

《個人資料保護法》第25條第5款規定，辦公室需“在其年度報告中公佈所有依本法律規定編制的意見書和發出的許可，尤其是第七條第二款和第九條第一款規定的許可”。

參考國際上的通用做法，在公佈該等意見書及許可時，辦公室作出了適當的節錄編輯，在不妨礙公眾瞭解該等法律文件的內容，特別是法律觀點及具體分析的前提下，避免影響申請機構的運作或影響其資料處理的技術安全，也避免相同的觀點和分析重複刊登。

Segundo o n.º 5 do artigo 25.º da Lei da Protecção de Dados Pessoais, o Gabinete tem de publicar “no seu relatório anual todos as autorizações e pareceres elaborados ou concedidos ao abrigo da presente lei, designadamente as autorizações previstas no n.º 2 do artigo 7.º e no n.º 1 do artigo 9.º”

Servindo como exemplo a prática internacional na publicação destes pareceres e autorizações, procedemos ao extracto e edição dos mesmos, tendo sempre em conta evitar a sobreposição dos trabalhos publicados, bem como a necessidade de não prejudicar a compreensão do conteúdo dos respectivos documentos jurídicos, sobretudo nos seus pontos jurídicos e na análise em concreto, a fim de não afectar o funcionamento ou a segurança técnica do tratamento das instituições requerentes em causa.



意見書
Pareceres



第02/P/2009/GDP 號意見書

事由：關於商號在經營場所張貼懷疑盜竊者的影像資料

本辦公室近期收到多名市民的舉報，指本澳部分商號基於保安目的，將從保安攝錄監察系統拍攝所得懷疑盜竊者的影像資料張貼於經營場所內。舉報人質疑商號這種公開當事人個人資料的做法，有違個人資料之處理目的，涉嫌違反第8/2005號法律（《個人資料保護法》）之相關規定。

基於履行第8/2005號法律及第83/2007號行政長官批示所賦予之職責，就市民所舉報之事實，本辦公室曾立案跟進。對舉報內容查證屬實之商號，本辦公室已根據《個人資料保護法》之相關規定，要求涉嫌違反上述法律規定的商號作出了相關的改善措施，包括立即停止張貼懷疑盜竊者的影像資料，並銷毀有關的影像資料。有關的商號亦已根據本辦公室之通知，執行了上述改善措施。

考慮到本澳現時商號張貼懷疑盜竊者影像資料的情況存在一定的普遍性，本辦公室作為《個人資料保護法》所指之公共當局，為監察、協調對該法律的遵守和執行，認為有必要向社會公開本辦公室處理商號在經營場所張貼懷疑盜竊者的影像資料事件所持之法律觀點，以便有關的商號清晰《個人資料保護法》對個人資料的處理規定，以及不遵守有關規定須承擔的法律後果，並對不符合上述法律規定的情況盡快予以糾正，以免觸犯法律。

一、《個人資料保護法》之適用

有關的商號將攝錄監察系統拍攝所得懷疑盜竊者的影像資料張貼於經營場所內（主要張貼於店舖之出入口的玻璃櫥窗或收銀機附近之顯眼位置），目的在於對意圖不軌者起阻嚇作用。且某些商號所張貼的涉嫌盜竊者的影像資料，更附有文字說明，指影像圖片上的人為“賊人”或“盜竊者”等。在張貼的影像資料中，相關人士的樣貌清晰可辨認，能清楚識別其身份。

根據《個人資料保護法》第4條第1款(一)項規定，“個人資料”是指與某個身份已確定或身份可確定的自然人（“資料當事人”）有關的任何資訊，包括聲音和影像。任何機構在經營場所內張貼懷疑盜竊者的影像圖片，只要有關的影像資料清晰可辨認，足以確定當事人身份，已屬第4條第1款(一)項所指的受法律保護的個人資料範疇。而根據同一法律第3條第3款的規定，對可以認別身份的人的影像資料進行處理受該法律所規範。

二、裝置攝錄監察系統之合法性及正當性

根據《個人資料保護法》第2條規定，個人資料處理的一般原則是，資料處理應以透明的方式進行，



並應尊重私人生活的隱私和《澳門特別行政區基本法》、國際法文書和現行法律訂定的基本權利、自由和保障。且第5條亦規定，個人資料應以合法的方式並在遵守善意原則和第二條所指的一般原則下處理；為了特定、明確、正當和與負責處理實體的活動直接有關的目的而收集，之後對資料的處理亦不得偏離有關目的；並須適合、適當及不超越收集和之後處理資料的目的。

一般來說，機構基於保安或保障其他合法利益，在經營場所範圍內裝置攝錄監察系統，其目的是合法的。但基於保安目的拍攝所得的所有影像資料之處理，包括懷疑盜竊者的影像資料，受保安目的所限制，不能用作其他用途，否則違反《個人資料保護法》第5條規定。

此外，根據《個人資料保護法》第6條規定，除法律訂明之其他情況外，處理個人資料須取得當事人的明確同意，方具備處理個人資料的正當性條件。法律訂明的其他情況包括該條第(五)項所指：“為實現負責處理個人資料的實體或被告知資料的第三人的正當利益，只要資料當事人的利益或權利、自由和保障不優於這些正當利益。”在這種情況下，無須當事人之明確同意，亦可處理其個人資料。機構在經營場所範圍內，基於保安理由裝置攝錄監察系統，以保護經營場所之財產或其他合法利益，其目的是合法及正當的，受法律保護。在此情況下，當事人之個人利益並不優於機構上述之正當利益。換言之，機構基於上述目的裝置攝錄監察系統，即使沒有當事人之明確同意，亦為法律所允許，符合上述法律第6條第(五)項規定。

但機構將攝錄監察所收集的懷疑盜竊者影像資料，在經營場所內公開張貼，或將涉嫌盜竊者指為“賊人”或“盜竊者”，則已偏離了收集影像資料作為內部保安用途之目的。如果攝錄監察系統的資料顯示某人在機構經營場所內實施盜竊行為，且機構決定追究，則須報警處理，並將懷疑盜竊者的影像資料交予警方調查，而不能私自將未經司法審判的懷疑盜竊者的影像資料公開於經營場所張貼，並將有關的人士冠以“盜竊者”之罪名。機構在此涉嫌充當了執法者角色，在法院作出判決前，將有關人士稱為“盜竊者”。對此，機構可能要承擔其他方面之法律責任。

三、法律後果

如前所述，機構基於保安理由，無須取得當事人的同意，亦具正當性處理攝錄監察資料。但此並不代表機構可私自將攝錄系統內涉嫌盜竊者的影像資料公開張貼示眾及在法院作出判決前冠以“盜竊者”之罪名。如果攝錄監察系統的資料顯示某人在機構經營場所內實施盜竊行為，且機構決定追究，須報警處理。機構公開張貼涉嫌盜竊者的影像資料的做法，在法律上可能產生以下的後果：

1. 違反《刑法典》的規定：公開張貼未經司法審判的涉嫌盜竊者的影像資料，並冠以“盜竊者”之罪名，有可能構成誹謗罪（見《刑法典》第174條規定）。

2. 違反《個人資料保護法》的規定：公開張貼涉嫌盜竊者的影像資料，已超出了基於保安理由收集該等資料的目的，無履行《個人資料保護法》第5條規定的義務，對涉嫌盜竊者資料的處理偏離了收集的目的，涉嫌違反《個人資料保護法》第33條第1款規定，可能構成行政違法，可被科處澳門幣4,000至40,000元罰款。同一行為，亦涉嫌違反同一法律37條第1款(三)項規定（與收集個人資料目的不符的情況下使用個人資料），可能構成犯罪行為，可處最高一年徒刑或一百二十日罰金。

四、負責處理個人資料實體之義務

機構作為負責處理個人資料實體（見《個人資料保護法》第4條第1款第(五)項規定），基於保安目的裝置攝錄監察系統，處理當事人的影像資料，須根據《個人資料保護法》之相關規定履行有關的義務，其中主要包括以下幾點：

1. 確保資料當事人權利

個人資料處理應以透明的方式進行（見《個人資料保護法》第2條規定），以保障當事人相關權利（見《個人資料保護法》第10至12條規定）。機構透過攝錄監察系統處理當事人的個人資料，有義務告知當事人處理資料的機構名稱、代表人身份、處理的目的、用途、資料的接收者或接收者的類別以及當事人查閱權及反對權之行使。

2. 制定個人資料處理政策或有關攝錄監察之《收集個人資料聲明》

為確保當事人權利之行使，以履行《個人資料保護法》規定之義務，裝置攝錄監察之機構須根據該法律第10條之規定，制定有關攝錄監察的“個人資料處理政策”及“收集個人資料聲明”，以更好保障機構及當事人雙方之利益，以免違反法律規定。

3. 保障影像資料處理的安全性

根據《個人資料保護法》第15條規定，負責處理個人資料的機構應採取適當的技術和組織措施保護攝錄監察系統所收集的當事人影像資料，避免資料的意外或不法損壞、意外遺失、傳播或查閱等，以及任何其他方式的不法處理。例如，有關的攝錄監察系統一般需有權限及密碼設置，以確保有關的影像資料不會被未經授權者查看及被用作其他用途。

主任

陳海帆

2009年5月27日

Parecer n.º 02/P/2009/GPDP

Assunto: Afixação de dados de imagens de suspeitos de furto nos estabelecimentos comerciais

Recentemente, o Gabinete para a Protecção de Dados Pessoais (GPDP) tem recebido queixas em relação a alguns estabelecimentos comerciais de Macau que, por finalidade de segurança, afixam dados de imagens dos suspeitos de furto captadas pelos sistemas de videovigilância instalados nos estabelecimentos comerciais. Os queixosos têm dúvidas em relação aos métodos utilizados pelos estabelecimentos comerciais que ao afixarem dados pessoais dos titulares, contrariam as finalidades de tratamento de dados pessoais, violando as disposições da Lei n.º 8/2005 (Lei da Protecção de Dados Pessoais).

Em cumprimento do previsto na Lei n.º 8/2005 e no Despacho do Chefe do Executivo n.º 83/2007, o GPDP abriu processos para acompanhar os factos denunciados pelos residentes. Depois da investigação e da confirmação dos factos constatados nas denúncias, o GPDP, nos termos da Lei da Protecção de Dados Pessoais, mandou aos estabelecimentos indiciados de violação das disposições acima mencionadas para adoptarem diversas medidas, nomeadamente a suspensão imediata da afixação de dados de imagens dos suspeitos de furto, assim como a destruição dos respectivos dados. Os estabelecimentos comerciais notificados pelo GPDP já implementaram as referidas medidas.

Tendo em conta que genericamente os estabelecimentos comerciais de Macau tendem a afixar dados de imagens dos suspeitos de furto, o GPDP, na qualidade de autoridade pública que se refere na Lei da Protecção de Dados Pessoais, para fiscalizar e coordenar o cumprimento e a execução da lei, o GPDP considera necessário tornar público o seu parecer jurídico relativo à afixação de dados de imagem de suspeitos de furto nos estabelecimentos comerciais esclarecendo sobre as disposições relativas ao tratamento de dados pessoais previstas na Lei da Protecção de Dados Pessoais assim como sobre as consequências jurídicas do incumprimento da mesma, por forma a que sejam corrigidas, quanto antes, as situações que violam a referida lei.

1. Aplicação da Lei da Protecção de Dados Pessoais

Os estabelecimentos comerciais, com o objectivo de surtir um efeito dissuasor junto das pessoas com intenções de furto, afixam as imagens de suspeitos de furto captadas pelos sistemas de videovigilância dentro dos recintos comerciais, principalmente nas montras, à entrada e saída ou junto das caixas. Alguns dados de imagens dos suspeitos de furto que os estabelecimentos comerciais afixam contêm palavras, apontando que a pessoa que está na imagem é um “ladrão”. Nas imagens afixadas, o rosto da pessoa é visível, sendo identificável.

De acordo com a alínea 1) do n.º 1 do artigo 4.º da Lei da Protecção de Dados Pessoais, «Dados pessoais» significa qualquer

informação, de qualquer natureza e independentemente do respectivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável («titular dos dados»). As imagens de suspeitos de furto captadas pelos sistemas de videovigilância dentro dos recintos comerciais, quando o titular está identificável, são dados pessoais protegidos pela mesma lei de acordo com a alínea 1) do n.º 1 do artigo 4.º. De acordo com o n.º 3 do artigo 3.º, a mesma lei aplica-se ao tratamento de imagens de pessoas identificáveis.

