Inquérito sobre as políticas e a regulamentação aplicáveis à recolha e proteção de dados utilizadas no âmbito do serviço postal internacional

Solicita-se aos operadores designados dos Países-membros da União que enviem o presente questionário (sem a carta de acompanhamento) o mais rapidamente possível, **o mais tardar até 19 de janeiro de 2024**, para o seguinte endereço:

Bonseung Ku
Expert associé «Conseil en matière de politiques et de régulation»
Bureau international
Weltpoststrasse 4
3015 BERNE
SUISSE

O questionário, devidamente preenchido, pode igualmente ser enviado por correio eletrónico (bonseung.ku@upu.int).

Se encontrar dificuldades durante o preenchimento do questionário, pode entrar em contacto com Bonseung Ku, da Secretaria Internacional (telefone: (+41 31) 350 35 24; endereço eletrónico: bonseung.ku@upu.int).

❑ Ministério de tutela (responsável pelo setor postal) ❑ Regulador (responsável pelo setor postal) ❑ Operador designado	
Nome da organização	
Nome completo ❑ Sra. ❑ Sr.	
Cargo/título	
Endereço	
País	
Telefone	Endereço eletrónico

Questionário

Parte I – Perguntas gerais Sim Não

1. No âmbito das suas operações postais nacionais, que regulamentações aplicáveis à proteção de dados/privacidade[1] tem de cumprir?

   - ❑ Regulamento Geral sobre a Proteção de Dados (regulamentação da União Europeia)
   - ❑ Lei Federal Suíça sobre a Proteção de Dados
   - ❑ Lei da Califórnia sobre o Respeito da Privacidade dos Consumidores
   - ❑ Lei Geral de Proteção de Dados Pessoais do Brasil
   - ❑ Nenhuma
   - ❑ Outra (especifique):

2. Existem regulamentações sobre a proteção de dados específicas para o setor postal[2] no seu país? ❑ ❑

   Caso tenha respondido «sim», especifique:

3. Existem outras regulamentações intersectoriais sobre a proteção de dados, por exemplo, aplicáveis à alfândega ou ao transporte, que são igualmente aplicáveis ao setor postal no seu país? ❑ ❑

   Caso tenha respondido «sim», especifique:

4. Com que finalidade recolhe e troca dados pessoais[3] com terceiros, no âmbito das operações dos serviços postais internacionais (assinale a(s) resposta(s) correspondente(s))?

   - ❑ Operações (recolha, tratamento, rastreamento/identificação dos objetos, endereçamento, distribuição, etc.)
   - ❑ Alfândega e segurança (como os dados eletrónicos prévios (EAD) e as mensagens ITMATT)
   - ❑ Qualidade de serviço (comentários dos clientes, desempenho em termos de distribuição, etc.)
   - ❑ Finanças e contabilidade (como as informações de faturação e os dados de pagamento)
   - ❑ Outra (especifique):

[1] O termo «regulamentações aplicáveis à proteção de dados/privacidade» refere-se às regras e normas que regem a forma como os dados pessoais são recolhidos, utilizados, armazenados e transmitidos.
[2] As regulamentações específicas do setor são as que se aplicam apenas ao setor postal e podem prever obrigações diferentes ou adicionais em relação às regulamentações gerais da proteção de dados.
[3] Os dados pessoais dizem respeito a qualquer informação que pode ser utilizada para identificar ou se referir a uma pessoa singular.

O Acordo Multilateral de Partilha de Dados da UPU, adotado pelo Conselho de Operações Postais em abril de 2021, é uma ferramenta jurídica criada para facilitar a troca de dados necessários para a exploração dos serviços postais internacionais e permitir a implementação dessas trocas de acordo com os Atos da União.

Este acordo integra e alarga as disposições de fundo dos acordos multilaterais de partilha de dados existentes estabelecidos a título privado pelos operadores designados dos Países-membros da União. O objetivo é refletir melhor as obrigações de partilha de dados pertinentes contidas nos Atos da União, estabelecendo, simultaneamente, as condições adequadas para um instrumento de alcance mundial gerido pela UPU.

5. Assinou o Acordo Multilateral de Partilha de Dados da UPU?

- ❑ Sim
- ❑ Não
- ❑ Outro (especifique):

Parte II – Responsabilidade

6. Dispõe de um responsável pela proteção de dados ou de uma pessoa semelhante encarregada de garantir o cumprimento das obrigações aplicáveis à proteção de dados e da privacidade (assinale apenas uma resposta)?

