Bowtie, the solution for Data Protection Impact Assessment (DPIA) under the GDPR

By Jeroen van Puijenbroek MBA LLM CIPP/e CIPM FIP

According to the General Data Protection Regulation (GDPR) every organisation which processes personal data needs to demonstrate compliance to the GDPR.[1] When a processing likely results in a 'high' privacy risk, a Data Protection Impact Assessment (DPIA) is mandatory. The European Data Protection Board (EDPB), the European privacy authority, has indicated that DPIAs, 'are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the Regulation. In other words, a DPIA is a process for building and demonstrating compliance.'

[1] The GDPR applies to the processing of personal data in the context of the activities of an organisation in the European Union, regardless of whether the processing takes place in the Union or not. The GDPR applies also to the processing of personal data of data subjects who are in the Union by an organisation established outside the Union, where the processing activities are related to the offering goods or services to data subjects in Union or monitoring their behaviour as far as their behaviour takes place in the Union.

What is a DPIA and what is the goal?

A DPIA is an instrument to describe the processing activity, evaluate the lawfulness of the processing, assess the risks and consequently determine the measures to prevent or minimize the possible negative consequences to an acceptable level.

When performing a DPIA, an organisation can gain insight into the privacy risks of a project, policy, program, service, product or other initiative. Early insight in the most important risks and anticipating on the risks prevents costly changes in processes, redesigning systems or stopping a project, and can reduce or prevent litigation costs and/or negative publicity. Besides, performing a DPIA helps to increase privacy awareness inside an organisation and improves the quality of personal data processing. A DPIA can also help in anticipating and reacting on privacy objections by society and can help in gaining public confidence because the organisation visibly incorporates privacy protection in the design of a project.

How to perform a DPIA?

A DPIA can roughly be split up in three parts:

I. Description of the processing activities

II. Evaluation of the lawfulness of the data processing

III. Risk assessment and risk treatment

Based on the description of the data processing (part I), the lawfulness of the data processing is evaluated (part II). If the data processing is lawful, the associated privacy risks are assessed based on the description of the data processing and afterwards measures are described to address the risks (part III). If is determined that the data processing is not lawful, it is recommended to first ensure that the data processing becomes lawful before proceeding with the risk assessment and risk handling (part III).

In the rest of this article only part III about risk assessment and treatment will be discussed.

Which ‘risks’ of a processing activity are we referring too? Article 35 GDPR describes ‘risks for the rights and freedom of natural persons’ but in practice, the term ‘privacy risk’ is often used. As a result, the emphasis in the risk assessment is often more on the risks for the organisation than on the risks for the natural person. The negative consequences for the organisation (reputation damage, loss of customer confidence, loss of turnover, loss of market value, fines, compensation / legal costs and so on) are of course also important (secondary) but are often the result of the infringement of the rights and freedoms of the natural person (primary). In addition, the term ‘privacy risk’ has become a catch-all term in which causes, consequences and sometimes even measures are characterized as ‘risk’. All of this can result in inadequate measures being taken to prevent or mitigate the ‘real’ primary risks.

In most DPIA Guidelines the risk assessment is a black box. As a result, the quality of the DPIA depends strongly on the knowledge and knowhow of the person/team who perform the DPIA. How the outcome is reached is not clear for the client. How can we perform the DPIA risk assessment in a structured and transparent way?

NOREA, the professional association for IT-auditors in the Netherlands, has recently published the 'NOREA Guidance DPIA'[2] in which all three of the above-mentioned parts of the DPIA are coped with in a structured way. The 'NOREA Guidance DPIA' does not only comply with the GDPR and the criteria issued by the EDPB for an acceptable DPIA but also ties in with ISO31000/31010 for developing the privacy risk assessment and risk treatment. In ISO 31010 several methods/techniques are described for performing risk assessments.

In the 'NOREA Guidance DPIA' the choice was made to work out the Bowtie methodology as an example for risk assessment. The Working Group believed that the Bowtie technique is a particularly powerful tool to explicitly analyse the negative consequences of risks and gain insight. Therefore, not only better measures are taken but through the visualisation a broader support base among stakeholders of the DPIA is accomplished. This can also contribute to a better argumentation of the risk appetite of the organisation.