2. Legalidade e legitimidade da instalação de sistemas de videovigilância.

De acordo com o artigo 2º da Lei da Protecção de Dados Pessoais, princípios gerais do tratamento de dados pessoais são: deve processar-se de forma transparente e no estrito respeito pela reserva da vida privada, bem como pelos direitos, liberdades e garantias fundamentais estabelecidos na Lei Básica da Região Administrativa Especial de Macau, nos instrumentos de direito internacional e na legislação vigente”. Além disso, e de acordo com o artigo 5.º, “Os dados pessoais devem ser: Tratados de forma lícita e com respeito pelo princípio da boa fé e dos princípios gerais enunciados no artigo 2.º; Recolhidos para finalidades determinadas, explícitas e legítimas e directamente relacionadas com o exercício da actividade do responsável pelo tratamento, não podendo ser posteriormente tratados de forma incompatível com essas finalidades; Adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e posteriormente tratados”.

De um modo geral, é lícita a instalação do sistema de videovigilância em estabelecimentos comerciais com o objectivo de garantir a segurança ou a protecção de outros interesses legais. No entanto, o processo de tratamento de dados de imagens captadas, nomeadamente de dados de imagem dos suspeitos do furto, usados para motivos de segurança, deve ser restrito, não podendo os dados ser usados para outros fins; caso contrário, é violado o artigo 5.º da Lei da Protecção de Dados Pessoais.

De acordo com o artigo 6.º da Lei da Protecção de Dados Pessoais, para além das outras situações previstas na lei só tem legitimidade para tratar os dados pessoais quando o seu titular tiver dado de forma inequívoca o seu consentimento. Numa das outras previstas na alínea 5) do mesmo artigo da lei mencionada, “Prossecação de interesses legítimos do responsável pelo tratamento ou de terceiro a quem os dados sejam comunicados, desde que não devam prevalecer os interesses ou os direitos, liberdades e garantias do titular dos dados”. Nestas circunstâncias, o tratamento dos dados pessoais não carece do consentimento inequívoca do seu titular, os estabelecimentos que instalem sistemas de videovigilância dentro do estabelecimento comercial por finalidades de segurança para protecção dos bens e estabelecimentos, estão com finalidades legais e legítimas, e então protegidos pela lei, uma vez que nestas circunstâncias os interesses dos titulares não prevalecem sobre os interesses legítimas das entidades. Isto é, mesmo que não tenham o consentimento explícito dos titulares, o acto que as entidades instalam sistemas de videovigilância por finalidades acima referidas, é permitido na lei, e está de acordo com o disposto na alínea 5) do artigo 6.º da lei.

Todavia, se as entidades afixarem publicamente dentro dos recintos comerciais dados de imagens dos suspeitos de furto captadas pelos sistemas de videovigilância, ou apontarem que a pessoa que está na imagem é suspeita da prática do “roubo” ou “furto”, afastam-se



do objectivo de segurança interna para a recolha de dados de imagem. Caso os dados do sistema de videovigilância venham a revelar que determinada pessoa praticou um furto no interior do estabelecimento comercial, e este decida apresentar queixa, deve participar às autoridades policiais para seguimento, assim como deve entregar os dados de imagem do suspeito de furto à polícia para efeitos de investigação. Não deve afixar publicamente os dados de imagem do suspeito de furto no estabelecimento comercial, afirmando que a pessoa em causa é “ladrão”, antes do julgamento. Desde modo, a entidade em si é considerada suspeita de ter assumido o papel de julgador, porque antes do tribunal proferir a decisão judicial, considerou a pessoa como “ladrão”. Como tal, é muito provável que a instituição está sujeita a outras responsabilidades legais.

3. Consequências jurídicas

Como mencionado anteriormente, as entidades que por finalidade de segurança têm legitimidade de captar imagens através dos sistemas de videovigilância, não necessitam de obter o consentimento dos titulares. Mas tal não significa que as entidades podem afixar publicamente, por iniciativa própria, dentro dos estabelecimentos comerciais dados de imagens dos suspeitos de furto captadas pelo sistema de videovigilância, e considerar alguém como “ladrão” antes do tribunal proferir a decisão judicial. Se os dados do sistema de videovigilância revelam que determinada pessoa praticou um acto de furto dentro de um estabelecimento comercial, e se decidir dar seguimento, deve participar a ocorrência às autoridades policiais. Nos termos legais, a afixação pública de dados de imagem do suspeito de furto pode ter as seguintes consequências:

- (1). Violação do Código Penal: afixar publicamente dados de imagem de suspeitos de furto, antes da decisão judicial, assim como imputar a alguém a qualidade de “ladrão”, pode constituir um crime de difamação (Vide artigo 174.º do Código Penal).
- (2). Violação da Lei da Protecção de Dados Pessoais: afixar publicamente os dados de imagem do suspeito de furto, que ultrapassem o objectivo da recolha de dados por razões de segurança, significa que não foram cumpridos os deveres previstos no artigo 5.º da Lei da Protecção de Dados Pessoais. Se o tratamento de dados de suspeitos de furto se afastar do objectivo da recolha, tal revela indícios de violação do n.º 1 do artigo 33.º da Lei da Protecção de Dados Pessoais, e constituir uma infracção administrativa sancionada com pena de multa de 4 mil a 40 mil patacas. O mesmo acto também indicia uma violação da alínea 3) do n.º 1 do artigo 37.º da mesma lei (desviar ou utilizar dados pessoais de forma incompatível com a finalidade determinante da recolha), e pode constituir uma infracção criminal punida com pena de prisão até um ano ou pena de multa até 120 dias.

4. Deveres do responsável pelo tratamento de dados pessoais

As entidades com qualidade de responsáveis pelo tratamento de dados pessoais, instalaram sistemas de videovigilância por finalidade de segurança e tratam os dados pessoais recolhidas por este sistema, devem cumprir o disposto na Lei da Protecção de Dados Pessoais nomeadamente nos seguintes aspectos:

(1). Salvaguardar os direitos dos titulares dos dados

O tratamento de dados pessoais deve processar-se de forma transparente (Vide artigo 2.º da Lei da Protecção de Dados Pessoais) e devem ser assegurados os direitos do titular dos dados (Vide artigos 10.º a 12.º da Lei da Protecção de Dados Pessoais). As entidades, que tratam dados pessoais através do sistema de videovigilância, têm a obrigação de informar o titular dos dados sobre a identidade do responsável pelo tratamento e do seu representante, finalidades do tratamento; destinatários ou categorias de destinatários dos dados; exercício dos direitos de acesso e oposição do titular dos dados.

(2). Elaborar políticas relativas ao tratamento de dados pessoais ou Declaração da Recolha de Dados Pessoais pelo sistema de videovigilância

Para assegurar o exercício dos direitos do titular dos dados, e a fim de cumprir os deveres da Lei da Protecção de Dados Pessoais, as entidades que instalaram sistema de videovigilância devem elaborar políticas relativas ao tratamento de dados pessoais ou Declaração da Recolha de Dados Pessoais de acordo do artigo 10.º da mesma Lei, para assegurar os interesses da entidade e dos titulares, de modo a evitar infringir a lei.

(3). Proteger a segurança do tratamento de dados de imagem

De acordo com o artigo 15.º da Lei da Protecção de Dados Pessoais, “O responsável pelo tratamento de dados pessoais deve pôr em prática as medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizados, e contra qualquer outra forma de tratamento ilícito.” Por exemplo, de um modo geral, o sistema de videovigilância deve ser equipado com medidas de segurança que consistem em fixar competência de acesso aos dados do pessoal e aproveitar o uso de cifra, com vista a garantir que os dados de imagem não venham a ser utilizados sem autorização e que não venham a ser utilizados para outras finalidades.

Aos 26 de Maio de 2009

A Coordenadora
Chan Hoi Fan



第06/P/2009/GPDP號意見書

節錄

事由：關於澳門電訊有限公司將固定電話用戶之登記資料公開刊登在“澳門住宅電話簿”的問題

本辦公室早前收到市民投訴，指澳門電訊有限公司（以下簡稱“澳門電訊”）在沒有徵得固定電話用戶同意的情況下，將其登記資料（包括姓名、電話號碼及地址）刊登在“澳門住宅電話簿”（下稱“電話簿”）予公眾取閱，涉嫌違反第8/2005號法律（《個人資料保護法》）之相關規定，基此，本辦公室就此立案跟進，考慮到社會及傳媒對上述問題的關注，故向市民公開本辦公室對處理上述問題所作的意見書摘要。

一、《個人資料保護法》的適用

“澳門電訊”發行的“電話簿”中載有本澳固定電話用戶的姓名、電話號碼及地址資料，此等資料均屬可確定用戶身份有關的個人資料，故根據第8/2005號法律（《個人資料保護法》）第4條第1款（一）項及第3條第1款的規定，有關資料的處理須受《個人資料保護法》規範。

二、處理個人資料的正當性

按照《個人資料保護法》第6條之規定：“個人資料的處理僅得在資料當事人明確同意或在以下必要的情況下方可進行：（一）執行資料當事人作為合同一方的合同，或應當事人要求執行訂立合同或法律行為意思表示的預先措施；（二）負責處理個人資料的實體須履行法定義務……（四）負責處理個人資料的實體或被告知資料的第三人在執行一具公共利益的任務，或者在行使公共當局權力……”。換言之，“澳門電訊”發行載有用戶個人資料的“電話簿”，須符合上述規定方具有正當性。

根據於1979年生效的9月22日第27-A/79/M號法令（前郵電司組織法）第1條之規定，本澳的公共郵政及公共電信服務由前郵電司負責¹。該法令第156條第4款f)項規定，在前郵電司行政委員會之建議下，前總督得設立福利部門，而該部門擁有本身之預算，其收入組成部分的其中一項為：倘由前郵電司負責印

¹ 原文為：“O publico de correios, telégrafos e telephones no território de Macau é desempenhado pelos Serviços de Correios e Telecomunicações, os quais manterão a abreviatura de CTT, ocupando-se de: b) Telecomunicações……”。

製“電話簿”時，收入來自於任何性質商業廣告之收入；但如“電話簿”是由私人負責印製，則收入來自於有關判給²。其後，前郵電司與“澳門電訊”於1981年簽署有關《澳門公共電訊服務特許合同》(Escritura de contrato de concessão do Serviço de Telecomunicações de Macau，以下簡稱《特許合同》)，當中第45條第2款及附件第VI部分第1條f)項規定，“澳門電訊”需承擔由前郵電司簽署的待決合同中有關“電話簿”及“黃頁”(“Lista telefónica”e“Páginas Amarelas”)的財政責任³。

由此可見，前郵電司早於1981年已將有關公共電信的特許經營業務判給“澳門電訊”，在相關《特許合同》中已訂明“澳門電訊”需承擔制作“電話簿”及“黃頁”的財政責任。雖然《特許合同》第2條規定了有關特許經營業務的批給經營期限自1981年開始，2001年12月31日結束，但在1999年12月10日澳門政府與“澳門電訊”重新修訂了《澳門公共電訊服務特許合同》(以下簡稱《新特許合同》)，當中第53條訂明，“……對現在所修改之契約的其餘條款，維持不變”。而第2條亦指出《新特許合同》的特許經營期限直至2011年12月31日結束。換言之，在《新特許合同》的批給期限屆滿前，“澳門電訊”仍須承擔制作本澳的“電話簿”及“黃頁”之財政責任。

從上述可見，“澳門電訊”自1981年獲批給特許經營本澳的公共電訊服務，直至《新特許合同》於2011年12月31日批給期限結束前，有責任發行“電話簿”及“黃頁”。

事實上，由電訊供應商負責發行“電話簿”是國際上的一貫做法。以葡萄牙及鄰近的香港特別行政區為例，葡萄牙第240/97號法令第1條核准的附件——固定電話服務的經營規章(Regulamento de Exploração do Serviço Fixo de Telefone)中第38及39條已明確規定，電訊供應商有責任透過設定簡單的密碼，向使用者公開提供有關固定電話用戶登記資料的資訊服務，但必須徵得固定電話用戶的同意及遵守保護個人資料及私人生活法律之相關規定。如果用戶明確要求電訊供應商就其電話號碼、住址，又或同時對該兩項資料作保密處理，則電訊供應商不應將有關資料載於電話簿上，且用戶無需為此承擔任何附加條件。此外，應透過出版及派發上述電話簿(包括文本或電子方式)，定期及免費向使用者提供相關資訊，並適當進行資料

