

EWAF25 -SOFTWARE DOCUMENTATION ANALYSIS – REV2

NLM-GUIDED DOCUMENTATION ASSESSMENT

MANUELE BARBIERI, LEO BIANCHI, EDOARDO PARETI

SUMMARY

INTRODUCTION	1
Run #1 (Thrively - Fairness Assessment):	1
Run #2 (Century Tech - Data Protection and Security Assessment):	1
CLASSIFICATION OUTCOMES:	2
ADDITIONAL NOTES:.....	2
RUN # 1.....	2
INPUTS:.....	2
ASSESSMENT RESULTS (WITHOUT FAIRNESS CHAPTER)	3
ASSESSMENT RESULTS (WITH FAIRNESS CHAPTER)	10
RESULTS (WITH COMMENTS):	15
RUN # 2.....	18
INPUTS:.....	18
ASSESSMENT RESULTS.....	19
RESULTS (WITH COMMENTS):	29

INTRODUCTION

The aim of this document is to present the results of the analyses performed by a local, private natural language model (NLM) when comparing a set of requisites (questions from TAI-SDF) against some documentation (in the form of PDF files).

The analyses are performed on documentation (available on the Internet) for educational software. The results are presents as a set of “runs”, where each run encompasses the inputs (software documentation), the user prompts (task, constraints...) and the obtained results (in form of a set of reports and a confusion matrix).

Run #1 (Thrively - Fairness Assessment):

The analysis presented in the current version of this document refers to documentation in RINA-C folder.

Run #2 (Century Tech - Data Protection and Security Assessment):

The analysis presented in the current version of this document refers to documentation that can be found at the following link:

<https://www.century.tech/wp-content/uploads/2024/02/CENTURY-Tech-Privacy-Policy-2024.pdf>

Which is also available in RINA-C folder.

CLASSIFICATION OUTCOMES:

TP: True Positive (the documentation addresses the question and the NLM correctly says it does)

TN: True Negative (the documentation does not address the question and the NLM correctly says it doesn't)

FP: False Positive (the documentation does not address the question and the NLM falsely says it does)

FN: False Negative (the documentation addresses the question and the NLM falsely says it doesn't)

ADDITIONAL NOTES:

The authors **highlighted** some NLM output sections that have been considered to be particularly relevant for the assessment.

RUN # 1

Considered SW: Thrively.

INPUTS:

System Prompt: You are an assistant whose role is to complete the given Task, considering the given Constraints and Inputs. You must strictly stick to the information in the Inputs in order to complete the Task. You are prohibited to infer or make assumptions: your answer must only depend on the given Inputs.

Task: You will be given in the Inputs a Question related to Thrively software, an AI-based learning platform targeted to discover and develop personal strengths, interests, and aspirations of every student to help them reach their full potential. Thrively can identify and understand the ways in which a student's best learn and his/her habits, as well as helping with identification of their career pathways, connecting their interests and personality types to the world of work.

In the Inputs you'll also be given Documentation about Thrively that contains the information you must consider to answer the Question.

Your Task is to check if the Documentation contains a satisfactory answer to the Question.

You will also be given AdditionalInformation as part of the Inputs to provide additional definitions you must consider when deciding whether the Documentation contains the information required to answer the Question.

Constraints: Motivate your answer with a brief explanation of why the Question is addressed or not by the Documentation.

AdditionalInformation: None

Examples: None

Computation details:

NLM: DeepSeek-r1:8b (distilled reasoning model)

NLM Backend: Ollama (local inference)

ASSESSMENT RESULTS (WITHOUT FAIRNESS CHAPTER)

1. Do you compute fairness metrics in evaluating the AI solution?

Report: Okay, so I need to figure out if the given Documentation addresses the Question provided. The Question is asking whether the Documentation includes information about computing fairness metrics when evaluating an AI solution. First, let me look at the Documentation. It's about a Strength Assessment platform used in the educational domain. From what I understand, this platform assesses students' strengths across various areas like Academic, Analytical, Appreciation, etc. It also considers their career aspirations and extracurricular interests. The goal seems to be helping students become self-aware and explore their potential through personalized profiles and project-based learning. Now, the AdditionalInformation is None, so I don't have any extra definitions to consider beyond what's in the Documentation. The Task is to check if the Documentation contains a satisfactory answer to the Question. The Constraints mention that I should motivate my answer with an explanation of why the Question is addressed or not by the Documentation. So, the key points from the Documentation are about assessing students' strengths and providing tools for educators to help them. **There's nothing mentioned about AI solutions, fairness metrics, or any evaluation processes related to AI systems.** The focus is entirely on student assessment and development, not on evaluating AI itself. Therefore, since the Documentation doesn't touch upon AI evaluation or fairness metrics, it doesn't address the Question at all. The Documentation provided does not address the question of computing fairness metrics in evaluating AI solutions. It focuses solely on a Strength Assessment platform for students, detailing their strengths and interests without mentioning anything related to AI evaluation or fairness metrics. Therefore, there is no information that answers the given question. ****Answer:** The Documentation does not contain any information about computing fairness metrics in evaluating AI solutions.**

2. Does the AI solution explain why it made a particular decision or return a specific result?

Report: Okay, so I need to figure out if the given Documentation from Thrively addresses the Question provided. The Question is asking whether the AI solution explains why it made a particular decision or returned a specific result. Looking at the Documentation, it's about a Strength Assessment platform used in education. It mentions that after an 80-question assessment, students receive personalized profiles based on 23 strengths. These include things like Academic, Analytical, Appreciation, etc. The documentation also talks about how educators can use this data to deliver project-based learning and provide enrichment opportunities. Students can connect with others who share their interests and track their progress in a Digital Portfolio. The AdditionalInformation section is empty, so I don't have any extra definitions to consider beyond what's in the Documentation. Now, considering the Constraints: I need to motivate my answer with why the Question is addressed or not by the Documentation. The examples

provided are about whether explanations are given for decisions or results. In the Documentation, there's no mention of AI making decisions or explaining its reasoning. It focuses on the Strength Assessment process and how educators and students can use the data. There's no discussion of algorithms, decision-making processes, or why specific strengths were identified over others. The platform's functionality is described, but not how the AI arrived at those results. So, the Documentation doesn't address the Question because it doesn't explain why particular decisions or results are made by the AI solution. It focuses more on the outcomes and how they can be used rather than the processes behind them. The Thrively Documentation does not address the Question regarding whether the AI solution explains its decision-making or results. The provided information focuses on the Strength Assessment process, outcomes, and their application by educators and students, without discussing the AI's algorithms or reasoning behind specific results. Therefore, the AI's decisions are not explained in the given materials. **Answer:** No, the Documentation does not address why the AI made particular decisions or returned specific results. It focuses on the Strength Assessment process and outcomes rather than explaining the AI's decision-making processes.

3. Is the AI solution accessible for people with disabilities?

Report: Okay, so I need to figure out if the given Documentation addresses whether the AI solution is accessible for people with disabilities. The Documentation provided talks about a Strength Assessment platform used in education. It mentions that after an 80-question assessment, students get personalized profiles based on their strengths, career aspirations, and extracurricular interests. The platform also offers project-based learning, enrichment activities, and connects students with others who share their interests, all tracked in a Digital Portfolio. The AdditionalInformation is none, so I only have the Documentation to go by. Now, the question is about accessibility for people with disabilities. The Documentation doesn't mention anything specific about accommodations or features that would make the platform accessible to individuals with disabilities. It focuses on strengths and career connections but doesn't touch on things like screen readers, sign language support, or other assistive technologies. I should check if there's any part where it talks about inclusivity or special education support. Scanning through the pages, I don't see any mention of accessibility features or partnerships with organizations that support disabled students. The platform seems to be more about personal development and career guidance without addressing the needs of students with disabilities. So, based on this, the Documentation doesn't provide information on how accessible the AI solution is for people with disabilities. It's focused on strengths and career pathways but lacks any details about accommodations or accessibility features. The Documentation provided does not address whether the AI solution is accessible for people with disabilities. While it discusses the Strength Assessment platform's features, such as personalized profiles and project-based learning, there is no mention of specific accessibility features or accommodations for individuals with disabilities. The focus is on strengths, career aspirations, and extracurricular interests without detailing how the platform might support students with diverse needs. Therefore, the Documentation does not adequately address the question of accessibility for people with disabilities.

4. Did you consider diversity and representativeness of end-users and/or subjects in the data?

Report: Okay, so I need to figure out if the given Documentation addresses whether diversity and representativeness of end-users and/or subjects in the data were considered. The Question is asking specifically about this. Looking at the Documentation provided, it talks about the Strength Assessment platform used in education. It mentions that after an 80-question assessment, students receive a personalized profile. The strengths measured include things like Academic, Analytical, Appreciation, Assertiveness, and so on, totaling 23 strengths. The AdditionalInformation section is empty, so I don't have any extra definitions to consider beyond what's in the Documentation. Now, considering diversity and representativeness: The Documentation doesn't explicitly mention anything about the diversity of the users or subjects involved in creating or validating the assessment. It does talk about the platform being used in the educational domain but doesn't specify if a wide range of students from different backgrounds was considered when developing the tool. I should check if there's any part where it mentions efforts to include diverse groups. Scanning through, I don't see anything that directly addresses this. The focus seems to be more on the features and strengths measured rather than the diversity aspects of the user base or data collection process. So, based on what's provided, there's no indication that diversity was considered in the end-users or subjects. Therefore, the Documentation doesn't address the Question adequately. The Documentation does not explicitly address whether diversity and representativeness were considered in the data. It focuses on the features of the Strength Assessment platform but lacks information about the diversity of users or subjects involved. Therefore, it does not adequately answer the question. ****Answer:**** The Documentation does not address whether diversity and representativeness were considered in the end-users or subjects, as it primarily focuses on the features and strengths measured rather than the diversity aspects of the user base.

