

Formulário de Proteção de Dados Pessoais

1. DIAGRAMA DE CONTEXTO DA ARQUITETURA, com a apresentação do desenho da solução proposta ou adquirida, identificando as suas componentes; breve descrição da finalidade; identificação das categorias dos titulares dos dados pessoais e dos destinatários; fluxos de dados pessoais tratados para efeitos da interpretação da rastreabilidade do tratamento de dados realizado e indicação do Encarregado de Proteção de Dados e respetivo contacto.

2. CLASSIFICAÇÃO E IDENTIFICAÇÃO DOS DADOS PESSOAIS

a. Dados Genéricos

Tipos de Dados Pessoais	S/N	Se "S", identificar quais:
a.1) Dados de identificação (ex: nome, número de identificação civil, ...);	S	Nome dos participantes e membros de grupo; documento de identificação (CC/passaporte) apenas quando o quiz o exigir (opção configurável pelo Município), armazenado cifrado com AES-256-GCM.
a.2) Dados de contacto (ex: morada, e-mail, telefone, telemóvel, ...);	S	E-mail (registo e autenticação na app).
a.3) Dados de faturação (ex: NIF, montante cobrado, data, IBAN, ...);	N	A participação é gratuita para o utilizador final; não são tratados dados de faturação de titulares na plataforma
a.4) Dados de vida familiar (ex: situação familiar, dados do agregado familiar, estado civil, ...);	N	
a.5) Dados da vida profissional (ex: CV, situação profissional, escolaridade, formação, distinções, diplomas, ...);	N	
a.6) Dados com informações de ordem financeira e patrimonial (ex: vencimento, situação financeira, dados bancários, rendimentos, património, ...);	N	
a.7) Dados de tráfego e de localização (ex: endereços IP, logs, identificadores dos terminais, identificadores de ligação, dados de data e hora, dados de GPS, GSM, pontos wi-fi, ...);	S	Coordenadas GPS e precisão reportada no momento do check-in em cada ponto de interesse (finalidade essencial do serviço, com consentimento específico registado); endereços IP e registos de acesso (logs) com data/hora, para segurança e auditoria. A localização é recolhida apenas durante a participação ativa num quiz (foreground), não em contínuo.
a.8) Dados de navegação na internet (ex: utilizador, cookies de terceiros, dados de navegação, device fingerprinting, medição de acesso a sites e interação através de ferramentas analíticas e de monitorização, ...);	S	Apenas mecanismos de sessão/authenticação estritamente necessários. Sem cookies de terceiros, device fingerprinting ou analítica comportamental; a telemetria de erros está configurada sem PII (sendDefaultPii desativado, replay com máscara de texto e média).
a.9) Outras categorias de dados pessoais não sensíveis	S	Fotografias tiradas pelos participantes nos pontos de interesse (galeria partilhada do grupo), com remoção automática de metadados EXIF (incl. geolocalização embebida) e acesso por URL assinado; tokens de dispositivo para notificações push (pseudónimos).

Tipos de Dados Pessoais	S/N	Se “S”, identificar quais:
a.10) Dados de perfis (ex: hábitos de vida, bom devedor, saudável, ...).	N	Não é efetuada definição de perfis nem decisões automatizadas sobre os titulares.

b. Dados Pessoais de Categorias Especiais

Tipos de Dados Pessoais	S/N	Se “S”, identificar quais:
b.1) Dados de origem racial ou étnica;	N	
b.2) Dados relativos a opiniões políticas, filiação sindical, convicções religiosas e filosóficas;	N	
b.3) Dados genéticos;	N	
b.4) Dados biométricos (ex: controlo de acesso físico, controlo de acesso lógico, impressão digital, voz, fotografia, imagem, ...);	N	As fotografias dos participantes não são objeto de qualquer tratamento biométrico ou de identificação automática.
b.5) Dados relativos à saúde, à vida sexual e à orientação sexual;	N	
b.6) Dados relativos às condenações e às infrações penais;	N	
b.7) Outro	N	

