CNPD
Comissão Nacional de Proteção de Dados

PARECER/2024/47

I. Pedido

0 Presidente da Câmara Municipal de Setúbal, em representação do Município de Setúbal, solicitou à Comissão Nacional de Proteção de Dados (CNPD) a emissão de parecer sobre o "Projeto de Regulamento de Exploração de Modalidades Afins de Jogos de Fortuna ou Azar e Outras forma de Jogo do Município de Setúbal".

2. Com o pedido foi junto o Projeto de Regulamento de Exploração de Modalidades Afins de Jogos de Fortuna ou Azar e Outras Formas de Jogo do Município de Setúbal e o Estudo de Impacto sobre a Proteção de Dados Pessoais, nos termos do n.º 4 do artigo 18º da Lei n.º 43/2004, de 18 de agosto.

1. 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, 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. 0 58/2019, de 8 de agosto, que executa na ordem jurídica interna o RGPD e n.º 4 do artigo 18º, da Lei n.º 43/2004, de 18 de agosto.

II. Análise

2. De acordo com a nota justificativa junta, o Regulamento visa a regulação da matéria referente à autorização de exploração das modalidades afins de jogos de fortuna ou azar e outras formas de jogo, nomeadamente rifas, tômbolas, sorteios, concursos publicitários, concursos de conhecimentos e passatempos, após a transferência de competências para os órgãos municipais operada pela Lei n.º 50/2018, de 16 de agosto e pelo Decreto-Lei n.º 98/2018, de 27 de novembro.

3. O Regulamento prevê, no artigo 11º, n.º 2, que o pedido de autorização para a exploração de modalidades afins de jogos de fortuna ou azar e outras formas de jogo seja formulado em requerimento que, para além do mais, contenha as seguintes menções: "a) Tratando-se de pessoa singular: identificação do requerente, com o nome, domicílio, número e validade de documento de identificação civil e número de identificação fiscal, e número de telefone e endereço de correio eletrónico não obrigatórios; b) Tratando-se de pessoa coletiva: i) (...) ii) identificação do representante legal, com o nome e o número de validade do documento de identificação civil e número de telefone e endereço de correio eletrónico não obrigatórios; (...)".

4. No caso de se tratar de pessoa coletiva o requerimento deve ser instruído, entre outros, com o comprovativo do número de identificação fiscal do requerente e comprovativo do ato de constituição do

requerente, designadamente cópia da escritura pública de constituição - alíneas a) e b) do artigo 12º do Regulamento.

5. O artigo 23º, com a epígrafe "Proteção de Dados", consagra uma declaração de princípio de que as operações de tratamento de dados pessoais realizadas pelo requerente nos concursos, devem observar os princípios consagrados no RGPD, especificando que o tratamento deve ser baseado "num fundamento de licitude válido e assegurado os deveres de informação aos respetivos titulares."

6. Para tanto, no n.º 2 desse artigo, dispõe-se que o requerente, enquanto responsável pelo tratamento dos dados pessoais, "deve aplicar as medidas técnicas e organizativas adequadas destinadas a aplicar com eficácia os princípios da proteção de dados e a incluir as garantias necessárias no tratamento, para assegurar que só são tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento e poder comprovar que este é realizado em conformidade com o Regulamento Geral de Proteção de Dados e protege os direitos dos titulares dos dados."

7. O n.º 3 dessa mesma disposição prevê que, também nos casos de transferência de dados pessoais para um país terceiro ou uma organização internacional, o requerente deve assegurar o cumprimento no Regulamento Geral de Proteção de Dados.

8. As secções IV e V que regulamentam o sorteio e os prémios contêm diversas referências a dados pessoais. Assim:

i) O representante da entidade com competência de fiscalização em cada sorteio deve registar em ata para além do mais "os dados dos vencedores" -artigo 24º, n.º 4;

ii) Após a determinação dos premiados o requerente obriga-se a anunciar pelos meios de publicidade indicados no regulamento do concurso, o nome dos mesmos – artigo 25º;

iii) As declarações comprovativas da entrega dos prémios devem conter, para além do mais, (…) a identificação civil do premiado, o prémio que recebeu e o consentimento expresso para o tratamento dos seus dados pessoais para as finalidades específicas associadas - artigo 27º, n.º 2;

iv) Sendo o premiado menor, a declaração será assinada pelo seu representante legal e prestado o consentimento expresso para tratamento dos seus dados e dos do menor premiado – artigo 27º, n.º 4.