To illustrate the use of Bowtie for risk assessment and treatment according to the NOREA Guide DPIA an example is described below.

Case Fleet management

The scope of the DPIA is the data processing for fleet management. The following purposes are recognized:

- Tax-compliant journey registration (passenger cars)
- Real-time track and trace (delivery vans for delivery services)
- Sustainability (stimulating Eco friendly driving behaviour of lease drivers)
- Fleet management
- Management information

Risk assessment

Regardless of the chosen technique, ISO31000 states that a risk assessment consists of three stages/ phases, namely risk identification, risk analysis and risk evaluation.

Risk identification

The first phase of the risk assessment is risk identification. The risk identification is primarily intended to find, recognize and describe the risks that could affect the achievement of objectives.

[2] The Dutch version of the 'NOREA Guideline DPIA' is published on > https://www.norea.nl/kennisgroep-privacy. The English version will be added soon to this page.

Identify the Hazard: Because the purposes (and also the bases for the data processing) differ from each other in this case, a separate Hazard is drafted for each combination of data processing/purpose. In this example, the Hazard is 'Fleet management - Stimulate Eco friendly driving behaviour of lease drivers'.

Identify the Critical Event(s): Within the Risk Source 'Fleet management - Stimulate Eco friendly driving behaviour of lease drivers 'several Critical Events can be identified, namely (not exhaustive):

- The source data is incorrect and/or the results are incorrectly determined.
- The source data and/or results are used by the fleet manager for other purposes.
- There is unauthorized access to the source data and / or the results (hacking, data leak and so on).
- The source data and/or results are changed (accidentally or unauthorized).
- The source data and / or results are deleted (accidentally or unauthorized).

In this example, the Critical Event is 'The source data and/or results are used by the fleet manager for other purposes'.

Identify the Threats: The Critical Event has a number of causes (Threats) that are for example (not intended to be comprehensive) 'Very detailed telematics data per lease car', 'The fleet manager has access to the source data' and 'As a result of the service-oriented mindset of employees, new reports are run at the request of a manager'. See the left half of the Bowtie diagram in figure 1.

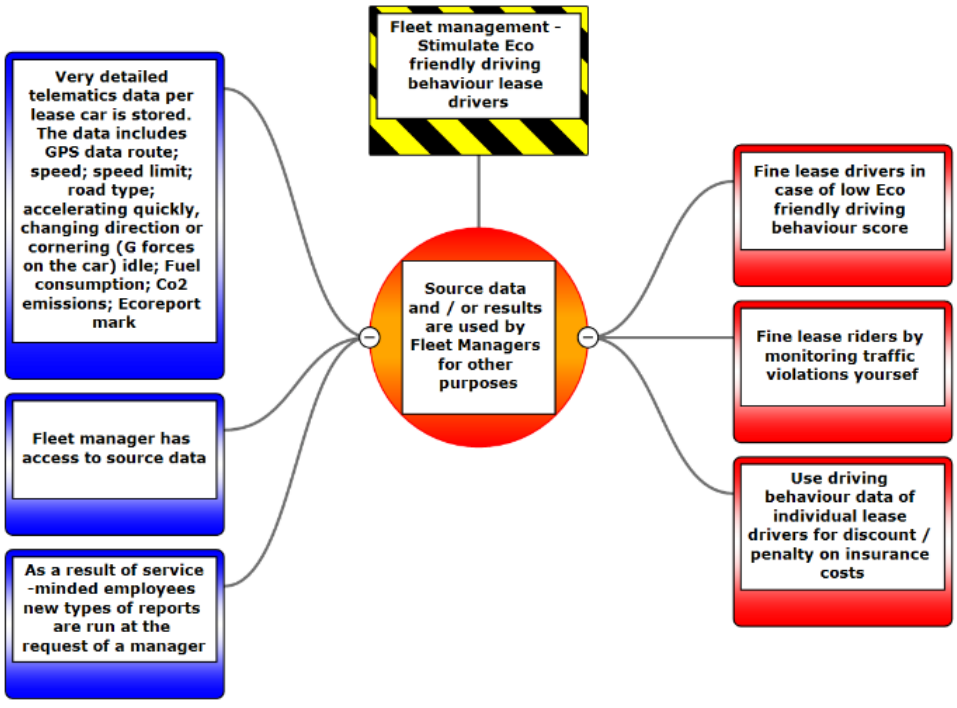

Figure 1: Initial Bowtie based on the risk identification (made with BowTieXP)

Identify the Consequences: The Critical Event has a number of negative Consequences that for example (not intended to be comprehensive) 'Fining lease riders in case of low Eco-friendly driving behaviour score', 'Fine traffic violations by monitoring traffic' and 'Use driving behaviour data of individual lease drivers for discount/penalty on insurance costs'. See the right half of the Bowtie diagram in figure 1.