2 原文為：“4. Os Serviços Sociais terão um orçamento próprio, cujas receitas serão constituídas: f) Pelas importâncias provenientes da publicidade comercial nas listas telefónicas ou de qualquer outra natureza, quando editadas pelos CTT, ou pela receita proveniente da adjudicação das mesmas, quando editadas por particulares;”。

3 原文為“Contratos pendentes, assinados pelos CTT para os quais as Telecomunicações de Macau assumem responsabilidade financeira...f) Lista telefónica e «Páginas Amarelas》.”。



更新，而電話簿所載的內容包括：名字、住址和用戶的電話號碼等⁴。

另外，香港《電訊條例》第2條規定，電訊供應商需提供的基本服務包括發行電話號碼索引列表（俗稱“電話簿”）。且香港政府⁵於2002年亦公佈了“固定及流動電訊服務營辦商保障顧客資料的實務守則”，當中明確訂明“固定電訊網絡服務的服務營辦商須就所有客戶的電話號碼提供電話簿服務，除非有關客戶已申請電話簿除名服務。服務營辦商應為電話查詢服務員制定清晰的營運指引，讓他們回應查詢有關申請電話簿除名服務的顧客的資料時有所依循，確保不會洩露該等客戶的資料”。同樣地，其他國家如美國⁶、加拿大⁷、澳洲⁸、紐西蘭⁹、西班牙¹⁰等，亦有專門設置電話簿查詢的服務。

由此可見，國際上對於透過文本或電子方式編製及發行“電話簿”，視為電訊供應商應有的義務，且屬於一項便民措施，存有一定的普遍性及認受性。

此外，根據“澳門電訊”的覆函所指，自1981年與前郵電司簽署《特許合同》後，已開始在固定電話服務的申請表(“Application Form for Fixed Telephone Line”)中載明“Telephone Calling Features (applicable to normal telephone)”欄目，目的是讓用戶在該表格上註明是否願意將其電話號碼作保密(Confidential)處理。而且，“澳門電訊”又表示，“當有客戶申請服務時，前線員工會作出解釋，包括：（一）來電顯示的限制；（二）不會刊登在‘電話簿’（不論實質的或電子版的）；（三）號碼不會在熱線號碼181和185披露”。

4 葡國第240/97號法令第38條規定：“1 —O operador é obrigado a prestar aos utilizadores serviços informativos, através de códigos abreviados, envolvendo a divulgação de dados referentes aos assinantes do SFT, desde que estes tenham autorizado essa divulgação. 2 —O operador está obrigado a observar as normas relativas à protecção de dados pessoais e da vida privada na prestação dos serviços informativos aos utilizadores. 3 —Nos casos em que o assinante expressamente o indique, deve o operador reservar-lhe a confidencialidade do número de telefone, ou da morada, ou de ambos, não os incluindo em listas do serviço telefónico, nem o divulgando através dos correspondentes serviços informativos, sem qualquer encargo adicional.”。第39條規定：“1 —As informações a que se refere o artigo anterior devem, designadamente, ser prestadas através da publicação e distribuição aos utilizadores de listas do service telefónico devidamente actualizadas, sob a forma impressa ou electrónica. 2 —As listas do serviço telefónico são divulgadas e distribuídas periódica e gratuitamente, devendo conter os seguintes elementos: a) O nome, a morada e o número de telefone de cada assinante.....”。

5 由香港消費者委員會、廉政公署、個人資料私隱專員公署及電訊管理局共同公佈。

6 網址為<http://www.whitepages.com/person>。

7 網址為<http://www.canada411.ca/>。

8 網址為<http://www.whitepages.com.au/wp/initResSearch.do?subscriberName=&location=>。

9 網址為<http://yellow.co.nz/whitepages/>。

10 網址為<http://engblancas.paginasamarillas.es/jsp/home.jsp?src=eng>。

基此，自1981年起客戶向“澳門電訊”申請固定電話服務時，已可自主選擇是否將其登記資料刊登於“電話簿”上，具有處理其個人登記資料的控制權。再者，由於“澳門電訊”的員工會即場向申請用戶解釋有關“保密”選項的範圍予客戶選擇，換言之，上述“澳門電訊”的做法實際上已等同徵得申請固定電話服務的客戶同意，將其登記資料公開刊登在“電話簿”上。此舉符合《個人資料保護法》第6條的規定，“澳門電訊”具有處理有關個人資料的正當性。

另一方面，據“澳門電訊”的網頁資料顯示，“澳門電訊”已獨家授權利達通黃頁有限公司負責出版“電話簿”，並已達18年之久。由此可知，利達通黃頁有限公司是受到“澳門電訊”的委託，處理客戶的個人資料並負責出版“電話簿”，屬於《個人資料保護法》規定的次合同人¹¹，故利達通黃頁有限公司同樣具正當性處理有關個人資料。

三、資訊權

根據《個人資料保護法》第10條之規定，除非資料當事人已經知悉，否則負責處理個人資料的實體或其代表人應保障資料當事人之資訊權，提供與其個人資料處理有關的資訊（包括：處理個人資料的目的／用途、資料接收者的類別，以及當事人享有查閱權及更正權的權利等）。

本個案中，現時固定電話的申請用戶單純以“澳門電訊”的員工即場對有關“保密”的選項範圍作出解釋，從而選擇是否將登記資料公開刊登於“電話簿”（包括文本或電子方式）。可見，員工的口頭解釋乃用戶了解有關“保密”選項範圍之唯一途徑，且直接影響申請用戶是否選擇使用相關的服務，員工是否有作出清晰的解說十分關鍵。而“澳門電訊”現時透過員工口頭向用戶解釋有關“保密”選項範圍的措施，可能會因應員工當時的情緒、服務對象及環境等因素而影響到解釋的內容，亦有可能出現解釋不清楚的情況。

另外，綜觀“澳門電訊”的固定電話用戶申請書——服務條款及細則表格(“Application Form for Fixed Telephone Line”), 除針對有關安裝費用方面的條款是以中文顯示外，其他欄目如申請用戶的個人資料、申請項目、帳單資訊、保密條款及有關更新、修改個人資料等資訊權的行使方面，均以英文顯示。

¹¹ 根據《個人資料保護法》第4條第1款（六）項之規定，次合同人為“受負責處理個人資料的實體的委託而處理個人資料的自然人或法人，公共實體、部門或任何其他機構”。



對此，值得注意的是，根據《澳門特別行政區基本法》第9條的規定，本澳的官方語言為中文及葡文。且在《特許合同》及《新特許合同》中第22條亦同樣訂明，“澳門電訊”在與行政當局、公眾及經濟活動的服務接觸中，得使用中文及葡文。故此，現時“澳門電訊”的固定電話用戶申請書——服務條款及細則表格(“Application Form for Fixed Telephone Line”)中大部分資訊以英文顯示，不符合上述規定的情況。

須知道，據本澳旅遊局的網頁資料顯示，現時澳門居民係以華人為主，一般使用的語言為中文¹²，葡籍及其他國籍人士只約占百分之六，故“澳門電訊”的上述做法，對於一些不諳英文的申請用戶而言，對其資訊權的行使會造成一定的損害。

再者，上指服務條款及細則表格(“Application Form for Fixed Telephone Line”)中的“Telephone Calling Features (applicable to normal telephone)”欄目，僅載有“Confidential”之單一選項，在此情況下，難以令人知悉當中的含義實際上是包括（一）來電顯示的限制；（二）不會刊登在“電話簿”（不論文本的或電子版的）；（三）號碼不會在熱線號碼181和185披露的內容。

綜上所述，“澳門電訊”應採取適當措施，例如：訂定清晰的內部政策或工作指引，以規範員工的回應內容；並在固定電話用戶的申請書——服務條款及細則表格(“Application Form for Fixed Telephone Line”)或其他文件中，清楚列明申請用戶可享有的權利及義務，加設包括中文等其他語言版本的申請表格，以及清楚註明“保密”選項的具體涵蓋範圍等。以便更好地確保資料當事人對有關固定電話申請的理解，避免出現不必要的爭拗，保障雙方的合法權益。

另一方面，根據已被廢止的第584/99/M號訓令核准之《公共電訊服務收費》顯示，過往的固定電話用戶如不欲個人資料刊載於“電話簿”，可選擇將電話號碼以“保密號碼”方式處理，但需繳付相應費用。但自第6/2001號行政命令核准之《公共電信服務收費》於2001年2月9日生效後，固定電話用戶選擇以“保密號碼”方式處理，無須再繳付任何費用。上述修改無疑是保障了當事人在無需再透過支付費用的情況下，行使反對權要求其個人資料免被公開的權力。

12 網址為<http://www.macautourism.gov.mo/cn/info/info.php>。

儘管上指反對權無需再透過支付費用來取得保障，然而，不排除固定電話用戶或其他市民不知悉上述服務的費用調整，誤以為仍需支付費用，而不願選擇以“保密號碼”的方式處理，這樣，對用戶行使資訊權方面可能造成一定的損害，基此，“澳門電訊”應採取措施對有關費用調整的情況作出宣傳，以使用戶或市民知悉其應有的權利。

四、安全性和保密性

根據《個人資料保護法》第15條第1款的規定：“負責處理個人資料的實體應採取適當的技術和組織措施保護個人資料，避免資料的意外或不法損壞、意外遺失、未經許可的更改、傳播或查閱，尤其是有關處理使資料經網絡傳送時，以及任何其他方式的不法處理；在考慮到已有的技術知識和因採用該技術所需成本的情況下，上述措施應確保具有與資料處理所帶來的風險及所保護資料的性質相適應的安全程度”。同一條文第3款則規定：“以次合同進行的處理，應由約束次合同人和負責處理資料實體的合同或法律行為為規範，並應特別規定次合同人只可按照負責處理資料的實體的指引行動，並須履行第一款所指的義務”。

基此，無論“澳門電訊”，抑或次合同人利達通黃頁有限公司，透過文本或電子方式編製及發行“電話簿”，均須遵循上述法律規定，即應採取確保具有與資料處理所帶來的風險及所保護資料的性質相適應的安全措施。

對此，尤需注意的是，雖然“澳門電訊”透過電子方式發行“電話簿”（俗稱“白頁”），目的旨在提供網上途徑方便市民查閱資料，然而，由於在登錄相關網頁¹³後，只需輸入用戶姓名，又或僅輸入用戶姓氏，已可查閱所有關連用戶的姓名、住宅電話及住址資料。在這情況下，不排除個別市民／機構會將查閱到的用戶資料大量進行複製，並轉載至另一系統建立資料庫，將資料用作其他甚至可能作不法的用途，偏離或超越收集和之後處理用戶資料的目的。故此，“澳門電訊”或利達通黃頁有限公司，均應採取適當措施，例如採取措施使“白頁”所載的用戶資料不易被大量複製及轉載，又或採取其他適當的安全及保密措施以保護有關個人資料。

13 網址為http://www.whitepages.com.mo/index_c.html。

五、結論及建議部分

綜合上述分析，鑑於“澳門電訊”發行載有固定電話用戶個人資料的“電話簿”，是作為特許經營公共電信業務實體的責任，且徵得資料當事人的明確同意，故符合《個人資料保護法》第6條（四）項的規定，具有處理有關個人資料的正當性。而利達通黃頁有限公司為“澳門電訊”的次合同人，故同樣具正當性處理有關個人資料。然而，本辦公室認為，在確保用戶的資訊權方面，“澳門電訊”仍需作出以下改善：

- (1) 為更好地確保資料當事人理解申請固定電話服務的細節，避免出現不必要的爭拗，保障雙方的合法權益，“澳門電訊”應採取適當的措施，例如：訂定清晰的內部政策或工作指引，以規範員工的回應內容；並在固定電話用戶的申請書——服務條款及細則表格(“Application Form for Fixed Telephone Line”)或其他文件中，清楚列明申請用戶可享有的權利及義務，加設包括中文等官方語言版本的申請表格，以及清楚註明“保密”選項的具體涵蓋範圍等。
- (2) 對於現時固定電話用戶選擇以“保密號碼”方式處理，無須再繳付任何費用的規定，“澳門電訊”宜採取適當措施對有關費用調整的情況作出宣傳，以使用戶或市民知悉其應有的權利。
- (3) 為免個別市民／機構將查閱“白頁”的用戶資料大量進行複製，並轉載至另一系統建立資料庫，將資料用作其他甚至可能作不法的用途，偏離或超越收集和之後處理用戶資料的目的。故“澳門電訊”或利達通黃頁有限公司應確保遵守《個人資料保護法》第15條有關安全性和保密性方面的規定，採取適當措施，例如採取措施使“白頁”所載的用戶資料不易被大量複製及轉載，又或採取其他適當的安全及保密措施以保護有關個人資料。

