ESMA_QA_2379

Submission Date
17/12/2024

Status: Question Rejected

Additional Information

Level 1 Regulation
Regulation (EU) 2022/2554 - The Digital Operational Resilience Act (DORA)

Topic
Other DORA topics

Subject Matter
Art. 1 ust. 1 DORA - systems supporting the business processes of financial entities

Question
Financial entities select ICT service providers based on risk assessment, taking into account the business continuity plan and a number of national and sectoral regulations regarding cybersecurity. In addition to standard contractual relationships with entrepreneurs, there are also solutions that financial entities use:
a) on the basis of a license, e.g. open source. The license provisions are not negotiated, and

the service is not individually parameterized for the investment company. The investment company has no influence on the shape of the service and the license provisions. The licenses contain provisions regarding automatic update of the tool, but do not contain provisions regarding, e.g. support or SLA, e.g. Adobe Acrobat Reader;
b) web applications, e.g. Lex/Legalis systems (review of legal acts), which employees access via a browser, the agreement does not involve installing the application on the employee's computer, but only providing a specified number of licenses for use by the company, or a web system for registering correspondence in the case of ordering a courier;
c) providers of employee benefits, e.g. medical care. They are not directly related to the company's business, employees use the application on private devices and log in with a private email address, while registration is necessary for the medical company to create an account for the employee;

Is it possible to apply the principle of proportionality, provided for in the DORA regulations, which will allow for proper identification of risks and the application of proportionate mitigants in the case of the above-mentioned services? In the opinion of the financial entity, the application of all the obligations indicated in the DORA regulations, in particular those concerning contractual provisions and reporting obligations, is disproportionate to the risk generated by the above solutions. The financial entity does not deny the need for each case of evaluation of the solution and review of its correct functioning, the number of entities in relation to which these obligations would have to be performed may affect the quality of the duties performed.

Are the services supporting a critical or important function all the services used as part of performing this function, including those that are quickly and relatively cheaply replaceable (e.g. Adobe Acrobat Reader, 7ZIP, e-mail encryption program)?