Draft the initial Bowtie diagram: In figure 1 is the initial Bowtie diagram illustrated based on the phase risk identification as part of the DPIA.

Risk analysis

The second phase of the risk assessment is risk analysis. The risk analysis is about understanding the nature, sources, and causes of the risks that you have identified and to estimate the level of risk. It is also used to study impacts and consequences and to examine the controls that exist and/or planned aforehand.

Assess the Contribution of the Threat to the Critical Event and the inherent risk of the Consequences: The Contribution of the Threats 'Very detailed telematics data per lease car is stored' and 'Fleet manager has access to source data' to the Critical Event are in this case rated as 'High contribution'. The Threat 'As a result of the service-oriented mindset of employees, new reports are run at the request of a manager' is rated as 'Medium contribution'.

The inherent risk is the risk that is inherent to the process without taking into account possible measures/controls. The expected value of a risk is the result of 'likelihood' times 'impact'. The estimate can be both quantified and qualified and in varying degrees of detail (for example, a 3x3 scale vs. a 5x5 scale). In this example a 5x5 risk matrix is used (see figure 2).

The inherent risk for the Consequences:

- 'Fine lease riders in case of low Eco-friendly driving behaviour score' is estimated D4 (Likely and Single Fatality).
- Fine lease riders by monitoring traffic violations yourself' is estimated C4 (Possible and Single Fatality).
- 'Use driving behaviour data of individual lease drivers for discount/penalty on insurance costs' is estimated as E4 (Very likely and Single Fatality).

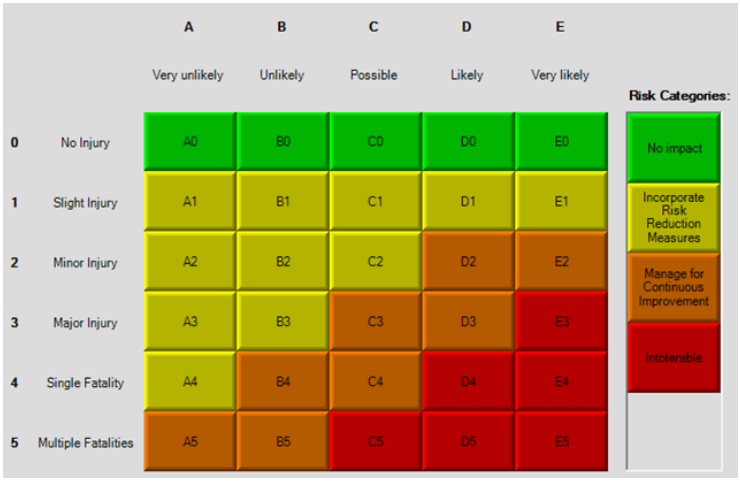

Figure 2: Risk matrix (source: BowTieXP)

Determine the existing Barriers and assess the Effectiveness: To prevent storing very detailed telematics data per lease car the control 'Flexible data collection setup' is part of the Telematic application. The option makes it possible to select which data types will be collected according to the need of the fleet manager of a company. The expected effectiveness of this software control is rated in this case as 'Very Good'. The Telematic application uses roll-based access and for authorization and the role 'Fleet manager' has no access to the source data. The expected effectiveness of this software is also rated as 'Very Good'. To prevent that employees of the fleet management staff of the organisation develop and run new types of templates because they are service minded towards the managers of the different departments the Telematic application comes with different electronic reporting templates. This software control is rated as 'Poor'.

Checking if the drawn-up working instructions/procedures, for which purposes data may be used are adhered, are Recovery Barriers to avoid or lessen all three Consequences in the example. The effectiveness of this behavioural control is rated 'Good'. For the Consequence 'Fine traffic violations by monitoring traffic yourself' the Recovery Barrier 'Drawing up reporting templates' is added. This software control is also rated 'Good'.