5. Did you test for specific target groups or problematic use cases?

Report: Okay, so I need to figure out if the given Documentation from Thrively addresses the Question provided. The Question is asking whether they tested for specific target groups or problematic use cases. Let me break this down step by step. First, looking at the Documentation, it's about a Strength Assessment platform used in education. It mentions that after an 80-question assessment, students receive personalized profiles based on 23 strengths. These include things like Academic, Analytical, Appreciation, Athleticism, Balance, etc. The platform also talks about using this information to help educators deliver project-based learning and provide enrichment opportunities. Additionally, it states that the Strength Assessment uses a taxonomy based on decades of research and experience with thousands of children. Now, considering the Question: Did you test for specific target groups or problematic use cases? I need to determine if the Documentation mentions anything about testing specific groups or identifying potential issues with how the tool is used. Looking through the Documentation, there's no mention of testing specific target groups. It doesn't talk about any demographic studies, group comparisons, or specific populations tested. Similarly, there's nothing about problematic use cases. The focus seems to be on the strengths assessed and how educators can use that data, but not on whether certain groups might face challenges with the tool. The AdditionalInformation is None, so I don't have extra definitions to consider here. Therefore, based on the given information, the Documentation doesn't address testing for specific target groups or problematic use cases. ****Answer:**** Based on the provided Documentation from Thrively, there is no mention of testing specific target groups or identifying problematic use cases. The focus is primarily on the strengths assessed and how educators can utilize that data. Therefore, the Documentation does not address these aspects. ****Constraints Addressed:**** - ****No Specific Target Groups:**** The documentation does not

indicate any studies or comparisons with different demographic groups. - ****No Problematic Use Cases:**** There is no discussion of potential issues or challenges related to the tool's usage. ****Conclusion:**** The Thrively platform's documentation does not provide information on testing specific target groups or identifying problematic use cases, thus it does not address the Question adequately.

6. Did the AI solution ensure a mechanism that allows for the flagging of issues related to bias, discrimination or poor performance of the AI system?

Report: Okay, so I need to figure out if the given Documentation from Thrively addresses the question about whether there's a mechanism for flagging issues related to bias, discrimination, or poor performance in their AI system. Let me start by understanding what the question is asking. The question is specifically about whether the AI solution has a way to identify and flag problems like bias or poor performance. So I need to look through the provided Documentation to see if it mentions anything related to monitoring, feedback mechanisms, or quality assurance processes for their AI systems. Looking at the Documentation, it's all about the Strength Assessment platform. It talks about how students are assessed against 23 strengths factors, and how educators can use this data to provide personalized learning experiences. The platform uses a taxonomy based on decades of research and combines various attributes like focus, social justice, appreciation, etc. Now, I don't see any mention in the Documentation about AI systems or mechanisms for flagging issues. It's focused more on the assessment process itself rather than the technical aspects of the AI used to deliver this assessment. There's no discussion of how the system ensures fairness, handles biases, or corrects performance issues. The AdditionalInformation section is empty, so I can't rely on that either. Therefore, based on what's provided, there's no indication that Thrively has a mechanism for flagging bias or poor AI performance. ****Answer:**** Based on the provided Documentation and AdditionalInformation, the question regarding whether the AI solution includes a mechanism for flagging issues related to bias, discrimination, or poor performance is not addressed. The documentation focuses on the Strength Assessment platform's structure and student evaluation process without mentioning any mechanisms for monitoring or addressing AI-related issues. Therefore, there is no evidence in the given materials that Thrively has implemented such a mechanism. ****Constraints Met:**** - The answer strictly depends on the provided Inputs. - No assumptions were made beyond what was given. ****Conclusion:**** The Documentation does not provide information about a mechanism for flagging issues related to bias or poor AI performance.

7. Did you assess the risk of the possible unfairness of the system onto the end user's communities?

Report: Okay, so I need to figure out if the given Documentation addresses the Question provided. The Question is asking whether the risk of unfairness in the system has been assessed for end users' communities. Let me break this down step by step. First, looking at the Documentation, it's about a Strength Assessment platform used in education. It mentions that after an 80-question assessment, students receive personalized profiles based on 23 strengths. The platform also considers career aspirations and extracurricular interests. The goal is to help students discover their innate strengths, set future goals, and connect present interests with future aspirations. The Documentation emphasizes that the Strength Assessment uses a taxonomy based on decades of research by doctors studying child development. It includes attributes like focus, social justice, appreciation, and social acumen, among others. It also mentions that no strength is more important than any other, providing a broad, non-

judgmental view of each child. Furthermore, the platform allows educators to deliver project-based learning, provides enrichment opportunities, connects students with community peers, and tracks activities in a Digital Portfolio. The science behind it is grounded in lifespan development, strength-based research, neural connectivity, optimal brain functioning, motivational variables, and years of experience with thousands of children. Now, considering the Question about assessing the risk of unfairness in the system affecting end users' communities. The Documentation doesn't explicitly mention anything about fairness or potential biases in the assessment process. It focuses on strengths identification, career connections, and educational support but doesn't address how the system might inadvertently favor certain groups over others or whether there are measures in place to prevent unfair treatment. So, based on this analysis, the Documentation does not directly address the risk of unfairness in the system. There's no mention of assessments for bias, fairness, or ensuring equitable outcomes for different communities. The Documentation provided does not explicitly address the assessment of risks related to unfairness in the system affecting end users' communities. While it details the strengths assessment process and its educational support features, there is no mention of measures taken to prevent biases or ensure equity. Therefore, the risk of unfairness is not addressed in the given materials.

8. Did the AI solution write clear privacy notices for children so that they are able to understand what will happen to their personal data and what rights they have?

Report: Okay, so I need to figure out if the given Documentation from Thrively addresses the Question about whether they provide clear privacy notices for children to understand their personal data and rights. Let me break this down step by step. First, the Question is asking specifically about privacy notices tailored for children. So, I'm looking for information in the Documentation that talks about how Thrively informs kids about their data and what their rights are. Looking at the Documentation provided, it's all about the Strength Assessment platform. It mentions personalized profiles, career aspirations, extracurricular interests, and how educators can use this info to help students. There's a lot about strengths like Academic, Analytical, Appreciation, etc., and how these are measured. It also talks about project-based learning, Digital Portfolios, and community connections. Now, the AdditionalInformation says there's none, so I don't have any extra definitions beyond what's in the Documentation. The Constraints mention motivating my answer with why the Question is or isn't addressed, so I need to explain that based on the given info. I don't see anything in the Documentation about privacy policies or notices for children. It focuses more on educational tools and student strengths rather than data protection. So, it seems like the Documentation doesn't address the specific issue of privacy notices for kids. The Thrively Documentation does not address the creation of clear privacy notices for children regarding their personal data and rights. While it emphasizes personalized profiles and educational tools, there is no mention of policies or measures to inform students about data protection. Therefore, the documentation does not satisfy the Question as it pertains to privacy notices specifically tailored for children.

9. In which way the result of the profiling made by the AI solution affect the children?

Report: Okay, so I need to figure out if the given Documentation adequately addresses the Question about how the AI profiling results affect children. Let me start by understanding both the question and the documentation. The Question is asking about the impact of the AI profiling on children. Specifically, it's

about how the results from this profiling affect them. The Documentation provided talks about a Strength Assessment platform used in education. It mentions that after an 80-question assessment, students receive a personalized profile. This profile is based on 23 different strength factors, which include things like Academic, Analytical, Appreciation, Athleticism, Balance, etc. The documentation goes into detail about each of these strengths and how they are measured. It also explains that the Strength Assessment helps educators deliver project-based learning, provides enrichment opportunities, connects students with peers who share their interests, and tracks progress through a Digital Portfolio. The assessment is based on decades of research and uses a broad definition of personality beyond typical tests. So, breaking this down: The AI profiling (Strength Assessment) identifies various strengths in children. These strengths are used to provide personalized feedback, which can help students understand their abilities. This self-awareness can motivate them and guide their future goals. Educators use this information to tailor learning experiences, which could make education more engaging and relevant for each child. The impact on children would likely include increased self-confidence, a better understanding of their strengths and interests, guidance in setting career aspirations, access to resources that match their strengths, and opportunities for growth in areas they excel in. It also mentions connecting with a community of peers with similar interests, which can foster social connections and collaboration. However, the Documentation doesn't explicitly state how these results affect children beyond providing personalized profiles and enrichment opportunities. It focuses more on what the platform does rather than the outcomes or effects on the children themselves. There's no mention of psychological impacts like increased confidence or motivation, or long-term benefits such as improved academic performance or career satisfaction. So, while the documentation explains the structure and components of the profiling, it doesn't directly address how these results influence or affect the children beyond providing personalized information and educational resources. Therefore, the Documentation may not fully satisfy the Question because it doesn't explicitly detail the effects on the children but rather focuses on the platform's features. The Documentation provided discusses the Strength Assessment platform, detailing its components and how educators use the results to tailor learning experiences for students. However, it does not explicitly address the impact of these profiling results on the children themselves. While it mentions benefits like personalized feedback and enrichment opportunities, it doesn't delve into specific outcomes such as increased self-confidence or improved academic performance. Therefore, the Documentation does not fully satisfy the Question as it focuses more on the platform's features rather than the effects on the children. **Answer:** The Documentation does not explicitly address how the AI profiling results affect children beyond providing personalized information and educational resources. It focuses on the platform's structure and components rather than detailing specific outcomes or impacts on the students.

