (Articles 6, 7, and 30)	See here
Lawfulness of Processing & User Consent (Article 6 & 7)	See here
Proof of Compliance (Article 30)	See here
Security Practices (Articles 25 and 32)	See here
DPIA Procedure and DPO's (Articles 35, 37, 38, and 39)	See here for DPIA Procedure See here for DPO Information

APPENDIX F - COOKIE CONSENT RECOMMENDATIONS

Installing Cookie Consent on WordPress

According to GDPR, cookie consent is something that is required by a number of different articles. It helps users have control of their site experience and protect their data safely. Since CWA International has cookies, cookie consent should be added. The following steps are how to implement a WordPress plug-in to activate cookie consent on the main site.

1. Install 'Cookie Notice' through the WordPress plug-in directory by downloading the files from [the WordPress site here](#).
2. Activate the plug-in using the left side menu and click 'Plugins' and click on Cookie Notice.
3. Go to the Cookie Notice settings and set the options you want
4. Click the "Add Compliance Features" button to start the Cookie Compliance integration
5. Create a Cookie Compliance account and select a plan
6. Log in to the Cookie Compliance web application anytime to customize the settings

Installing this plugin and managing it with all of the information needed will suffice for compliance.

APPENDIX G - SECURITY PRACTICE RECOMMENDATIONS

G.1 SAMPLE PODIO ADMINISTRATOR AGREEMENT

By signing below, I confirm that I understand the responsibility that I have as a Podio administrator in protecting my administrator account. My administrator credentials permit access to personal user data stored in the Podio database, and if my account becomes compromised, I will directly be putting the personal user data of others at risk. In order to minimize the chance that my account will become compromised, I agree to the following:

- 1) I will change my Podio password once every 90 days, to a completely unique and previously unused password
- 2) I will not re-use my Podio password on any other platform
- 3) I will enable Two-Factor Authentication on my Podio Administrator account
- 4) I will notify the controllers of the Podio database immediately if I believe suspicious activity has occurred under my account
- 5) I will undergo a brief cybersecurity awareness training, and agree to review the cybersecurity awareness training material at least once a year
- 6) I understand my responsibility in protecting the data of other individuals, by taking steps to protect my account

Signed,

G.2 RECOMMENDATIONS FOR SECURITY PRACTICES

Security Recommendations

GDPR requires a number of security practices that will help strengthen defense against hackers or attacks. While these tasks are not specific to one location or one system, they are general recommendations that will help improve both user experience and data safety. Below are various suggestions that will help both cybersecurity and physical security to be in compliance with both Article 32 and Article 25.

- 1) Podio databases should be backed up regularly. Having one person responsible for this task, and completing it about once a month is a good idea, and can take as little as 5 minutes. See the "[Podio Database Backups](#)" document.
- 2) Podio administrators should read and sign a brief statement outlining the importance of protecting their administrator accounts. This statement should explain the responsibility that a Podio administrator has in protecting the personal data it can access. An example of this statement can be found in the "[Sample Podio Administrator Agreement](#)" document.
- 3) Podio administrator accounts should have Two-Factor Authentication enabled on their accounts. The Podio website has a [help page](#) for setting up Two-Factor Authentication. A smartphone app will be needed to utilize Two-Factor Authentication, and it is recommended to use either Google Authenticator ([Android](#) / [iOS](#)) or Authy ([Android](#) / [iOS](#)).
- 4) Podio administrators should change their passwords every 90 days. This is to minimize the chance that the password was compromised elsewhere, and that the compromised password can be used to gain access to Podio.
- 5) CWA employees should be required to ensure that their personal devices are running the most up-to-date firmware. This applies to both mobile devices and laptops. This will minimize the risk of a malicious attacker capitalizing on out-of-date firmware with security vulnerabilities. See [here](#) for updating iOS devices, [here](#) for updating Android devices, [here](#) for updating Windows devices, and [here](#) for updating MacOS devices.
- 6) Administrators of systems storing personal data, such as Podio, The Hood, or WordPress, should complete an annual cybersecurity awareness training course. [Wizer Training](#) offers a free cybersecurity awareness training course, complete with videos and knowledge checkpoint quizzes. The course only takes about 25 minutes to complete, and covers important topics like phishing, social engineering, Two-Factor Authentication, the importance of strong passwords, ransomware, and physical security. A lead from a specific CWA chapter can set up a Wizer account, and then assign training to all of the administrators of systems within their organization.
- 7) Personal laptops for CWA employees should be encrypted. This minimizes the chance that personal data of others on the laptops can be stolen if the laptop is stolen. See [this](#) guide from Apple on how to enable harddrive encryption on MacOS devices, and [this](#) guide from Microsoft on how to enable harddrive encryption on Windows devices.

- 8) Personal laptops for CWA employees should have antivirus software installed on them. Our team recommends MalwareBytes antivirus software. [This guide](#) showcases how to install MalwareBytes for Windows, and [this guide](#) showcases how to install MalwareBytes for MacOS. Our team recommends the free version of MalwareBytes. Note that our team also highly recommends **not** utilizing McAfee antivirus software.
- 9) CWA chapters that retain documents that may contain sensitive personal data on them should have a locked filing cabinet somewhere on the premises. The key to this filing cabinet should be given to only one individual.

G.3 INSTRUCTIONS FOR BACKING UP PODIO DATABASES

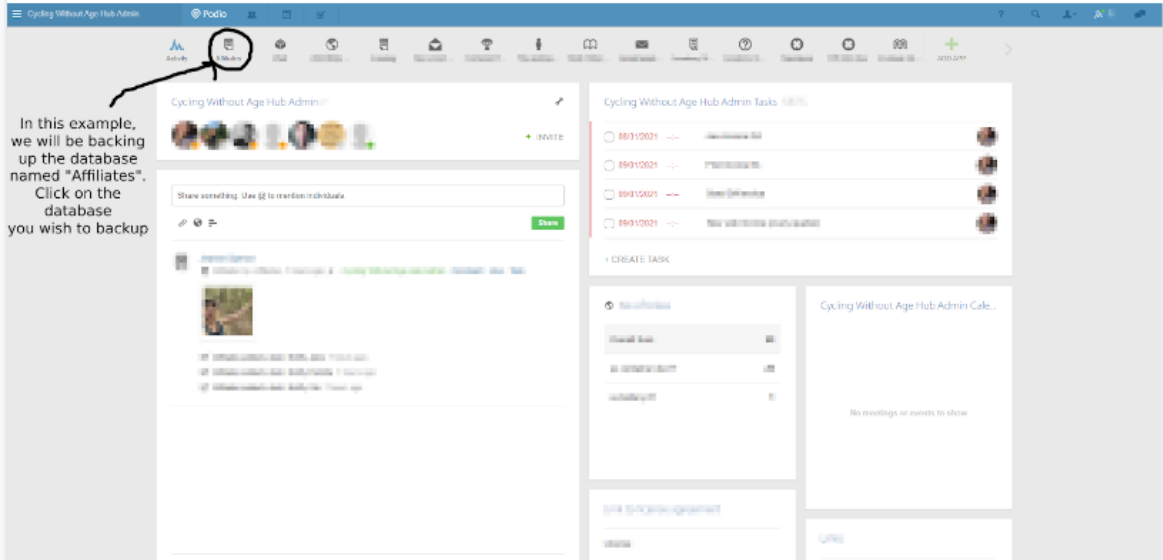
Backups of Podio databases should be taken regularly to prevent loss of data if a Podio database is accidentally deleted or corrupted. There are two different recommended ways of accomplishing this.