另一方面，對於“澳門電訊”負責印製“電話簿”之責任，一直沿用於28年前訂立的《特許合同》中之條款，單憑有關表述，未足以對相關事宜作出明確規範。故本辦公室建議，日後在簽訂新的《澳門公共電訊服務特許合同》時，明確在合同中訂明特許經營公共電信業務實體對於“電話簿”印製方面之具體責任條款，例如：訂明獲特許經營的電訊營運商須負責出版及派發“電話簿”（包括文本或電子方式），定期及免費向用戶提供相關資訊，並適當進行資料更新，且訂明“電話簿”所載有的個人資料種類等。

主任

陳海帆

2009年9月8日

1111100 私 10 隱 10 1 P 0 1 R 10 1 1 I V A 0 0 C I D 1 0 0 A 1 1 D 1 E 1 0 0 0

Parecer
n.º 06/P/2009/GPDP
(Extracto)

Tradução

Assunto: Sobre a publicação, pela Companhia de Telecomunicações de Macau, dos dados do registo dos utilizadores de telefones fixos, na Lista Telefónica Residencial de Macau

Este gabinete recebeu, no passado recente, reclamações, apresentadas por vários cidadãos, contra a Companhia de Telecomunicações de Macau (adiante designada por CTM) que publicou, sem o consentimento dos seus titulares, os dados do registo (inclusive nome, número de telefone e morada) dos utilizadores de telefones fixos, na Lista Telefónica Residencial de Macau (adiante designada por Lista Telefónica), que é distribuída ao público, o que configura infracção à disposição prevista na Lei n.º 8/2005 (Lei da Protecção de Dados Pessoais). Tendo acompanhado o processo e considerado a preocupação da comunidade e da imprensa sobre o assunto, este Gabinete torna público o extracto do parecer relativo à questão.

I. Aplicação da Lei da Protecção de Dados Pessoais

Os dados do nome, número de telefone e informação da morada dos assinantes de telefones fixos de Macau, contidos na Lista Telefónica publicada e distribuída pela CTM, são dados de identificação dos seus titulares, pelo que o tratamento dos mesmos está sujeito à protecção de dados pessoais, ao disposto na alínea 1) do n.º 1 do artigo 4.º e no n.º 1 do artigo 3.º da Lei n.º 8/2005, Lei da Protecção de Dados Pessoais.

II. Legitimidade do tratamento de dados pessoais

Segundo o artigo 6.º da Lei da Protecção de Dados Pessoais: “O tratamento de dados pessoais só pode ser efectuado se o seu titular tiver dado, de forma inequívoca, o seu consentimento ou se o tratamento for necessário para: 1) Execução de contrato ou contratos em que o titular dos dados seja parte interessada ou de diligências prévias à celebração do(s) mesmo(s) ou declaração da vontade negocial efectuadas a seu pedido; 2) Cumprimento de obrigação legal a que o responsável pelo tratamento esteja sujeito; ... 4) Execução de uma missão de interesse público ou no exercício de poderes de autoridade pública em que esteja investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados; ...”. Assim sendo, a CTM só tem legitimidade de publicar e distribuir a Lista Telefónica, que contém dados pessoais dos assinantes, quando cumprir as acima referidas disposições.

De acordo com o estipulado no artigo 1.º do Decreto-Lei n.º 27-A/79/M, de 22 de Setembro, (Diploma Orgânico da Direcção dos Serviços de Correios e Telecomunicações de Macau), que entrou em vigor em 1979, “[o] público de correios, telégrafos e telefones no território de Macau é desempenhado pelos Serviços de Correios e Telecomunicações”¹. Segundo a alínea f) do n.º 4 do artigo 156.º

1. O original refere que: “O público de correios, telégrafos e telefones no Território de Macau é desempenhado pelos Serviços de Correios e Telecomunicações, os quais manterão a abreviatura de CTT, ocupando-se de: b) Telecomunicações.....”.



do mesmo diploma, faziam parte do orçamento próprio dos Serviços Sociais, criados pelo Governador sob a proposta do Conselho de Administração dos CTT, as receitas provenientes da publicidade comercial nas listas telefónicas ou de qualquer outra natureza, quando editadas pelos CTT, ou pela receita proveniente da adjudicação das mesmas, quando editadas por particular². Posteriormente, em 1981, os antigos CTT assinaram com a CTM a Escritura de Contrato de Concessão do Serviço de Telecomunicações de Macau (a seguir designado por Contrato), estipulando no n.º 2 do artigo 45.º e na alínea f) do artigo 1.º da parte VI do Anexo, que a CTM assume a responsabilidade financeira dos contratos pendentes, assinados pelos CTT³, da lista telefónica e das páginas amarelas.

É evidente que os antigos Serviços de Correios e Telecomunicações de Macau concederam, em 1981, à CTM, os negócios por aqueles adjudicados, relativos aos serviços de telecomunicações, pelo que a CTM é obrigada a assumir, no âmbito do Contrato, a responsabilidade financeira de publicar a Lista Telefónica e as Páginas Amarelas. Apesar de o prazo de concessão, determinado no artigo 2.º do Contrato, se iniciar em 1981 e terminar em 31 de Dezembro de 2001, o governo de Macau e a CTM fizeram, em 10 de Dezembro de 1999, a Revisão do Contrato de Concessão do Serviço Público de Telecomunicações (a seguir designado por Novo Contrato) e determinaram, no seu artigo 53.º, que “[e]m tudo o mais, se mantém a versão agora revista”. O artigo 2.º do Novo Contrato estipula que a concessão termina a 31 de Dezembro de 2011. Isto quer dizer que, até ao termo do prazo de concessão do Novo Contrato, a CTM continua a assumir a responsabilidade financeira de publicar a Lista Telefónica e as Páginas Amarelas do território de Macau.

Pelo exposto, a CTM, que detém, desde 1981, a concessão do serviço público de telecomunicações de Macau e continuará a detê-la até ao termo do prazo concedido no Novo Contrato, 31 de Dezembro de 2011, assume a responsabilidade de publicar e distribuir a Lista Telefónica e as Páginas Amarelas.

É, de facto, uma prática internacionalmente comum caber aos prestadores do serviço público de telecomunicações a publicação de listas telefónicas, tal como acontece em Portugal e na Região Administrativa Especial de Hong Kong. Em Portugal estipula-se, nos artigos 38.º e 39.º do Regulamento de Exploração do Serviço Fixo de Telefone (SFT), aprovado pelo Decreto-Lei n.º 240/97, que a operadora é obrigada a prestar aos utilizadores serviços informativos, através de códigos abreviados, envolvendo a divulgação de dados referentes aos assinantes dos SFT, desde que estes tenham autorizado essa divulgação. No entanto, a operadora está obrigada a observar as normas relativas à protecção de dados pessoais e da vida privada. Nos casos em que o assinante expressamente o indique, deve a operadora reservar-lhe a confidencialidade do número de telefone, ou da morada, ou de ambos, não os incluindo em listas do serviço telefónico, nem o divulgando através dos correspondentes serviços informativos, sem qualquer encargo adicional. Além disso,

2. O original refere o seguinte : “4. Os Serviços Sociais terão um orçamento próprio, cujas receitas serão constituídas: f) Pelas importâncias provenientes da publicidade comercial nas listas telefónicas ou de qualquer outra natureza, quando editadas pelos CTT, ou pela receita proveniente da adjudicação das mesmas, quando editadas por particulares;”.

3. O original refere o seguinte : “ Contratos pendentes, assinados pelos CTT pelos quais a Companhia de Telecomunicações de Macau assumem responsabilidade financeira...f) Lista Telefónica e Páginas Amarelas”.

as informações anteriormente referidas devem ser prestadas aos utilizadores através da publicação e distribuição, periódica e gratuita, de listas do serviço telefónico devidamente actualizadas, sob a forma impressa ou electrónica, devendo as mesmas conter elementos como o nome, a morada e o número de telefone de cada assinante, etc⁴.

Em Hong Kong, por sua vez, estipula-se, no artigo 2.º da “Ordenança de Telecomunicações”, que os serviços básicos a prestar pela operadora do serviço público de telecomunicações incluem a publicação da Lista de Números de Telefones (normalmente denominada Lista Telefónica). O governo de Hong Kong⁵ publicou, igualmente, em 2002, o “Código sobre práticas de protecção de dados dos utilizadores pelas operadoras de telecomunicações fixas e móveis” (Code of Practice on Protection of Customer Information for Fixed and Mobile Service Operators), em que está expressamente definido: “As operadoras que prestam serviços de redes telefónicas fixas devem disponibilizar, a todos os seus utilizadores, os serviços da Lista Telefónica, a não ser que os mesmos solicitem, expressamente, a confidencialidade dos respectivos dados. As operadoras de serviços de telecomunicações devem difundir, junto dos seus funcionários, instruções claras quanto às informações a prestar sobre utilizadores que requereram a respectiva confidencialidade, devendo assegurar, igualmente, que nenhuma informação relativa a estes utilizadores é fornecida pelos seus operadores”. Há semelhantes serviços de informações de listas telefónicas em outros países como os EUA⁶, Canadá⁷, Austrália⁸, Nova Zelândia⁹, Espanha¹⁰, entre outros.

Pode considerar-se, entretanto, que a publicação e a distribuição da Lista Telefónica, sob a forma impressa ou electrónica, é internacionalmente reconhecida como obrigação das operadoras do serviço público de telecomunicações, constituindo a mesma uma medida facilitadora da vida dos cidadãos e tendo um certo nível de popularidade e aceitabilidade.

4. Estipula-se no artigo 38.º do Decreto-Lei n.º 240/97, de Portugal que: “1 —O operador é obrigado a prestar aos utilizadores serviços informativos, através de códigos abreviados, envolvendo a divulgação de dados referentes aos assinantes do SFT, desde que estes tenham autorizado essa divulgação. 2 —O operador está obrigado a observar as normas relativas à protecção de dados pessoais e da vida privada na prestação dos serviços informativos aos utilizadores. 3 —Nos casos em que o assinante expressamente o indique, deve o operador reservar-lhe a confidencialidade do número de telefone, ou da morada, ou de ambos, não os incluindo em listas do serviço telefónico, nem o divulgando através dos correspondentes serviços informativos, sem qualquer encargo adicional.”—E o artigo 39.º define: “1 —As informações a que se refere o artigo anterior devem, designadamente, ser prestadas através da publicação e distribuição aos utilizadores de listas do serviço telefónico devidamente actualizadas, sob a forma impressa ou electrónica. 2 —As listas do serviço telefónico são divulgadas e distribuídas periódica e gratuitamente, devendo conter os seguintes elementos: a) O nome, a morada e o número de telefone de cada assinante.....”.

5. Publicado, conjuntamente, pelo Conselho de Consumidores, CCAC, Comissariado de Privacidade e Dados Pessoais (PCPD) e Autoridade de Telecomunicações, todos de Hong Kong.

6. O link é: <http://www.whitepages.com/person>.

7. O link é: <http://www.canada411.ca/>.

8. O link é: <http://www.whitepages.com.au/wp/initResSearch.do?subscriberName=&location>.

9. O link é: <http://yellow.co.nz/whitepages/>.

10. O link é: <http://engbhttp://yellow.co.nz/whitepages/lancas.paginasamarillas.es/jsp/home.jsp?src=eng>



Além disso, a CTM respondeu no seu ofício que, após a assinatura do Contrato, em 1981, com a antiga Direcção dos Serviços de Correios e Telecomunicações, passou a dispor, no Formulário de Pedido do Serviço Telefónico Fixo, de uma “Observação para Chamadas Telefónicas”, aplicável a telefones normais, através da qual os assinantes podem solicitar a confidencialidade do respectivo número. E acrescentou que “quando os seus funcionários atendem pedidos de serviço telefónico estão aptos a prestar informações relativas a: 1) Limite de CND (demonstração do número da chamada); 2) Exclusão do número de telefone na Lista Telefónica, tanto na forma impressa como electrónica; 3) Não divulgação do número na linha verde 181 nem na 185.

