



譯本
TRADUÇÃO

澳門特別行政區政府
Governo da Região Administrativa Especial de Macau
行政公職局
Direcção dos Serviços de Administração e Função Pública

Resposta à interpelação escrita apresentada pelo Deputado à Assembleia Legislativa Kou Ngon Seng

Em cumprimento das instruções do Chefe do Executivo, e após ter auscultado os pareceres da área de segurança e da Direcção dos Serviços da Protecção de Dados Pessoais, apresento a seguinte resposta à interpelação escrita do Deputado Kou Ngon Seng, datada de 21 de Abril de 2026, enviada a coberto do Ofício n.º 0513/GSG/SAAL/2026 da Assembleia Legislativa, de 24 de Abril de 2026, e recebida pelo Gabinete do Chefe do Executivo a 27 de Abril de 2026:

1. Em relação ao ponto 1 da interpelação

De acordo com a área de segurança, o Governo da RAEM já definiu, através da Lei da cibersegurança e da Lei da Protecção de Dados Pessoais, bem como nos documentos relativos às normas técnicas, incluindo a Regulação de padrões de gestão da cibersegurança e a Regulação de técnicas de gestão de vulnerabilidades da cibersegurança, os requisitos de gestão de segurança e técnicas que os operadores de infra-estruturas críticas (doravante designados por operadores) devem cumprir na construção e operação dos diversos tipos de sistema de informação das redes, os quais devem apresentar, anualmente, um relatório de cibersegurança. O Centro de Alerta e Resposta a Incidentes de Cibersegurança (doravante designado por CARIC) monitoriza, em conformidade com a lei, 24 horas por dia, 7 dias por semana, o tráfego de saída de dados dos operadores, dando-lhes assistência na identificação precoce, na prevenção de ataques ou de incidentes cibernéticos, e organiza proactivamente, de forma abrangente, o rastreio de cibersegurança, para que os operadores detectem vulnerabilidades na



譯本
TRADUÇÃO

澳門特別行政區政府
Governo da Região Administrativa Especial de Macau
行政公職局
Direcção dos Serviços de Administração e Função Pública

segurança e se preparem para responder a potenciais riscos de fuga de dados.

O Centro de Computação em Nuvem do Governo é dotado de um sistema de cibersegurança, implementando o regime de gestão de segurança, e existe uma equipa especializada para a supervisão sistemática, para a detecção e a prevenção de intrusões de rede e a resposta a ataques de má-fé 24 horas por dia, para garantir que as plataformas de governação electrónica importantes, nomeadamente a Conta Única de Macau e a Plataforma para Empresas e Associações, bem como os serviços electrónicos prestados pelas referidas plataformas, possam funcionar num ambiente seguro e estável. A Direcção dos Serviços de Administração e Função Pública (SAFP) supervisiona de forma contínua o risco de ataques cibernéticos e reage atempadamente, intensificando a capacidade de detecção e prevenção de invasões aos equipamentos e ao sistema informático. O Centro de Computação em Nuvem do Governo desde a entrada em funcionamento, não registou nenhum incidente de cibersegurança.

E ainda, as entidades públicas e privadas devem assegurar, nos termos da Lei da Protecção de Dados Pessoais (LPDP), a segurança e confidencialidade do tratamento de dados pessoais e adoptar as medidas técnicas e de organização adequadas para proteger os dados pessoais; estas medidas devem ter um nível de segurança adequado aos riscos próprios do sistema de tratamento de dados, à natureza dos dados a proteger, aos conhecimentos técnicos e aos custos. A Direcção dos Serviços da Protecção de Dados Pessoais (DSPDP) cumpre as suas atribuições de fiscalização, supervisionando o tratamento de dados pessoais pelos responsáveis pelo tratamento em ambiente de conformidade.