- 1) Podio databases can be saved as Excel files. See [“How to Backup a Podio Database as an Excel File”](#). Some general comments regarding this method:
 - a) Ensure that the Excel files are encrypted with passwords. The [“How to Backup a Podio Database as an Excel File”](#) document covers how to accomplish this. The password should only be known by the person within the organization who would be responsible for restoring the Podio database from the Excel file if an issue were to arise. This limits the amount of people with access to the personal data stored within the Excel file.
 - b) The encrypted Excel file should be stored in a cloud storage space used for the organization, and not a personal storage space such as a personal laptop or a personal Google Drive. This ensures that the ownership of the personal data is the organization, and not an individual within the organization. A great example of this is uploading the encrypted Excel file to an organization’s shared Google Drive for CWA employees.
 - c) The encrypted Excel file should be deleted from the personal computer of the person who downloaded the file from Podio, after the file has been uploaded to the organization’s cloud storage system. The file should only exist in one location, which is the organization’s cloud storage system, such as the organization’s shared Google Drive for CWA employees.
 - d) Only the most recent Excel file should exist within the organization’s cloud storage system. This is because the purpose of the backup is to have the most recent copy of the database stored in case of accidental deletion or corruption. Having older backups can be a security risk by storing personal data of users that may have previously requested their data to be deleted. When uploading the most recent Excel file to the cloud storage, delete the previous encrypted Excel backup file from the cloud storage.
- 2) An automated Podio backup tool, such as the one by [Momentum Tools](#) can be utilized. Some general comments regarding this method:
 - a) Only the most recent backup file should be stored. This is because the purpose of the backup is to have the most recent copy of the database stored in case of accidental deletion or corruption. Having older backups can be a security risk by storing personal data of users that may have previously requested their data to be deleted.
 - b) Ensure only the person who would be responsible for restoring the Podio database from the backup if an issue were to arise has access to the cloud backup login. This limits the amount of people with access to the personal data stored within the Excel file.

G.4 BACKING UP A PODIO DATABASE AS AN EXCEL FILE WALKTHROUGH

1) On the Podio dashboard, navigate to the database that you wish to take a backup of.

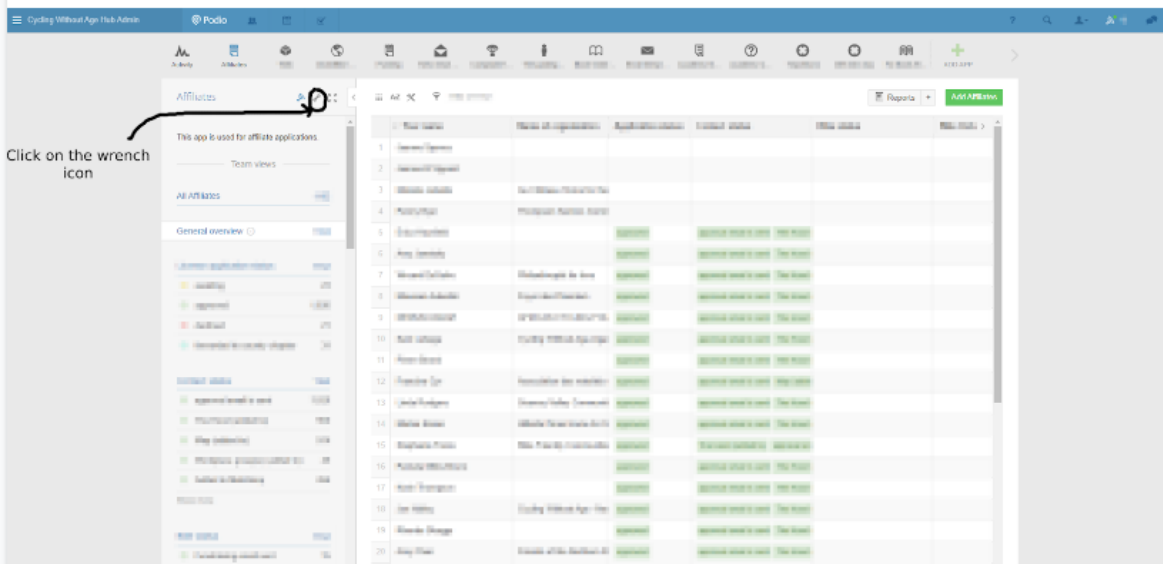
In this example, we will be backing up the database named "Affiliates". Click on the database you wish to backup



The screenshot shows the Podio dashboard for the 'Cycling Without Age Hub Admin' workspace. The 'Affiliates' database is selected, and a red circle highlights the wrench icon in the top right corner of the database view. The dashboard includes a header with navigation icons, a main content area with a task list, and a sidebar with various widgets.

2) Click on the Wrench icon in the database.

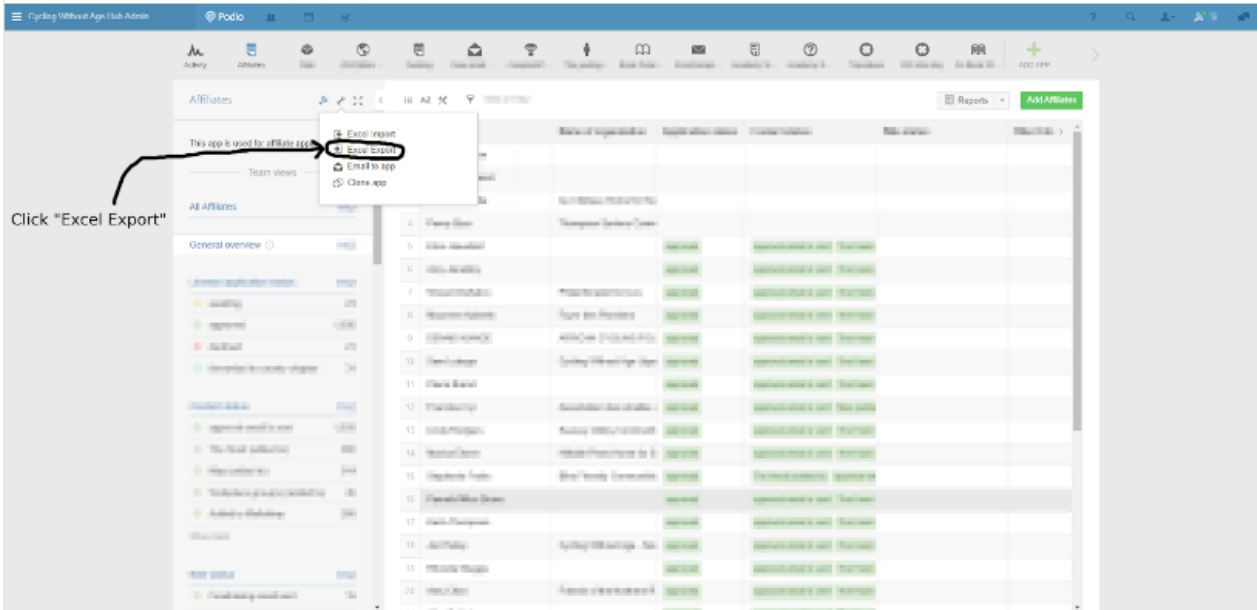
Click on the wrench icon



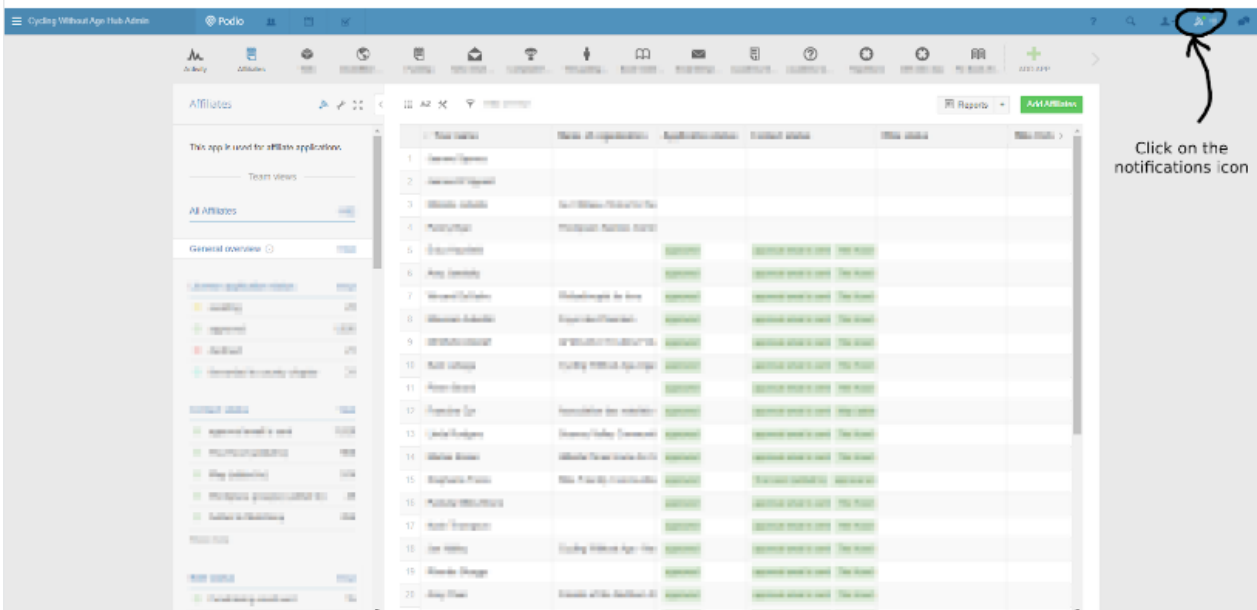
The screenshot shows the 'Affiliates' database view in Podio. A red circle highlights the wrench icon in the top right corner of the database view. The view displays a list of 20 items with columns for 'Row name', 'Status of registration', 'Registration status', 'Finalized status', 'File status', and 'File link'. The left sidebar shows the 'Affiliates' database selected.