10. Can the AI solution stop profiling of children if they ask you for?

Report: Okay, so I need to figure out if the given Documentation from Thrively addresses the Question posed. The Question is asking whether the AI solution can stop profiling of children if they ask for it. Let me break this down step by step. First, let's understand what the Documentation says. It describes a Strength Assessment platform used in education. After an 80-question assessment, students receive a personalized profile with information about their strengths, career aspirations, and extracurricular interests. The goal is to help students become self-aware and explore their potential through project-based learning, enrichment activities, and community connections tracked in a Digital Portfolio. The Strength Assessment uses a taxonomy based on decades of research and includes 23 different strengths,

such as Academic, Analytical, Appreciation, Assertiveness, Athleticism, Balance, Compassion, Coordination, Creative Skill, Creative Thinking, Drive, Flexibility, Focus, Fun-loving, Independence, Leadership, Memory, Patience, Resilience, Social, Social Justice, Verbal, and Worldly. Each strength is described in detail. Now, the Question is about whether the AI can stop profiling if a child asks. The key here is understanding what "profiling" means in this context. Profiling could imply that the system is creating detailed profiles of students based on their strengths and other assessed data. The Documentation mentions that these profiles are used to provide personalized recommendations, project-based learning opportunities, and connections to communities aligned with their interests. So, does the AI stop profiling upon request? **The Documentation doesn't explicitly mention any mechanism for a student or parent to opt out or request that their profile be deleted or not used.** It focuses on how the platform uses the information to help students explore their strengths and potential pathways. There's no indication of user control over the data collection or usage beyond the initial assessment. Therefore, based on the provided Documentation, there's no evidence that the AI solution allows for stopping or modifying profiling upon a child's request. **The system seems designed to utilize the collected information to support educational and developmental goals without giving users an option to disable such profiling.** The Thrively platform's documentation does not address the ability of children to stop profiling upon request. It focuses on using student data to provide personalized resources and opportunities, but there is no mention of user control over data collection or usage. Therefore, the AI solution as described does not allow for stopping profiling if a child asks. ****Answer:**** The Documentation does not explicitly address whether the AI can stop profiling children upon their request. It focuses on using the information to provide personalized resources and opportunities without mentioning an option for users to opt out or disable profiling.

ASSESSMENT RESULTS (WITH FAIRNESS CHAPTER)

1. Do you compute fairness metrics in evaluating the AI solution?

Report: Okay, so I need to figure out if the given Documentation addresses the Question about whether Thrively computes fairness metrics in evaluating their AI solution. Let me start by understanding what each part is. The Question is asking specifically if Thrively uses fairness metrics when evaluating their AI solution. From the Documentation provided, it talks a lot about AI fairness in education, mentioning things like bias mitigation mechanisms and specific fairness metrics like Disparate Impact Discrimination Index (DIDI). It also discusses how data biases can affect AI systems and the steps taken to address these issues. So, I need to check if the Documentation includes information on fairness metrics. The term "fairness metrics" is mentioned in the context of evaluating AI solutions, specifically using DIDI as an example. This suggests that Thrively does consider such metrics when assessing their AI tools. I should make sure there's no assumption here. The Documentation clearly states that they use mechanisms to detect and mitigate bias, including fairness metrics like DIDI. Therefore, it does address the question. The Documentation provided explicitly discusses the use of fairness metrics in evaluating AI solutions, specifically mentioning the Disparate Impact Discrimination Index (DIDI) as a measure used to assess fairness. This indicates that Thrively incorporates such metrics when evaluating their AI tools.

****Answer:**** Yes, the Documentation addresses the Question by explaining that Thrively uses fairness metrics like DIDI to evaluate AI solutions, aiming to mitigate biases and ensure fair outcomes.

2. Does the AI solution explain why it made a particular decision or return a specific result?

Report: Okay, so I need to figure out if the given Documentation addresses the Question provided. The Question is asking whether the AI solution explains why it made a particular decision or returned a specific result. Looking at the Documentation, it's about AI Fairness in education, specifically discussing issues like bias, transparency, and how AI systems might perpetuate unfairness. It mentions that AI-powered tools can reflect biases from their training data, leading to unfair assessments. There's also talk about mitigation mechanisms like pre-processing, processing techniques, and post-processing to address these biases. However, the Documentation doesn't explicitly explain why specific decisions were made by the AI. It talks about fairness metrics like Disparate Impact Discrimination Index (DIDI) but doesn't go into detail on how or why particular outcomes occurred. There's no step-by-step explanation of how the AI arrived at a conclusion or decision. So, while it discusses potential biases and mitigation strategies, it doesn't provide the reasoning behind each decision made by the AI solution. Therefore, the Documentation doesn't fully address the Question as it doesn't explain the reasoning for specific results. The Documentation provided does not adequately address the Question of explaining why a particular decision or result was made by the AI solution. While it discusses issues like bias mitigation and fairness metrics, it lacks explicit explanations of how the AI arrived at specific outcomes. Therefore, the answer to the Question is that the Documentation does not sufficiently explain the reasoning behind decisions. ****Answer:**** The Documentation does not adequately address why a particular decision or result was made by the AI solution. It discusses potential biases and mitigation strategies but does not provide the reasoning for specific outcomes.

3. Is the AI solution accessible for persons with disabilities?

Report: Okay, so I need to figure out if the given Documentation addresses whether the AI solution is accessible for persons with disabilities. Let me start by reading through the Documentation carefully. The Documentation talks about AI fairness in education, specifically mentioning issues like bias and unfair outcomes, especially for marginalized groups. It also discusses how AI-powered tools can perpetuate biases from training data, leading to unfair assessments. There's a section on mitigation measures, including data preprocessing, processing techniques, and postprocessing to adjust predictions. It mentions the use of fairness metrics like Disparate Impact Discrimination Index (DIDI) to measure bias in AI outputs. However, I don't see any specific information about accessibility features for persons with disabilities. The focus is more on fairness and bias mitigation rather than accommodations or tools that make the AI solution accessible to individuals with disabilities. So, while the Documentation addresses biases and unfairness, it doesn't touch on accessibility features necessary for people with disabilities. Therefore, it doesn't satisfactorily answer whether the AI solution is accessible for persons with disabilities. The Documentation provided does not address the accessibility of the AI solution for persons with disabilities. It focuses on bias mitigation and fairness issues but lacks information on specific accommodations or features designed to make the AI solution accessible to individuals with disabilities. Therefore, it does not satisfactorily answer whether the AI solution is accessible for persons with disabilities. ****Answer:** The Documentation does not address accessibility for persons with disabilities, focusing instead on bias mitigation and fairness.**

4. Did you consider diversity and representativeness of end-users and/or subjects in the data?

Report: Okay, so I need to figure out if the given Documentation addresses the Question about diversity and representativeness of end-users and/or subjects in the data. The Question is asking whether the developers considered how diverse or representative their data sources are when building the AI system. Looking at the Documentation provided, it talks a lot about AI fairness and bias in education. It mentions that AI systems can perpetuate biases from the training data, leading to unfair outcomes for marginalized groups. For example, essay grading might be biased if the training data reflects only certain cultural backgrounds or writing styles. The documentation also discusses mitigation measures like pre-processing to balance group representation, processing techniques to integrate fairness, and post-processing to adjust predictions. **They use metrics like Disparate Impact Discrimination Index (DIDI) to measure bias. So, they are aware of the need for fair data and have mechanisms in place to mitigate biases based on diverse data sources. This suggests that they considered diversity and representativeness when developing the system.** The Documentation addresses the Question by acknowledging the importance of diversity and representativeness in data. It discusses how biases can arise from inadequate or biased data and implements mitigation strategies, such as balancing group representation and using fairness metrics like DIDI. These measures indicate that **the developers considered diverse data sources and aimed to reduce bias, thus addressing the concerns raised by the Question.**

5. Did you test for specific target groups or problematic use cases?

Report: Okay, so I need to figure out if the given Documentation addresses the Question about whether specific target groups or problematic use cases were tested for Thrively. The Question is asking if they've tested for particular groups or issues that might arise from their AI-based learning platform. Looking at the

Documentation provided, it's focused on AI fairness in education, specifically discussing how AI can perpetuate biases and the measures taken to mitigate these issues. It mentions things like data bias, user interaction bias, and uses metrics like Disparate Impact Discrimination Index (DIDI) to assess fairness. However, the Documentation doesn't mention anything specific about Thrively's target groups or any problematic use cases they've identified or tested for. It talks in general terms about AI in education but doesn't tie it back to Thrively's features or how they might affect certain student groups. So, even though the documentation discusses fairness and bias mitigation, it doesn't directly address whether specific target groups were tested or if problematic use cases were identified and assessed for Thrively. It seems more like a general statement about AI in education rather than something specific to Thrively's practices. The Documentation provided does not specifically address whether Thrively has tested for specific target groups or problematic use cases. While it discusses AI fairness in education, including bias mitigation measures and metrics like DIDI, these are presented in a general context applicable to AI systems in education rather than focusing on Thrively's unique features or practices. Therefore, the Documentation does not directly answer the Question as it pertains to Thrively specifically. ****Answer:****

The Documentation does not specifically address whether Thrively has tested for specific target groups or problematic use cases. It discusses general AI fairness considerations but does not tie these to Thrively's features or practices.

6. Did the AI solution ensure a mechanism that allows for the flagging of issues related to bias, discrimination or poor performance of the AI system?

