CNPD
Comissão Nacional
de Proteção de Dados

PARECER/2024/20

I. Pedido

1. A Senhora Presidente da Autoridade de Supervisão de Seguros e Fundos de Pensão solicitou à Comissão Nacional de Proteção de Dados (CNPD) que se pronunciasse sobre o "Projeto de Norma Regulamentar relativa à comunicação de incidentes de caráter severo relacionado com as TIC"

2. A CNPD emite parecer no âmbito das suas atribuições e competências, enquanto autoridade administrativa independente com poderes de autoridade para o controlo dos tratamentos de dados pessoais, conferidos pela alínea *c)* do n.º 1 do artigo 57.º, a alínea *b)* do n.º 3 do artigo 58.º e n.º 4 do artigo 36.º, todos do Regulamento (UE) 2016/679, de 27 de abril de 2016 – Regulamento Geral sobre a Proteção de Dados (doravante RGPD), em conjugação com o disposto no artigo 3.º, no n.º 2 do artigo 4.º e na alínea *a)* do n.º 1 do artigo 6.º, todos da Lei n.º 58/2019, de 8 de agosto, que executa na ordem jurídica interna o RGPD.

II. Análise

3. O projeto de norma regulamentar[1] *sub iudice* encontra-se em fase de consulta pública, como se afirma no parágrafo 5 do pedido de parecer, cujo prazo terminará no dia 1 de julho de 2024.

4. Nos termos do artigo 18º, n.º 4 da Lei n.º 43/2004, alterada pela Lei n.º 58/2019, de 8 de agosto, esta Comissão emite parecer, no âmbito das suas competências, "... sobre disposições legais e regulamentares em preparação [que] devem ser remetidos à CNPD pelo titular do órgão com poder legiferante ou regulamentar, instruídos com o respetivo estudo de impacto sobre a proteção de dados pessoais."

5. Estando perante, pois, proposta ainda não consolidada, eventualmente sujeita a discussão e posterior deliberação e adoção, que poderão incluir -ou não-, a final, diferenças mais ou menos significativas em relação a proposta ou ante projeto sujeito a auscultação, sublinha a CNPD que deve ser entendido aquele comando normativo como tendo por objeto propostas disciplinadoras *finais,* sob pena de se poder reputar comprometida a utilidade, atualidade (e/ou integridade analítica objetiva) dos conteúdos levados a parecer, bem como o seu

[1] Doravante, Projeto Regulamentar ou Projeto.

juízo relativamente à conformidade preventiva com a legislação de proteção de dados pessoais que possa estar em causa e que, de resto, inspirou o legislador no desenho desta competência concreta atribuída a esta Autoridade. Por conseguinte, será essa versão *final* a que deverá ser comunicada à CNPD para emissão do competente parecer.

Isto posto,

6. Pretende a ASF emitir norma regulamentar ao abrigo do disposto no n.º 4 do artigo 81.º do regime jurídico de acesso e exercício da atividade seguradora e resseguradora (RJASR), aprovado pela Lei n.º 147/2015, de 9 de setembro, no n.º 4 do artigo 150.º do regime jurídico da constituição e do funcionamento dos fundos de pensões e das entidades gestoras de fundos de pensões (RJFP), aprovado pela Lei n.º 27/2020, de 23 de julho, na alínea *a)* do n.º 1 e no n.º 2 do artigo 34.º, no artigo 36.º e no artigo 39.º do regime jurídico da distribuição de seguros e de resseguros (RJDS), aprovado pela Lei n.º 7/2019, de 16 de janeiro, bem como na alínea *a)* do n.º 3 do artigo 16.º dos seus Estatutos.

7. Em suma, o novo projeto regulamentar visa criar um novo mecanismo de comunicação à ASF de incidentes de caráter severo relacionados com as tecnologias de informação e comunicação pelas entidades sujeitas à sua supervisão, como decorre do artigo primeiro do diploma em análise, enquadrando-se nas práticas de governação eficaz, face à utilização crescente das tecnologias de informação e comunicação na prestação de serviços na atividade supervisionada, com os riscos operacionais e de segurança que estas podem comportar.

8. Assim, as normas aplicar-se-ão às empresas de seguros e de resseguros com sede em Portugal, às sociedades gestoras de fundos de pensões autorizadas em Portugal, bem como aos mediadores de seguros, resseguros e de seguros a título acessório residentes ou com sede em Portugal, que não sejam microempresas ou pequenas ou médias empresas de acordo com os critérios previstos no Decreto-Lei n.º 372/2007, com exceção dos mediadores de seguros que também sejam instituições de crédito, incluindo-se, no primeiro e terceiro casos, o exercício da atividade através de sucursal ou em regime de livre prestação de serviços no território de outros Estados membros da União Europeia.

