REPÚBLICA FRANCESA

O primeiro-ministro

Projeto de decreto sobre a proteção de dados estratégicos e sensíveis no mercado da computação em nuvem

NOR:

Público-alvo: *administrações e operadores do Estado, grupos de interesse público*

Assunto: *…*

Entrada em vigor: *o decreto entra em vigor no dia seguinte ao da sua publicação.*

Nota: *….*

Referências: *o decreto aplica o artigo 31.º da Lei n.º 2024-449, de 21 de maio de 2024, relativa à segurança e regulamentação do espaço digital. Pode ser consultado no sítio Web Légifrance (http://www.legifrance.gouv.fr).*

O primeiro-ministro,

Sobre o relatório de XX,

Tendo em conta o Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.º 526/2013 (Regulamento Cibersegurança),

Tendo em conta a Diretiva (UE) 2015/1535 do Parlamento Europeu e do Conselho, de 9 de setembro de 2015, relativa a um procedimento de informação no domínio das regulamentações técnicas e das regras relativas aos serviços da sociedade da informação,

Tendo em conta o Código da Defesa, nomeadamente o artigo D. 3126-2,

Tendo em conta o Despacho n.º 2005-1516, de 8 de dezembro de 2005, relativo ao intercâmbio eletrónico entre utilizadores e autoridades administrativas e entre autoridades administrativas, nomeadamente o seu artigo 9.º,

Tendo em conta a Lei n.º 2016-1321, de 7 de outubro de 2016, relativa à República Digital, nomeadamente o artigo 16.º,

Tendo em conta a Lei n.º 2024-449, de 21 de maio de 2024, relativa à segurança e regulação do espaço digital, nomeadamente o artigo 31.º,

Tendo em conta o Decreto n.º 2014-445, de 30 de abril de 2014, relativo às funções e à organização da Direção-Geral da Segurança Interna,

Tendo em conta o Decreto n.º 2015-350, de 27 de março de 2015, com a redação que lhe foi dada, relativo à qualificação dos produtos de segurança e dos prestadores de serviços de confiança para as necessidades de segurança dos sistemas de informação,

Tendo em conta a notificação n.º XX enviada à Comissão Europeia em XXX,

Após consulta do Conselho de Estado (Secção da Administração),

Decreta:

Artigo 1.º

A lista dos grupos de interesse público a que se refere o artigo 31.º, n.º I, da referida Lei de 21 de maio de 2024 inclui:

- o grupo de interesse público conhecido como «Agência de Saúde Digital (ANS)»,
- o grupo de interesse público conhecido como «Agência Nacional de Investigação da SIDA (ANRS)»,
- o grupo de interesse público conhecido como «Agência para a Promoção da Formação e do Intercâmbio Educativo e Científico»,
- o grupo de interesse público «Centro de Acesso Seguro a Dados (CASD)»,
- o grupo de interesse público «Centro de Recursos para a Prevenção da Radicalização»,
- o grupo de interesse público «Escola Nacional de Veterinária»,
- o grupo de interesse público «Grupo de Interesse Público sobre Fontes Radioativas Seladas de Elevada Atividade (GIP SOURCES HA)»,
- o grupo de interesse público «Sistema Nacional de Registo da Procura de Habitação Social (GIP SNE)»,
- o grupo de interesse público «Modernização das Declarações Sociais (GIP-MDS)»,
- O grupo de interesse público «Observatório da Ciência e da Tecnologia».