Assim, a partir de 1981, ao pedirem o serviço telefónico fixo, os utilizadores começaram a poder decidir sobre a inclusão ou não dos respectivos dados na Lista Telefónica e a ter o direito ao controlo do tratamento de seus dados de registo. Além disso, os funcionários da CTM explicam, no momento em que atendem os utilizadores que solicitam o serviço telefónico, a possibilidade de aderir ao “número confidencial”. Isto quer dizer que a CTM, através dessas práticas, solicita expressamente aos subscritores do serviço telefónico fixo o seu consentimento para publicação dos respectivos números na Lista Telefónica, tendo, assim, legitimidade de tratamento dos dados pessoais dos assinantes, prevista no artigo 6.º da Lei da Protecção de Dados Pessoais.

Por outro lado, conforme informação disponibilizada no respectivo website, a CTM tem adjudicada à empresa Directel Macau, Ltd., desde há 18 anos, a publicação da Lista Telefónica. Assim, a Directel Macau, Ltd., na qualidade de subcontratante¹¹ e de acordo com a Lei da Protecção de Dados Pessoais, tem legitimidade para proceder ao tratamento dos dados pessoais dos assinantes da CTM.

III. Direito de informação

De acordo com o previsto no artigo 10.º da Lei da Protecção de Dados Pessoais o responsável pelo tratamento de dados ou o seu representante deve garantir o direito de informação dos titulares, prestando-lhes informações sobre o tratamento dos seus dados pessoais, incluindo as finalidades do tratamento, as categorias de destinatários de dados bem como os direitos de acesso e de rectificação, entre outras.

No presente caso, as informações verbais dos funcionários da CTM, relativamente ao item do “número confidencial” constituem, actualmente, a única forma de os subscritores do serviço telefónico fixo tomarem conhecimento da possibilidade de autorizarem, ou não, a divulgação de seus dados de registo na Lista Telefónica, quer sob a forma impressa quer electrónica. Então, pode-se afirmar que o esclarecimento verbal dos funcionários é o único meio para os utilizadores conhecerem as possíveis opções do item do “número

11. Segundo o estipulado no 6) do n.º1 do artigo 4º da Lei da Protecção de Dados Pessoais, o subcontratante é a “pessoa singular ou colectiva, a entidade pública, o serviço ou qualquer outro organismo que trate os dados pessoais por conta do responsável pelo tratamento”.

confidencial”, estando a opção pelo serviço, por parte dos assinantes, directamente dependente do esclarecimento dos funcionários. No entanto, o conteúdo do esclarecimento verbal poderá ser afectado pela capacidade de persuasão dos funcionários, por factores ambientais ou do destinatário do serviço, entre outros, sendo também possível a indução em erro do utilizador por falta de clareza da informação ou má compreensão da mesma.

Outro ponto a ter em atenção é que a maior parte dos itens do Formulário de Pedido do Serviço Telefónico Fixo (Application Form for Fixed Telephone Line), da CTM, a preencher pelos subscritores, nomeadamente, os dados pessoais, os serviços a contratar, a informação da conta e do número confidencial, bem como do exercício do direito de informação de actualização e de rectificação de dados pessoais, se encontra redigido em inglês. Apenas os itens relativos ao custo do serviço de instalação da linha estão em chinês.

De salientar que, segundo o previsto no artigo 9.º da Lei Básica da Região Administrativa Especial de Macau, as línguas oficiais do território são o chinês e o português. Ainda segundo o artigo 22.º do Contrato e do Novo Contrato, as línguas que a CTM deve utilizar nos contactos de serviço com a Administração, com o público e com as actividades económicas são a chinesa e a portuguesa. Por isso, o Formulário de Pedido do Serviço Telefónico Fixo, apresentando a maior parte dos itens em inglês, não observa as referidas disposições legais.

Segundo as informações disponibilizadas no website da Direcção dos Serviços de Turismo, hoje em dia, a maior parte dos residentes de Macau são de etnia chinesa, que utiliza normalmente o chinês¹² como forma de comunicação e apenas 6% dos residentes são portugueses ou de outras nacionalidades. Assim, a prática da CTM poderá prejudicar, de algum modo, o direito de informação daqueles que solicitem o serviço mas não compreendam a língua inglesa.

Além disso, encontra-se, no espaço “Observação para Chamadas Telefónicas (aplicável a telefones normais)” do Formulário de Pedido do Serviço Telefónico Fixo acima referido, apenas um item relativo a “número confidencial”, o que, por si só, não permite aos utilizadores compreender que o mesmo inclui, de facto, três opções: 1) Limite de CND; 2) Exclusão do número de telefone na Lista Telefónica, sob a forma tanto impressa como electrónica; 3) Não divulgação do número na linha verde 181 nem na 185.

Pelo exposto, a CTM deve tomar as medidas adequadas no sentido de clarificar inequivocamente a informação a disponibilizar, tais como: preparar políticas ou instruções internas bem explícitas para esclarecimento dos seus funcionários; adicionar, de forma clara,

12. O link é: <http://www.macautourism.gov.mo/cn/info/info.php>.



quer no Formulário de Pedido do Serviço Telefónico Fixo quer em outros documentos similares, os direitos e deveres dos assinantes; disponibilizar formulários em chinês e outras línguas, bem como clarificar o âmbito concreto do item relativo ao “número confidencial”, a fim de facilitar e clarificar a compreensão dos titulares de dados sobre o pedido de telefone fixo, evitar eventuais disputas, garantindo os direitos e os legítimos interesses de ambas as partes.

Além disso, segundo o Tarifário do Serviço Público de Telecomunicações, aprovado pela Portaria n.º 584/99/M, já revogada, os utilizadores de telefones fixos que não quisessem ver os respectivos dados pessoais divulgados na Lista Telefónica, podiam pedir o número confidencial pagando a respectiva tarifa. Com a entrada em vigor, em dia 9 de Fevereiro de 2001, do Tarifário do Serviço Público de Telecomunicações, aprovado pela Ordem Executiva n.º 6/2001, os utilizadores de telefones fixos podem pedir o número confidencial sem precisarem de assumir qualquer encargo adicional. Tal alteração veio garantir, definitivamente, o direito dos interessados de exercer a objecção da publicação dos seus dados pessoais, sem qualquer encargo adicional.

Não estando tal direito suficientemente explícito por parte dos formulários da CTM, é muito provável que os assinantes do serviço de telefone fixo ou outros residentes não tenham conhecimento da alteração do tarifário, o que os levou a não optar pelo número confidencial para não pagar a respectiva tarifa. Isso poderá, eventualmente, prejudicar o direito de informação dos utilizadores, pelo que a CTM deve tomar medidas para divulgar a informação relativa à alteração do tarifário de forma a que os seus assinantes e a população local tomem conhecimento e percebam os seus direitos.

IV. Segurança e confidencialidade

De acordo com o estipulado no n.º 1 do artigo 15.º da Lei da Protecção de Dados Pessoais “o responsável pelo tratamento deve pôr em prática as medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizados, nomeadamente quando o tratamento implicar a sua transmissão por rede, e contra qualquer outra forma de tratamento ilícito, devendo elas assegurar, atendendo aos conhecimentos técnicos disponíveis e aos custos resultantes da sua aplicação, um nível de segurança adequado em relação aos riscos que o tratamento apresenta e à natureza dos dados a proteger”. No n.º 3 do mesmo artigo estipula-se que “a realização de operações de tratamento em subcontratação deve ser regida por um contrato ou acto jurídico que vincule o subcontratante ao responsável pelo tratamento e que estipule, designadamente, que o subcontratante apenas actua mediante instruções do responsável pelo tratamento e que lhe incumbe igualmente o cumprimento das obrigações referidas no n.º 1”.

Assim, tanto a CTM como a Directel Macau, Ltd., que é, neste caso, o subcontratante, têm de cumprir, quando publicarem e distribuírem a Lista Telefónica, sob a forma quer impressa quer electrónica, a legislação acima citada, tomando as medidas de segurança adequadas relativamente aos riscos que o tratamento apresenta e à natureza dos dados a proteger.

De notar, especialmente, que a CTM disponibiliza a Lista Telefónica electrónica (normalmente conhecida como Páginas Brancas) para facilitar aos residentes a consulta de informações necessárias através da Internet. Com a entrada, no respectivo website¹³, do nome ou apenas do apelido de determinado assinante podem encontrar-se dados como o nome completo, o número de telefone fixo e a morada. Pode, então, acontecer que qualquer indivíduo tenha acesso e reproduza os dados dos assinantes e os transfira para a criação de outro ficheiro ou os utilize para outras finalidades, eventualmente ilícitas, o que é incompatível com as finalidades de recolha de dados, possibilitando, assim, o tratamento excessivo dos mesmos. Por isso, é imperioso que a CTM e a Directel Macau, Ltd. tomem as medidas adequadas, incluindo medidas para prevenir a reprodução em grande escala e a transferência dos dados contidos nas “páginas brancas”, ou outras medidas de salvaguarda da segurança e confidencialidade dos dados pessoais dos seus utilizadores.

V. Conclusão e sugestões

Com base nas análises acima apresentadas e considerando que a CTM publica e distribui a Lista Telefónica que contém os dados dos utilizadores de telefones fixos, para o que tem o prévio e expresso consentimento dos mesmos, assumindo a responsabilidade de entidade concessionária dos serviços públicos de telecomunicações, possuindo, ainda, a legitimidade para tal, prevista no n.º 4 do artigo 6.º da Lei da Protecção de Dados Pessoais e que a Directel Macau, Ltd., como o subcontratante da CTM, tem a mesma legitimidade, este Gabinete considera, no entanto, que, no aspecto da garantia do direito de informação dos seus assinantes, a CTM deve proceder aos seguintes melhoramentos:

- (1) A fim de garantir que os titulares dos dados compreendam, de forma inequívoca, os pormenores do pedido do serviço telefónico fixo, evitar possíveis disputas e garantir os direitos e interesses de ambas as partes, a CTM deve tomar as medidas adequadas como, por exemplo: adoptar políticas ou instruções internas, bastante explícitas, para uniformizar o conteúdo dos esclarecimentos dos seus funcionários; apresentar, claramente, os direitos e deveres dos assinantes no Formulário de Pedido do Serviço Telefónico Fixo ou em outros documentos; disponibilizar formulários de pedido nas línguas oficiais pormenorizando o âmbito do item do “número confidencial”, entre outras.
- (2) A CTM deve alertar claramente os seus utilizadores para o facto de poderem optar pela confidencialidade dos seus números telefónicos fixos sem qualquer encargo adicional, salvaguardando, assim, o direito à informação dos seus utilizadores e demais residentes.

13. O link é: http://www.whitepages.com.mo/index_c.html



- (3) É necessário prevenir que os dados incluídos nas “páginas brancas” possam ser reproduzidos de forma algo descontrolada, possibilitando a criação de ficheiros paralelos que podem ser utilizados para outras finalidades, eventualmente ilícitas, ou para posterior tratamento excessivo dos mesmos, o que é incompatível com as finalidades a que esta recolha e tratamento legítimo se destina. Para tal, a CTM ou a Directel Macau, Ltd. devem cumprir rigorosamente as disposições relativas à segurança e confidencialidade, previstas no artigo 15º da Lei da Protecção de Dados Pessoais, tomando as medidas adequadas, prevenindo e impossibilitando a reprodução e transferência dos dados dos assinantes atrás referidas ou implementando outras medidas de segurança e confidencialidade mais eficientes e fiáveis.

Além disso, a CTM tem assumido a responsabilidade de publicar e distribuir a Lista Telefónica no âmbito das disposições previstas no Contrato, assinado há vinte e oito anos atrás, não regularizando, de modo explícito e detalhado, o respectivo processo. Por isso, este Gabinete sugere que, em futura revisão da Escritura de Contrato de Concessão do Serviço de Telecomunicações de Macau, se acrescentem e clarifiquem, inequivocamente, as disposições relativas às responsabilidades concretas a assumir pela entidade concessionária dos serviços de telecomunicações no que respeita à publicação e distribuição da Lista Telefónica. Essas disposições devem incluir, nomeadamente, que a responsabilidade de publicação e distribuição da Lista Telefónica, quer na forma impressa quer na electrónica, cabe às operadoras concessionárias do serviço de telecomunicações; que estas prestam, periódica e gratuitamente, informações devidamente actualizadas aos seus utilizadores; e que as categorias dos dados pessoais a conter na Lista Telefónica sejam claras, etc.