9. No artigo 33º, que regulamenta o "Tratamento de dados pessoais", o Município de Setúbal apresenta-se como responsável pelo tratamento de dados pessoais recolhidos no âmbito da exploração da atividade em causa, (alínea a) do n.º 3).

10. São identificadas duas atividades de tratamento de dados pessoais pelo Município de Setúbal: a primeira é o tratamento de dados no âmbito do pedido de autorização para exploração de modalidades afins de jogos de fortuna ou azar, em que os dados recolhidos são: o nome, número e validade do documento de identificação civil NIF, morada, telefone e endereço de correio eletrónico. A segunda ocorre no âmbito de declaração

comprovativa da entrega dos prémios e os dados recolhidos são a identificação civil do premiado, o prémio que recebeu e em que concurso e a declaração de consentimento para o tratamento dos seus dados pessoais para as finalidades específicas associadas.

11. Aparentemente, e independentemente da via de entrega dos requerimentos, (pessoalmente, por correio postal ou correio eletrónico), estes são desmaterializados e encaminhados, através da plataforma de gestão documental pela unidade orgânica denominada Secção de Atendimento e Gestão Documental (SEAGD) para o Gabinete de Apoio ao Empresário e Consumidor (GAEC).

12. Os documentos que tenham sido apresentados em suporte papel, após a sua desmaterialização, são remetidos ao Setor de Arquivo e Documentação, (SARQ), unidade que os mantém em arquivo até à sua eliminação decorridos 120 meses - alínea j) do artigo do 33º do Projeto de Regulamento).

13. Esse é também o prazo de conservação dos dados pelo Município de Setúbal, justificado por corresponder ao "prazo de prescrição dos direitos correspetivos, nomeadamente o prazo prescricional da responsabilidade financeira reintegratória, de acordo com o disposto no n.º 1, do artigo 70º, da Lei 98/97, de 26 de agosto (…)" – alínea K, do artigo 33º do Projeto de Regulamento.

14. Não se encontra previsto quem tem acesso aos registos.

15. A plataforma eletrónica de gestão documental é utilizada pelo Município para análise, instrução e elaboração de relatório com proposta de decisão e envio ao Presidente da Câmara Municipal, ou a quem tiver poderes delegados para proferir despacho de deferimento ou indeferimento do pedido.

16. A plataforma eletrónica para a tramitação do procedimento de forma desmaterializada é o "ERP Medidata".

17. A sociedade "Medidata.Net, Sistemas de Informação para Autarquias, SA, constitui-se como subcontratante, enquanto entidade gestora das aplicações "ERP Medidata "utilizadas pelo Município de Setúbal. Este subcontratante, na medida do estritamente necessário à execução do contrato de manutenção das aplicações SIGMA licenciadas ao Município, garante a execução de medidas técnicas e organizativas com vista ao cumprimento do RGPD, sendo que estas não foram indicadas nos documentos enviados e não constam do contrato outorgado a 25 de agosto de 2023, consultado no Portal dos contratos públicos.

18. No artigo 6º da AIPD são elencadas as medidas mitigadoras dos riscos e é feita a declaração de que para cumprir as normas do RGPD, em matéria de arquitetura de segurança das redes e sistemas de informação e procedimentos a adotar, (…) "o Município cumpre, em todas as aplicações e sistemas de informação, os requisitos técnicos constantes da Resolução do Conselho de Ministros n.º 41/2018, que define as orientações técnicas para a Administração Pública, quanto a esta matéria, (…)" .

19. Na alínea b), que se reporta à autenticação de utilizadores, prevê-se que os "Dados de sessão (e outros) [sejam] encriptados em URL;" (Uniform Resource Locater). Este procedimento não constitui uma boa prática, porquanto, mesmo encriptados, os dados de sessão ou utilizador não deverão em caso algum passar por URL, que é um elemento visível até em tráfego seguro (HTTPS).