Row name	Status of registration	Registration status	Finalized status	File status	File link
1. General System					
2. General System					
3. General System					
4. General System					
5. General System					
6. General System					
7. General System					
8. General System					
9. General System					
10. General System					
11. General System					
12. General System					
13. General System					
14. General System					
15. General System					
16. General System					
17. General System					
18. General System					
19. General System					
20. General System					

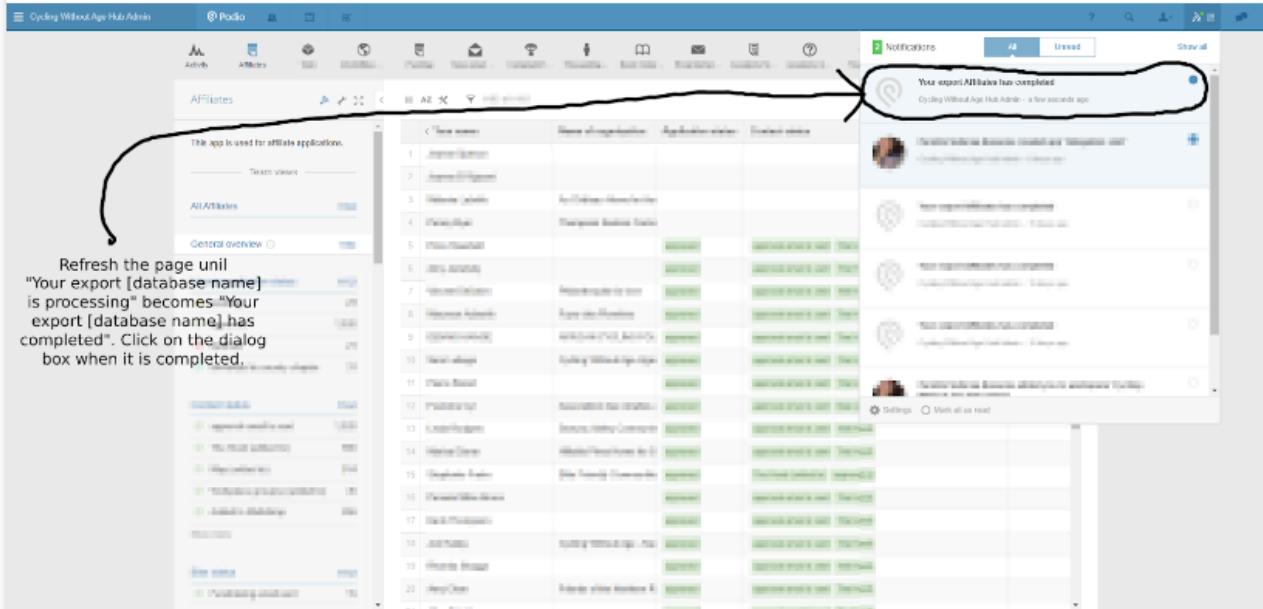
3) Select "Excel Export".