Report: Okay, so I need to figure out if the given Documentation addresses the Question about whether the AI solution ensures a mechanism for flagging issues related to bias, discrimination, or poor performance. Let me break this down step by step. First, the Question is asking specifically about a mechanism that flags such issues. The Documentation provided talks about AI fairness in education, mentioning things like data biases, mitigation mechanisms, and uses terms like Disparate Impact Discrimination Index (DIDI). It also discusses how the system reduces human bias through uniform criteria but acknowledges that inherent biases can still be a concern. I'm trying to see if there's any mention of a specific mechanism or tool that flags issues. The Documentation mentions "mitigation measures" and "fairness metrics," which include DIDI, but it doesn't explicitly say that the system has a flagging feature. It talks about how biases are addressed through data preprocessing, processing techniques, and postprocessing adjustments, but not necessarily a way to detect and flag problematic instances in real-time or during use. So, while the Documentation discusses bias mitigation and fairness metrics, it doesn't clearly state that there's a mechanism for flagging specific issues. It focuses more on the theoretical approaches rather than an operational tool for detection. Therefore, I think the Documentation doesn't fully address the Question as it doesn't mention a flagging system. The Documentation discusses various methods to mitigate bias and assess fairness metrics like DIDI but does not explicitly describe a mechanism for flagging specific issues related to bias or poor performance. It focuses on theoretical approaches rather than operational tools, thus not addressing the Question fully. ****Answer:**** The Documentation does not explicitly mention a mechanism for flagging issues related to bias, discrimination, or poor AI performance. While it discusses mitigation measures and fairness metrics, it doesn't provide details on an actual flagging system.

7. Did you assess the risk of the possible unfairness of the system onto the end user's communities?

Report: Okay, so I need to figure out if the given Documentation addresses the Question about whether they assessed the risk of unfairness in their system towards end users' communities. Let me break this down step by step. First, the Question is asking specifically about an assessment of the risk of unfairness. The Documentation provided talks a lot about AI fairness in education, mentioning issues like bias in data and how it can affect assessments. It also discusses mitigation mechanisms such as pre-processing, processing techniques, and post-processing to address these biases. They mention metrics like Disparate Impact and the DIDI index to measure fairness. So, I need to see if the Documentation not only identifies potential unfairness but also assesses the risk of it. The term "assess" here is crucial because it's about evaluating whether there's a problem before taking steps to mitigate it. Looking at the Documentation, they do talk about assessing biases and implementing measures to mitigate them. They mention data bias, user interaction bias, and have fairness metrics like DIDI to quantify disparities. This suggests that they've not only identified potential issues but also assessed how significant these risks are. However, I should be careful here. The word "assess" can sometimes mean different things. In this context, it's about evaluating the risk of unfairness, which involves looking at whether their system could inadvertently cause unfair treatment. The Documentation does discuss assessing biases and using metrics to measure disparities, which implies they've evaluated the risks. But wait, is there any part where they explicitly state that they have assessed the risk? They talk about considering biases and implementing mitigation measures but don't explicitly say they performed a formal assessment of the risk. It's more about the mechanisms in place rather than an actual evaluation or quantification of the risk itself. So, maybe the answer is that while they discuss potential biases and have measures to mitigate them, there isn't explicit documentation showing that they've assessed the risk of unfairness on end users' communities. They might be more focused on preventing issues rather than assessing whether the system is currently at risk. I think I need to check if the Documentation includes any section or statement where they evaluate the likelihood or impact of unfairness. From what's provided, it seems they're more on the prevention and mitigation side without explicitly stating an assessment of the risk. **The Documentation discusses potential biases in AI systems and outlines mitigation strategies, including fairness metrics like DIDI to measure disparities. However, it does not explicitly state that a formal assessment of the risk of unfairness was conducted.** The focus is more on preventing issues rather than evaluating the current risk. Therefore, while they have measures in place, there's no explicit mention of assessing the risk itself. ****Answer:** The Documentation discusses potential biases and mitigation strategies but does not explicitly address whether a formal assessment of the risk of unfairness was conducted.**

8. Did the AI solution write clear privacy notices for children so that they are able to understand what will happen to their personal data and what rights they have?

Report: Okay, so I need to figure out if the given Documentation addresses the Question about whether Thrively's AI solution wrote clear privacy notices for children that they can understand. Let me start by reading both the Question and the Documentation carefully. The Question is asking specifically about privacy notices tailored for children, ensuring they can understand what happens to their data and their rights. The Documentation provided talks a lot about AI in education, fairness, bias mitigation, and uses terms like "strength assessment," "AI-driven assessment tool," and mentions things like uniform criteria and reducing human biases. Looking at the Documentation, I don't see any mention of privacy notices or anything related to how data is handled for children. It focuses more on the technical aspects of AI in assessments, fairness issues, and mitigation techniques but doesn't touch on privacy policies or child-

friendly language. There's no discussion about how personal data is collected, stored, or protected, nor how it might be explained to children in an age-appropriate way. So, even though Thrively seems to focus on understanding students' strengths and providing personalized learning experiences, the provided Documentation doesn't address the creation of privacy notices for children. It's more about the technical aspects of AI usage rather than the user-facing aspects like privacy communication. Therefore, based on the given information, the Documentation does not satisfy the Question because it lacks any content related to privacy notices or child-friendly explanations of data handling. The Documentation provided does not address the creation of privacy notices for children. It focuses on technical aspects of AI in education, such as bias mitigation and assessment tools, without mentioning anything about privacy policies or how data is communicated to children. Therefore, it does not satisfy the Question regarding clear privacy notices for children. ****Answer:** The Documentation does not contain information about clear privacy notices for children, focusing instead on AI's role in assessments and fairness.**

9. In which way the result of the profiling made by the AI solution affect the children?

Report: Okay, so I need to figure out how the AI profiling results affect children in Thrively. Let me start by looking at the documentation provided. **The documentation talks about AI fairness in education and mentions that deploying AI can lead to unfair outcomes if biases are present in the data.** It specifically discusses how AI-powered essay grading might favor certain writing styles or cultural backgrounds over others, which could disadvantage students from marginalized groups. This makes me think that the profiling results could inadvertently reinforce existing biases. There's also a section on bias mitigation mechanisms. The system uses pre-processing to balance data representation, in-processing to integrate fairness into algorithms, and post-processing to adjust predictions. These measures aim to reduce disparities based on protected attributes like race or gender. The fairness metrics include Disparate Impact Discrimination Index (DIDI), which measures how negatively AI outputs affect different groups. A higher DIDI indicates more disparity, so the system uses this to assess and mitigate unfair impacts. **Putting this together, the profiling affects children by potentially causing unfair treatment if biases aren't addressed.** However, Thrively has mechanisms in place to detect and reduce these biases, aiming for fairer outcomes. The AI profiling results in Thrively can affect children by potentially leading to unfair treatment if biases exist in the data used. The system addresses this issue through bias mitigation strategies such as balanced data representation, algorithmic fairness integration, and prediction adjustments. Additionally, it uses metrics like DIDI to monitor and reduce disparities, aiming for fairer outcomes.

10. Can the AI solution stop profiling of children if they ask you for?

Report: Okay, so I need to figure out if the given Documentation addresses whether the AI solution can stop profiling of children when asked. Let me start by reading through the Documentation carefully. The Documentation talks about AI fairness in education and mentions issues like bias and unfairness due to AI systems trained on biased data. It also discusses how AI grading might reflect human biases, leading to unfair assessments. There's a section on mitigation measures, including pre-processing, processing techniques, and post-processing to adjust model predictions for fairness. It specifically mentions the Disparate Impact Discrimination Index (DIDI) as a fairness metric used to quantify bias in AI models. The documentation seems focused on how AI can introduce biases but also outlines steps taken to mitigate

these issues. Now, the question is about whether the AI can stop profiling of children if asked. Profiling here likely refers to collecting or using personal data that could lead to biased assessments. The Documentation doesn't explicitly mention user interaction bias mitigation beyond what's already covered. It talks about adapting AI behavior based on feedback but doesn't specify how users can request profiling to be stopped. I don't see any direct information on user mechanisms to halt profiling. The focus is more on the technical aspects of reducing bias in data and models rather than user control or requests. So, while the documentation addresses fairness and mitigation, it doesn't provide a clear method for stopping profiling when requested by users. The Documentation provided does not explicitly address whether the AI solution can stop profiling of children when asked. While it discusses fairness and mitigation measures to reduce bias in AI systems, such as using the Disparate Impact Discrimination Index (DIDI), it does not specify mechanisms for user interaction or requests to halt profiling. Therefore, there is no clear indication that the AI system can respond to user requests to stop profiling children.

RESULTS (WITH COMMENTS):

Q1: Do you compute fairness metrics in evaluating the AI solution?

Original: The original documentation does not address fairness metrics at all. NLM recognizes it. → **TN**

Edited: The edited documentation does address fairness metrics with an explicit metric (DIDI). NLM recognizes it. → **TP**

Q2: Does the AI solution explain why it made a particular decision or return a specific result?

Original: The original documentation does not address explainability of its outcomes at all. NLM recognizes it. → **TN**

Edited: The edited documentation does address explainability of its outcomes at all. NLM recognizes it. → **TN**

Q3: Is the AI solution accessible for people with disabilities?

Original: The original documentation does not address accessibility issues at all. NLM recognizes it. → **TN**

Edited: The edited documentation does not address accessibility issues at all. NLM recognizes it. → **TN**

Q4: Did you consider diversity and representativeness of end-users and/or subjects in the data?

Original: The original documentation does not address diversity and representativeness issues at all. NLM recognizes it. → **TN**

Edited: The edited documentation does address diversity and representativeness issues, since it includes also a fairness metric. NLM recognizes it. → **TP**

Q5: Did you test for specific target groups or problematic use cases?