3. IDENTIFICAÇÃO E LOCALIZAÇÃO DOS DADOS PESSOAIS TRATADOS, incluindo a **lista** dos “Ficheiros de Dados Pessoais”

Designação dos Ficheiros de Dados Pessoais” (suporte papel ou digital) ou de bases de dados a proteger	Identificação da localização - O tratamento de dados pessoais e a localização dos mesmos deverá estar toda sediada dentro da União Europeia, não permitindo armazenamento nem qualquer fluxo transfronteiriço de dados para países terceiros ou organizações internacionais. <i>[indicar a alínea correspondente para cada ativo elencado]</i> a) Nas instalações da CML; b) Nas instalações do subcontratante em território nacional; c) Nas instalações do subcontratante em território da União Europeia;
Base de dados aplicacional (PostgreSQL/PostGIS) — contas de utilizador, consentimentos, participações, check-ins (coordenadas), respostas, documentos de identificação cifrados	c) Nas instalações do subcontratante em território da União Europeia
Armazenamento de multimédia — fotografias dos participantes (EXIF removido, acesso por URL assinado)	c) Infraestrutura em território da União Europeia
Cópias de segurança da base de dados (diárias, com PITR)	c) Nas instalações do subcontratante em território da União Europeia
Registos de aplicação e auditoria (logs, sem PII em claro)	c) Nas instalações do subcontratante em território da União Europeia

4. MEDIDAS TÉCNICAS E ORGANIZATIVAS APLICADAS

Medidas técnicas e organizativas	S/N	Se "S", identificar quais:
5.1 Pseudonimização	S	5.1 Identificadores internos nos registos técnicos e de telemetria (nunca e-mail/nome); tokens de dispositivo pseudónimos; ambientes de teste e demonstração exclusivamente com dados sintéticos (seed), sem dados reais.
5.2 Cifragem dos dados pessoais	S	5.2 TLS em todas as comunicações (HTTPS obrigatório, certificados Let's Encrypt renovados automaticamente); documentos de identificação cifrados com AES-256-GCM com chave dedicada gerida em cofre, separada dos segredos de autenticação.
5.3 Destinadas a assegurar a confidencialidade, a integridade e a resiliência permanentes dos sistemas e dos serviços de tratamento	S	Isolamento multi-tenant row-level com verificação em todas as queries e testes de regressão de acesso cross-tenant no CI; RBAC com 4 perfis (superadmin, administrador do cliente, staff read-only, jogador); verificação de ownership em todos os fluxos de participação; API stateless com escalabilidade horizontal.
5.4 Destinadas a restabelecer atempadamente a disponibilidade e o acesso aos dados pessoais em caso de incidente físico ou técnico	S	Cópias de segurança diárias com point-in-time recovery (PITR/WAL), armazenadas em localização distinta; procedimentos de restauro documentados e testados; modo de manutenção controlado com comunicação aos utilizadores.
5.5 Processos para testar, apreciar e avaliar periodicamente a eficácia das medidas técnicas e organizativas a fim de garantir a segurança do tratamento.	S	Revisões de segurança formais registadas (última: 0 achados críticos; os achados altos foram corrigidos e verificados); análise de vulnerabilidades de dependências como gate obrigatório no CI (npm audit, nível high); testes automatizados de lógica de negócio, autenticação e isolamento de dados.
5.6 De identificação e de autorização do utilizador	S	Autenticação com palavra-passe (hash argon2id); sessões JWT de curta duração (15 min) com refresh token rotativo revogável e deteção de reutilização (revogação de todas as sessões); bloqueio progressivo de conta após 5 tentativas falhadas; rate limiting dedicado nos endpoints de autenticação; registo de tentativas falhadas como evento de segurança auditado.
5.7 De proteção de dados durante a transmissão	S	HTTPS/TLS obrigatório em todas as interfaces; CORS restrito por origem; headers de segurança (CSP, HSTS, X-Frame-Options, Referrer-Policy); URLs de fotografias assinados (HMAC) com validade limitada.
5.8 De proteção de dados durante a conservação	S	Cifragem AES-256-GCM dos dados mais sensíveis (documentos de identificação); remoção de metadados EXIF das fotografias; validação de ficheiros por assinatura binária (magic bytes) e limite de dimensão; segregação de ambientes (dev/staging/produção) com bases de dados isoladas.
5.9 Destinadas a garantir a segurança física dos locais onde os dados pessoais são tratados	S	Datacenter do fornecedor de infraestrutura na UE com certificação de segurança da informação — evidências do fornecedor a apresentar após fixação da infraestrutura de produção (antes da entrada em exploração).
5.10 Destinadas a garantir o registo cronológico de acontecimentos	S	Registo de auditoria das ações de administração e dos eventos de segurança (com data/hora do servidor); timestamps do servidor em todas as operações de jogo; histórico de consentimentos apenas por inserção (nunca alterado ou apagado).
5.11 Destinadas a garantir a configuração do sistema, incluindo a configuração por defeito	S	Segredos obrigatórios validados no arranque (a aplicação não arranca sem eles em produção); configuração segura por omissão; limites de payload; armazenamento seguro nativo nas apps (Keychain/EncryptedSharedPreferences); infraestrutura definida em ficheiros versionados.
5.12 De governação e de gestão interna do serviço informático e do serviço de segurança informática	S	Processo documentado de revisão de segurança com registo de achados e decisões; princípio do menor privilégio nos perfis; gestão formal de segredos em cofre; monitorização de erros e disponibilidade com alertas.
5.13 De certificação/garantia dos processos e dos produtos	S	Práticas alinhadas com os referenciais ISO/IEC 27001/27002; sem certificação própria à data. Compromisso de utilização de infraestrutura de alojamento certificada (ISO/IEC 27001) e de evolução do programa de certificação — evidências em sede de contratação.
5.14 Destinadas a garantir a minimização dos dados	S	Recolha limitada ao necessário: e-mail e nome para a conta; localização apenas no momento do check-in e durante participação ativa; documento de identificação apenas se o Município o configurar como exigido; telemetria sem PII.
5.15 Destinadas a garantir a qualidade dos dados	S	Validação de todas as entradas no servidor (DTOs com validação declarativa) e no