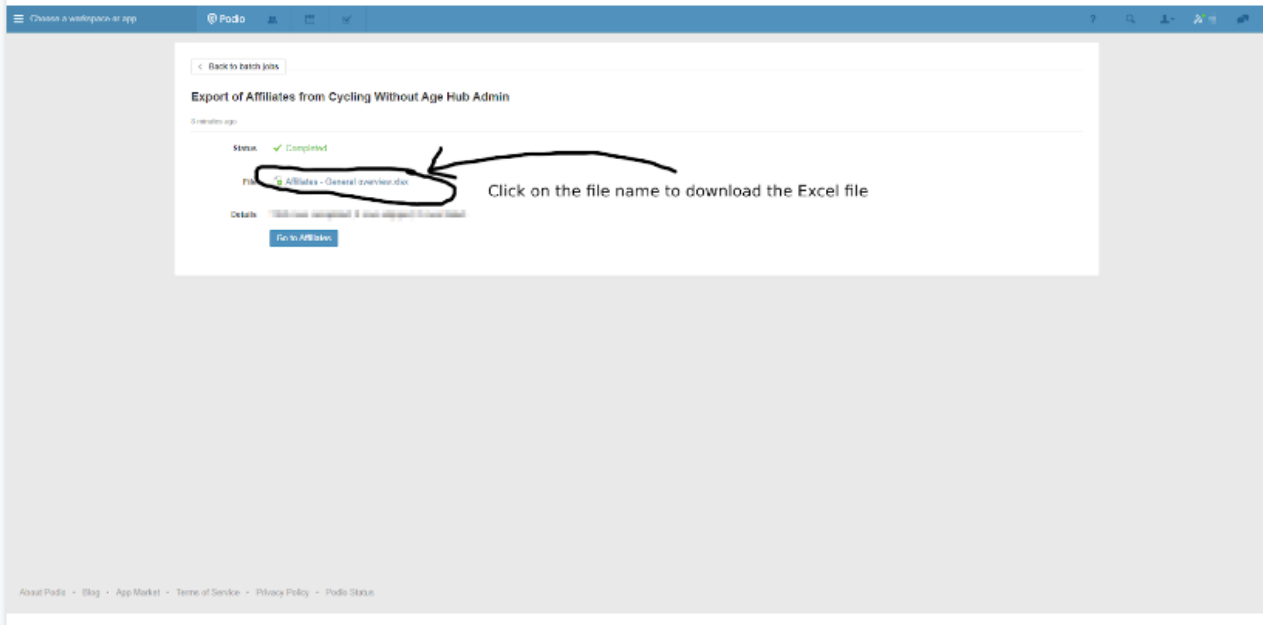
4) Click on the "Notifications" icon



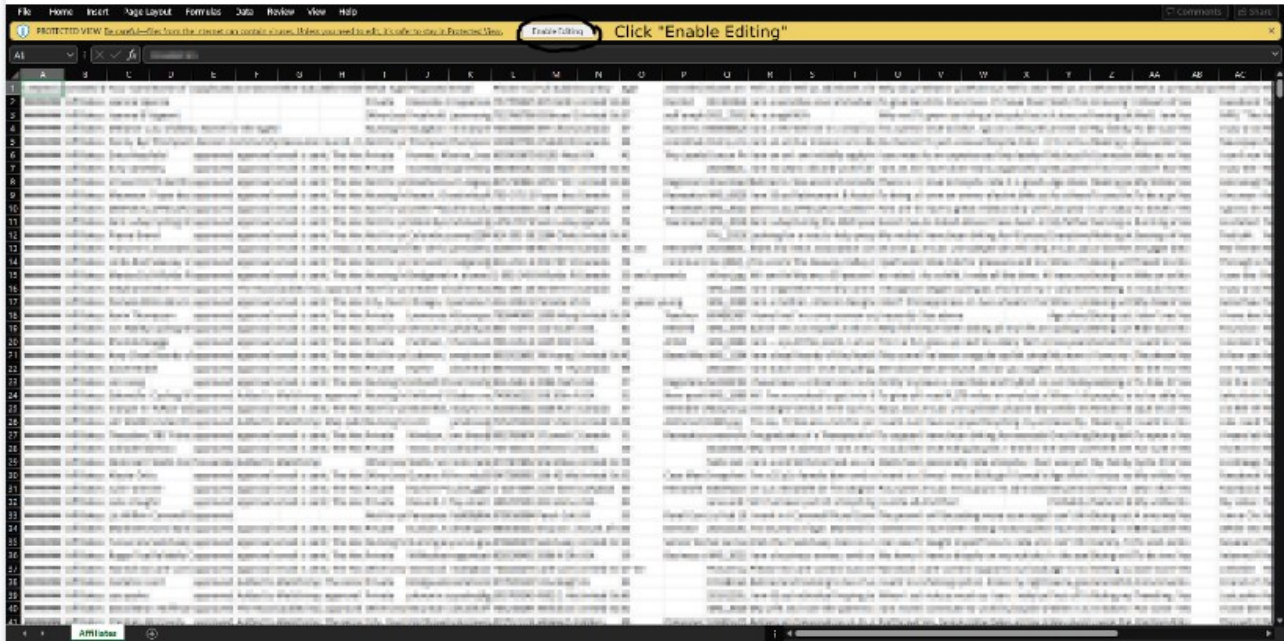
- Refresh the page every minute or so until the message about your export processing turns into the message about your export being completed. This may take up to 5-10 minutes for very large databases. Click on the message when ready.



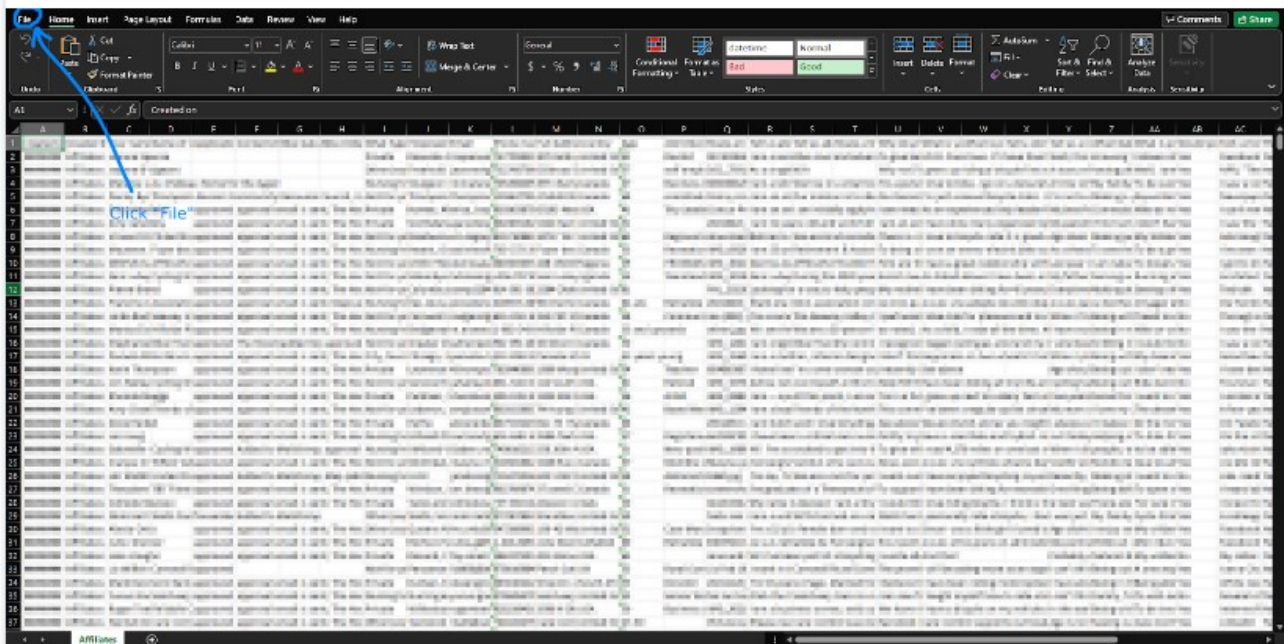
- Click on the file name to download the Excel file



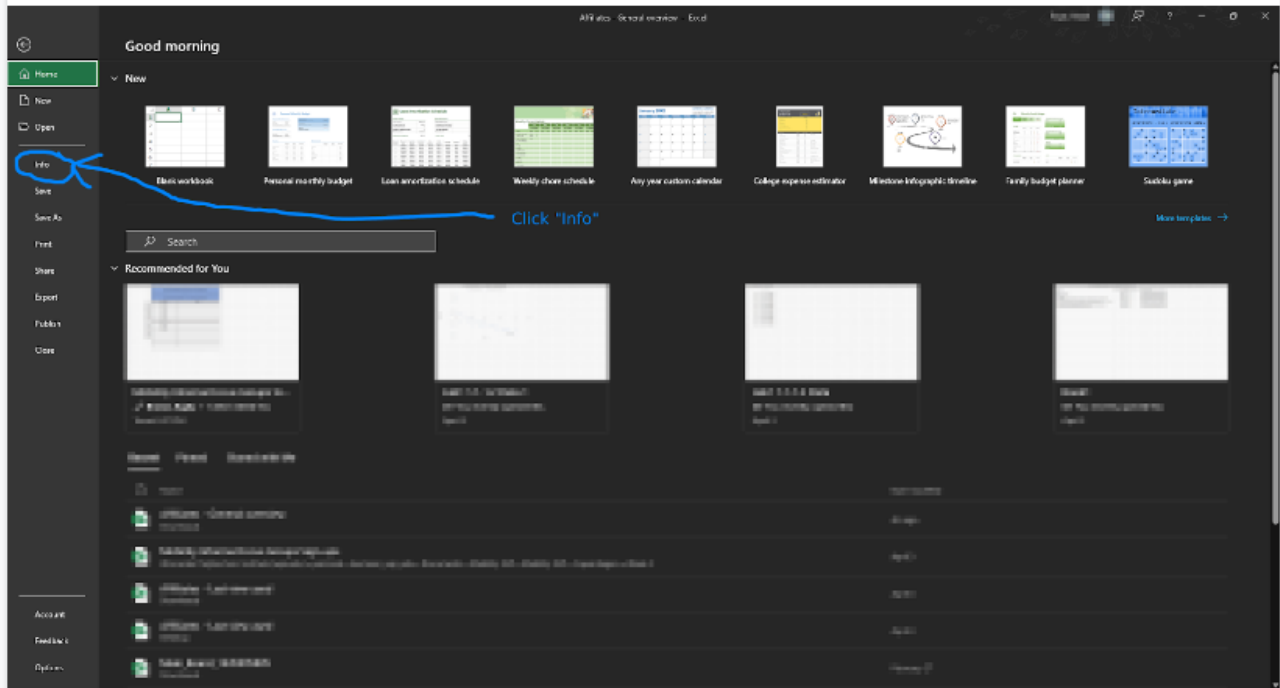
- 7) Open the Excel file that was downloaded. It is usually located in the "Downloads" folder of your computer.
- 8) Click "Enable Editing"



