To: Mr. Valdis Dombrovskis
Executive Vice-President, DG Financial Stability, Financial Services and Capital Markets Union
European Commission

Ms. Margrethe Vestager
Executive Vice-President, DG Competition European Commission

Mr. Juhan Lepassaar
Executive Director ENISA

Cc: Mr. Gabriel Bernardino, Chairman of the EIOPA

20 March 2020

Pan-European Insurance Forum's views on increasing cyber security through digital operational resilience

Dear Executive Vice-President Dombrovskis,

Cyber-attacks have increased in severity and frequency over the past years which has led to growing cyber risks across sectors. As the Pan-European Insurance Forum (PEIF), we therefore appreciate that the European Commission (EC) has made strengthening cybersecurity one of its ambitions for *making Europe fit for the Digital Age* and has launched a consultation to explore how an enhanced cross-sectoral digital operational resilience framework for financial services could be set up. The EC consultation runs in parallel to an EIOPA consultation on guidelines on Information and Communication Technology (ICT) security and governance for insurers.

We fully support that both the EC and EIOPA have the intend to tackle cyber related issues in a broad sense, i.e. ensuring resilience and security of the EU financial industry. As representatives of major European insurers, we would like to draw your attention to the following aspects:

1. We welcome EIOPA's draft ICT guidelines, which describe well-known good practices in ICT security and governance, as they will result in a harmonized interpretation of regulatory standards across Europe. **We recommend aligning the guidelines with already existing international IT / Information Security standards in order to create international convergence of ICT risk oversight.** For instance, the guidelines should re-use frameworks and terminology such as (1) the operational risk framework under Solvency II, (2) the National Institute of Standards and Technology (NIST) guidelines and taxonomy, and (3) international existing norms such as ISO 27001.

2. With regard to the EC consultation, we appreciate the effort to create a comprehensive framework for digital operational resilience. However, we believe that **a cross-sectoral regulation would provide a more consistent and harmonized overall level of digital operational resilience than a sector specific approach**. Despite convergence in high level requirements, the technical specifications and supervisory practices that are currently in place differ across sectors and jurisdictions, leading to a complex and fragmented regulatory landscape within the EU.

We thus support a European regulation which sets robust and specific minimum standards based on clear definitions across sectors in a proportional and risk-based approach. **We encourage to make the regulation compulsory across sectors via the review of the NIS Directive, i.e. transforming the Directive into a binding Regulation. The regulation should avoid heterogeneous levels of interpretation and enforcement by supervisory bodies.** To support regulatory convergence and a level playing field, the regulation should as much as possible make use of already existing international definitions and standards (e.g. NIST, FSB cyber lexicon).

To increase knowledge, preparedness and resilience across sectors, **we believe that a common taxonomy that describes threats, methods and types of cyber-attacks is needed**. This common taxonomy could serve several purposes such as (1) enabling other regulated firms to identify and respond to cyber threats, or (2) building a retrospective approach to enable trend analysis and public awareness. Incidents data need to be shared and this can only be efficient if there is a common taxonomy.

3. **To enhance cyber resilience in an overarching way across sectors, we strongly support the joint and aligned initiative for robust and harmonized standards under the umbrella of the European Union Agency for Cybersecurity (ENISA).** We further support the efforts to establish ENISA as a platform for cyber security intelligence and information exchange as such a platform would strengthen operational collaboration between legitimate private and public players within Europe.

4. In addition, **we support a specific framework, certification and oversight regime for ICT providers (including cloud providers).** Such a framework would make it easier for e.g. cloud users to validate their risk control effectiveness and receive relevant assurance. Current sector-specific outsourcing regulation and supervision of the outsourcing party do not reach the source of the risk which typically concentrates at provider level (not at the level of insurers).

PEIF insurers stand ready to provide their knowledge and expertise to make Europe fit for the Digital Age. We look forward to engaging with you and your services to build a framework that will be effective in strengthening cyber security in Europe.

Yours sincerely,

Thomas Buberl
Chairman of the Pan-European Insurance Forum

About the Pan-European Insurance Forum (PEIF)

PEIF is an informal forum for the CEOs of major European insurers (Aegon, Allianz, AVIVA, AXA, Generali, MAPFRE, Munich Re, RSA, Swiss Re, UNIQA, and Zurich) to exchange and present views on policy and regulatory issues amongst themselves and with others. PEIF companies represent around two-thirds of the STOXX® Europe Insurance.

PEIF Secretariat: peifsecretariat@axa.com
EU Transparency Register: 03667978021-69