譯本
TRADUÇÃO

澳門特別行政區政府
Governo da Região Administrativa Especial de Macau
行政公職局
Direcção dos Serviços de Administração e Função Pública

2. Em relação ao ponto 2 da interpelação

Relativamente à educação e formação em cibersegurança, o SAFP organiza anualmente acções de educação e formação neste âmbito destinadas aos trabalhadores dos serviços públicos de diferentes níveis e áreas, com o intuito de reforçar a consciência dos trabalhadores dos serviços públicos, da sua responsabilidade pela cibersegurança, bem como aumentar a capacidade do pessoal da área informática no que concerne ao domínio e cumprimento dos requisitos técnicos de cibersegurança. Disponibiliza também acções de formação para a obtenção da certificação profissional em cibersegurança, para melhorar as aptidões profissionais de cibersegurança do pessoal técnico. Em 2025, um total de 4 900 trabalhadores participaram nestas acções de formação, incluindo dirigentes e chefias dos serviços, pessoal informático e técnico e pessoal administrativo geral.

A área de segurança revelou que na Regulação de padrões de gestão da cibersegurança exige-se expressamente que os operadores, incluindo os serviços públicos, assegurem a participação dos seus trabalhadores em acções de sensibilização sobre cibersegurança, de formação de competências técnicas, de acordo com o respectivo posto de trabalho. Os serviços que compõem o CARIC vão, também, continuar a realizar diversas actividades destinadas aos operadores, como acções de formação, fóruns, exercícios de simulação de incidente e visitas de intercâmbio, relacionadas com a cibersegurança.

Além disso, a DSPDP tem organizado sessões de esclarecimento e seminários temáticos sobre a LPDP para entidades públicas e privadas, com o



譯本
TRADUÇÃO

澳門特別行政區政府
Governo da Região Administrativa Especial de Macau
行政公職局
Direcção dos Serviços de Administração e Função Pública

objectivo de lembrar os princípios e as responsabilidades do tratamento de dados pessoais, a fim de reforçar a consciência da protecção de dados pessoais. A DSPDP tem organizado, em média e anualmente, 10 sessões de esclarecimento para os serviços públicos, contando com a participação anual de mais de 500 trabalhadores. A DSPDP está a preparar os materiais do curso e irá lançar um curso de formação *online* em colaboração com o Centro de Formação Jurídica e Judiciária, entre outros serviços, com vista a aumentar os conhecimentos dos trabalhadores dos serviços públicos sobre a protecção de dados pessoais.

3. Em relação ao ponto 3 da interpelação

No que concerne à supervisão de cibersegurança, a área de segurança revelou que a regulamentação vigente relativa à cibersegurança determina que os operadores no estabelecimento de um regime de gestão do acesso quando efectuado por pessoal externo aos sistemas de informação das redes, incluindo a celebração de acordos de confidencialidade com os adjudicatários, restrição rigorosa de acesso, reprodução ou revelação de dados sem autorização, e ainda que, no processo de desenvolvimento e de teste dos sistemas, se deva evitar o uso de dados pessoais verdadeiros e de dados sensíveis, a fim de prevenir fugas. A violação das respectivas disposições, o incumprimento dos deveres de cibersegurança, bem como as consequências perversas, imputáveis aos operadores ou adjudicatários, podem constituir infracções administrativas reguladas pela Lei da cibersegurança, ou mesmo ilícitos criminais, puníveis segundo a lei penal.

Ao nível técnico, o CARIC promove o reforço da supervisão dos operadores



譯本
TRADUÇÃO

澳門特別行政區政府
Governo da Região Administrativa Especial de Macau
行政公職局
Direcção dos Serviços de Administração e Função Pública

sobre os adjudicatários, através de diferentes meios, incluindo a definição de procedimentos de apreciação para a realização de *login* à distância em sistemas informáticos por parte dos adjudicatários para fornecerem os serviços de manutenção, bem como a adopção de tecnologias como o *Bastion Host*, para controlar e registar os processos operacionais dos adjudicatários, com vista a prevenir e melhor evitar a ocorrência de incidentes de fuga de dados.

Mais ainda, a DSPDP revelou que quando se trate de tratamento de dados de subcontrato, os respectivos serviços ou entidades devem escolher o subcontratante que ofereça garantias suficientes em termos de segurança técnica e de organização do tratamento, devem ainda, através de documento escrito, obrigar e orientar o subcontratante sobre a forma de proceder ao tratamento dos dados e, posteriormente, têm a responsabilidade de fiscalizar, de forma contínua, a execução do subcontrato e das medidas de garantia.

13 de Maio de 2026

A Directora do SAFP,

Leong Weng In