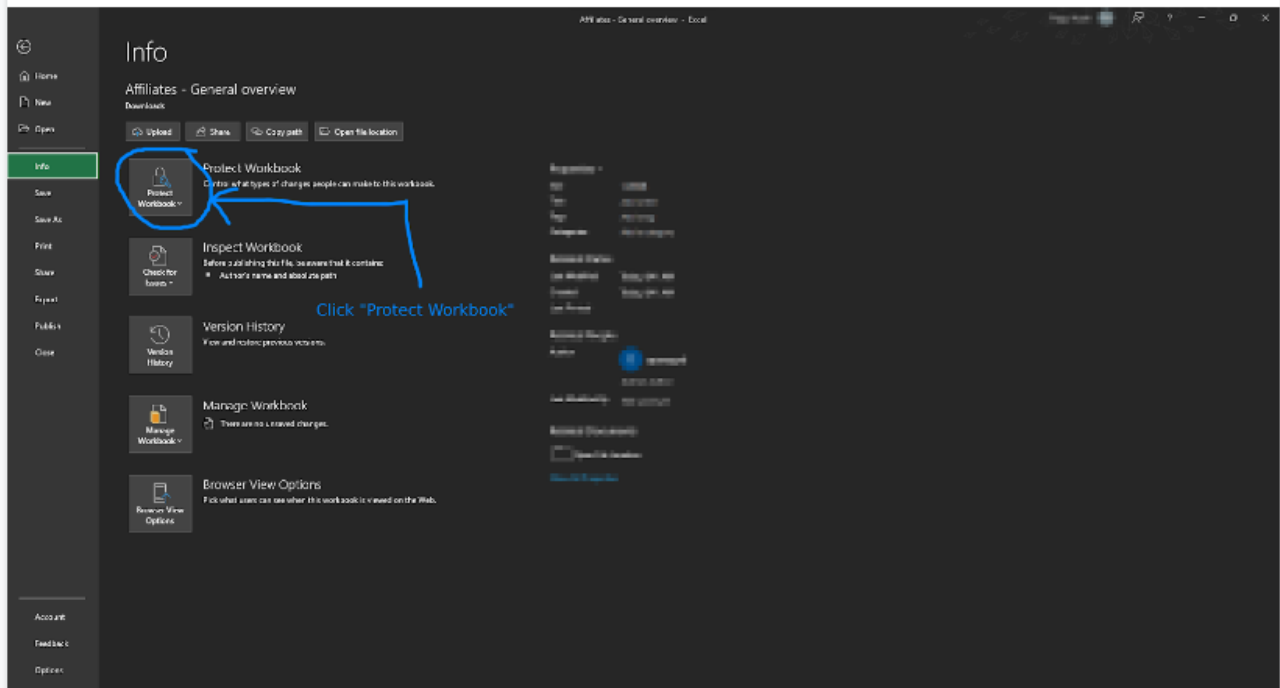
- 9) Click "File" in the top right corner



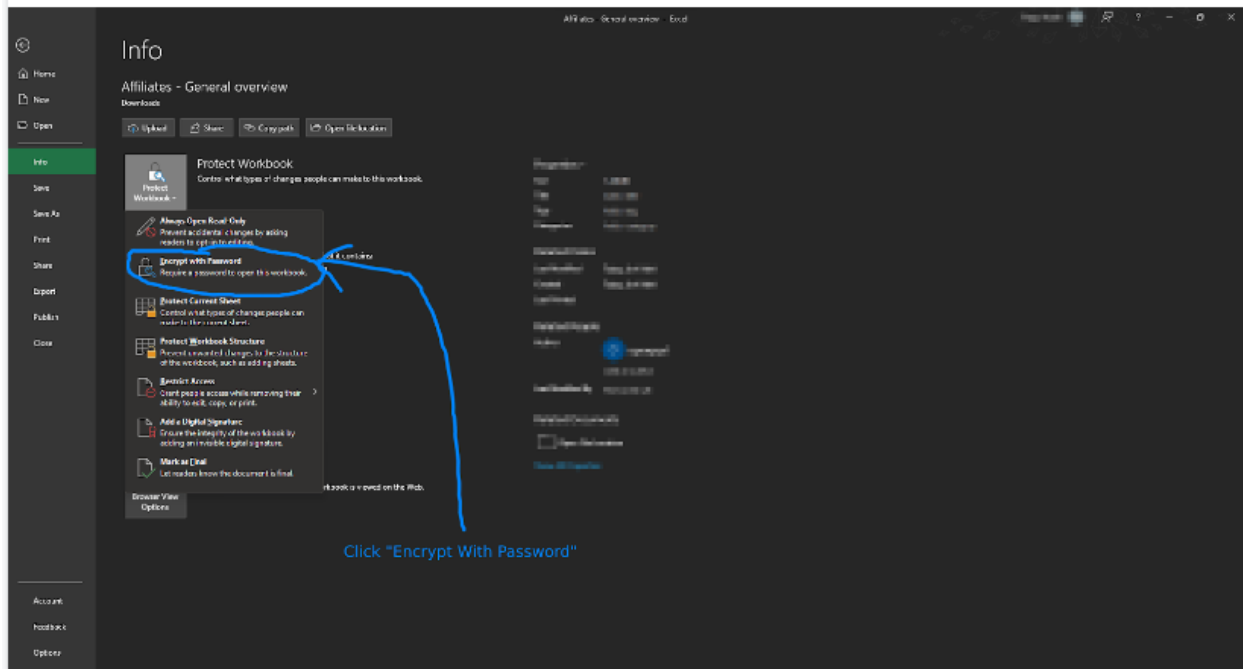
10) Click "Info" on the left side



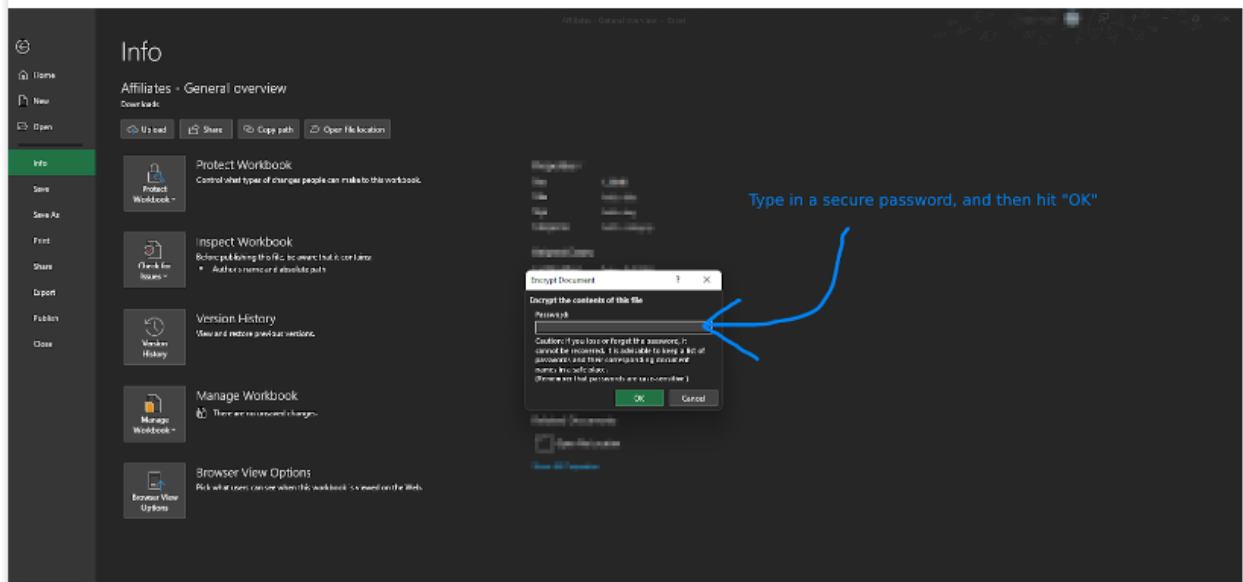
11) Click "Protect Workbook"



12) Click "Encrypt With Password"



13) Enter in a secure password. As stated in "[Podio Database Backups](#)", only the person who would be responsible for restoring the Podio database from the Excel file in the event of a database issue should know this password. Then hit "OK"



14) After re-entering the password when prompted, File -> Save the Excel file. Upload the file to the cloud storage of your choice (such as a CWA shared Google Drive), and then delete the Excel file off of your local computer.

APPENDIX H – LAWFULNESS OF PROCESSING AND USER CONSENT RECOMMENDATIONS

It is recommended that CWA have a new process for applicants to apply to become affiliates and start a CWA chapter in their local community. The process will be broken into two halves: Phase 1 and Phase 2.

Phase 1

The current new affiliate sign-up form posted on the CWA website should be edited such that it only asks to collect the full name, and email address of the applicant. The form should also have an area where the new affiliate can consent to their data being collected through the form, as well as can agree to the CWA Generosity Pledge. Each of these selectors should include both a “Yes” and a “No” button, in order to properly constitute consent. Additionally, this form should have a “file upload” button, where an applicant can submit a 3-5 minute video of themselves answering the script found in the example on the following page:

Cycling Without Age Affiliate Agreement

You are about to apply to become a Cycling Without Age Affiliate. Before submitting an application to register for a Cycling Without Age initiative, please make sure you have read and understood the Affiliate Agreement. After your submission, this is what will happen: Our panel will review your application and we will be looking to match you with an existing affiliate. Within 3 weeks, we will send you a welcome letter if the panel approves your application.