Original: The original documentation does not address if and how testing for specific target groups or problematic use cases was performed at all. NLM recognizes it. → **TN**

Edited: The edited documentation does not address if and how testing for specific target groups or problematic use cases was performed at all. NLM recognizes it. → **TN**

Q6: Did the AI solution ensure a mechanism that allows for the flagging of issues related to bias, discrimination or poor performance of the AI system?

Original: The original documentation does not address if a mechanism that allows for the flagging of issues related to bias, discrimination or poor performance of the AI system is present at all. NLM recognizes it. → **TN**

Edited: The edited documentation does not address if a mechanism that allows for the flagging of issues related to bias, discrimination or poor performance of the AI system is present at all. NLM recognizes it. → **TN**

Q7: Did you assess the risk of the possible unfairness of the system onto the end user's communities?

Original: The original documentation does not address the risk of possible unfairness in the system's outcomes. NLM recognizes it. → **TN**

Edited: The edited documentation does not address the risk of possible unfairness in the system's outcomes. It talks about fairness but not about a formal bias risk assessment. NLM recognizes it. → **TN**

Q8: Did the AI solution write clear privacy notices for children so that they are able to understand what will happen to their personal data and what rights they have?

Original: The original documentation does not address clear privacy notices for children at all. NLM recognizes it. → **TN**

Edited: The edited documentation does not address clear privacy notices for children at all. NLM recognizes it. → **TN**

Q9: In which way the result of the profiling made by the AI solution affect the children?

Original: Quoting the NLM: "the Documentation doesn't explicitly state how these results affect children beyond providing personalized profiles and enrichment opportunities. It focuses more on what the platform does rather than the outcomes or effects on the children themselves. There's no mention of psychological impacts like increased confidence or motivation, or long-term benefits such as improved academic performance or career satisfaction". The authors consider the Documentation not able to clearly state how the profiling made by the AI solution affects the students → **TN**

Edited: Quoting the NLM: “The documentation talks about AI fairness in education and mentions that deploying AI can lead to unfair outcomes if biases are present in the data”, which is true. → **TP**

Q10: Can the AI solution stop profiling of children if they ask you for?

Original: The original documentation does not address any mechanism to stop students profiling at all. NLM recognizes it. → **TN**

Edited: The edited documentation does not address any mechanism to stop students profiling at all. NLM recognizes it. → **TN**

Overall:

A reasoning NLM performed well on small tasks like assessing if fairness metrics (Q1) or solutions to stop children profiling (Q10) are clearly stated in the documentation. However, questions like Q9 can be ambiguous for an NLM.

Confusion Matrix (Without Fairness):

		Predicted	
		Positive:	Negative:
Total:		0	10
Actual	Positive:	True Positive: 0	False Negative: 0
	Negative:	False Positive: 0	True Negative: 10

Precision = 100%

Recall = 100%

Confusion Matrix (With Fairness):

		Predicted	
		Positive:	Negative:
Actual	Total:	0	10
	Positive:	True Positive: 3	False Negative: 0
	Negative:	False Positive: 0	True Negative: 7

Precision = 100%

Recall = 100%

RUN # 2

Considered SW: Century Tech.

INPUTS:

System Prompt: You are an assistant whose role is to complete the given Task, considering the given Constraints and Inputs. You must strictly stick to the information in the Inputs in order to complete the Task. You are prohibited to infer or make assumptions: your answer must only depend on the given Inputs.

Task: You will be given a Documentation that describes how Century Tech company and services handle user data privacy and security.

Your Task is to check if the Documentation contains a satisfactory answer to the Question.

You will also be given Additional Information as part of the Inputs to provide additional definitions you must consider when deciding whether the Documentation contains the information required to answer the Question.

Constraints: Motivate your answer with a brief explanation of why the Question is addressed or not by the Documentation.

Additional Information: CenturyTech is an edtech company that uses artificial intelligence (AI) to create personalized learning experiences. Century Tech focuses on helping educators and students by offering tools for adapting lessons to individual learning styles and needs. The platform provides a range of features, including data analytics, content creation, and assessment tools. It aims to improve student outcomes by making learning more tailored and efficient.

Examples: None

Computation details:

NLM: DeepSeek-r1:8b (distilled reasoning model)

NLM Backend: Ollama (local inference)

ASSESSMENT RESULTS

Q1. If you reuse already existing data for the purposes of training and development of the AI system, has the database been compiled and data collected in accordance with data protection regulations?

Report: Okay, so I need to figure out if the Century Tech documentation addresses whether their database is compiled and data collected in accordance with data protection regulations when reusing existing data for AI training. Let me start by understanding the question. The user wants to know if Century Tech ensures that their database, which includes personal data from users, meets data protection regulations when they reuse this data for training and developing AI systems. This is important because data privacy laws require organizations to handle such data responsibly. Looking at the provided documentation, I'll go through each section to see how it relates to this question. First, the Privacy Notice starts by explaining what personal data means and the purpose of the notice. It mentions that Century Tech collects various types of data from different groups like teachers, students, parents, etc. The notice also talks about how they process this data for providing services, improving the platform, and other legitimate interests. In section 2, it explains their role as a data processor when working with educational establishments and as a data controller when users subscribe directly. This is crucial because it shows how they handle different scenarios, which might affect data protection measures. Section 3 covers how to contact them, which isn't directly relevant but confirms the process for queries. Sections 4 and 5 detail what personal data they collect, including identity, contact, registration, financial, transaction, profile, behavioral, technical, and marketing data. This extensive list indicates the variety of data they handle, which is important because different data types have varying protection requirements. Section 6 discusses responsibility for students' data, emphasizing that educational establishments are responsible for ensuring consent, especially for minors. This shows they understand their obligations regarding minor's data. Sections 7 and 8 explain how they collect and use personal data, categorizing the purposes like account creation, service provision, browsing, interactive features, etc. Each purpose has a legal basis, which is necessary for compliance with GDPR or similar regulations. Section 9 talks about sharing personal data only when legally permitted, using contractual arrangements and security mechanisms. This reassures that they don't share data without justification. Sections 10-12 cover obtaining consent,

third-party links, transfers outside the EEA, retention periods, confidentiality, minors' data, rights as a data subject, and complaints. These sections provide information on how they handle data beyond collection and processing, which is relevant for compliance. The Additional Information states that Century Tech uses AI for personalized learning tools, which ties into their use of data for training purposes. Now, considering all this, the documentation covers what personal data they collect, how it's used, legal bases for processing, consent handling, data transfers, and rights. It also mentions security measures and compliance with regulations. However, there's no explicit mention of whether existing data is compiled and collected in accordance with regulations specifically for AI training purposes. The question is about reusing existing data for AI, which might involve specific considerations like data minimization, purpose limitation, or ensuring that the data processing aligns with the intended use. The documentation doesn't explicitly address these aspects when it comes to AI training. It does mention using data for analysis and improvement, but not specifically for AI systems. Therefore, while the documentation provides a broad overview of their data handling practices, it doesn't directly confirm compliance with data protection regulations specifically for reusing existing data in AI training. They might be compliant without explicitly stating it, but the documentation doesn't address this point clearly. The Century Tech documentation outlines their approach to personal data collection and processing, covering various aspects such as types of data, legal bases for processing, consent handling, security measures, and rights of data subjects. While it provides a comprehensive overview of their data practices, it does not explicitly address whether the reuse of existing data for AI training is conducted in accordance with data protection regulations. The documentation mentions using data for analysis and improvement but does not specifically highlight compliance with regulations related to AI training purposes. Therefore, while Century Tech likely adheres to relevant data protection standards, the documentation does not explicitly confirm this specific aspect.

Q2. Did you anonymize and aggregate incoming data using practice data-scrubbing pipelines: considering removing personally identifiable information (PII) and outlier or metadata values that might allow de-anonymization?

Report: Okay, so I need to figure out if the Century Tech documentation adequately addresses whether they anonymize and aggregate incoming data using data-scrubbing pipelines to remove PII and other metadata that could allow de-anonymization. First, I'll look through the provided Documentation. It starts with a privacy notice effective from May 1, 2024. The purpose is to explain how Century Tech processes personal data in connection with their business, including their website and services. In Section 2, it talks about who they are and their role as either a data processor for educational establishments or a data controller when users sign up directly. It mentions that they collect various types of data like identity, contact, registration, financial, transaction, profile, behavioral, technical, and marketing data. Section 5 goes into how they use personal data, categorizing it based on different scenarios (like account creation, purchases, browsing, etc.). They mention using this data for purposes such as providing services, improving the platform, customer service, surveys, promotions, events, and advertising. In Section 7, under "Insight, analysis, and retargeting through Cookies," they explain that they use cookies to collect behavioral and technical data. This helps them analyze usage and improve their platform. They also mention sharing personal data with third parties for marketing purposes, like social media platforms. Section 12 discusses transfers outside the UK and EEA, stating they comply with legal obligations and put safeguards in place. Section 13 talks about how long they keep data, up to six years from service supply, unless used for a specific purpose or suppression lists. Sections on confidentiality, security measures,

minors' data, and rights as a data subject are also included. The documentation emphasizes compliance with applicable laws and provides information on user rights like access, rectification, erasure, restriction, portability, objection, and consent withdrawal. Now, considering the AdditionalInformation: Century Tech uses AI for personalized learning tools, focusing on adapting lessons to individual needs. They offer data analytics, content creation, and assessment features aiming to improve student outcomes. The question is about anonymizing and aggregating data using scrubbing pipelines to remove PII and metadata that could de-anonymize. The documentation doesn't explicitly mention data-scrubbing pipelines or specific methods for anonymization beyond general processing of personal data. It does talk about cookies and third-party sharing but not in the context of data anonymization techniques. While the document outlines how they handle personal data, it's unclear if they specifically use scrubbing pipelines to aggregate and anonymize data. Terms like "data-scrubbing pipelines" or specific methods aren't mentioned, so there's no direct evidence they employ such practices. The documentation provided by Century Tech does not explicitly address the use of data-scrubbing pipelines for anonymizing and aggregating incoming data. While it outlines various aspects of personal data handling, including collection, processing, and third-party sharing, it does not specifically mention or detail the implementation of such techniques as data-scrubbing pipelines. Therefore, there is no direct evidence that Century Tech employs these specific methods for data anonymization. ****Answer:**** The documentation does not explicitly address whether Century Tech uses data-scrubbing pipelines to anonymize and aggregate incoming data. While it details their approach to personal data handling, including collection and processing purposes, it lacks explicit mention of such techniques.

