Forsikring & Pension

The Danish Financial Supervisory Authority [Finanstilsynet]

Sent to jesu@ftnet.dk, jja@ftnet.dk (cc: eu.mail@ftnet.dk)

06.02.2020

Forsikring & Pension
Philip Heymans Allé 1
2900 Hellerup
Tlf.: 41 91 91 91
fp@forsikringogpension.dk
www.forsikringogpension.dk

Henriette Günther Sørensen
Chefkonsulent
Dir. 41 91 91 74
hgs@forsikringogpension.dk

Sagsnr. GES-2020-00042
DokID 396846

Input to the Danish consultation response regarding the EU Commission's consultation on cyber resilience

The Danish Financial Supervisory Authority is asking for input to the EU Commission's consultation on cyber resilience. The Danish Financial Supervisory Authority is preparing a comprehensive Danish consultation response to be submitted to the EU Commission. Insurance & Pension Denmark (hereafter referred to as F&P) is pleased to have the opportunity to provide input to a comprehensive Danish consultation response to be presented to the EU Commission.

On 19 December 2019, the EU Commission launched a consultation on cyber resilience. The consultation seeks to identify the need to amend existing rules, including, in particular, the Network and Information Security (NIS) Directive, as well as possible new legislation regarding 'digital operational resilience for financial services'. The consultation is part of a major policy initiative by the EU to deal with the ever-increasing use of 'Information and Communication Technology' (ICT) in the financial sector and the security challenges that this causes.

F&P's consultation response focuses on possible new legislation on 'digital operational resilience for financial services'. The consultation response does not address any changes to the Network and Information Security (NIS) Directive. F&P expects something more concrete from the European Commission in terms of possible amendments to the NIS Directive. This is purportedly coming in Q4 2020.

There is generally significant support from F&P for more focused action from the EU, helping to enhance cyber resilience in both the EU and Denmark. The insurance and pension sector is pleased to be involved in this work. We support the EU's agenda to address the ever-increasing use of ICT in the financial sector and the security challenges arising from this.

The cyber security agenda is a top priority in the Danish insurance and pension sector. There is close coordination and knowledge sharing in the sector. The sector is working to ensure close collaboration between the entire financial sector and the National Bank of Denmark (through the Financial Sector Forum for Operational Resilience, FSOR), the Danish Financial Supervisory Authority (through the Decentralized Unit for Cyber and Information Security for the Financial Sector

(DCIS)), and the Centre for Cyber Security (CFCS). Each company in the Insurance and Pension sector invests considerable resources on preventing cyber incidents, protecting citizens' personal information and ensuring that staff are well trained. Cyber security is a very high priority in the sector.

F&P takes the view that the framework, in its current form, does not provide an adequate basis for assessing the need for new regulation, and the value it provides in addressing the questions in the framework. The European initiative should focus on how we share knowledge and work together to enhance the robustness of our cyber security. The cyber threat is a reality and it *is* important to protect the financial sector in Denmark and throughout the EU. F&P is asking for more attention to be paid to the EU's and the state's responsibility to reduce the risk to the sector by, for example, drawing up measures designed to curb criminal activity.

Instead the spotlight is usually targeted at businesses. If businesses are hit by cyberattacks, they are regarded more as perpetrators than as victims, and are therefore liable to be punished. F&P is genuinely concerned that so many bodies in both the public and private sectors are now being set up in Denmark to address the threat from cyberattacks that the impact of cyber security measures are being undermined due to silo mentality and bureaucracy.

The sector already has many different bodies just at national level. These bodies now include FSOR, DCIS, CFCS and Nordic Financial CERT (NFCERT) as well as the National Board of Digitization [Digitaliseringsstyrelsen].

Here are some more specific comments on the digital operational resilience framework:

Initial points concerning an assessment of the value of the 'digital operational resilience framework':

- There are already many good initiatives on cyber and information security, taken at the local level by companies, but also by various consultancy and audit companies. For example, there are many so-called maturity models that seek to assess a company's readiness in terms of cyber and information security. It is difficult to see how this European framework differs, and what it contributes in terms introducing something new – and something that does not already exist and is already in place.
- The F&P sector is well advanced when it comes to implementing cyber and information security measures. The national risk analysis of the bank and the F&P sector, respectively, shows that the impact of cyberattacks on society varies. The banking sector is more time-critical, whereas the F&P is not time-critical in the same way. It is therefore advisable to take a more risk-based approach to European initiatives, as the need also differs in terms of whether we are dealing with banks or insurance companies.
- Viewed from a broader perspective, the framework may be justified in that the EU obtains a clearer picture of the level of security in the financial sector in different EU member states. This will provide more information for raising the general level of security across EU member states.
- Pooling cyber and information security incidents, using this information to enable countries to share their experiences with a view to strengthening cyber security, and taking on board recommendations to counter current cyber and security incidents, will be a positive outcome. The EC3 Europol Cybercrime Centre is already, to a certain extent, taking a broader view of current cyber

and security incidents and is issuing a weekly report on what they have observed.

The following points refer to possible regulation of the framework:

- F&P currently takes the view that it is important to enhance knowledge sharing and cooperation in the EU. It is crucial that new legislation increases the value of cyber security work. New legislation should therefore not be rushed through and should certainly not be based on the existing questionnaire (framework). The Danish Financial Supervisory Agency also has some questionnaires that they use for inspections. The questionnaires could possibly be used as a supplement if the questions have not already been covered. However, there is a big difference between using a framework as a guideline (such as ISO27001) and being subject to a requirement to follow it.
- The framework should take into account the differences in the financial sector, including differences in risks and levels of "maturity" (i.e. experience and readiness). One disadvantage is that less "mature" companies might regard their security arrangements to be adequate simply by complying with the rules. This would then require the framework bar to be set relatively high to achieve the minimum level of cyber security.
- F&P anticipates that it will be difficult to ascertain whether the companies are complying with the framework in its present form. Our attitude towards the framework is therefore also highly dependent on the consequences of a breach of compliance.

Final points regarding the shape and structure of the framework itself:

- The questions in the framework must cover a wide range of issues, which they do. However, it also means that they will have a varying degree of relevance depending on the maturity level of those answering the questions.
- The framework is currently only under review. F&P also deems that the framework has not been sufficiently prepared. There are a number of flaws. Many of the questions relating to maturity level also are difficult to answer. The response options should also be modified, so that respondents have less scope to submit open responses and are given more controlled response options, meaning that the respondent completing the questionnaire will only receive an answer indicating the "security level". Open responses mean that the "recipient" must extract the answer and give their subjective assessment of the answer. Instead, if you have to choose between predefined response options, the feedback can be processed much more effectively. You therefore obtain feedback you can actually use.