Identify Escalation factors: If by accident the wrong role is assigned to the Fleetmanager (or someone else), the person is authorized to have access to the telematic source data (Escalation Factor). To find out who had access to the source data all users that have had access will be logged and the log file will be checked periodically (Escalation Factor Barrier)

Assess the Residual risk of the Consequences: Taken into account all described Barriers and its effectiveness the residual risk for the Consequences:

- 'Fine lease riders in case of low Eco-friendly driving behaviour score' is B4 (Unlikely and Single Fatality).
- 'Fine lease riders by monitoring traffic violations yourself' is B2 (Unlikely and Minor Injury).
- 'Use driving behaviour data of individual lease drivers for discount/penalty on insurance costs' is C4 (Possible and Single Fatality).

Draft the concept Bowtie diagram: In figure 3 is the concept Bowtie diagram illustrated based on the phase risk analysis as part of the DPIA.

Risk evaluation

The third and final phase of the risk assessment is risk evaluation. The results from the risk analysis are compared with risk criteria in order to determine whether or not a specified level of risk is acceptable or tolerable.

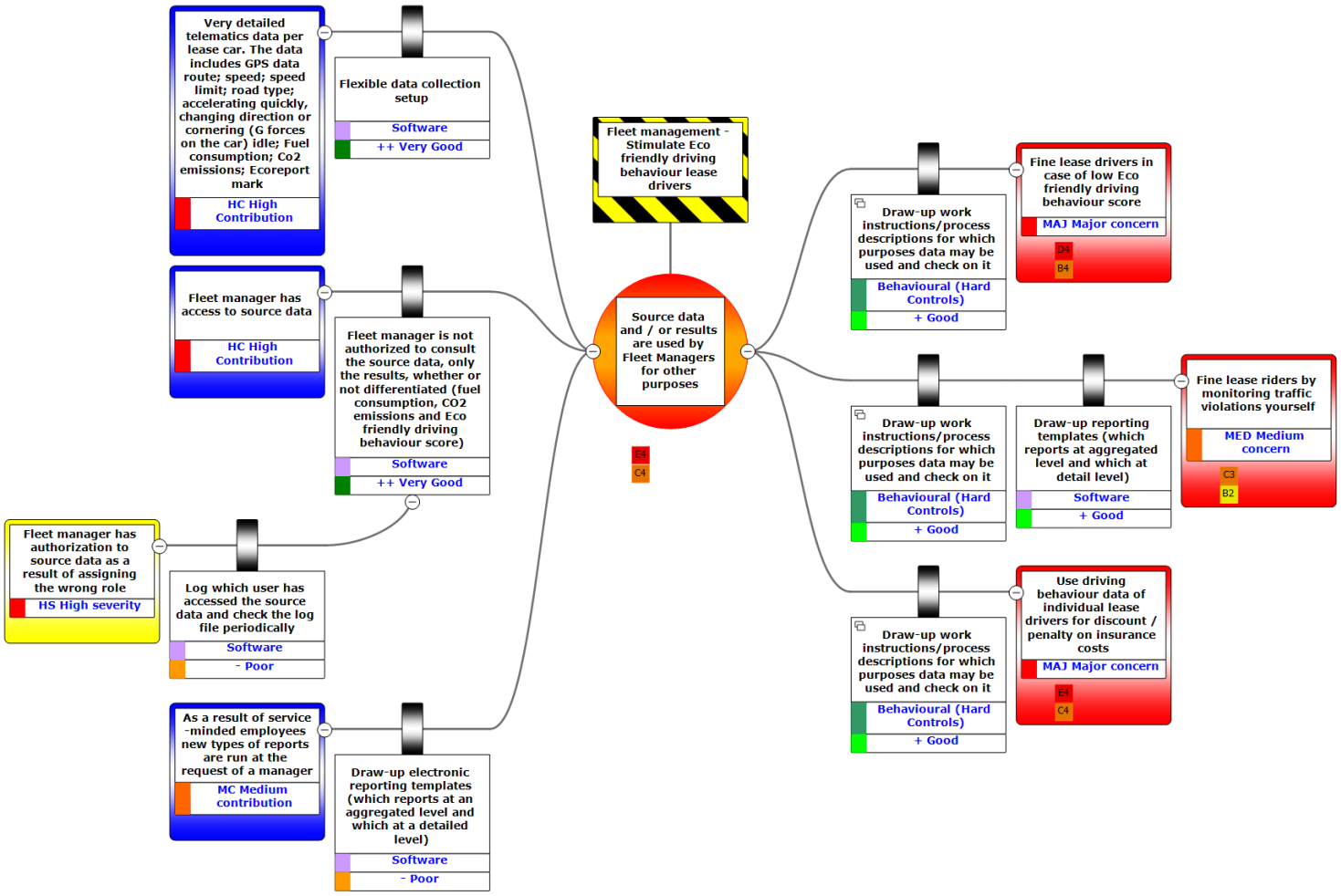

Figure 3: Concept Bowtie based on the risk analysis (made with BowTieXP)

This can lead to the decision to:

- do nothing (accept risk): Accepting the residual risk for the data subject, as long as it is lower than 'high', and for the organisation depends on the risk appetite of the organisation.
- consider options for risk treatment (control risk): If the existing/ proposed measures for a negative consequence are not effective and the organisation is unwilling/ unable to accept the residual risk, an option is to replace these measures and/or to add new measures.
- revise goals/review the purposes (eliminate risk): If the organisation does not want to/cannot accept the residual risk and cannot take modified/new measures, the organisation can also review the purposes of the data processing; change or cancel one or more purposes so that negative consequences are prevented or limited.