Your Name*

Your Email*

Please provide your email so we can contact you after reviewing your application.

Please record a brief (3-5 minute) video of yourself answering all of these questions:

- **Tell us a little bit about yourself.**
- **Tell us about the organization you are representing (if any).**
- **Why do you want to start Cycling Without Age in your local area?**

Additionally, please pick one question and answer it in the same video:

- **What is your relationship with bicycles?**
- **Tell us a story from your life where age didn't matter.**
- **What makes you happy?**
- **What is your wildest dream?**

This will help us better understand you as a potential future member of our movement, and provide us with an opportunity to familiarize ourselves with your face and story! If you have any questions or concerns with this, please e-mail (the Global Community Captain)

Using the file upload button below, please upload your video response.

No file selected.

Do you give CWA consent to collect your personal information and data through this form?

- Yes
- No

I have read and agreed with CWA's Generosity Pledge.

- Yes
- No

Thank you for your application! We look forward to getting to know you better!

Proof of Compliance Recommendations

GDPR requires documentation for an organization to prove its own compliance since it is the responsibility of the organization itself. Within this is a requirement for a data flowchart, and an example of CWA International's current data mapping [can be found here](#). The current data documentation for CWA International that the flowchart was created from [can be found here](#). More information on creating GDPR-compliant flowcharts [can be found here](#).

In addition, there is a free, open-source tool called Everlaw, which clearly lays out various justifications and controller/processor details that will help prove compliance. This document should be filled out within a month of the GDPR Knowledge Base being completed and turned over to new ownership. It also should be updated every time a new data processing step is performed, or an old one is changed. [The template spreadsheet can be found here](#).

These two pieces of information will create justification and transparency for users and will be enough to prove compliance within CWA International's systems.

APPENDIX J – USER RIGHTS RECOMMENDATIONS

J.1– ACKNOWLEDGING USER RIGHTS

Improving/Acknowledging User Rights

Chapter 3 of GDPR covers articles 13-23, all focused on user rights and how the data subject can manage their personal information being processed or used. It also explains the controller's role in the processing of this data. There is an emphasis on the clarity of these rights. The majority of these articles can be covered in a single privacy policy document that can be added to the WordPress site. In addition, there should be a second document that is sent out once the user's information is being processed that again outlines all of the rights that they have.

Privacy Policy:

Within this folder, there is a subfolder with two templates. One is a [general privacy policy template](#) that any organization or website can use. The other is [the same template but edited](#) to remove sections that are unnecessary for CWA International. The green highlighted sections are parts of information that must be added by the organization themselves. Yellow highlighted sections are paragraphs that must be added to be compliant with Chapter 3. Most of the sections that must be added are under part IV, "Your Rights Regarding The Use of Your Personal Information". The following rights must be clearly outlined within this document:

1. The right to access: Data subjects can access their own information and request updates on processing. This section must outline how a data subject would contact the controller and request this information, and the timeline and expectations the controller should meet while fulfilling this request.
2. The right to rectification: Data subjects are able to request their personal information to be updated without any old information being stored. In other words, all data must be updated the way the data subject wants and requests without refusal. Describe the process by that subjects can reach out and request this and how the controller will execute it. Communication from the controller's side must also be explicitly stated.
3. The right to erasure: Data subjects can request deletion of their personal information at any point and cannot be refused unless there is legal justification. Outline a process of how a user can request this and what the steps would be from the controller's end for full transparency. Communication from the controller's side must also be explicitly stated.
4. The right to restriction of processing: Data subjects can restrict the processing of their information if one of the following is true: the accuracy of the information is contested, the processing is unlawful and there is opposition from the data subject, the controller no longer has use for the personal data but they are required by the subject for legal claims, or the subject has exercised article 20 (the right to object) based on a unique situation. This must be explicitly outlined in the privacy policy document. Communication from the controller's side must also be explicitly stated.

5. The right to data portability: This can briefly be mentioned in the privacy policy as a right, but it does not need to be explained. However, there need to be steps taken to ensure that the personal information that is sent to the data subject when requested or another controller is machine-readable and clear.
6. The right to object: If a data subject is in a particular and unique situation, they have the right to object to any processing of their personal information. The controller cannot object unless there are legitimate grounds for continuing. In addition, any personal information that was used for marketing purposes can be objected to at any point and processing will end for those purposes. It should be made explicitly clear what steps will be taken if an objection occurs to emphasize clarity for the users.

Outside of part IV, part II, “How We Use and Share Information”, must have a section added that describes the legal justification for storing and processing the data that CWA International collects. This privacy policy must be added to WordPress so that users have access to it. The process for doing so [can be found here](#).

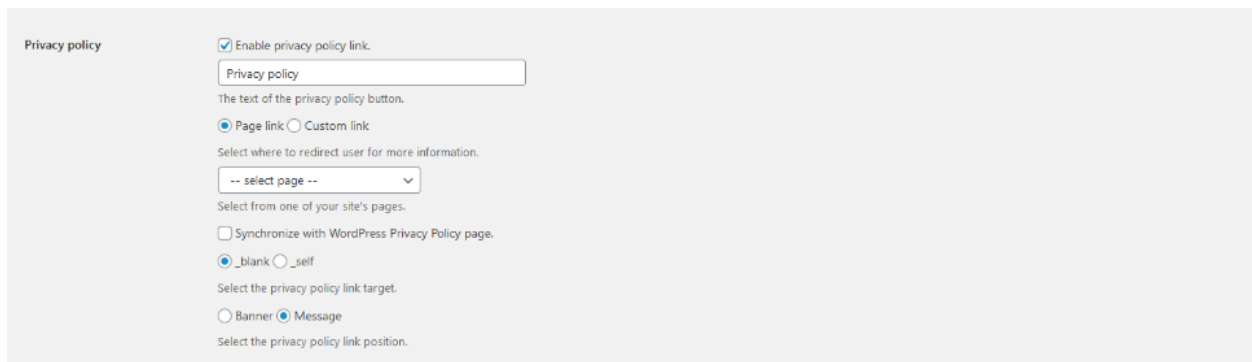
Separate Documentation:

Outside of the privacy policy, article 13 requires a restatement of rights when the processing of the information has begun. Therefore a second document with the content of part IV should also be created. The wording of this document can be nearly identical to what was written before. It should be sent out or displayed once the new affiliate form has been submitted (when processing begins for that data).

J.2– HOW TO UPDATE THE PRIVACY POLICY

While there is no legal process for creating a privacy policy, the CWA WordPress site will need to be clear about data collection. Within this folder are two templates. One is a general template for writing a privacy policy, but the other is that same template edited to fit CWA International’s processes. Below is a suggestion on how to implement a privacy policy on the cyclingwithoutage.org website.

1. On WordPress, create a new page. This is done by going to the left administrator menu, hovering over “Pages”, and selecting “Add New”. Title the page “Privacy Policy”.
2. Copy and paste the information from the completed template into the paragraph section of the editor’s view. Make sure that it's still formatted properly. Publish the page.
3. Once the page is published, go to the left menu again, hover over “Theme Settings” and select “Footer”.
4. Add a line to the left half of the footer that says “Privacy Policy”. Highlight the text with the cursor and click the chain link icon above the textbox. Copy and paste the URL of the new Privacy Policy page.
5. Additionally, if it is not already installed, use the plug-in Cookie Notice and add a link to the Privacy Policy page there.



The image shows a screenshot of the 'Privacy policy' settings in a WordPress plugin. The settings are as follows:

- Enable privacy policy link.
- Privacy policy:
- The text of the privacy policy button.
- Page link Custom link
- Select where to redirect user for more information.
- select page --
- Select from one of your site's pages.
- Synchronize with WordPress Privacy Policy page.
- _blank _self
- Select the privacy policy link target.
- Banner Message
- Select the privacy policy link position.

An example of how to implement privacy policy in the Cookie Notice plug-in

These steps are recommendations. The Privacy Policy page on WordPress can live anywhere on the site as long as it is made public for all users to access.