Aos 8 de Setembro de 2009

A Coordenadora
Chan Hoi Fan

Autorizações

Segundo as informações prestadas pelo Cliente, os dados a serem tratados, via "interconexão" com o Banco de Hong Kong, incluem: nome dos clientes, tipo, número e local de emissão de documentos de identificação, código comercial, etnia, idade, data e local de nascimento, sexo, nacionalidade, país de residência, estado civil, contactos (morada, telefones, e-mail, etc.), estado profissional, cargo, ocupação, natureza dos negócios, nome do empregador, nível de escolaridade, origem do capital, objectivo da abertura da conta, estado de

許可

Autorizações

第01/A/2009/GPDP號許可

事由：關於A銀行申請與香港B銀行以“互聯”方式處理其“客戶資料”

A銀行就香港B銀行以“互聯”方式處理其“客戶資料”事宜，向本辦公室申請“個人資料互聯”許可。

根據A銀行提供的資料，A銀行與香港B銀行“互聯”的資料包括：客戶姓名、身份證明文件類別、號碼及發出地點、中文商業電碼、年齡、出生日期及地點、性別、國籍、居住國家、婚姻狀況、聯絡方法（地址、電話及電郵等）、職業狀況、職位、行業/業務性質、僱主名稱、教育程度、資金來源、開戶目的、住宅狀況、銀行帳戶種類及號碼、是否擁有汽車及交易紀錄。根據第8/2005號法律（《個人資料保護法》）第3條及第4條第1款第（一）項規定，有關的資料屬於身份已確定人士的個人資料，對上述資料的處理受該法律所規範。

根據《個人資料保護法》第4條第1款第（十）項規定：“資料的互聯是指一個資料庫的資料與其他一個或多個負責實體的一個或多個資料庫的資料的聯繫、或同一負責實體但目的不同的資料庫的資料聯繫的處理方式。”香港B銀行透過內部聯網系統連接A銀行的“客戶資料”，兩者資料庫的資料建立聯繫，屬上述法律定義的“個人資料互聯”處理方式。

根據《個人資料保護法》第22條規定，“資料的互聯”屬須預先監控的處理個人資料方式，須經本辦公室許可。且根據同一法律第9條規定：法律規定或具組織性質的規章性規定未規定的個人資料的互聯，須由負責處理個人資料實體或與其共同負責的實體根據第22條第1款的規定向本辦公室提出申請並取得許可。個人資料的互聯應符合法律或章程規定的目的和負責處理個人資料的實體的正當利益；不得導致歧視或削減資料當事人的權利、自由和保障；須有適當的安全措施及考慮需互聯的資料的種類。

根據A銀行提供的資料，A銀行為香港B銀行設立於澳門之分行，與香港B銀行建立“互聯”處理“客戶資料”，目的為配合總行對A銀行進行遙距監察、風險管理、稽核及資訊系統支援等工作。換言之，A銀行基於業務運作需要，須將其“客戶資料”提供予香港B銀行處理，“互聯”處理該等資料的方式符合負責處理個人資料的實體的正當利益。根據第32/93/M號法令（《金融體系法律制度》）第79條第1款d)項規定“信用機構為減少風險及增加經營活動之安全而組織相互提供資訊系統之可能性”，屬於銀行保密義務的例外情況。故A銀行與香港B銀行“互聯”處理“客戶資料”，屬經營正當銀行業務所需而使用有關的資訊系統，符合上述法令的規定。A銀行與香港B銀行就上述個人資料的處理建立“互聯”，符合《個人資料保護法》第5條第1款（二）項的規定，對資料的處理沒有偏離收集的目的。



就“個人資料互聯”的建立有否任何歧視或削減資料當事人的權利、自由及保障方面。A銀行與香港B銀行“互聯”處理“客戶資料”，“互聯”的方式主要是便於香港B銀行對A銀行“客戶資料”的處理，以及為客戶提供所需服務，有關的處理不存在歧視或削減資料當事人的權利、自由和保障。

就“個人資料互聯”須有適當的安全措施方面，根據A銀行提供的資料，其與香港B銀行建立“個人資料互聯”是透過集團的數據專線連接香港B銀行，外人無法接入；並安裝專用網絡防火牆及防病毒軟件，以防黑客及電腦病毒入侵。關於A銀行處理資料的安全措施方面，所有處理資料的資訊科技設備均安裝及使用在設有24小時保安監控的範圍內……，並安裝專用防火牆及防病毒軟件；只有指定職員在有職務需要的情況下，才可被授予權限以運用相關之電腦系統，指定職員均有個人密碼，而其相關運用過程均有記錄，以供查核……；當進行資料輸入、更改、刪除以及傳送時，該等處理行為將記錄於有關系統內，以供查證已更新及傳送之資料於何時及由誰作出；客戶數據……每天均有備份及異地儲存。另外，A銀行與香港B銀行之間就資料的處理，簽定了服務合約，當中包括保密條款(Confidentiality)，以確保個人資料處理的機密性。

綜上所述，本辦公室根據《個人資料保護法》第9條及第22條1款(三)項的規定，許可A銀行基於上述所指的目的，在保障資料安全處理及不削減當事人的權利的情況下，與香港B銀行建立“互聯”處理“客戶資料”。

主任
陳海帆

2009年1月5日

Autorização n.º 01/A/2009/GPDP

Tradução

Assunto: Pedido do Banco A relativo ao tratamento, por “interconexão” com o banco B de Hong Kong, de dados dos seus clientes

O Banco A solicitou, ao GPDP, autorização de “interconexão de dados pessoais” para o tratamento de “dados dos seus clientes”, com o Banco B de Hong Kong.

Segundo as informações prestadas pelo Banco A, os dados a serem tratados, via “interconexão” com o Banco B de Hong Kong, incluem: nome dos clientes, tipo, número e local de emissão de documentos de identificação, código comercial chinês, idade, data e local de nascimento, sexo, nacionalidade, país de residência, estado civil, contactos (morada, telefone, e-mail, etc.), estado profissional, cargo, ocupação / natureza dos negócios, nome do empregador, nível de educação, origem do capital, objectivo da abertura da conta, estado de habitação, tipo e número da conta bancária, veículos e registos de venda e compra. Segundo o estipulado no artigo 3.º e na alínea 1) do n.º 1 do artigo 4.º da Lei n.º 8/2005, Lei da Protecção de Dados Pessoais, os dados referidos são dados pessoais dos indivíduos identificados e o seu tratamento está sujeito a esta lei.

O artigo 4.º da Lei da Protecção de Dados Pessoais estipula, na sua alínea 10) do n.º 1 que a “interconexão de dados” é uma forma de tratamento que consiste na possibilidade de relacionamento dos dados de um ficheiro com os dados de um ficheiro ou ficheiros mantidos por outro ou outros responsáveis, ou mantidos pelo mesmo responsável com outra finalidade. O Banco B de Hong Kong tem acesso, pelo sistema de ligação interna bancário, aos “dados dos clientes” do Banco A, pelo que o relacionamento dos ficheiros dos dois bancos configura “interconexão de dados pessoais”, definida e regulada pela lei acima citada.

De acordo com o estipulado no artigo 22.º da Lei da Protecção de Dados Pessoais, a “interconexão de dados”, como a forma de tratamento de dados pessoais sob o controlo prévio, está sujeito à autorização do GPDP. De acordo com o artigo 9.º da mesma lei, a interconexão de dados pessoais que não esteja prevista em disposição legal ou disposição regulamentar de natureza orgânica está sujeita à autorização do GPDP, solicitada pelo responsável ou em conjunto pelos correspondentes responsáveis dos tratamentos, nos termos previstos no n.º 1 do artigo 22.º. A interconexão de dados pessoais deve ser adequada à prossecução das finalidades legais ou estatutárias e de interesses legítimos dos responsáveis dos tratamentos; não devendo implicar a discriminação ou diminuição dos direitos, liberdades e garantias dos titulares dos dados; devendo ser rodeada de adequadas medidas de segurança; e tendo em conta o tipo de dados objecto de interconexão.

Segundo as informações prestadas pelo Banco A este é uma sucursal do Banco B de Hong Kong, instalada em Macau, tendo o tratamento, via “interconexão de dados” com o Banco B de Hong Kong, de dados dos seus clientes, a finalidade de facilitar os trabalhos de fiscalização à distância, verificação e apoios ao sistema informático por parte da sua sede. Isto quer dizer que o Banco



A deve disponibilizar, devido à necessidade dos negócios, os dados dos seus clientes ao Banco B de Hong Kong, e o tratamento dos dados, através da forma de interconexão, corresponde aos interesses legítimos do responsável pelo tratamento dos dados pessoais. De acordo com o estipulado na alínea d) do n.º 1 do artigo 79.º do Decreto-Lei n.º 32/93/M (Regime Jurídico do Sistema Financeiro): “A possibilidade de as instituições de crédito organizarem um sistema de informações recíprocas, com o fim de reduzir o risco e aumentar a segurança das operações”, constituindo, portanto, caso excepcional de sigilo bancário, pelo que o estabelecimento de interconexão pelo Banco A e Banco B para o tratamento de dados dos clientes é baseado no sistema informático necessário aos negócios bancários, correspondendo ao previsto nas disposições legais referidas. A interconexão entre o Banco A e o Banco B de Hong Kong, para o tratamento dos respectivos dados pessoais está no âmbito do previsto no 2) do n.º 1 do artigo 5.º da Lei da Protecção de Dados Pessoais, sendo compatível com a sua finalidade de recolha.

Em relação à discriminação ou diminuição dos direitos, liberdades e garantias dos titulares dos dados, resultantes do estabelecimento de interconexão de dados pessoais, o Banco A e o B efectuem o tratamento de dados dos clientes, via interconexão, com vista a, principalmente, facilitar o tratamento de dados dos clientes do Banco A, pelo Banco B de Hong Kong, a fim de lhes prestar necessários serviços, não implicando o tratamento a discriminação ou diminuição dos direitos, liberdades e garantias dos titulares dos dados.

Em relação às adequadas medidas de segurança requerida pela interconexão de dados pessoais o Banco A, segundo as informações por este prestadas, estabelece a interconexão com o Banco B de Hong Kong, através de cabos exclusivos de dados, restritos à entrada dos alheios, e protegida com sistemas de *firewall* de Internet e aplicações antivírus que previnam *hackers* e vírus que os ataquem. As medidas de segurança do Banco A para o tratamento dos dados incluem, por sua vez, as seguintes: todos os equipamentos de ciência e tecnologia informáticas instalam-se e utilizam-se nas zonas sob o controlo de segurança de 24 horas por dia ...; protegidos com sistemas de *firewall* e antivírus especiais; só os funcionários, de determinado cargo, com necessidade profissional e com respectiva autorização, têm o acesso ao relativo sistema informático; os funcionários autorizados têm próprio código individual e será recordado todo o processo do tratamento dos respectivos dados, para a futura verificação ...; os actos de entrada, alteração, cancelamento e transferência de dados são registados no respectivo sistema para verificar, no futuro, por quem e quando forem feitas a actualização e a transferência dos dados; todos os dias produz-se uma cópia, a depositar em outro local, dos dados dos clientes. Além disso, foi assinado entre o Banco A e o Banco B um contrato de serviços em relação ao tratamento de dados que contenha cláusulas de confidencialidade a fim de garantir o sigilo do tratamento dos dados pessoais.

Pelo exposto, o GPDP autoriza, no âmbito do artigo 9.º e do 3) do n.º 1 do artigo 22.º da Lei da Protecção de Dados Pessoais, o Banco A a estabelecer, com o objectivo referido e sob a condição de garantir a segurança do tratamento dos dados e não implicar a diminuição dos direitos dos seus titulares, a “interconexão” com o Banco B de Hong Kong, para efectuar o tratamento dos “dados dos clientes”.

Aos 5 de Janeiro de 2009

A Coordenadora
Chan Hoi Fan

第02/A/2009/GPDP號許可

事由：A銀行申請與中國B銀行“互聯”處理其職員資料

A銀行就中國B銀行以“互聯”方式處理其職員個人資料事宜，向本辦公室申請“個人資料互聯”許可。

A銀行申請與中國B銀行“互聯”的職員資料包括職員的姓名、身份證明文件號碼及種類、出生日期、性別、國籍、職位、學歷、工作資歷、婚姻狀況、薪金、部門、入職時間、津貼、帳戶號碼、稅務編號、社保編號、父母及子女姓名。根據第8/2005號法律（《個人資料保護法》）第4條第1款第（一）項規定，上述資料屬於身份已確定的職員的個人資料。根據同一法律第3條規定，對上述資料的處理受《個人資料保護法》規範。

根據《個人資料保護法》第4條第1款第（十）項規定：“資料的互聯是指一個資料庫的資料與其他一個或多個負責實體的一個或多個資料庫的資料的聯繫、或同一負責實體但目的不同的資料庫的資料聯繫的處理方式。”A銀行透過數據專線將職員之個人資料傳送至中國B銀行，兩者資料庫的資料建立聯繫，屬上述法律規定的“個人資料互聯”處理方式。

根據《個人資料保護法》第22條規定，“資料的互聯”屬須預先監控的處理個人資料方式，須經本辦公室許可。其中同一法律第9條規定：法律規定或具組織性質的規章性規定未規定的個人資料的互聯，須由負責處理個人資料實體或與其共同負責的實體根據第22條第1款的規定向本辦公室提出申請並取得許可。個人資料的互聯應符合法律或章程規定的目的和負責處理個人資料的實體的正當利益；不得導致歧視或削減資料當事人的權利、自由和保障；須有適當的安全措施及考慮需互聯的資料的種類。

A銀行是中國B銀行在澳門特別行政區設立之銀行分行。根據A銀行提供的資料，A銀行向中國B銀行提供職員資料目的用作銀行集團的人力資源管理，記錄分行人力資源狀況。換言之，A銀行與中國B銀行建立“個人資料互聯”，是基於監管運作及統一資料管理需要，有關的處理方式符合負責處理個人資料實體的正當利益，故A銀行與中國B銀行就上述個人資料的處理建立“互聯”，符合《個人資料保護法》第5條第1款（二）項規定，對資料的處理沒有偏離收集的目的。

就“個人資料互聯”的建立有否任何歧視或削減資料當事人的權利、自由及保障方面。A銀行與中國B銀行“互聯”處理職員資料，目的主要是便於中國B銀行集中管理A銀行的職員資料，“個人資料互



聯”的建立與A銀行處理其職員資料的目的相符，在資料處理方面不存在歧視當事人的權利。

就“個人資料互聯”須有適當的安全措施方面，根據A銀行提供的資料，其與中國B銀行建立“個人資料互聯”，具體的傳送方式是透過雙方間建立的數據專線進行，資料保安措施包括：有關的資料系統設有密碼保護，以及僅有權限者才可以查閱相關資料。A銀行並提供有關其分行及其銀行集團所制定加強信息系統安全及機密資源管理的實施細則，包括《A銀行信息科技管理制度—AD系統管理手冊》及《中國B銀行信息科技管理制度(2008版)—安全管理辦法機密資源管理實施細則(海外分行)》。

綜上所述，本辦公室根據《個人資料保護法》第9條及第22條1款(三)項的規定，許可A銀行與中國B銀行基於上述所指的目的，且在保障資料安全處理及不削減當事人的權利的情況下，“互聯”處理職員資料。

主任

陳海帆

2009年4月28日

Autorização n.º 02/A/2009/GPDP

Tradução

Assunto: Pedido do Banco A relativo ao tratamento, por “interconexão” com o Banco B da China, de dados dos seus funcionários

O Banco A solicitou ao GPDP autorização para proceder à “interconexão de dados pessoais” com o Banco B da China, para o tratamento de dados dos seus funcionários.

Os dados objecto de “interconexão” entre o Banco A e o Banco B da China incluem: nome do funcionário, número e tipo do documento de identidade, data de nascimento, sexo, nacionalidade, cargo, habilitações, experiência profissional, estado civil, salário, departamento, data de início da profissão, subsídios, número de conta bancária, número de contribuinte, número da inscrição na segurança social, nomes dos pais e dos filhos. De acordo com a alínea 1) do n.º 1 do artigo 4.º da Lei n.º 8-2005 (Lei da Protecção de Dados Pessoais), estes são dados relativos a funcionários identificados, pelo que o seu tratamento está sujeito à referida lei, nos termos do seu artigo 3.º.

De acordo com a alínea 10) do n.º 1 do artigo 4.º da Lei da Protecção de Dados Pessoais: “a interconexão de dados é forma de tratamento que consiste na possibilidade de relacionamento dos dados de um ficheiro com os dados de um ficheiro ou ficheiros mantidos por outro ou outros responsáveis, ou mantidos pelo mesmo responsável com outra finalidade”. Através da linha exclusiva, o Banco A transmite os dados pessoais dos seus funcionários para o Banco B da China e estabelece-se, deste modo, um relacionamento entre ficheiros dos dois Bancos, por conseguinte, é subsumível ao modo de tratamento de “interconexão de dados pessoais”.

De acordo com o estipulado no artigo 22.º da Lei da Protecção de Dados Pessoais, a “interconexão de dados”, como forma de tratamento de dados pessoais sob controlo prévio, está sujeita a autorização do GPDP. De acordo com o artigo 9.º da mesma lei, a interconexão de dados pessoais que não esteja prevista em disposição legal ou disposição regulamentar de natureza orgânica está sujeita à autorização do GPDP, solicitada pelo responsável ou em conjunto pelos correspondentes responsáveis dos tratamentos, nos termos previstos no n.º 1 do artigo 22.º. A interconexão de dados pessoais deve ser adequada à prossecução das finalidades legais ou estatutárias e de interesses legítimos dos responsáveis dos tratamentos; não devendo implicar a discriminação ou diminuição dos direitos, liberdades e garantias dos titulares dos dados; devendo ser rodeada de adequadas medidas de segurança; e ter em conta o tipo de dados objecto de interconexão.

O Banco A é a filial do Banco B da China, estabelecido na Região Administrativa Especial de Macau. Segundo as informações fornecidas pelo Banco A, este fornece os dados dos seus funcionários ao Banco B da China, tendo em vista a administração dos recursos humanos do grupo bancário e o registo de recursos humanos de bancos filiais. Ou seja, é pela necessidade de supervisão do funcionamento e de gestão centralizada dos dados que o Banco B da China procede ao tratamento destes dados do Banco A, por meio



de “interconexão”, sendo a forma de tratamento adequada aos interesses legítimos do responsável pelo tratamento de dados. Portanto, o estabelecimento de “interconexão de dados pessoais” entre os dois bancos está de acordo com a alínea 2) do n.º 1 do artigo 5.º da Lei da Protecção de Dados Pessoais, sendo o tratamento compatível com a finalidade de recolha dos mesmos.

Quanto à questão da eventual discriminação ou diminuição dos direitos, liberdades e garantias dos titulares de dados, pelo estabelecimento de “interconexão de dados pessoais”, a finalidade pela qual o Banco A e o B da China procedem ao tratamento de dados dos seus funcionários, por “interconexão”, é, essencialmente, facilitar a gestão centralizada dos dados dos funcionários pelo Banco B da China, estando o estabelecimento de “interconexão de dados pessoais” em conformidade com a finalidade do tratamento de dados dos funcionários do Banco A, não implicando a discriminação ou diminuição dos direitos, liberdades e garantias dos seus titulares.

Relativamente à necessidade de adequadas medidas de segurança na “interconexão de dados pessoais”, segundo as informações fornecidas pelo Banco A, a concretização da “interconexão de dados pessoais” com o Banco B da China é baseada na transmissão de dados, através de linha exclusiva, instalada entre os dois bancos. As medidas de segurança e protecção de dados incluem: a protecção do sistema de dados por código, assim como a autorização exclusiva para consulta das informações. O Banco A forneceu também as normas pormenorizadas, elaboradas pelos bancos filiais e pelo grupo bancário, de execução da gestão de recursos confidenciais e de fortalecimento da segurança do sistema informático, em que constam o “Sistema de Gestão de Ciência e Tecnologia Informática do Banco A – Boletim de Gestão do Sistema AD” e o “Sistema de Gestão de Ciência e Tecnologia Informática do Banco B da China (2008) – Normas Pormenorizadas de Execução de Gestão de Recursos Confidenciais e de Medidas de Segurança (Filiais Ultramarinos).

Pelo exposto, o GPDP autoriza, no âmbito do artigo 9.º e da alínea 3) do n.º 1 do artigo 22.º da Lei da Protecção de Dados Pessoais, o Banco A a estabelecer, com o objectivo referido e sob a condição de garantir a segurança do tratamento dos dados e não implicar a diminuição dos direitos dos seus titulares, a “interconexão”, com o Banco B da China, para efectuar o tratamento dos “dados dos funcionários”.

Aos 28 de Abril de 2009

A Coordenadora
Chan Hoi Fan

第03/A/2009/GPDP號許可

事由：A銀行申請與香港B銀行“互聯”處理其客戶及僱員資料

A銀行就與香港B銀行以“互聯”方式處理客戶及僱員的個人資料，向本辦公室申請“個人資料互聯”許可。

A銀行申請與香港B銀行“互聯”處理客戶及僱員資料，其中客戶資料是指企業客戶的賬戶持有人、賬戶股東、賬戶董事及賬戶授權操作人員的相關資料，具體資料包括：姓名、身份證明文件號碼及副本、年齡/出生日期、性別、國籍、聯絡方法、銀行帳戶號碼及收入。而僱員資料則包括：姓名、身份證明文件號碼及副本、年齡/出生日期、性別、國籍、婚姻狀況、子女姓名、聯絡方法、銀行帳戶號碼、收入、醫生證明、與刑事違法行為有關之資料、政治社團或工會關係、醫療檢查結果及疾病記錄，以及僱員在銀行集團以外銀行的收入證明、月結單、借貸情況及資產淨值等資料，當中僱員的政治社團或工會關係、醫療檢查結果及疾病記錄屬於第8/2005號法律（《個人資料保護法》）第7條所指之敏感資料。根據《個人資料保護法》第4條第1款第（一）項規定，以上客戶及僱員資料屬於身份已確定人士的個人資料。同一法律第3條規定，有關個人資料的處理受該法律所規範。

根據《個人資料保護法》第4條第1款第（十）項規定：“資料的互聯是指一個資料庫的資料與其他一個或多個負責實體的一個或多個資料庫的資料的聯繫、或同一負責實體但目的不同的資料庫的資料聯繫的處理方式。”A銀行透過電訊專線將客戶及僱員的資料傳送予香港B銀行，兩者資料庫的資料建立聯繫，屬上述法律規定的“個人資料互聯”處理方式。

根據《個人資料保護法》第22條規定，“資料的互聯”屬須預先監控的處理個人資料方式，須經本辦公室許可。其中同一法律第9條規定：法律規定或具組織性質的規章性規定未規定的個人資料的互聯，須由負責處理個人資料實體或與其共同負責的實體根據第22條第1款的規定向本辦公室提出申請並取得許可。個人資料的互聯應符合法律或章程規定的目的和負責處理個人資料的實體的正當利益；不得導致歧視或削減資料當事人的權利、自由和保障；須有適當的安全措施及考慮需互聯的資料的種類。

A銀行與香港B銀行屬同一銀行集團成員。根據A銀行提供的資料，A銀行現時所有業務操作以及與人力資源相關之事宜都交由香港B銀行統籌管理，故有必要以“互聯”方式將其客戶及僱員資料交予香港B銀行處理。A銀行基於業務運作及人力資源管理的需要，將客戶及僱員資料提供予同一集團成員香港B銀行處理，兩者以“互聯”方式處理客戶及僱員資料符合A銀行的正當利益。就客戶資料處理方面，根據第32/93/M號



法令（《金融體系法律制度》）第79條第1款d)項規定“信用機構為減少風險及增加經營活動之安全而組織相互提供資訊系統之可能性”，屬於銀行保密義務的例外情況。故A銀行與香港B銀行“互聯”處理客戶資料，屬經營正當銀行業務所需而使用有關的資訊系統，符合上述法令的規定。有關客戶及僱員個人資料“互聯”之建立為香港B銀行管理A銀行業務運作及人力資源所必需，符合《個人資料保護法》第5條第1款(二)項的規定，對資料的處理沒有偏離收集的目的。