9. O projeto regulamentar é composto por 8 (oito) artigos. Se o primeiro e segundo artigos se destinam a fixar o objeto do diploma e o seu âmbito subjetivo, o terceiro e quarto cumprem, já, fins interpretativos quanto ao mecanismo que se pretende instituir – se, no primeiro, se fixam um conjunto de definições para efeitos hermenêuticos do dispositivo normativo (definições relativas), no segundo, sob epígrafe "Classificação de incidentes relacionados com as TIC", oferece-se um conjunto de critérios que permitirão concluir quando se estará defronte de um incidente severo.

10. Será o caso, por exemplo, quando:

a) Existe um acesso doloso, não autorizado e efetivo às redes e sistemas de informação da entidade; ou

b) O incidente afeta serviços críticos da entidade e, cumulativamente, verificam-se duas ou mais das seguintes situações:

i) O número de clientes afetados pelo incidente é superior a 10% do total de clientes que utilizam o serviço afetado ou é superior a cem mil clientes;

ii) A duração do incidente é superior a 24 horas ou o tempo de indisponibilidade do serviço crítico é superior a duas horas;

iii) O incidente afeta a disponibilidade, autenticidade, integridade ou confidencialidade dos dados, com impacto ou potencial impacto negativo na implementação dos objetivos de negócio ou no cumprimento de exigências regulatórias;

iv) O incidente tem impacto económico, nomeadamente quando os custos e as perdas diretos e indiretos incorridos pela entidade devido ao incidente excedam ou são suscetíveis de exceder os cem mil euros, excluindo eventuais montantes recuperáveis;

v) O incidente tem impacto reputacional, nos termos previstos nos n.ºs 3 e 4.

11. Assente que seja estar-se perante incidente severo, nesta aceção normativa, adentrar-se-á no previsto nos artigos 5.º a 7º do projeto regulamentar, *i.e.*, terão as entidades mencionadas no ponto 8 desta peça de proceder à comunicação à ASF desses incidentes, através da apresentação de uma notificação inicial, um relatório intercalar, e um relatório final.

12. O demais que nesse artigo 5º se concretiza, quanto a esses elementos, vem assim disciplinado:

2 – As entidades previstas no n.º 1 do artigo 2.º devem assegurar que a informação prestada é completa e rigorosa e, quando tal não seja possível nos casos das alíneas a) e b) do número anterior, que são apresentados valores estimados com base na informação disponível.

3 – Quando apresentarem o relatório intercalar ou final, as entidades previstas no n.º 1 do artigo 2.º devem atualizar, sempre que possível, a informação prestada anteriormente.

4 – Quando, após reavaliação, concluam que o incidente comunicado nunca cumpriu os critérios de classificação previstos no artigo anterior, as entidades previstas no n.º 1 do artigo 2.º devem apenas enviar à ASF um relatório final com a informação relacionada com a reclassificação do incidente como não severo.

5 – Sem prejuízo da manutenção da responsabilidade das entidades previstas no n.º 1 do artigo 2.º, a comunicação de incidentes nos termos do presente artigo pode ser subcontratada a um terceiro prestador de serviços, em conformidade com o regime aplicável em matéria de subcontratação.

6 – Deve ser designado pelo órgão de administração das entidades previstas no n.º 1 do artigo 2.º um responsável pela comunicação de incidentes de carácter severo relacionados com as TIC, que, no caso das entidades referidas nas alíneas a) e b) daquela disposição, pode ser o responsável pela função de segurança da informação.

7 – O responsável a que se refere o número anterior deve, juntamente com a comunicação prevista na alínea a) do n.º 1, tomar conhecimento da informação relativa ao tratamento de dados pessoais constante do formulário referente a essa comunicação.

13. Feita esta exposição descritiva, da leitura conjugada dos artigos 4.º e 5.ª do Projeto Regulamentar não é possível perceber qual é a informação que está em causa, ou dito doutro modo, que dados preenchem os teores das referidas notificações e relatórios e, muito menos, por conseguinte, se existe -sequer- um tratamento de dados pessoais, e a qual a sua ontologia, composição e forma.

14. Na verdade, de nenhum artigo parece resultar esse quadro, o que prejudica irremediavelmente qualquer análise que possa ser realizada quanto à sua conformidade em relação à legislação em vigor de proteção de dados pessoais, sequer quanto à sua licitude.

Vejamos,

15. No artigo 5.º refere-se, somente, o que deve verificar-se para que se esteja perante incidente severo. Trata-se de uma qualificação material ou adjetiva do incidente de segurança. Nada se adianta quanto a que dados é que devem ser tratados e/ou comunicados, em diferentes categorias e em função dessas – várias – qualificações, nomeadamente se existem dados pessoais.