Q3. Do you monitor the compliance of training data processing with data protection requirements?

Report: Okay, so I need to figure out if the Century Tech documentation addresses whether they monitor compliance with data protection requirements when processing training data. Let me start by understanding the question: Do they check that their handling of training data meets necessary privacy regulations? Looking at the provided Documentation, it's a Privacy Notice from Century-Tech. The document outlines how they process personal data, including for students, teachers, parents, etc. It mentions compliance with applicable laws and regulatory requirements, but I'm not sure if it specifically talks about monitoring or ensuring that training data is compliant. I should check each section. Section 2 talks about their role as a data processor or controller depending on the scenario. They mention complying with changes in law or regulations, which suggests they aim to stay compliant. However, there's no explicit mention of actively monitoring compliance during data processing for training purposes. Section 7 discusses how they use personal data, including for training and development. It says they process data to improve their services but doesn't specify if they monitor this against privacy standards. Section 12 mentions transferring data outside the EEA with safeguards, which is about compliance when moving data, not necessarily monitoring during processing. The AdditionalInformation states that Century Tech uses AI for personalized learning tools, focusing on student outcomes. They have features like data analytics and content creation. But again, nothing directly about monitoring compliance in training data handling. So, while the documentation covers their commitment to privacy laws and how they process data, it doesn't explicitly address whether they actively monitor or ensure that training data processing meets required standards. Therefore, the answer is no, the documentation does not satisfactorily answer the question. The Century Tech documentation does not explicitly address whether they monitor compliance with data protection requirements when processing training data. While it outlines their commitment to privacy laws and data handling practices, there's no mention of

actively monitoring or ensuring that training data meets necessary standards. Therefore, the answer is:
Answer: The Documentation does not satisfactorily address whether Century Tech monitors compliance with data protection requirements for training data processing.

Q4. Did you take measures to enhance privacy-by-design, such as via encryption, pseudonymization, anonymization and aggregation?

Report: Okay, so I need to figure out if the Century Tech documentation addresses the question about measures taken to enhance privacy-by-design, such as encryption, pseudonymization, anonymization, and aggregation. Let me start by understanding each part of the task. First, the question is asking whether Century Tech has implemented measures like encryption, pseudonymization, etc., to enhance privacy-by-design. The documentation provided includes a Privacy Notice, which outlines how they handle user data. I need to check if this document mentions any of these specific techniques. Looking through the documentation, I see sections about personal data collection, types of data processed, and how it's used. It also talks about cookies and third-party links but doesn't explicitly mention encryption or pseudonymization. The closest is when it discusses "Technical Data," which includes IP addresses and browser information, but that's more about tracking than encryption. The AdditionalInformation says Century Tech uses AI for personalized learning and has features like data analytics. However, the documentation doesn't specify if these are implemented with encryption or other privacy measures. I should also consider if any legal basis is mentioned that would imply such measures without explicit mention. The document does talk about compliance with applicable laws but doesn't detail specific technical safeguards beyond general security practices. So, putting it together, while there's some mention of data collection and processing, there's no clear indication of using encryption or other privacy-by-design techniques as listed in the question. The Century Tech documentation does not explicitly address measures such as encryption, pseudonymization, anonymization, or aggregation to enhance privacy-by-design. While it outlines data handling practices and compliance with legal requirements, it lacks specific details on implementing these technical safeguards. Therefore, the documentation does not sufficiently address the question regarding privacy-by-design measures.

Q5. Did you handle any sensitive data with care: complying with required laws and standards, providing users with clear notice and give them any necessary controls over data use, following best practices such as encryption in transit and rest?

Report: Okay, so I need to figure out if the Century Tech documentation adequately addresses the question about handling sensitive data with care, complying with laws, providing clear notices, giving users controls, and using encryption both in transit and at rest. Let me break this down step by step. First, the question is pretty detailed, covering several aspects of data privacy and security. The documentation provided includes a Privacy Notice that outlines how Century Tech processes personal data. I'll need to check each part of the question against the documentation. Starting with compliance: The document mentions that they comply with applicable laws and regulations, but it doesn't specify which ones. It's good to know they comply, but without knowing exactly which laws, it might be a bit vague. However, since the AdditionalInformation says they're an edtech company using AI for personalized learning, maybe they're subject to GDPR or other relevant data protection laws. Next, user notice and controls: The Privacy Notice does mention that users can contact them via email or post with questions about their

rights. It also explains how personal data is collected and used. However, it doesn't explicitly state whether they provide clear notices at the time of data collection or during account setup. I think they do mention consent where necessary, especially for minors, but it's a bit unclear if the controls are clearly detailed. Encryption: The document doesn't explicitly say that data is encrypted both in transit and at rest. It does talk about using cookies and other technologies, which implies some form of security, but encryption specifics are missing. Without this, it's hard to confirm they meet the standard for sensitive data protection. Data minimization: They mention collecting only necessary personal data, which aligns with data minimization. That's good. Third-party processing: The document states that third parties are used for services like IT and marketing, but it doesn't specify if these third parties comply with data protection standards. This is a concern because without ensuring third-party compliance, there could be vulnerabilities. Account security: They don't provide details on how user accounts are secured, such as multi-factor authentication or password policies. This is another point where the documentation falls short. Data retention: The document says they retain data for up to six years from service supply and mentions suppression lists for marketing opt-outs. That's clear but could be improved by specifying exact durations based on specific data types. Access rights: They do mention users can exercise their rights, like access, rectification, erasure, etc., which is good. However, the process might not be clearly detailed, making it hard for users to know how to enforce these rights. Putting this all together, while the documentation covers some aspects well, like data minimization and user rights, it's lacking in areas like encryption specifics, third-party compliance, account security details, and clear notices about data collection and usage. These omissions mean the documentation doesn't fully address the question, especially concerning sensitive data handling and encryption. The Century Tech documentation addresses some aspects of data privacy but falls short in critical areas, particularly regarding encryption, third-party compliance, and user controls. Here's a structured summary: 1. **Compliance**: The document states compliance with applicable laws but doesn't specify which ones, which could be a concern depending on the relevant regulations. 2. **User Notice and Controls**: While it mentions user rights and contact methods, it lacks explicit details on clear notices during data collection and comprehensive controls for users to manage their data preferences. 3. **Encryption**: There's no mention of encryption in transit or at rest, which is crucial for sensitive data protection. 4. **Data Minimization**: The company collects only necessary data, which is good but could be enhanced with more specifics on what constitutes minimization. 5. **Third-Party Processing**: While third parties are used, their compliance with data protection standards isn't specified, posing potential vulnerabilities. 6. **Account Security**: Details on securing user accounts (e.g., multi-factor authentication) are absent, leaving room for improvement. 7. **Data Retention**: Clear retention policies exist but could benefit from more specific durations based on data types. 8. **Access Rights**: Users can exercise rights, but the process isn't clearly detailed, hindering their ability to enforce these rights effectively. In conclusion, while the documentation covers some essential aspects, it lacks critical information regarding encryption, third-party compliance, and user controls, which are vital for ensuring robust data privacy practices.

Q6. In case of data processing for vulnerable individuals (children, patients, employees, etc), did you define and if so, do you implement a storage policy and further privacy strategies (e.g. minimization, hiding, separation or abstraction) for the personal data?

Report: Okay, so I need to figure out if the Century Tech documentation addresses the question about their storage policies and privacy strategies for vulnerable individuals, like children or employees. Let me

start by reading through the provided documentation carefully. The Privacy Notice starts with some general info about what personal data is and how it's collected. It mentions that they process data from various groups: teachers, students, parents, etc. I'm looking specifically for parts where they talk about handling data for vulnerable individuals. In section 5, it says they collect identity, contact, registration, financial, transaction, profile, behavioral, technical, and marketing data. But I don't see a specific mention of storage policies or strategies for these groups. They do discuss how they handle personal data in general but not tailored approaches for vulnerable people. Section 6 talks about responsibility for students' data, noting that schools must ensure consent. It mentions that once a student turns 13, they need direct consent again. That's good, but it doesn't cover other vulnerable groups like employees or patients. Looking at section 8, "Sharing Personal Data," they mention sharing with third parties but don't specify any special measures for sensitive data of vulnerable individuals. Section 12 discusses transfers outside the UK and EEA, which is about data protection laws but not specific policies for these groups. Section 15 mentions minors' privacy but doesn't go into detail about storage policies or additional privacy strategies beyond what's required by law. The Additional Information says Century Tech uses AI to create personalized learning experiences. They focus on adapting lessons based on individual needs, which implies they handle sensitive data. However, the documentation doesn't explicitly outline storage policies or further privacy strategies beyond general compliance. So, while there are some mentions of handling minors' consent and data collection, the documentation doesn't clearly define or implement specific storage policies or additional privacy strategies for vulnerable individuals beyond what's legally required. It seems they rely on third-party processors without detailed explanations. The Century Tech documentation addresses aspects of personal data handling but does not explicitly outline specific storage policies or additional privacy strategies tailored for vulnerable individuals such as children, patients, or employees. While it mentions the collection and processing of various types of data and includes general measures like consent handling for minors, it lacks detailed policies on how sensitive data is stored or protected beyond compliance with legal standards. Therefore, the documentation does not fully address the implementation of specific strategies for vulnerable groups, relying instead on third-party processes without further detail.