Artigo 2.º

I - Para a aplicação do artigo 31.º da referida Lei de 21 de maio de 2024, o prestador de serviços privado deve implementar os seguintes critérios de segurança e proteção de dados:

- uma política de segurança da informação e de gestão dos riscos documentada que integre a cadeia de subcontratação,
- um sistema seguro de gestão dos recursos humanos para o pessoal envolvido na prestação do serviço,
- ferramentas e procedimentos para a gestão segura dos equipamentos que implementam o serviço e os sistemas de informação,
- medidas de segurança física, ambiental e lógica, tais como a utilização de mecanismos de encriptação, o controlo do acesso e a gestão da identidade do utilizador,
- procedimentos de gestão de incidentes de segurança da informação e medidas de continuidade das atividades,
- medidas para o cumprimento das disposições legais em vigor em França e das medidas de proteção de dados, em especial as contratuais, para dados tratados ou armazenados contra qualquer acesso por parte de autoridades públicas de países terceiros não autorizados pelo direito da União Europeia ou pelo direito de um Estado-Membro, incluindo, em especial, as condições que regem a detenção do capital e dos direitos de voto na empresa do prestador de serviços e o estabelecimento do prestador de serviços e de eventuais subcontratantes.

Um quadro, desenvolvido pela Agência Francesa para a Cibersegurança nas condições do referido Decreto de 27 de março de 2015, estabelece os requisitos relativos a esses critérios. A consulta necessária para a criação e o desenvolvimento deste quadro de referência para o sistema de informação do Estado deve ser realizada em conjunto com a Direção Digital Interministerial.

II - A fim de cumprir os requisitos em matéria de proteção de dados e de segurança previstos no artigo 31.º, n.º I, da referida Lei de 21 de maio de 2024, as administrações em causa devem recorrer aos serviços de computação em nuvem prestados por um prestador de serviços privado qualificado, adjudicados nas condições previstas no capítulo III do referido decreto de 27 de março de 2015 e que preencham os critérios referidos no ponto I do presente artigo, ou de uma certificação europeia de nível pelo menos equivalente.

III - São excluídos do âmbito de aplicação do presente artigo os sistemas de informação operacionais e de comunicação, os sistemas de informação científica e técnica e os sistemas de informação que envolvam, requeiram ou contenham meios ou informações classificados que integrem o sistema de informação e de comunicação de defesa, bem como os sistemas de informação e de comunicação operados pelos serviços referidos no artigo D. 3126-2 do Código da Defesa e no artigo 1.º do referido Decreto de 30 de abril de 2014.

Artigo 3.º

I - Se uma administração já tiver iniciado, à data da entrada em vigor do artigo 31.º da referida Lei de 21 de maio de 2024, um projeto que preencha as condições estabelecidas no referido artigo e que utilize um serviço de computação em nuvem prestado por um prestador de serviços privado que não aplique os critérios de segurança e proteção de dados definidos no artigo 2.º do presente decreto, esta pode solicitar, de acordo com os procedimentos estabelecidos por despacho do primeiro-ministro, uma derrogação às obrigações previstas no mesmo artigo.

Esta derrogação não pode exceder 18 meses se existir uma oferta aceitável de serviços de computação em nuvem, na aceção do n.º II do presente artigo, disponível em França. Caso

não exista uma oferta aceitável de serviços em nuvem disponível em França à data do pedido de derrogação, a derrogação não pode exceder um ano antes de um eventual novo pedido.

Esta derrogação é concedida por decisão fundamentada do ministro responsável pelo projeto e validada pelo primeiro-ministro.

É tornada pública nas condições previstas no livro III do Código das Relações Públicas.

II - A avaliação da aceitabilidade, na aceção do artigo 31.º, n.º III, da Lei de 21 de maio de 2024 acima referida, de uma oferta de serviços de computação em nuvem baseia-se nos seguintes critérios:

- a necessidade funcional que a oferta pode satisfazer, tendo em conta as tarefas da administração em causa,
- as condições financeiras,
- as condições operacionais e técnicas de segurança e proteção dos dados tratados pelo fornecedor da oferta, em conformidade com os requisitos estabelecidos no artigo 2.º do presente decreto,
- as condições de fim de contrato e as garantias de reversibilidade,
- as condições de controlo, sustentabilidade e independência na aceção do artigo 16.º da referida Lei de 7 de outubro de 2016.

Feito em,

Pelo primeiro-ministro: