A Superintendência de Seguros Privados (SUSEP) publicou, no dia 03/08/2021, a Circular nº 638/2021, decorrente do Edital de Consulta Pública nº 15/2021, que apresenta novas disposições sobre o tema da segurança cibernética a ser aplicável às sociedades supervisionadas (seguradoras, entidades abertas de previdência complementar, sociedades de capitalização e resseguradores locais).

A Circular visa alinhar o mercado securitário com as disposições legais existentes e deve ser interpretada conjuntamente com a Lei Geral de Proteção de Dados Pessoais (LGPD), com as normas a serem editadas pela Autoridade Nacional de Proteção de Dados (ANPD) e com a legislação consumerista, se o caso.

Como regra geral, a Circular impõe às supervisionadas o dever de gestão do risco cibernético, que deve estar em conformidade com o Sistema de Controles Internos (SCI) e com a Estrutura de Gestão de Riscos (EGR) da Companhia.

A norma traz diversas novidades, das quais destacamos:

- Previsão de uma “Política de Segurança Cibernética”, que deverá:

- Contemplar os objetivos da segurança cibernética e o compromisso dos órgãos internos com a melhoria dos processos a ela relacionados;

- Prover diretrizes para (i) a classificação dos dados conforme a sua relevância; (ii) a implementação de novos processos e procedimentos de segurança cibernética; e (iii) terceirização de serviços de processamento e armazenamento de dados, em especial os relevantes; e

- Ser compatível com o porte da Companhia, incluindo a natureza e a complexidade das suas operações, bem como o seu grau de exposição ao risco cibernético.

- A obrigatoriedade de a Companhia possuir e manter atualizados processos, procedimentos e controles para identificar e reduzir vulnerabilidades, bem como detectar, responder e se recuperar de incidentes, que deverão ser previstos no plano de continuidade de negócios.

- A Companhia deverá comunicar à SUSEP, no prazo máximo de 5 (cinco) dias úteis a partir do conhecimento do evento, a ocorrência de incidentes relevantes, detalhando a extensão do dano causado e, se o caso, as ações em curso para regularização completa da situação e os respectivos responsáveis e prazos.

- Necessidade de documentar em Relatório anual a efetividade da prevenção e tratamento de incidentes feitos pela companhia.

- A Companhia deverá informar a SUSEP, em até 30 dias após a formalização dos contratos, sobre a terceirização de serviços de processamento e armazenamento de dados, incluindo dados sobre a denominação do prestador, a atividade que será por ele exercida e os países e regiões onde os serviços serão prestados e os dados serão gerenciados, bem como qualquer alteração contratual sobre essas condições. A Companhia deverá adequar os contratos já vigentes até o dia 01/09/2024.

- Caberá à Companhia exigir que os prestadores dos serviços de processamento e armazenamento de dados observem as disposições legais e normativas em vigor, bem como que possuam processos, medidas e procedimentos sobre segurança cibernética não inferiores aos seus próprios, o que não exime a Companhia do cumprimento das suas obrigações legais e normativas.

A Circular obriga à guarda de diversos documentos envolvendo a segurança cibernética da Companhia, que, por força da Circular SUSEP nº 605/2020, devem ser armazenados por 5 (cinco) anos.

Por fim, embora a Circular entre em vigor em 01/09/2021, as supervisionadas dos segmentos S1 ou S2 (definidos pela Resolução CNSP nº 388/2020) deverão se adequar até 30/06/2022, enquanto as dos segmentos S3 ou S4 possuem prazo até 01/09/2022.

A íntegra da circular pode ser acessada neste link.

SUSEP Circular No. 638/2021: Rules About Cybersecurity

On August 3, 2021, the Superintendence of Private Insurance (SUSEP) published Circular No. 638/2021, resulting from SUSEP Public Consultation No. 15/2021, which introduces new provisions about cybersecurity to be applied to supervised companies (insurers, open entities of complementary pensions, capitalization companies and local reinsurers).

The Circular seeks to align the insurance market with existing legal provisions and should be interpreted in accordance with the General Data Protection Law (LGPD), with rules to be issued by the National Data Protection Authority (ANPD), and with consumer legislation, if applicable.

As a general rule, the Circular imposes on supervised companies the duty to manage cyber risk, which must be in compliance with the Company's Internal Controls System (SCI) and Risk Management Framework (EGR).

The rule introduces several innovations, of which we highlight:

- Creation of a "Cybersecurity Policy", which shall:

- Contemplate the purposes of cybersecurity and internal departments' commitment with improving the processes related to it;

- Provide guidelines for (i) classification of data according to its sensitivity; (ii) implementation of new cybersecurity processes and procedures; and (iii) outsourcing of data processing and storage services, especially the relevant ones; and

- Be compatible with the Company's size, including the nature and complexity of its operations and its level of exposure to cyber risk.

- The Company must have and keep updated processes, procedures and controls to identify and reduce vulnerabilities as well as to detect, respond to and recover from incidents, which must be provided for in the business continuity plan.

- The Company must communicate SUSEP, within a maximum of 5 (five) business days from the knowledge of the event, about the occurrence of relevant incidents, detailing the extent of the damage caused and, if applicable, the actions in progress for the complete regularization of the situation and the respective responsible persons and deadlines.

- The obligation to document the results of the Company's prevention and treatment of incidents in an annual report.

- The Company must inform SUSEP, within 30 days after the signing of the contracts, about any outsourcing of data processing and storage services, including the name of the provider, the activity to be performed by the provider and the countries and regions where the services will be provided and the data will be managed, as well as any contractual changes to these conditions. The Company must adapt the contracts already in effect by September 1, 2024.

- The Company will be responsible for requiring that the providers of data processing and storage services comply with the legal and regulatory provisions in force as well as that they have cybersecurity processes, measures and procedures that are not inferior to its own, which does not exempt the Company from complying with its legal and regulatory obligations.

The Circular provides for the obligation to keep several documents involving the Company's cybersecurity, which, pursuant to SUSEP Circular No. 605/2020, must be stored for a minimum period of 5 (five) years.

Finally, although the Circular comes into force on September 1, 2021, the supervised companies in segments S1 or S2 (defined by CNSP Resolution No. 388/2020) must comply until June 30, 2022, while companies in segments S3 or S4 have until September 1, 2022.

The full Circular can be accessed at this link.

Fonte: Demarest, 11.08.2021