- ❑ Temos um responsável ou uma equipa dedicada à proteção de dados que monitoriza e atualiza regularmente as nossas políticas e os nossos procedimentos
- ❑ Contamos com o apoio de consultores ou auditores externos que analisam periodicamente as nossas políticas e os nossos procedimentos e prestam aconselhamento sobre esta matéria
- ❑ Não dispomos de um responsável nem de uma equipa dedicada à proteção de dados que monitoriza e atualiza regularmente as nossas políticas e os nossos procedimentos
- ❑ Outro (especifique):

7. De que forma demonstra a sua responsabilidade em termos de proteção de dados/privacidade aos seus clientes e parceiros (assinale a(s) resposta(s) correspondente(s))?

- ❑ Publicamos a nossa política e as nossas declarações sobre a proteção de dados no nosso *site* e em outros canais de comunicação
- ❑ Realizamos avaliações e auditorias regulares dos impactos da proteção de dados[4] e comunicamos os resultados aos nossos parceiros
- ❑ Não dispomos de meios específicos para demonstrar a nossa responsabilidade em termos de confidencialidade dos dados
- ❑ Outra (especifique):

[4] Uma avaliação dos impactos da proteção de dados é um processo destinado a identificar e reduzir os riscos associados ao tratamento dos dados pessoais.

Parte III – Obrigações de informação

8. Como informa os titulares dos dados[5] sobre os meios utilizados para tratar os seus dados pessoais e as finalidades com que são tratados[6] (assinale a(s) resposta(s) correspondente(s))?

- ❑ Política de privacidade
- ❑ Condições gerais
- ❑ Endereço eletrónico
- ❑ Termos de consentimento
- ❑ Os titulares dos dados não são informados
- ❑ Outro (especifique):

9. De que forma garante que os dados pessoais são tratados apenas para as finalidades para as quais foram recolhidos (assinale a(s) resposta(s) correspondente(s))?

- ❑ Análise e atualização regulares das políticas de privacidade e dos termos de consentimento para que estejam alinhados com as finalidades específicas da recolha de dados
- ❑ Comunicação clara e transparente com os titulares dos dados relativamente à utilização prevista dos seus dados pessoais e obtenção do seu consentimento explícito para qualquer finalidade adicional
- ❑ Não estabelecemos nenhum método para garantir que os dados pessoais são tratados apenas para as finalidades para as quais foram recolhidos
- ❑ Outro (especifique):

Parte IV – Confidencialidade e segurança das trocas de dados

10. De que forma previne a transmissão não autorizada das informações confidenciais[7] (assinale a(s) resposta(s) correspondente(s))?

- ❑ Fornecemos regularmente programas de formação e sensibilização para as obrigações em termos de proteção de dados/privacidade
- ❑ Dispomos de políticas e procedimentos escritos que especificam os papéis e as responsabilidades das pessoas que tratam os dados e as consequências do seu incumprimento
- ❑ Utilizamos medidas técnicas e organizacionais[8] para proteger as informações confidenciais contra qualquer acesso, utilização, alteração ou divulgação não autorizado

[5] Os titulares dos dados são qualquer pessoa singular podendo ser identificada, direta ou indiretamente, através de dados como um nome, um número de identificação ou dados de localização, ou através de características específicas da identidade física, fisiológica, genética, mental, económica, cultural ou social da pessoa. Por outras palavras, o titular dos dados é um utilizador final cujos dados pessoais podem ser recolhidos.

[6] O tratamento dos dados pessoais refere-se a qualquer operação ou conjunto de operações realizadas sobre os dados pessoais, como a recolha, o armazenamento, a utilização, a divulgação ou a supressão.

[7] A transmissão não autorizada de informações confidenciais refere-se à divulgação ou utilização de informações reservadas a certas pessoas ou entidades.

[8] As medidas técnicas incluem os mecanismos como a encriptação ou os controlos de acesso para preservar as informações, e as medidas organizacionais incluem a implementação de procedimentos e práticas para gerir e reduzir os riscos associados ao tratamento dos dados.

- ❑ Monitorizamos e avaliamos as atividades de tratamento dos dados e comunicamos qualquer violação e incidente às autoridades competentes e às partes interessadas
- ❑ Outro (especifique):

Relativamente às perguntas 11 a 15, a UPU reconhece o facto de que poderá estar a utilizar as tecnologias e os serviços fornecidos pelo Centro de Tecnologias Postais (CTP), em particular o IPS e o Sistema de Declaração para a Alfândega (CDS), bem como, em alguns casos, a hospedagem de *softwares* do CTP (como a nuvem e .POST). Nesses casos, uma parte das respostas às perguntas que se seguem pode resultar das operações do CTP. Contudo, pedimos-lhe que responda a essas perguntas e complete as suas respostas com as medidas que toma localmente.