16. *Mutatis mutandis*, o mesmo sucede no tocante à obrigação de comunicação: em momento algum se vê definida qual a informação que ali deve ser colocada e comunicada – e, naturalmente, se existirão ou não dados pessoais. Ademais, como melhor se procurará explicar infra, mesmo uma vista holística dos documentos juntos, inclusivamente o Anexo II quanto à "informação relativa ao tratamento de dados pessoais", não parece lograr conclusão mais esclarecida.

17. E, no artigo 6.º, apenas se definem os prazos que pautam a comunicação dos elementos (notificação e relatórios) a dar a conhecer à ASF.

18. Isto considerando, não pode esta Comissão pronunciar-se sobre tais aspetos, desconhecendo-se qual a pretensão da Requerente. Mas, não pode também deixar de dizer-se, no caso de se prever, efetivamente, tratamento de dados pessoais (de clientes ou outros), não poderá prescindir-se de traçar um regime concreto e específico para o seu tratamento, em conformidade com a legislação em vigor, que presentemente inexiste.

19. Elemento integrador, pelo menos indicativamente, poderia constituir o artigo 7.º do projeto regulamentar, onde se lê, sob epígrafe "Meios de Comunicação" que:

1 – Os elementos de informação referidos no n.º 1 do artigo 5.º são enviados à ASF através do preenchimento de formulários próprios, constantes da seguinte plataforma dedicada para o efeito: [em preparação].

2 – Os formulários referidos no número anterior, bem como as alterações aos mesmos, são disponibilizados no sítio da ASF na Internet, após aprovação pelo Conselho de Administração desta Autoridade.

20. Todavia, como se vê, o respetivo formulário estará em preparação (e não foi enviado qualquer esboço à CNPD), pelo que se desconhecem os "campos" que este possa vir a conter, no sentido de contribuir para o esclarecimento da informação que dessas notificações e relatórios possa constar.

21. Não obstante, sublinha-se que, a existir, efetivamente, um tratamento de dados pessoais, os meios a utilizar na comunicação não são matéria acessória ou secundária – antes são fundamentais para a segurança e justificação do tratamento dos dados, devendo ser cuidadosamente pensada a forma, plataforma, tecnologia, possibilidades de acesso, entre outras, também a dever constar no competente projeto, e a possibilitar, desde logo, uma análise sobre possíveis riscos e sua mitigação.

22. Se será no referido formulário que virão concretizados ou dada execução de tratamento aos dados que terá previamente de estar previsto em projeto regulamentar, aquele assumirá, também, um papel importante para a avaliação do cumprimento dos princípios previstos no artigo 5.º do RGPD.

23. A única menção a dados pessoais presente na documentação enviada vem exclusivamente no artigo 5.º nº 7, onde consta que "*7 – O responsável a que se refere o número anterior deve, juntamente com a comunicação prevista na alínea a) do n.º 1, tomar conhecimento da informação relativa ao tratamento de dados pessoais constante do formulário referente a essa comunicação.*"

24. O responsável aí referido será quem, designado pelos órgãos de administração das entidades supra referidas, assume o ónus da comunicação de incidentes severos à ASF.

25. O conteúdo desta disposição aparece, porém, indefinida e difícil de aferir, particularmente se se considerar, como se deixou dito supra, que se desconhece como será concretizado o formulário de comunicação, onde, aparentemente, de acordo com este inciso, constará informação relativa ao tratamento de dados pessoais.

26. Ainda assim, não se sabendo que dados, afinal, estão em causa, não se percebe se se trata, *somente,* dos dados pessoais do próprio responsável comunicante, ou se se pretenderá referir a quaisquer outros, distinção de suma importância na constituição de um regime de proteção de dados como o que se pretende.

27. Pelas mesmas razões, não é possível criticamente bem analisar o Anexo II – Informação Relativa ao Tratamento de Dados Pessoais.

28. Se, por um lado, se poderá considerar, dado o teor daquele n.º 7 e do título do Anexo II, que se poderá tratar da execução do direito de informação relativo ao tratamento de dados pessoais do responsável pela comunicação (ainda que, como se disse, não parece coincidir com a última parte do inciso, onde se escreve "*…informação relativa ao tratamento de dados pessoais constante do formulário referente a essa comunicação"*), por outro, não parece ser esse Anexo absolutamente consonante com essa interpretação

29. Repare-se que, na alínea b), segundo parágrafo, desse documento, se prevê que "*No preenchimento de campos abertos ou descritivos não devem ser colocadas informações que permitam a identificação direta ou indireta de pessoais singulares (dados pessoais), sendo que, caso ocorra, a ASF poderá proceder à sua eliminação."*

30. Ainda que se excecione tratar-se de campos abertos ou descritivos, não se consegue aferir a extensão deste comando, já que não existe, como se disse, qualquer concretização sobre que dados serão tratados, e de quem, a verter, aparentemente, no abstrato formulário. No entanto, parece poder abrir-se a porta para colocar a hipótese de, afinal, não se tratar de um *mero* direito de informação a favor do responsável pela comunicação o que, junto à não previsão dos dados a comunicar mercê dos incidentes, corporizados em notificação e relatórios, torna objetivamente inapreciável o ajuste desta matéria.