J.3– PRIVACY POLICY TEMPLATE

Privacy Policies are agreements that specify what type of data a website collects from users and how that data will be used. Known as “personal information” or “personally identifiable information,” regulated data typically includes anything that can be used to identify an individual, and is not limited to a user’s name. Personal information may include a user’s address, date of birth, marital status, contact information, ID issue and expiration date, financial records, credit information, medical history, where one travels, and intentions to acquire goods and services, among others.

While no single federal law requires that websites have a Privacy Policy, the sum of federal and state legislation suggest that you should. Regulations vary by geographical region and jurisdiction as well as by subject matter so be sure to check local laws when drafting your Policy. Privacy Policies should be updated whenever a change occurs in the way a website collects or utilizes user information.

Consider linking your Privacy Policy with your Terms of Use to ensure cohesive application of relevant laws. If you would like to be more specific with your users, consider a Data Usage Policy or Data Usage Statement.

Instructions

1. Delete this first page of instructions before using your template
2. Fields **[in brackets]** are placeholders for your information
3. This template is provided “as is” - please consult your own legal counsel before use.
4. For more detailed instructions for this template, or to find more detailed and comprehensive Privacy Policies, visit [UpCounsel](#)

Disclaimer

UpCounsel, Inc. is located at 580 Market Street, 5th Floor, San Francisco, CA 94104. UpCounsel, Inc. is not a law firm, nor is it a substitute for hiring an attorney or a

law firm. UpCounsel, Inc. may provide access to self-help services at your direction, but *does not provide legal advice*. Nothing herein shall be construed as the provision of legal advice. UpCounsel, Inc. cannot and will not provide any kind of advice, explanation, opinion, or recommendation to a user of this template about possible legal rights, remedies, defenses, options, selection of forms or strategies, and nothing herein shall be construed as such. The information contained in this template is *general* legal information, and a user should not construe this template as legal advice to be applied to a specific factual situation. Use of the template contained herein does not create or constitute an attorney-client relationship between the user of this template and UpCounsel, Inc., its employees, or any other person associated with UpCounsel, Inc. The law differs in each legal jurisdiction and may be interpreted or applied differently depending on your location or situation. As such, you should not rely on the template contained herein without first consulting an attorney about your specific situation.

The template contained herein is provided “as is.” UpCounsel, Inc. does not provide any express or implied warranties of merchantability, suitability, or completeness of the information in this template. You use this template at your own risk. Neither UpCounsel, Inc., nor its agents, officers, employees, or affiliates, are liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including procurement of substitute goods or services, loss of use or profits, or business interruption), even if UpCounsel, Inc. has been advised of the possibility of such damages, on any theory of liability, whether in contract, strict liability, or tort, arising in any way out of the use of or inability to use this template. Some jurisdictions do not allow the limitation of incidental or consequential damages, so this limitation may not apply to you.

Please remove this instructional page before use

Privacy Policy Template for a Basic Website with User-Generated Content

[COMPANY NAME] PRIVACY POLICY

[Company Name] (the “Company”) is committed to maintaining robust privacy protections for its users. Our Privacy Policy (“Privacy Policy”) is designed to help you

understand how we collect, use and safeguard the information you provide to us and to assist you in making informed decisions when using our Service.

For purposes of this Agreement, “Site” refers to the Company’s website, which can be accessed at [Company URL] [or through our mobile application].

“Service” refers to the Company’s services accessed via the Site, in which users can [description of services].

The terms “we,” “us,” and “our” refer to the Company.

“You” refers to you, as a user of our Site or our Service.

By accessing our Site or our Service, you accept our Privacy Policy., and you consent to our collection, storage, use, and disclosure of your Personal Information as described in this Privacy Policy.

I. INFORMATION WE COLLECT

We collect “Non-Personal Information” and “Personal Information.” **Non-Personal Information** includes information that cannot be used to personally identify you, such as anonymous usage data, general demographic information we may collect, referring/exit pages and URLs, platform types, preferences you submit, and preferences that are generated based on the data you submit and the number of clicks. **Personal Information** includes your email [insert specifically what personal information your website collects, i.e. address, date of birth, marital status, contact information, etc.], which you submit to us through the New Affiliate Form on the Site.

1. Information collected via Technology

To activate the Service you do not need to submit any Personal Information. To use the Service thereafter, you do not need to submit further Personal Information. However, in an effort to improve the quality of the Service, we track information provided to us by your browser or by our software application when you view or use the Service, such as the website you came from (known as the “referring URL”), the type of browser you use, the

device from which you connected to the Service, the time and date of access, and other information that does not personally identify you. We track this information using cookies, or small text files which include an anonymous unique identifier. Cookies are sent to a user's browser from our servers and are stored on the user's computer hard drive. Sending a cookie to a user's browser enables us to collect Non-Personal information about that user and keep a record of the user's preferences when utilizing our services, both on an individual and aggregate basis. For example, the Company may use cookies to collect the following information:

[list typical things you may want to track]

The Company may use both persistent and session cookies; persistent cookies remain on your computer after you close your session and until you delete them, while session cookies expire when you close your browser. [For example, we store a persistent cookie to track ()].

2. Information you provide us by registering for an account

In addition to the information provided automatically by your browser when you visit the Site, to become a subscriber to the Service you will need to create a personal profile. You can create a profile by registering with the Service and entering your email address, and creating a user name and a password. By registering, you are authorizing us to collect, store and use your email address in accordance with this Privacy Policy.

II. HOW WE USE AND SHARE INFORMATION

Personal Information:

Add a paragraph here regarding why you store the Personal Information on users]

Except as otherwise stated in this Privacy Policy, we do not sell, trade, rent, or otherwise share for marketing purposes your Personal Information with third parties without your consent. We do share Personal Information with vendors who are performing services for the Company, such as the servers for our email communications who are provided access to the user's email addresses for purposes of sending emails from us.

Those vendors use your Personal Information only at our direction and in accordance with our Privacy Policy.

In general, the Personal Information you provide to us is used to help us communicate with you. For example, we use Personal Information to contact users in response to questions, solicit feedback from users, provide technical support, and inform users about promotional offers.

We may share Personal Information with outside parties if we have a good-faith belief that access, use, preservation, or disclosure of the information is reasonably necessary to meet any applicable legal process or enforceable governmental request; address fraud, security or technical concerns; or to protect against harm to the rights, property, or safety of our users or the public as required or permitted by law.

Non-Personal Information:

In general, we use Non-Personal Information to help us improve the Service and customize the user experience. We also aggregate Non-Personal Information in order to track trends and analyze use patterns on the Site. This Privacy Policy does not limit in any way our use or disclosure of Non-Personal Information and we reserve the right to use and disclose such Non-Personal Information to our partners, advertisers, and other third parties at our discretion.

You acknowledge and consent that such transfers may occur and are permitted by this Privacy Policy and that any acquirer of our assets may continue to process your Personal Information as set forth in this Privacy Policy. If our information practices change at any time in the future, we will post the policy changes on the Site so that you may opt-out of the new information practices. We suggest that you check the Site periodically if you are concerned about how your information is used.

III. HOW WE PROTECT INFORMATION

[Once changes have been made to the data processing based on recommendations or other steps, fill this section out]

IV. YOUR RIGHTS REGARDING THE USE OF YOUR PERSONAL INFORMATION

[Add a paragraph regarding access to the personal information and how the data subject might obtain it from the controller] You have the right at any time to prevent us from contacting you for marketing purposes. When we send a promotional communication to a user, the user can opt-out of further promotional communications by following the unsubscribe instructions provided in each promotional e-mail. Please note that notwithstanding the promotional preferences you indicate by either unsubscribing of the Site, we may continue to send you administrative emails including, for example, periodic updates to our Privacy Policy.