11. Possui um plano de emergência[9] e um sistema de *backup* para garantir a continuidade do serviço e a retoma das atividades em caso de interrupção imprevista ou de qualquer outra situação de emergência (assinale apenas uma resposta)?
    - ❑ Sim
    - ❑ Não
    - ❑ Outro (especifique):

12. Como monitoriza e comunica as violações de segurança[10] relacionadas com os dados pessoais trocados com outras partes (assinale apenas uma resposta)?
    - ❑ Dispomos de uma equipa ou unidade de segurança dedicada que monitoriza e comunica todas as violações de segurança
    - ❑ Dispomos de uma política ou procedimento de resposta a uma violação de segurança que orienta as nossas atividades de monitorização e comunicação
    - ❑ Contamos com as funcionalidades de segurança ou os alertas dos nossos sistemas ou redes para detetar e comunicar qualquer violação de segurança
    - ❑ Não monitorizamos nem comunicamos as violações de segurança
    - ❑ Outro (especifique):

13. Que partes notifica em caso de violação de segurança (assinale a(s) resposta(s) correspondente(s))?
    - ❑ Secretaria Internacional da UPU
    - ❑ Autoridades locais de proteção dos dados
    - ❑ Titulares dos dados afetados
    - ❑ Terceiros afetados
    - ❑ Não notificamos as violações de segurança a ninguém

[9] Um plano de emergência é um conjunto de procedimentos e ações que se destinam a prevenir, preparar, reagir e recuperar de qualquer ameaça ou interrupção que possa afetar os serviços postais (como as catástrofes naturais, os acidentes ou os ciberataques).

[10] Uma violação de segurança é um evento que compromete a confidencialidade, integridade ou disponibilidade dos dados trocados com outras partes, como o acesso, a divulgação ou a alteração não autorizados, ou a perda ou destruição.

- ❑ Outro (especifique):

14. Qual é o prazo em que notifica as partes interessadas da violação de segurança (assinale apenas uma resposta)?

- ❑ Em vinte e quatro horas
- ❑ Em setenta e duas horas
- ❑ Numa semana
- ❑ Num mês
- ❑ Não notificamos as violações de segurança
- ❑ Outro (especifique):

15. Com que frequência realiza auditorias ou avaliações de segurança[11] da infraestrutura e do ambiente operacional utilizados para a troca de dados com terceiros (assinale apenas uma resposta)?

- ❑ Uma vez por mês
- ❑ Uma vez por trimestre
- ❑ Duas vezes por ano
- ❑ Todos os anos
- ❑ Nunca
- ❑ Outro (especifique):

Parte V – Conservação dos dados

16. De que forma determina o período de conservação dos dados[12] para os dados pessoais que trata (assinale apenas uma resposta)?

- ❑ Seguimos o período de conservação da nossa jurisdição local
- ❑ Seguimos o período de conservação da jurisdição mais restritiva aplicável
- ❑ Conservamos os dados pessoais enquanto for necessário
- ❑ Conservamos os dados pessoais por um período fixo de dez anos a partir da sua receção
- ❑ Outro (especifique):

[11] As auditorias ou avaliações de segurança são avaliações sistemáticas das políticas, dos procedimentos e controlos que protegem a confidencialidade, integridade e disponibilidade dos dados trocados com outras partes.
[12] O período de conservação corresponde ao período de tempo durante o qual os dados pessoais são conservados para o seu tratamento, armazenamento ou arquivamento, antes de serem eliminados ou destruídos de forma segura.

17. Como elimina os dados pessoais[13] após o período de conservação ou quando deixam de ser necessários (assinale a(s) resposta(s) correspondente(s))?

- ❑ Eliminamos os dados pessoais de todos os sistemas e dispositivos
- ❑ Destruímos os dados pessoais através de trituração, incineração ou desmagnetização
- ❑ Devolvemos os dados pessoais à parte remetente ou são transferidos a um terceiro autorizado pela parte remetente
- ❑ Anonimizamos ou agregamos os dados pessoais para eliminar todas as informações pessoais ou sensíveis
- ❑ Conservamos os dados pessoais para efeitos de arquivamento, investigação ou estatísticos, com as devidas medidas de proteção
- ❑ Outro (especifique):

Parte VI – Direitos de acesso

18. Que tipo de direitos de acesso fornece aos titulares dos dados[14] (assinale a(s) resposta(s) correspondente(s))?

- ❑ Direito de acesso
- ❑ Direito de retificação
- ❑ Direito de eliminação
- ❑ Direito à portabilidade dos dados
- ❑ Direito de oposição
- ❑ Direito à limitação do tratamento
- ❑ Não existem direitos específicos
- ❑ Outro (especifique):

[13] A eliminação dos dados pessoais significa a supressão, destruição ou anonimização dos dados pessoais de forma segura e irreversível, para que não estejam acessíveis e não sejam armazenados ou divulgados por partes não autorizadas.

[14] Os direitos de acesso dos titulares dos dados são os direitos de que as pessoas singulares dispõem para aceder, corrigir, eliminar ou limitar o tratamento dos seus dados pessoais detidos por uma organização.

