Article 5:

Our model may not subvert people’s decision making, it should offer people the option of taking a safer route but not force them to do this. We also can't take advantage of people’s vulnerabilities (we aren't planning on either of these).

Article 6:

Our AI system is intended to be used as a safety component (safer driving)

It does use third-party as we aren't directly related to ANWB (yet)

Therefore, the system is high risk

Article 7:

If the commission were to assess our AI system

A: Our intended purpose is to improve road safety by warning people about dangerous roads and choosing safer options or driving more carefully in those areas.

B: The AI system would likely be used by those who already opt to drive more safely

C: Personal data is removed for the purpose of assessing road safety.

D: The AI system only informs and doesn't make any decisions by itself. Recommendations shouldn't lead to more harm, but if users drive more carelessly due to not receiving a notification of approaching a dangerous road this could lead to harm.

E: The AI system is new so hasn't already caused harm.

F: see E

G: Opting out from outcomes is practical as the driver can still choose the road themselves.

H: The users of the AI system are the drivers; they are not put in a vulnerable position by our ML model.

I: If drivers approach a high-risk road, they can still opt to change their route by taking a turn somewhere so the decision is corrigible, however this might be a problem if hastily taken a corner.

J: The product is likely to improve road safety.

K:

Article 9:

1: we must establish a risk management system, and document what we do with it.

2: identify reasonably foreseeable risks that can be seen when using the system; estimate risk of using, as well as misusing the app (misuse would probably be irrelevant, unless people drive less safe in high-risk zones),

We can do this by identifying false positives/negatives or false classifications of roads in our case and try to mitigate the amount.

We will address the likelihood and impact of the risks

For long-term we would develop strategies to minimise the risks by keeping algorithms up to date and making sure data quality is as high as possible.

Article 10:

Required to have good quality datasets for training validation and testing

We can ensure we have this by

Having high-quality data representing road safety (ANWB dataset is representative of the data)

Data should be relevant to road conditions (The data is categorised by road)

Have diverse data to avoid bias (Data is from all over Breda)

Implement processes to ensure data integrity and secure handling (Password login to access data, columns that seem wrong aren't used)

Article 11:

Create and maintain comprehensive technical documentation

We should document our architecture, algorithms and our source in a separate file

We should state our intended purpose (Improving road safety by classifying roads as dangerous and informing end users of these roads)

Include performance metrics of the models

Maintain documentation on improvements (markdowns on models and changes)

Article 12: Keep logs to monitor the system operations (this would only be relevant post deployment; therefore, it is irrelevant for the scope of our project.

Logs of outputs are still relevant so we should keep those.

Article 13: Provide clear information on ai to users

Provide detailed instructions on how the AI works

Describe the limitations of the system

Offer a way to contact services to assist.

Article 14: Ensure human oversight is in place to mitigate risk

Humans should be able to override the decisions the model makes

Staff would have to be trained to intervene (Not relevant yet in our case, since we won't use the model for real-time cases yet.

Continuously monitor the performance and involve humans in critical decision making (Continuous monitoring is relevant during and after deployment not before.)

Article 15: Ensure systems are accurate and secure

Test the model with different conditions

Update the model to improve performance and address new data (new data might not be relevant for the scope of our project)

Implement cybersecurity measures to protect the data (Password and vpn protection on the data)

Article 16: Implement quality management for the model

Develop a procedure to ensure quality remains high

Conduct external audits to ensure compliance (we can ask fellow students or perhaps the teachers to check if they feel our model is compliant)

Make sure we all try to help each other improve by integrating feedback.

Article 17: Document the quality management system with our policies and objectives

Document the procedures for design

Meet quality management standards

Improve based on received feedback (limited in scope due to our project scope)

Article 18:

Maintain documents after placing on the market (we won't actually place it so this is irrelevant)

Update the documents (irrelevant for the same reason)

Accessible to relevant authorities (irrelevant for the same reason)

Article 19:

Automatically generate logs (Output is documented earlier, new data won't be input during the scope of the project.)

Logs must be retained for a sufficient period to enable monitoring. (Should we log things we can maintain them, but we likely won't add new events.)

Logs must be integral to prevent tampering. (See before)

Article 20:

If a large problem arises, we have the duty to pull the plug, and take appropriate measures to get the model back on track. (Since our model is more of a proof of concept than an actual product this will likely not be relevant).

Article 21:

Should a relevant authority ask for information and documentation we will provide it, as well as the automatically generated logs. This will be confidentially shared. (This is unlikely to happen, but if it will we should be ready).

Article 22:

Article 22 references launching AI systems from outside the EU in the EU, since we are in the EU this is irrelevant for us.

Article 23:

Article 23 talks about an importer, if we were to sell this product to ANWB they would be the importer therefore this is not relevant for us.