Compliance with the GDPR does not mean that there should be no risks at all to the rights and freedoms of the data subject. After all, every data processing entails a risk for the data subject. The residual risks for those involved may not be 'high'. If that is the case, the organisation must consult the local Data Protection Authority prior to processing.

The organisation may, to a certain extent, determine itself what its risk appetite is for the risks of those involved. The risk appetite depends on many factors. The risk appetite will be different between different sectors (for example social media versus financial institutions), but the risk appetite will also differ between organisations within the same sector.

Based on the risk appetite of the organisation in this example, the organisation does not want to accept the residual risks for 'Fine lease riders in case of low Eco-friendly driving behaviour score' and 'Use driving behaviour data of individual lease drivers for discount/penalty on insurance costs'.

To lower the residual risk two new Recovery Barriers are proposed. These are 'Agree with the working counsel that possible granted fines as result of low Eco-friendly driving score will be withdrawn' and 'Agree with the working counsel that the lease driver has to give his/her consent for using the driving behaviour data for discount on insurance costs'

Additionally, the Preventive Barrier 'Draw-up an electronic reporting template' is replaced because of the low effectiveness with 'Additional reports are only run after approval of higher management'.

Taken into account the new Barriers and its effectiveness, the residual risk for the Consequences:

- 'Fine lease riders in case of low Eco-friendly driving behaviour score' is B2 (Unlikely and Minor Injury)
- 'Fine lease riders by monitoring traffic violations yourself' is A2 (Very unlikely and Minor Injury)
- 'Use driving behaviour data of individual lease drivers for discount/penalty on insurance costs' is C2 (Possible and Minor Injury).

Draft the final Bowtie diagram: In figure 4 the final Bowtie diagram is illustrated based on the phase risk evaluation as part of the DPIA.

