Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by RDSPs for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact

COMMISSION IMPLEMENTING REGULATION (EU) 2018/151

of 30 January 2018

laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by **[**F1RDSPs**]** for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union(1), and in particular Article 16(8) thereof,

Whereas:

(1) In accordance with Directive (EU) 2016/1148, **[**F1RDSPs**]** remain free to take technical and organisational measures they consider appropriate and proportionate to manage the risk posed to the security of their network and information systems, as long as those measures ensure an appropriate level of security and take into account the elements provided for in that Directive.

(2) When identifying the appropriate and proportionate technical and organisational measures, the **[**F2RDSP**]** should approach information security in a systematic way, using a risk-based approach.

(3) In order to ensure the security of systems and facilities, **[**F1RDSPs**]** should perform assessment and analysis procedures. These activities should concern the systematic management of network and information systems, the physical and environmental security, the security of supplies and the access controls.

(4) When carrying out a risk analysis within the systematic management of network and information systems, **[**F1RDSPs**]** should be encouraged to identify specific risks and quantify their significance, for example by identifying threats to critical assets and how they may affect the operations, and determining how best to mitigate those threats based on current capabilities and resource requirements.

(5) Policies on human resources could refer to the management of skills, including aspects related to the development of security related skills and awareness-raising. When

deciding on an appropriate set of policies on security of operation, the **[**F1RDSPs**]** should be encouraged to take into account aspects of change management, vulnerability management, formalisation of operating and administrative practices and system mapping.

(6) Policies on security architecture could comprise in particular the segregation of networks and systems as well as specific security measures for critical operations such as administration operations. The segregation of networks and systems could enable a **[**F2RDSP**]** to distinguish between elements such as data flows and computing resources that belong to a client, group of clients, the **[**F2RDSP**]** or third parties.

(7) The measures taken with regard to the physical and environmental security should ensure the security of an organisation's network and information systems from damage caused by incidents such as theft, fire, flood or other weather effects, telecommunications or power failures.

(8) The security of supplies such as electrical power, fuel or cooling could encompass the security of the supply chain that includes in particular the security of third party contractors and subcontractors and their management. The traceability of critical supplies refers to the ability of the **[**F2RDSP**]** to identify and record sources of those supplies.

(9) The users of digital services should encompass natural and legal persons who are customers of or are subscribers to an online marketplace or a cloud computing service, or who are visitors to an online search engine website in order to undertake keyword searches.

(10) When defining the substantiality of the impact of an incident, the cases laid down in this regulation should be considered as a non-exhaustive list of substantial incidents. Lessons should be drawn from the implementation of this Regulation and from the work of the Cooperation Group as regards the collection of best practice information on risks and incidents and the discussions on modalities for reporting notifications of incidents as referred to in points (i) and (m) of Article 11(3) of Directive (EU) 2016/1148. The result could be comprehensive guidelines on quantitative thresholds of notification parameters that may trigger the notification obligation for **[**F1RDSPs**]** under Article 16(3) of Directive (EU) 2016/1148. Where appropriate, the Commission could also consider reviewing the thresholds currently laid down in this Regulation.

(11) In order to enable competent authorities to be informed about potential new risks, the **[**F1RDSPs**]** should be encouraged to voluntarily report any incident whose characteristics have been previously unknown to them such as new exploits, attack-vectors or threat actor, vulnerabilities and hazards.

(12) This Regulation should apply on the day following the expiry of the deadline for transposition of Directive (EU) 2016/1148.

(13) The measures provided for in this Regulation are in accordance with the opinion of the Network and Information Systems Security Committee referred to Article 22 of Directive (EU) 2016/1148,

HAS ADOPTED THIS REGULATION:

Textual Amendments

F1 Word in Regulation substituted (20.1.2021) by The Network and Information Systems (Amendment etc.) (EU Exit) Regulations 2019 (S.I. 2019/653), **Sch. para. 14(3)**; 2020 c. 1, Sch. 5 para. 1(1)

F2 Word in Regulation substituted (20.1.2021) by The Network and Information Systems (Amendment etc.) (EU Exit) Regulations 2019 (S.I. 2019/653), **Sch. para. 14(2)**; 2020 c. 1, Sch. 5 para. 1(1)

(**1**) OJ L 194, 19.7.2016, p. 1.