Q7. Did you assess the degree of anonymization and possible risk of re-identification?

Report: Okay, so I need to figure out if the Century Tech documentation addresses whether they assess the degree of anonymization and possible risk of re-identification. Let me start by understanding what the question is asking. The question is about assessing how well the company anonymizes data and the potential risk that someone could re-identify it. So, I'm looking for information in the provided Privacy Notice that talks about their methods for anonymizing data and any steps they take to prevent re-identification. First, I'll read through the documentation again. The document starts by explaining what personal data is and then goes into how they collect and process it. It mentions things like Identity Data, Contact Data, Registration Data, etc., which are all types of personal information. Looking at Section 5, "HOW WE COLLECT AND RECEIVE PERSONAL DATA," they mention using cookies and other technologies to gather Behavioral Data and Technical Data. This is about data collection methods but doesn't directly talk about anonymization. In Section 6, "WHAT PERSONAL DATA WE COLLECT OR RECEIVE," they list various types of data, including Identity Data, Contact Data, etc., but again, no mention of how this data is anonymized or the risks involved. Moving to Section 7, "HOW WE USE YOUR PERSONAL DATA," it explains different purposes for processing data. It mentions legal bases like contract obligations and legitimate interests. There's a mention of using Profile Data and Behavioral Data for things like personalizing

marketing, but nothing about how this data is made anonymous or the risk of re-identification. Section 8 talks about sharing personal data with third parties, stating that they have contractual arrangements and security mechanisms in place. This implies some consideration for security, but it doesn't specify measures related to anonymization. In Section 12, "TRANSFERS OUTSIDE THE UK AND THE EUROPEAN ECONOMIC AREA," they mention compliance with legal obligations when transferring data outside the EEA. This includes having safeguards, which might include anonymization techniques, but it's not explicitly stated. Section 13 discusses retention periods and confidentiality, emphasizing security measures. Again, while important for overall security, it doesn't address how data is anonymized or re-identification risks. Looking through Section 9, "SHARING PERSONAL DATA," they mention sharing with third parties under certain conditions, but no specifics on anonymization techniques. Section 15 deals with personal data of minors and the company's compliance with applicable laws. No mention here about anonymization either. The Additional Information provided mentions that Century Tech uses AI for personalized learning tools, which implies handling a lot of user data. However, this doesn't directly address their approach to anonymizing or re-identification risks. Putting it all together, the documentation covers what personal data is collected and how it's used but doesn't explicitly discuss methods for anonymization or the risk assessment process regarding re-identification. It mentions security measures like contractual arrangements and encryption, which might imply some consideration of these issues, but there's no explicit section or information about assessing the degree of anonymization or re-identification risks. The Century Tech documentation does not explicitly address the assessment of data anonymization or the risk of re-identification. While it provides details on personal data collection and processing, as well as security measures like contractual arrangements and encryption, there is no specific section or information discussing methods for anonymizing data or assessing re-identification risks. Therefore, the documentation does not adequately address these aspects.

Q8. Did you consider the privacy and data protection implications of data collected, generated or processed over the course of the AI system's life cycle?

Report: Okay, so I need to figure out if the provided Documentation from Century Tech addresses the question about considering privacy and data protection implications in their AI system's lifecycle. Let me break this down step by step. First, the Question is asking whether the company has thought about the privacy and data protection aspects throughout their AI system's life cycle. That means I need to check if the documentation covers how they handle data from collection, through processing, storage, usage, and eventual disposal or retention. Looking at the Documentation provided, it starts with a Privacy Notice effective from May 2024. It outlines what personal data is collected, how it's used, who has access to it, and the rights of data subjects. The document mentions that they process personal data for various purposes like providing services, marketing, analytics, etc. I notice sections about how they collect data through cookies and other technologies, which ties into the AI system's use of data for analysis. They also discuss sharing personal data with third parties, which is relevant to their AI partners or service providers. The Additional Information states that Century Tech uses AI to create personalized learning experiences, using features like data analytics and content adaptation. This suggests they handle a lot of sensitive information about educators and students. Now, checking the Constraints: The documentation must be reviewed for any mention of privacy considerations in the AI context. I don't see specific sections addressing AI-specific privacy implications, like bias mitigation or transparency in AI decisions. The document focuses more on general data protection rather than the unique aspects of AI systems. The company does mention compliance with applicable laws and having a legal basis for processing, which is

good. They also outline rights of data subjects, such as access, rectification, erasure, etc., which are essential for privacy. However, without explicit discussion of how AI's lifecycle is managed regarding privacy—like data minimization, consent handling in AI models, or transparency in AI decisions—the documentation doesn't fully address the question. They might be compliant with GDPR and other regulations, but they haven't detailed their approach to AI-specific privacy challenges. So, while they provide a solid overview of their general privacy practices, they fall short in addressing the targeted aspects of their AI system's data handling. The Documentation from Century Tech addresses general privacy principles such as data collection, usage, and subject rights but does not specifically address AI-specific privacy implications. While it outlines compliance with legal requirements and provides basic information on data handling, it lacks detailed discussions on AI-related challenges like bias mitigation or transparency in AI decisions. Therefore, the company's documentation does not fully satisfy the question regarding their AI system's lifecycle privacy considerations.

Q9. Did you define the requirements concerning data protection and security at the origin, while taking into account the available standards and best practices?

Report: Okay, so I need to figure out if the Century Tech documentation adequately addresses the question about their requirements concerning data protection and security, considering available standards and best practices. First, I'll read through the provided Documentation carefully. The Privacy Notice starts with a purpose section explaining how they handle personal data. It mentions that they collect various types of data, including identity, contact, registration, financial, transaction, profile, behavioral, technical, and marketing information. The documentation outlines how they use this data for providing services, improving the platform, marketing, events, and legal compliance. They also mention security measures like confidentiality, encryption, and access controls. Additionally, there's a section on third-party sharing with contractual arrangements to protect data. Looking at the Additional Information, CenturyTech uses AI for personalized learning tools, which likely involves handling sensitive student data. Best practices in data protection usually include clear consent, data minimization, encryption, access control, and regular audits. The Documentation does cover these areas: types of data collected, purposes, legal bases for processing, security measures, third-party sharing, user rights, and compliance with UK GDPR. It also mentions obtaining consent where necessary and provides information on how to contact for rights exercises. However, I notice that while the documentation is comprehensive, it might not go into specifics about each best practice in depth. For example, it doesn't explicitly mention encryption standards beyond stating they have security measures. Also, there's no detailed information on data minimization or retention policies beyond the general six years. Moreover, the section on minors' data mentions compliance but doesn't elaborate on specific protections like age-appropriate consent mechanisms. The Cookie Policy reference is made, but without providing details of what it entails. In summary, while the documentation addresses key aspects of data protection and security, it could be more detailed in certain areas to fully align with best practices. The Century Tech documentation adequately addresses several key aspects of data protection and security, including data types, purposes, legal bases for processing, security measures, third-party sharing, user rights, and compliance with UK GDPR. However, there are areas where it could be more detailed to fully align with best practices:

1. **Data Collection and Use**: The documentation outlines various data types and their uses, which is essential for transparency.
2. **Security Measures**: It mentions confidentiality, encryption, and access controls but lacks specifics on encryption standards and protocols.
3. **Third-Party Sharing**: Details contractual arrangements to protect data, which is a best practice.
4. **User Rights**: Clearly outlines

rights such as access, rectification, erasure, restriction, portability, objection, and consent withdrawal. 5. ****Compliance and Legal Obligations****: Mentions compliance with UK GDPR and legal obligations but could elaborate on specific regulatory requirements. 6. ****Minors' Data Protection****: Provides some information but lacks specifics on age-appropriate consent mechanisms. 7. ****Cookie Policy Reference****: Mentions the Cookie Policy without detailing its contents, which is a point for improvement. In conclusion, while the documentation covers essential elements of data protection and security, enhancing details in areas like encryption standards, minors' protections, and cookie policies would improve alignment with best practices.

Q10. Did you define the time limits for erasure of stored personal data?

Report: Okay, so I need to figure out if the Century Tech documentation addresses whether they define time limits for erasing stored personal data. Let me start by reading through the provided Privacy Notice carefully. First, I'll look for any sections that mention data retention periods. The document has several sections: Purpose of the Notice, About Us, How to Contact Us, Who We Collect Data From, etc. I see a section titled "HOW LONG WE KEEP YOUR PERSONAL DATA" which is under number 13. This seems relevant because it discusses how long personal data is retained. In this section, it says that they may retain personal data for up to six years from the date of service supply. They also mention that if data is only useful for a short period, like for a specific activity or campaign, they won't keep it longer than necessary. Additionally, if someone opts out of marketing communications, some data might be kept on a suppression list indefinitely, but they won't use it to send further marketing without consent. So, the documentation does specify a time limit for erasure in certain cases, especially when data is no longer needed or when a user requests deletion. However, there's also mention of indefinite retention for suppression lists with an opt-out option, which might not be as clear on the exact erasure timeline. I should check if the question specifically asks about the time limits for erasure. The question is whether they define the time limits for erasing stored personal data. The documentation does provide a timeframe in most cases but notes exceptions, so it's addressed. The Century Tech documentation addresses the time limits for erasing stored personal data by specifying retention periods and procedures for deletion. It outlines that personal data is retained for up to six years after service supply or as needed for specific activities, with an option for users to request deletion. Additionally, suppression lists may retain data indefinitely but only for marketing purposes, which can be opted out of. Thus, the documentation defines these time limits and procedures adequately.