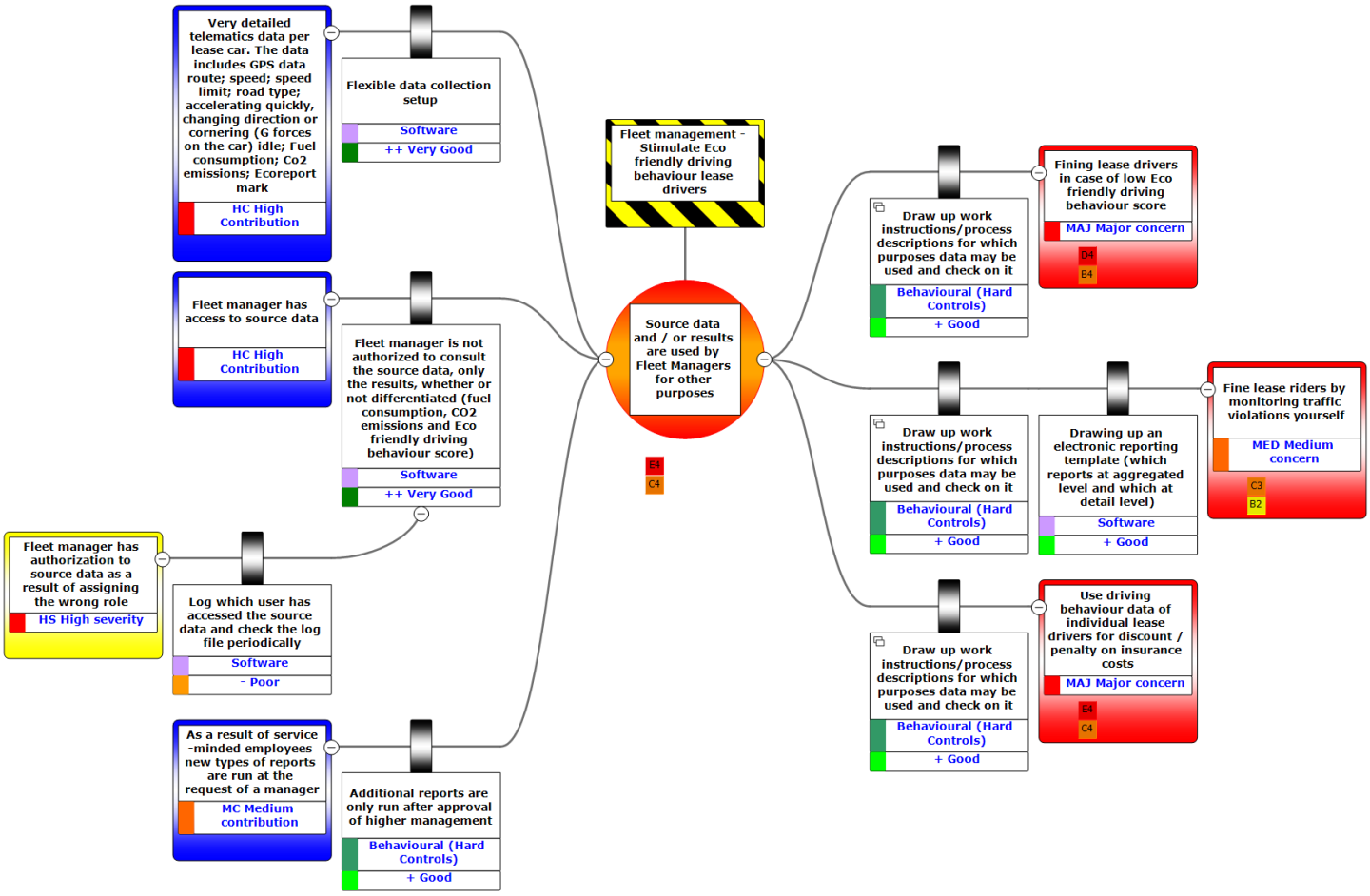

Figure 4: Final Bowtie based on the risk evaluation (made with BowTieXP)

Risk treatment

Based on the risk assessment performed, insight has been gained in both the risks and a set of measures to prevent/mitigate these risks to an acceptable level. The measures can be prioritized, timelines for implementation can be established, actions to be taken and responsible departments/officers can be appointed and so on.

Preferably, all measures are implemented before starting the new processing activity in order for the processing activity to be in line with the risk appetite of the organization. In any case, the measures that ensure that the residual risk is below the 'High' level must be implemented. If this cannot be achieved, the processing of the personal data is not allowed according to the GDPR.

Contact

Jeroen van Puijenbroek
j.vanpuijenbroek@2privacy.nl

References

1. The GDPR applies to the processing of personal data in the context of the activities of an organisation in the European Union, regardless of whether the processing takes place in the Union or not. The GDPR applies also to the processing of personal data of data subjects who are in the Union by an organisation established outside the Union, where the processing activities are related to the offering goods or services to data subjects in Union or monitoring their behaviour as far as their behaviour takes place in the Union.

2. The Dutch version of the 'NOREA Guideline DPIA' is published on https://www.norea.nl/kennisgroep-privacy. The English version will be added soon to this page.