20. Existe a possibilidade real de acesso VPN a partir do exterior sendo, por isso, necessário que o sistema deixe de estar exposto às vulnerabilidades de uma rede externa.

21. Tenha-se em consideração que parte dos ataques de software malicioso são concretizados escondendo o código infetado em ficheiros anexados a mensagens de correio eletrónico, (uma das vias de envio de pedido de autorização). Esses ficheiros, aparentemente fidedignos, uma vez abertos, podem executar instruções arbitrárias no computador e enviar vírus informático através da rede local. Podem ainda ocorrer ataques de Phishing em que as mensagens têm hiperligações maliciosas. Para estas situações não estão previstas medidas mitigadoras do risco.

22. O Projeto de Regulamento prevê o registo de atividade (logs) das operações realizadas sobre dados pessoais, com informação sobre quem, onde, quando e qual a ação praticada. Relativamente a estes registos dos acessos não é indicado nenhum prazo para a sua manutenção. Também não está definido quem tem o privilégio de acesso.

23. Um dos riscos identificados na AIPD é a perda de informação. Contudo, nenhuma medida mitigadora é apresentada para evitar essa ameaça, ou reduzir esse risco, o que importa fazer, adotando uma política de criação de cópias de segurança, validadas e guardadas em local de acesso controlado e, se possível, encriptadas.

24. A CNPD não pode avaliar as medidas técnicas e organizacionais a que o subcontrante está vinculado, porquanto o contrato publicitado não contém tal informação, sendo remetido para o caderno de encargos, que se desconhece.

25. O tratamento de dados pessoais deve obedecer aos princípios que enformam esta matéria e que se encontram enunciados no artigo 5º do RGPD, designadamente os da licitude, necessidade, adequação e minimização.

26. O artigo 25º do Regulamento prevê a obrigatoriedade do requerente, após a determinação dos premiados, (…) "anunciar pelos meios de publicidade indicados no regulamento do concurso (…) o nome dos mesmos, bem como o último dia do prazo em que os prémios podem ser levantados."

27. No respeito pelos princípios da necessidade e minimização a CNPD entende que deverá ser concedida aos premiados a possibilidade de se pronunciarem sobre se aceitam, ou não, a publicitação do seu nome, sendo que a transparência na atribuição dos prémios poderá ser garantida por outras formas.

III. Conclusões:

Nos termos e com os fundamentos acima expostos a CNPD pronuncia-se no sentido das medidas mitigadoras elencadas não se mostrarem suficientes à salvaguarda dos dados pessoais tratados e recomenda que:

a) Seja obrigatória a autenticação de dois fatores "Utilização de autenticação MFA";

b) A medida mitigadora de "Dados de Sessão (e outros) encriptados em URL" seja revista;

c) Seja assegurado que a rede onde se ligam utilizadores externos não faculte o acesso direto às aplicações e bases de dados;

d) Sejam adotadas medidas mitigadoras do risco de ataques de Phishing;

e) Seja definido quem tem acesso aos registos dos dados pessoais alvo de tratamento;

f) Seja adotada uma política de cópias de segurança e que as mesmas sejam validadas, e se possível encriptadas, e guardadas em local de acesso controlado;

g) Seja concedida aos premiados a possibilidade de se pronunciarem sobre se aceitam, ou não, a publicitação do seu nome;

h) Seja seguida a recomendação da Resolução do Conselho de Ministros n.º 41/2018, concretamente que os sistemas de armazenamento garantam redundância e disponibilidade, não devendo existir nenhum ponto único de falha.

Aprovada na reunião de 5 de novembro de 2024

Paula Meira Lourenço (Presidente)

Assinado por: **PAULA CRISTINA MEIRA LOURENÇO**
Data: 2024.11.05 20:57:56+00'00'
Certificado por: **Diário da República**
Atributos certificados: **Presidente - Comissão Nacional de Proteção de Dados**

CARTÃO DE CIDADÃO