Q11. Did you put in place procedures to verify the implementation of the storage periods?

Report: Okay, so I need to figure out if the Documentation provided by Century Tech addresses the question: "Did you put in place procedures to verify the implementation of the storage periods?" Let me break this down step by step. First, I'll look at the question itself. It's asking whether the company has established procedures to ensure that their data storage periods are correctly implemented. This likely refers to how they manage and enforce retention policies for user data, ensuring that data isn't stored longer than necessary and is securely disposed of when no longer needed. Looking at the Documentation provided, I'll scan through each section to see if there's any mention of data storage periods or retention policies. The document covers several areas: purpose of the privacy notice, how personal data is collected, use of data, sharing practices, consent, third-party links, transfers outside the EEA, data

retention duration, confidentiality, minors' data, and rights of data subjects. In section 13, "HOW LONG WE KEEP YOUR PERSONAL DATA," it states: "In respect of personal data that we process in connection with the supply of our Services or otherwise under this Privacy Notice, we may retain your personal data for up to six years from the date of supply of the relevant Services and in compliance with our data protection obligations. We may then destroy such files without further notice or liability." This section directly addresses retention periods by specifying that user data is retained for up to six years after the service is supplied. It also mentions that if data is only useful for a short period, it's not retained longer than necessary. Additionally, if someone opts out of marketing communications, their data is kept on a suppression list indefinitely but not used for further marketing unless they opt back in. So, the Documentation does include information about storage periods and the procedures (retention policies) in place to manage these durations. It outlines how long different types of data are retained and under what circumstances this retention occurs, which directly answers the question. The Documentation addresses the implementation of storage periods through its section on "HOW LONG WE KEEP YOUR PERSONAL DATA," detailing retention durations and procedures for managing user data retention. This includes specifying a maximum retention period of six years after service supply and practices for data disposal upon retention expiration.

Q12. Did you define and put in place the necessary and appropriate technical measures for the storage of personal data?

Report: Okay, so I need to figure out if the Century Tech documentation adequately answers the question: "Did you define and put in place the necessary and appropriate technical measures for the storage of personal data?" First, I'll look through the provided Documentation. The document is a Privacy Notice from Century-Tech, which outlines how they handle user data privacy and security. I notice that the document mentions several technical measures, like using cookies and other similar technologies to collect behavioral and technical data. It also talks about encryption for email addresses when advertising on social media platforms. Additionally, it references compliance with applicable laws and regulations, which suggests they have a framework in place. However, I'm not seeing explicit details about specific technical measures beyond the mention of cookies and encryption. There's no information about data encryption methods (like SSL/TLS), access controls, or how personal data is stored securely. The document doesn't provide specifics on how data is encrypted, protected during transmission, or how access is controlled. The Additional Information states that Century Tech uses AI for personalized learning tools, which might involve handling sensitive student data. This implies a need for robust security measures beyond what's mentioned in the Privacy Notice. Since the documentation doesn't go into depth about technical measures like encryption protocols, access controls, or secure storage practices, it doesn't fully address the question. It mentions some measures but lacks detailed information that would satisfy the requirement of defining and implementing appropriate technical measures. The Century Tech documentation addresses some aspects of technical measures, such as using cookies and encryption for social media advertising, but it does not provide sufficient detail on critical security practices like data encryption methods or access controls. Therefore, the documentation does not adequately define and implement necessary technical measures for personal data storage. ****Answer:**** The Documentation does not fully address the question. While it mentions some technical measures like cookies and encryption, it lacks detailed information on essential aspects such as encryption protocols, secure storage practices, and access controls, which are crucial for ensuring appropriate handling of personal data.

Q13. Did you define and put in place the necessary and appropriate organizational measures for the storage of personal data?

Report: Okay, so I need to figure out if the Century Tech documentation adequately answers the question: "Did you define and put in place the necessary and appropriate organizational measures for the storage of personal data?" First, I'll look through the provided Documentation. The Privacy Notice mentions several things about how they handle personal data. They talk about collecting various types of data from different groups like teachers, students, parents, etc. They also discuss their approach to processing this data, including using cookies and other technologies for behavioral analysis. I notice that the documentation includes sections on how they use personal data, such as for providing services, marketing, analytics, and events. It also mentions legal compliance and security measures, like confidentiality and technical safeguards. There's a section about third-party links and transfers outside the EEA, where they state they comply with applicable laws. However, I'm not seeing explicit mention of specific organizational measures beyond general statements about data protection, confidentiality, and compliance. The Additional Information says Century Tech uses AI for personalized learning but doesn't add much to the documentation's content. The question is whether they've defined and implemented necessary measures. The Privacy Notice does talk about processes like consent, data collection methods, retention policies, and sharing practices, which are organizational measures. They also mention compliance with laws and having a data protection supervisory authority (ICO in this case). So, while the documentation covers aspects of personal data handling, it might not go into as much detail as needed on specific organizational measures. It's more about what they do rather than how they ensure those processes are secure and compliant. The Century Tech documentation addresses the handling of personal data through various sections, including data collection, processing purposes, security measures, and compliance with legal requirements. While it covers aspects like consent, retention, and third-party interactions, it does not explicitly detail specific organizational measures beyond general statements. Therefore, while it provides foundational information on data practices, it may lack depth in outlining detailed organizational measures for secure data handling.

RESULTS (WITH COMMENTS):

Q1. If you reuse already existing data for the purposes of training and development of the AI system, has the database been compiled and data collected in accordance with data protection regulations?

Comment: While Century Tech likely adheres to relevant data protection standards, the documentation does not explicitly confirm this specific aspect. → **TN**

Q2. Did you anonymize and aggregate incoming data using practice data-scrubbing pipelines: considering removing personally identifiable information (PII) and outlier or metadata values that might allow de-anonymization?

Comment: The documentation does not explicitly address whether Century Tech uses data-scrubbing pipelines to anonymize and aggregate incoming data. While it details their approach to personal data

handling, including collection and processing purposes, it lacks explicit mention of such techniques. → **TN**

Q3. Do you monitor the compliance of training data processing with data protection requirements?

Comment: there's no mention of actively monitoring or ensuring that training data meets necessary standards → **TN**

Q4. Did you take measures to enhance privacy-by-design, such as via encryption, pseudonymization, anonymization and aggregation?

Comment: While the documentation outlines data handling practices and compliance with legal requirements, it lacks specific details on implementing these technical safeguards → **TN**

Q5. Did you handle any sensitive data with care: complying with required laws and standards, providing users with clear notice and give them any necessary controls over data use, following best practices such as encryption in transit and rest?

Comment: while the documentation covers some essential aspects, it lacks critical information regarding encryption, third-party compliance, and user controls, which are vital for ensuring robust data privacy practices → **TN**

Q6. In case of data processing for vulnerable individuals (children, patients, employees, etc), did you define and if so, do you implement a storage policy and further privacy strategies (e.g. minimization, hiding, separation or abstraction) for the personal data?

Comment: the documentation does not fully address the implementation of specific strategies for vulnerable groups, relying instead on third-party processes without further details → **TN**

Q7. Did you assess the degree of anonymization and possible risk of re-identification?

Comment: While it provides details on personal data collection and processing, as well as security measures like contractual arrangements and encryption, there is no specific section or information discussing methods for anonymizing data or assessing re-identification risks → **TN**

Q8. Did you consider the privacy and data protection implications of data collected, generated or processed over the course of the AI system's life cycle?

Comment: While it outlines compliance with legal requirements and provides basic information on data handling, it lacks detailed discussions on AI-related challenges like bias mitigation or transparency in AI decisions → **TN**

Q9. Did you define the requirements concerning data protection and security at the origin, while taking into account the available standards and best practices?

Comment: while the documentation covers essential elements of data protection and security, enhancing details in areas like encryption standards, minors' protections, and cookie policies would improve alignment with best practices → **TN**

Q10. Did you define the time limits for erasure of stored personal data?

Comment: the documentation defines these time limits and procedures adequately → **TP**

Q11. Did you put in place procedures to verify the implementation of the storage periods?

Comment: The Documentation addresses the implementation of storage periods through its section on "HOW LONG WE KEEP YOUR PERSONAL DATA," detailing retention durations and procedures for managing user data retention → **TP**

Q12. Did you define and put in place the necessary and appropriate technical measures for the storage of personal data?

Comment: . While the documentation mentions some technical measures like cookies and encryption, it lacks detailed information on essential aspects such as encryption protocols, secure storage practices, and access controls, which are crucial for ensuring appropriate handling of personal data → **TN**

Q13. Did you define and put in place the necessary and appropriate organizational measures for the storage of personal data?

Comment: while the documentation provides foundational information on data practices, it may lack depth in outlining detailed organizational measures for secure data handling → **TN**

Confusion Matrix:

	Predicted	
	Positive:	Negative:
Total:	2	11
13		

Actual	Positive: 2	True Positive: 2	False Negative: 0
	Negative: 11	False Positive: 0	True Negative: 11

Precision = 100%

Recall = 100%