Article 24:

Article 24 talks about the distributor which would also be ANWB not us who has to verify we adhere to standards.

Article 25:

Article 25 states that everyone involved within the AI is responsible for the legal distribution of the AI which would relate to us. Other parts involve handing the AI system over the creators have to make sure the new owners have the necessary knowledge to keep working on it. This would be relevant only if ANWB wishes to take over our models.

Article 26:

Organisational oversight must be present for high-risk AI systems as well as instructions to use it, this must be done by trained individuals.

Data must remain relevant for the intended purpose, and continuously monitored

Employers must know they work with AI, and public authorities must comply with registration obligations

People affected by AI decision making should be informed of this.

All these points are also covered in other points, so it doubles as a bit of a summary too.

Article 27:

We need to describe how the AI system will be used, during which time and the frequency of usage, categories of natural persons likely to be affected (no one, it is an opt in system), specific harm it might have on people (people potentially driving less safe because they are in a "low risk" zone)

Articles 28-39, part of section 4, are all about authorities that check whether AI systems are compliant with the rules. They do not pertain to actions we have to consider to be within legal parameters.

Article 40: Should a request from the European Commission come in we would have to follow their standardisation request, we would have to adhere to published standards. It is also requested that our models are as efficient as possible, so no computational power is wasted.

Article 41:

Article 41 addresses the adherence to standard rules, or where there is a lack of there is a requirement to prove adherence to the rules in other ways. If we meet the created standards, which we should if following the previous points, then this isn't important.

Article 42:

This article says that if an AI system has been trained and tested on specific settings (like our model being trained on specifically Breda), then it is compliant with the rules in article 10. It also mentions that if we have a cybersecurity statement of conformity then we comply with the requirements of article 15. If we wish to deploy the model for ANWB we would have to get a statement of conformity.

Article 43:

Article 43 discusses the processes of assessing if our model meets the correct standards, and how we would have to go about having our model assessed to meet the required standards. Therefore, if we follow the steps from earlier we should be fine.

Article 44:

Article 44 mentions the specifics of certificates and are not relevant for us. What is relevant is that if our model is deemed to no longer meet the requirements then they can ask us to change the model.

Article 45:

Mentions the obligations of notified bodies, this is what they must do after we tell them what we have done and is not relevant for us.

Article 46:

This mentions exceptions to the rule in the case of public safety or environmental protection concerns. Our model does not apply to these and therefore this rule is not applicable to our situation.

Article 47:

We need a written document of conformity for each of the systems mentioned previously. This document must be kept available for 10 years, as well as be in a language that can be understood (English should suffice).

Article 48:

AI systems are subject to CE law; therefore, a CE mark would have to be present somewhere in documentation where it is easily accessible.

Article 49:

Before putting our model on the market, we must register in the EU database, if we work with ANWB they likely have an authorised representative who would do this.

Article 50:

We must inform users that they are dealing with an AI model. This can be done by having this mentioned explicitly before users use the app.

Article 51:

This is a commission classification based on impact capability and computational power. We do not require as much computational power as is mentioned here for our preliminary model.

Article 52:

If we do end up meeting the requirements set by article 51, we will have to notify the commission. They will then investigate further.

Article 53:

This links back to keeping up to date logs of our model including training and testing processes and evaluations. This part mentions that we have to share this information with the commission if our system gets large enough to be investigated under article 51

Article 54:

Article 54 is for representatives of companies from outside the EU. We are inside the EU, so this is not applicable to us.

Article 55:

This article mentions following the standard protocols set earlier in articles 24 and 40.

Article 56:

The EU AI office is drafting rules for how to use AI, these rules are not yet implemented and should be within a year of the act going into effect. Once these come into practice we should adhere to them. This is not yet relevant for us.

Article 57:

There should be an AI sandbox on national level where the model can be tested before being deployed, if this is satisfied our model is fine. This is however not an action we necessarily have to take but more of a check if we indeed fit all the requirements

Article 58:

Same sandbox as 57, not our responsibility.

Article 59:

Same sandbox as 57, not our responsibility.

Article 60:

The testing of AI models in real world instances must be submitted to the AI office to receive a permit for testing. The testing must be done within 6 months unless an extension is approved.

Article 61:

When/if we test our model, we will have to have explicit consent from everyone involved in the test, this consent must be dated and documented as well as a copy given to the person who is partaking in the test.

Article 62:

As mentioned earlier there are standardised templates being created as well as sandboxes developed where testing can take place. SMEs (small and medium-sized enterprises) have priority access to these so they can get started. Should we wish to deploy these models we would have to contact them to see the availability of these.

Article 63:

This mentions that a microbusiness that is not linked to a larger company is exempt from several quality management systems. We would be linked to ANWB, so this is not relevant to us.