19. Qual é o tempo de resposta[15] aos pedidos ou consultas de outras partes ou dos titulares dos dados (assinale apenas uma resposta)?

- ❑ Um dia de calendário
- ❑ Um a três dias de calendário
- ❑ Quatro a sete dias de calendário
- ❑ Duas ou três semanas
- ❑ Um mês
- ❑ Não existe tempo de resposta específico
- ❑ Outro (especifique):

20. Qual é o processo[16] que segue para responder aos pedidos de informação de terceiros ou dos titulares dos dados (assinale a(s) resposta(s) correspondente(s))?

- ❑ Dispomos de uma política e de um procedimento formais para avaliar e responder aos pedidos de informação de terceiros e documentamos e seguimos todos os pedidos e as respostas
- ❑ Dispomos de orientações gerais para responder aos pedidos de informação de terceiros, mas não temos nenhuma política nem nenhum procedimento formal e não documentamos nem seguimos os pedidos e as respostas
- ❑ Não dispomos de nenhum processo específico para responder aos pedidos de informação de terceiros, que são tratados caso a caso, consoante a natureza e a origem do pedido
- ❑ Não respondemos aos pedidos de informação de terceiros, exceto em caso de obrigação legal
- ❑ Outro (especifique):

Parte VII – Registo das atividades de tratamento dos dados

21. De que forma mantém um registo das atividades de tratamento dos dados[17]? Quais são o formato e a estrutura gerais dos seus registos das atividades de tratamento dos dados (assinale apenas uma resposta)?

- ❑ Utilizamos uma ferramenta informática dedicada
- ❑ Utilizamos uma folha de cálculo ou um documento
- ❑ Utilizamos um diário de bordo físico ou eletrónico
- ❑ Não mantemos nenhum registo das atividades de tratamento dos dados

[15] Uma resposta é uma comunicação que reconhece, responde ou dá seguimento a um pedido ou uma consulta de um terceiro, por exemplo, através de uma carta ou de um *e-mail*.
[16] Os processos de resposta aos pedidos de informação de terceiros podem incluir a receção, verificação, priorização, atribuição, recuperação, compilação, análise, aprovação e o envio das informações.
[17] Os registos das atividades de tratamento dos dados são documentos ou registos que descrevem os dados pessoais que recolhe, utiliza, armazena e partilha enquanto operador designado.

- ❑ Outro (especifique):

22. Que informações sobre as atividades de tratamento dos dados reúne nos seus registos (assinale a(s) resposta(s) correspondente(s))?

- ❑ Nome e dados de contacto de cada parte que trata os dados
- ❑ Categorias e fontes dos dados tratados
- ❑ Descrição das medidas de segurança técnicas e organizacionais
- ❑ Outro (especifique):

23. Com que frequência revê e atualiza o seu registo das atividades de tratamento dos dados (assinale apenas uma resposta)?

- ❑ Pelo menos uma vez por ano
- ❑ De seis em seis meses
- ❑ De três em três meses
- ❑ Intervalos superiores a três meses
- ❑ Nunca ou raramente
- ❑ Outro (especifique):

Parte VIII – Formação e sensibilização

24. A sua organização fornece formação em proteção de dados[18] aos seus funcionários (assinale apenas uma resposta)?

- ❑ Sim, dispomos de programas de formação regulares e completos dedicados à proteção de dados para todos os funcionários
- ❑ Sim, mas as formações são mínimas e não são atualizadas regularmente
- ❑ Não, atualmente, a nossa organização não fornece formação em proteção de dados aos seus funcionários
- ❑ Outro (especifique):

[18] As formações podem incluir todos os métodos que se destinam a formar os funcionários para os princípios, processos e responsabilidades aplicáveis em termos de proteção de dados/privacidade, incluindo sessões de formação presenciais, formações à distância, recursos e materiais, etc.

Parte IX – Experiência prática

25. Já se deparou com dificuldades ou desafios[19] na recolha, tratamento, transmissão ou receção de dados (assinale apenas uma resposta)?

- ❑ Sim, frequentemente
- ❑ Sim, ocasionalmente
- ❑ Não, nunca
- ❑ Não sabe
- ❑ Outro (especifique):

26. Caso tenha respondido «sim» à pergunta anterior, quais foram as principais causas ou fontes das dificuldades ou dos desafios encontrados (assinale a(s) resposta(s) correspondente(s))?

- ❑ Normas ou sistemas técnicos incompatíveis ou obsoletos
- ❑ Falta de clareza ou coerência nas exigências ou nos formatos aplicáveis aos dados
- ❑ Obstáculos ou restrições legais ou regulamentares
- ❑ Erros ou atrasos humanos ou operacionais
- ❑ Outro (especifique):

[19] As dificuldades e os desafios podem incluir problemas técnicos, problemas de qualidade dos dados, violações da segurança dos dados ou violações de privacidade e obstáculos regulamentares ou legais.