[Add a paragraph regarding fixing/erasing personal data without delay]

[Add a paragraph regarding the right of restricting any processing]

[Add a paragraph regarding the right of objecting processing]

[Add a paragraph regarding the right not to be subject to automated decision making or profiling]

V. LINKS TO OTHER WEBSITES

As part of the Service, we may provide links to or compatibility with other websites or applications. However, we are not responsible for the privacy practices employed by those websites or the information or content they contain. This Privacy Policy applies solely to information collected by us through the Site and the Service. Therefore, this Privacy Policy does not apply to your use of a third-party website accessed by selecting a link on our Site or via our Service. To the extent that you access or use the Service through or on another website or application, then the privacy policy of that other website or application will apply to your access or use of that site or application. We encourage our users to read the privacy statements of other websites before proceeding to use them.

VI. CHANGES TO OUR PRIVACY POLICY

The Company reserves the right to change this policy and our Terms of Service at any time. We will notify you of significant changes to our Privacy Policy by sending a notice to the primary email address specified in your account or by placing a prominent notice on our site. Significant changes will go into effect 30 days following such notification. Non-material changes or clarifications will take effect immediately. You should periodically check the Site and this privacy page for updates.

VII. CONTACT US

If you have any questions regarding this Privacy Policy or the practices of this Site, please contact us by sending an email to [\[Insert Company Email\]](#).

Last Updated: This Privacy Policy was last updated on [\[Insert Date\]](#).

APPENDIX K - DATA PROTECTION OFFICER & DPIA RESOURCES

K.1 DATA PROTECTION OFFICER RESOURCES

Data Protection Officers

Under Article 37 of the General Data Protection Regulation, it is mandatory for an organization to have a Data Protection Officer when:

1. The organization is a public authority or body;
2. If your core activities require regular and systematic monitoring of data subjects on a large scale; or
3. If your core activities involve large scale processing of special categories of personal data and data relating to criminal convictions.¹

As of 25 April 2022, this team determined that the appointment of a DPO was not necessary because CWA International does not fulfill the above criteria that require a DPO.

However, if the situation arises in which a Data Protection Impact Assessment must be conducted (see [Recommendations for DPIA Procedures](#)), a DPO is also required.

The Spring 2022 WPI Research Team advises that all partners should check their individual country's data protection law to ensure that a Data Protection Officer is not required due to country laws.

The resources below provide additional information on the criteria for appointing a legal DPO.

References

Data Protection officers. Data Protection Officers in Denmark - DLA Piper Global Data Protection Laws of the World. (n.d.). Retrieved April 14, 2022, from <https://www.dlapiperdataprotection.com/index.html?t=data-protection-officers&c=DK>

The DPO (Data Protection Officer) role under the GDPR. IT Governance. (n.d.). Retrieved April 14, 2022, from <https://www.itgovernance.eu/da-dk/data-protection-officer-dpo-under-the-gdpr-dk>

¹ These qualifiers are per <https://www.itgovernance.eu/da-dk/data-protection-officer-dpo-under-the-gdpr-dk>

K.2 DATA PROTECTION IMPACT ASSESSMENT RESOURCES

Data Protection Impact Assessment

Under Article 35 of the General Data Protection Regulation, organizations that are conducting processing that is considered “high risk” must complete a Data Protection Impact Assessment.

As of 25 April 2022, this team determined that the conducting of a Data Protection Impact Assessment was not necessary because CWA International was not collecting Data from the following nine criteria¹:

1. Evaluation or Scoring
2. Automated-decision making with legal or similar significant effect
3. Systematic monitoring
4. *Sensitive data or data of highly personal nature**
5. Data processed on a large scale
6. Matching or combining datasets
7. *Data concerning vulnerable data subjects**
8. Innovative use or applying new technological or organizational solutions
9. When the processing in itself “presents data subjects from exercising a right or using a service or contract”

Should that change, the following form should be filled out **before** that data is collected as a documentation of the risk protection.

■ [dpia-template-v1.pdf](#)

References:

Article 29 Data Protection Working Party. (2017). Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679. United Nations. <https://ec.europa.eu/newsroom/article29/items/611236>

Data Protection Impact Assessment (DPIA) under the GDPR. GDPR.eu. (2019, March 8). Retrieved April 14, 2022, from <https://gdpr.eu/data-protection-impact-assessment-template/>

Examples of processing 'likely to result in high risk'. ICO. (n.d.). Retrieved April 14, 2022, From <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/>

¹ *Items in italics are those the WPI IQP Spring 2022 team deemed potential processing avenues that may be pursued later that would require a DPIA to be conducted before they are performed. See Reference 1 for more information. Additionally, the Guidelines on Data Protection Impact Assessment Document is provided in the GDPR Knowledge Base*

Age, Cycling Without. "Cykling Utan Ålder in the Forest." Flickr, Yahoo!, 14 Nov. 2018, <https://www.flickr.com/photos/cyklingudenalder/45875563901>.

Article 29 Data Protection Working Party. (2017). Guidelines on Data Protection Impact

Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. United Nations. <https://ec.europa.eu/newsroom/article29/items/611236>

Ashoka. (2020, April 13). *The right to relate: Cycling without age*. Forbes. Retrieved January 21, 2022, from <https://www.forbes.com/sites/ashoka/2020/04/13/the-right-to-relate-cycling-without-age/?sh=db1d063a7070>

Cameron, K. S. (2011). Diagnosing and changing organizational culture: Based on the competing values framework (Third edition.). Jossey-Bass.

Coulon, J. (2020, September 19). *'Cycling Without Age' Brings the Joy of Riding to Those Who No Longer Can*. Bicycling.com. Retrieved January 19, 2022, from <https://www.bicycling.com/culture/a30300121/cycling-without-age-nonprofit/>

Cycling Without Age. (2017, March 6). Article of Association for Cycling Without Age. Copenhagen, Denmark. Retrieved January 20, 2022 from https://cyclingwithoutage.org/wp-content/uploads/2019/11/Vedt%C3%A6gter_Articles-of-Association-6.3.2017-Cycling-Without-Age.pdf

Data Protection Impact Assessment (DPIA) under the GDPR. GDPR.eu. (2019, March 8). Retrieved April 14, 2022, from <https://gdpr.eu/data-protection-impact-assessment-template/>

Examples of processing 'likely to result in high risk'. ICO. (n.d.). Retrieved April 14, 2022, From <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/>

GDPR Enforcement Tracker—List of GDPR fines. (n.d.). Retrieved February 17, 2022, from <https://www.enforcementtracker.com>

Getting Started Cycling Without Age. (2019, July 12). Retrieved January 21, 2022, from <https://cyclingwithoutage.org/the-pilot/>

Henriksen-Bulmer J., Faily S., Jeary S. (2019) Implementing GDPR in the Charity Sector: A Case Study. In: Kosta E., Pierson J., Slamanig D., Fischer-Hübner S., Krenn S. (eds) Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data. Privacy and Identity 2018. IFIP Advances in Information and Communication Technology, vol 547. Springer, Cham. https://doi.org/10.1007/978-3-030-16744-8_12

Jaskyte, K., & Dressler, W. W. (2005). Organizational Culture and Innovation in Nonprofit Human Service Organizations. *Administration in Social Work*, 29(2), 23–41. https://doi.org/10.1300/J147v29n02_03

McAllister, C. (n.d.). WHAT ABOUT SMALL BUSINESSES? THE GDPR AND ITS CONSEQUENCES FOR SMALL U.S.-BASED COMPANIES. 12, 26.

Michael, K., Kobran, S., Abbas, R., & Hamdoun, S. (2019). Privacy, data rights and cybersecurity: Technology for good in the achievement of Sustainable Development Goals. *2019 IEEE International Symposium on Technology and Society (ISTAS)*. <https://doi.org/10.1109/istas48451.2019.8937956>

[Schein, E. H. \(1996\). Culture: The Missing Concept in Organization Studies. *Administrative Science Quarterly*, 41\(2\), 229. https://doi.org/10.2307/2393715](https://doi.org/10.2307/2393715)

“The Right to Relate’ by Cycling without Age.” *Cycling Without Age*, 9 Dec. 2021, <https://cyclingwithoutage.org/>.

Zendesk and Copenhagen Cycles. (2019, May 15). *Can A Trishaw ride change the world?* Cycling Without Age. Retrieved January 20, 2022, from <https://cyclingwithoutage.org/sustainable-development-goals/>

ITGP. (2019). Eu General Data Protection Regulation (GDPR): An implementation and compliance guide.