31. Simplificando, parece partir-se de um pressuposto de existência de tratamento de dados pessoais, sem que se diga qual ou quais, ou em relação a quem, ou se lhe enderece um regime, mas também se proíbe, ao mesmo tempo, parcialmente ou não, certos tratamento de dados pessoais, sem que venham circunstanciadas quaisquer razões, num ou noutro caso.

32. Ainda assim, genericamente, pode deixar-se um conjunto de notas quanto a pontos específicos desse Anexo II.

33. Prescreve-se na alínea e), sob epígrafe conservação que *"Os dados pessoais recolhidos serão conservados enquanto forem necessários ao cumprimento das finalidades inerentes à supervisão da entidade supervisionada e, após a sua cessação, pelo tempo correspondente ao prazo prescricional do procedimento criminal ou contraordenacional aplicável por ilícitos relacionados com a atividade seguradora e de gestão de fundos de pensões."*

34. Nestes casos, deverá igualmente ser especificado o prazo de conservação dos dados pessoais recolhidos, de forma mais concreta possível, clara e desejavelmente taxativa, ou de marco objetivo que os concretize, em função e em consideração de cada uma das finalidades concretas que autorizam a sua recolha e tratamento,

devendo ser reduzidos ao essencial para esse cumprimento finalístico - conforme dispõe o artigo 5.º, aliena e) e Considerando 39 do RGPD, só assim se podendo avaliar a sua justa proporcionalidade. Ademais, deve fixar-se os prazos para o apagamento ou a sua revisão periódica.

35. Relativamente à transferência de dados pessoais, deve, também, especificar-se com clareza quais as circunstâncias concretas em que estas possam ocorrer que, *in casu*, aparecem omissas, não se bastando com remissões legais de caráter genérico. Adicionalmente, deve, se justificada a transferência, verter-se as informações constantes no artigo 13º do RGPD, concretamente, os destinatários (ou categorias de destinatários) dos dados pessoais, e quais os fins que as justificam.

36. Acrescente-se, ainda, que haverá que considerar o disposto na alínea *f)* do n.º 1 do artigo 13.º do RGPD, pois desta norma decorre que o responsável pelo tratamento deve informar o titular dos dados da transferência de dados pessoais para um país terceiro, indicando a existência de uma decisão de adequação adotada pela Comissão nos termos do artigo 45.º do RGPD, ou, na sua falta, a referência às garantias apropriadas ou adequadas e aos meios de obter cópias das mesmas, ou onde foram disponibilizadas. Note-se que, neste caso, deverá existir um acordo de colaboração que apresente garantias adequadas e nele estejam previstos os direitos oponíveis e efetivos dos titulares dos dados, bem como medidas corretivas eficazes, nos termos impostos pelo artigo 46.º deste diploma da União.

37. Na verdade, este tipo de operações não só exige o cumprimento das condições especialmente previstas nos artigos 44.ª e seguintes do RGPD, como pressupõe, a montante, o cumprimento do princípio de licitude previsto no artigo 5.ª, n.º1, alínea a) e o artigo 6.ª do mesmo Diploma, cuja avaliação, como se disse, se encontra neste momento impossível de realizar.

38. Finalmente, sublinha a CNPD que a presente Proposta Regulamentar deveria ser acompanhada por uma avaliação de impacto, nos termos conjugados dos artigos 18.º n.º 4 da Lei 43/2004, 7.º da Lei 58/2019, e 35.º do RGPD.

III. Conclusão

53. Nos termos e com os fundamentos expostos a CNPD recomenda:

a) Regular, densificando, quais aos dados a tratar no presente mecanismo, particularmente, se e quando envolvem dados pessoais de pessoas singulares e, em caso afirmativo, estabelecer-se um regime próprio e especificado para o seu tratamento neste projeto regulamentar, nomeadamente as suas

condições subjetivas, objetivas e técnicas, sem as quais não é possível a esta Comissão emitir um juízo concreto sobre proteção de dados.

b) Existindo tratamento de dados pessoais, a ponderação de realização de avaliação prévia de impacto, nos termos conjugados dos artigos 18.º n.º 4 da Lei 43/2004, 7º da Lei 58/2019, e 35º do RGPD.

Lisboa, 2 de julho de 2024

José Vegar Velho (Vogal)

Assinado por: **JOSÉ CARLOS VEGAR ALVES VELHO**
Data: 2024.07.02 17:20:31+01'00'