Medidas técnicas e organizativas	S/N	Se "S", identificar quais:
		cliente; pontuação e correção calculadas exclusivamente no servidor; coordenadas e distâncias verificadas server-side.
5.16 Destinadas a garantir uma limitação da conservação dos dados	S	Eliminação em cascata dos dados associados quando uma participação é eliminada; políticas de retenção a acordar com o Município por tipo de dados (com eliminação ou anonimização no termo dos prazos).
5.17 Destinadas a garantir a responsabilidade	S	Histórico de consentimentos versionado (tipo, decisão, data/hora, versão do texto); auditoria de ações administrativas; celebração de Acordo de Tratamento de Dados (art.º 28.º RGPD) nos termos definidos pelo Município.
5.18 Destinadas a permitir a portabilidade dos dados e a garantir o seu apagamento	S	Modelo de dados documentado em formatos abertos (PostgreSQL/JSON), permitindo exportação; funcionalidade de exportação/eliminação self-service para o titular em desenvolvimento (roadmap próximo), sendo os pedidos assegurados de imediato por via operacional com o Município.
5.19 Destinadas a garantir que os subcontratantes ulteriores ficam obrigados a poder prestar assistência ao responsável pelo tratamento e que asseguram o cumprimento do RGPD	S	Fornecedores de infraestrutura (alojamento na UE, armazenamento de multimédia, notificações push, telemetria de erros) vinculados a acordos de tratamento de dados nos termos do art.º 28.º; lista completa sujeita a autorização prévia do Município (ver ponto 8).
5.20 Outra	S	Medidas anti-fraude que protegem a integridade dos resultados: validação server-side de distância e plausibilidade de velocidade nos check-ins; tokens QR aleatórios não sequenciais.