就“個人資料互聯”的建立有否任何歧視或削減資料當事人的權利、自由及保障方面。A銀行與香港B銀行“互聯”處理客戶及僱員資料，主要是受銀行既定的操作模式所限，A銀行需將所有業務操作及人力資源相關事宜交由香港B銀行進行集中管理，兩者資料庫“互聯”的建立與A銀行處理其客戶及僱員資料的目的相符，在資料處理方面不存在歧視當事人的權利、自由和保障。

就“個人資料互聯”須有適當的安全措施方面，因上述“互聯”資料種類涉及僱員之敏感資料，故除考慮《個人資料保護法》第15條有關處理的安全性規定外，亦須包括16條有關資料處理之特別的安全措施之規定。根據A銀行提供的資料，以“互聯”方式傳送資料時，A銀行與香港B銀行透過專線連接，經郵箱傳遞客戶及僱員資料，系統並設有加密裝置。資料的安全措施包括：對系統用戶進行身份鑑別，並根據系統內容及存取資料的級別，設定不同強度之鑑別程序，避免非授權用戶存取資料；對系統用戶進行權限管理，藉以控制存取；保存完整的獲授權存取目錄，並定期更新，以保證授權的有效性；對系統資料進行風險分析，以採取不同層級的加密保護，確保系統資料的機密性及完整性。關於處理僱員的敏感資料應有之特別安全措施，包括控制使用、控制查閱、控制引入以及將健康和性生活有關的個人資料，同其他個人資料分開作邏輯分離等（見《個人資料保護法》第16條規定）。A銀行就敏感資料採取的特別安全措施包括：用以儲存僱員資料的電腦系統設有高度保護裝置(firewall)，防止黑客或未經許可人士登入系統；僅核定部門及獲授權職員方可處理敏感資料；用戶身份及權限之設定均經過嚴格審批，以處理不同程度的敏感資料；系統自動記錄登入用戶，用作日後跟蹤及查核之用。

綜上所述，本辦公室根據《個人資料保護法》第9條及第22條1款(三)項的規定，許可A銀行與香港B銀行基於上述所指的目的，且在保障資料安全處理及不削減當事人的權利的情況下，“互聯”處理客戶資料及僱員資料。

主任

陳海帆

2009年5月4日

Autorização n.º 03/A/2009/GPDP

Tradução

Assunto: Pedido do Banco A para o tratamento, por “interconexão” com o Banco B de Hong Kong, de dados dos seus clientes e funcionários

O Banco A solicitou ao GPDP autorização para tratamento, por “interconexão de dados pessoais” com o Banco B de Hong Kong, dos dados dos seus clientes e funcionários.

O pedido do Banco A para o tratamento, por “interconexão” com o Banco B de Hong Kong, dos dados dos seus clientes e funcionários, dos quais, os dos clientes, se referem a informações relacionadas com os titulares das contas dos clientes empresariais, accionistas das contas, administradores das contas e operadores das contas autorizados, incluindo, nomeadamente: nome, número e cópia de documentos de identificação, idade/data de nascimento, sexo, nacionalidade, contactos, número de conta bancária e rendimento; enquanto os dados dos funcionários incluem: nome, número e cópia de documentos de identificação, idade/data de nascimento, sexo, nacionalidade, estado civil, nomes dos filhos, contactos, número de conta bancária, rendimento, certificado médico, registo criminal, relações com associações políticas ou sindicatos, resultados de exames médicos e registos de doenças, bem como informações relativas aos rendimentos e as respectivas listas mensais, empréstimos e valores líquidos dos respectivos bens, entre outras, encontradas em bancos fora do grupo bancário onde trabalham. Dos quais, as relações com associações políticas ou sindicatos, os resultados de exames médicos e registos de doenças são considerados dados sensíveis, definidos no artigo 7.º da Lei n.º 8/2005, Lei da Protecção de Dados Pessoais. Segundo o estipulado na alínea 1) do n.º 1 do artigo 4.º desta lei, os dados dos clientes e funcionários, acima referidos, são dados relativos a pessoas identificadas, estando, por isso, e de acordo com o artigo 3.º da mesma lei, o tratamento dos mesmos sujeito à Lei da Protecção de Dados Pessoais.

O artigo 4.º da Lei da Protecção de Dados Pessoais estipula, na alínea 10) do n.º 1, que a “interconexão de dados” é uma forma de tratamento que consiste na possibilidade de relacionamento dos dados de um ficheiro com os dados de um ficheiro ou ficheiros mantidos por outro ou outros responsáveis, ou mantidos pelo mesmo responsável com outra finalidade. O Banco A efectua, através de cabos electrónicos exclusivos, a transferência de dados dos seus clientes e funcionários ao Banco B de Hong Kong, pelo que o relacionamento dos ficheiros dos dois bancos configura “interconexão de dados pessoais”, definida e regulada pela lei acima citada.

De acordo com o estipulado no artigo 22.º da Lei da Protecção de Dados Pessoais, a “interconexão de dados”, como a forma de tratamento de dados pessoais sob o controlo prévio, está sujeito à autorização do GPDP. De acordo com o artigo 9.º da mesma lei, a interconexão de dados pessoais que não esteja prevista em disposição legal ou disposição regulamentar de natureza orgânica está sujeita à autorização do GPDP, solicitada pelo responsável ou em conjunto pelos correspondentes responsáveis dos tratamentos, nos termos previstos no n.º 1 do artigo 22.º. A interconexão de dados pessoais deve ser adequada à prossecução das finalidades legais ou estatutárias e de interesses legítimos dos responsáveis dos tratamentos; não devendo implicar a discriminação ou diminuição dos direitos, liberdades



e garantias dos titulares dos dados; devendo ser rodeada de adequadas medidas de segurança; e ter em conta o tipo de dados objecto de interconexão”.

O Banco A e o Banco B de Hong Kong são ambos membros do mesmo grupo bancário. A operação de todos os negócios e os assuntos relacionados com os recursos humanos do Banco A, segundo as informações por este prestadas, são da responsabilidade do Banco B de Hong Kong, sendo, portanto, necessário fornecer, por meio de “interconexão”, os dados dos seus clientes e funcionários para o Banco B poder efectuar o tratamento dos mesmos. O Banco A disponibiliza, em função da necessidade dos negócios e da gestão dos recursos humanos, os dados dos seus clientes e funcionários ao Banco B de Hong Kong, membro do mesmo grupo bancário, correspondendo o relacionamento e tratamento dos dados, através de interconexão, aos interesses legítimos do Banco A. O estipulado na alínea d) do n.º 1 do artigo 79.º do Decreto-Lei n.º 32/93/M (Regime Jurídico do Sistema Financeiro) consigna: “A possibilidade de as instituições de crédito organizarem um sistema de informações recíprocas, com o fim de reduzir o risco e aumentar a segurança das operações”, constituindo caso excepcional quebra do sigilo bancário, pelo que a “interconexão” entre o Banco A e o Banco B de Hong Kong, para o tratamento de dados dos clientes com recurso ao sistema informático, é resultante da necessidade dos negócios bancários legítimos, estando a mesma prevista nas disposições legais acima referidas. Ora, o estabelecimento de interconexão de dados pessoais dos clientes e funcionários é considerado necessário para o Banco B poder efectuar a gestão dos negócios bancários e dos recursos humanos do Banco A, e compatível com a finalidade de recolha dos mesmos, prevista no 2) do n.º 1 do artigo 5.º da Lei da Protecção de Dados Pessoais.

Em relação à discriminação ou diminuição dos direitos, liberdades e garantias dos titulares de dados, resultantes do estabelecimento de interconexão de dados pessoais, o tratamento de dados dos clientes e funcionários pelos Bancos A e B, via interconexão, é requerido pelo modelo do funcionamento destes bancos, devendo o Banco A passar os seus negócios e assuntos relativos aos recursos humanos, para o Banco B de Hong Kong efectuar a gestão centralizada, sendo o estabelecimento de interconexão dos ficheiros de ambos compatível com a finalidade do tratamento de dados dos clientes e funcionários do Banco A, não implicando o tratamento dos referidos dados a discriminação dos direitos, liberdades e garantias dos titulares dos mesmos.

Em relação às adequadas medidas de segurança, requeridas pela “interconexão de dados pessoais” e pelo facto de os dados dos funcionários envolvidos na “interconexão” acima referida serem sensíveis, devem ser tidas em conta, não só as disposições relativas à segurança do tratamento previstas no artigo 15.º da Lei da Protecção de Dados Pessoais, mas, também, observadas as medidas especiais de segurança previstas no artigo 16.º da mesma lei para o tratamento dos referidos dados. Segundo as informações prestadas pelo Banco A, os dados dos clientes e funcionários serão transferidos, via “interconexão”, através de cabos electrónicos exclusivos que o ligam ao Banco B de Hong Kong, estando o sistema sob o controlo de rigorosas medidas de protecção. As medidas de segurança incluem nomeadamente: identificação dos utilizadores do sistema que dispõem, ainda, de diferentes níveis de identificação correspondentes ao conteúdo e ao nível de sigilo dos dados a recolher e conservar, a fim de evitar o acesso de utilizadores não autorizados; controlo do acesso dos utilizadores aos dados por meio de gestão de autorizações; conservar a lista completa dos acessos autorizados mantendo-a devidamente actualizada, a fim de garantir a validade das autorizações; analisar os possíveis riscos do sistema para adoptar a protecção

de diferentes níveis com vista a garantir a confidencialidade e integridade dos dados armazenados no sistema. As especiais medidas de segurança para o tratamento dos dados sensíveis dos funcionários incluem o controlo da introdução, o controlo da utilização, o controlo de acesso e a separação lógica entre os dados referentes à saúde e à vida sexual e os restantes dados pessoais, entre outras (vide o estipulado no artigo 16.º da Lei da Protecção de Dados Pessoais). As especiais medidas de segurança, a adoptar pelo Banco A, para o tratamento dos dados sensíveis incluem, nomeadamente: o sistema informático que conserva os dados dos funcionários é altamente protegido com *firewall* para prevenir ataques de *hackers* ou acessos não autorizados; apenas os departamentos e funcionários autorizados podem efectuar o tratamento dos dados sensíveis; os utilizadores e os poderes que lhes estão atribuídos são expressas e rigorosamente autorizados para poderem efectuar o tratamento dos dados com diferentes níveis de sensibilidade; e o sistema regista, automaticamente, os acessos dos utilizadores para *follow-up* ou verificações, no futuro.

Pelo exposto, o GPDP autoriza, no âmbito do artigo 9.º e da alínea 3) do n.º 1 do artigo 22.º da Lei da Protecção de Dados Pessoais, o Banco A a estabelecer, com o objectivo referido e sob a condição de garantir a segurança do tratamento dos dados e não implicar a diminuição dos direitos dos seus titulares, a “interconexão”, com o Banco B de Hong Kong, para efectuar o tratamento de dados dos clientes e funcionários.

Aos 4 de Maio de 2009

A Coordenadora
Chan Hoi Fan



第04/A/2009/GPDP號許可

事由：關於勞工事務局申請以“互聯”方式處理治安警察局的“外地僱員及聘用僱主系統”資料

勞工事務局就以“互聯”方式處理治安警察局的“外地僱員及聘用僱主系統”資料，向本辦公室申請“個人資料互聯”許可。而治安警察局則透過公函確認上述“互聯”申請事宜。

勞工事務局申請以“互聯”方式處理治安警察局“外地僱員及聘用僱主系統”的資料如下：外地僱員的姓名、性別、出生日期、國籍、非本地勞工身份咭（藍卡）編號及有效期、所持證件所屬國或地區、護照編號及種類、工人類型（技術／非技術／自身利益）、職業、工作連續性（日數）、僱主編號、僱主名稱、僱主地址及電話、合同編號、生效及屆滿日期。根據第8/2005號法律（《個人資料保護法》）第4條第1款第（一）項規定，上述外地僱員資料、聘用僱主¹（僅限以個人身份聘用僱員的情況）資料屬於與身份已確定人士相關的個人資料，受法律保護。根據同一法律第3條規定，對上述資料的處理受《個人資料保護法》規範。

根據《個人資料保護法》第4條第1款第（十）項規定：“資料的互聯是指一個資料庫的資料與其他一個或多個負責實體的一個或多個資料庫的資料的聯繫、或同一負責實體但目的不同的資料庫的資料聯繫的處理方式。”勞工事務局透過政府內部網絡(Informac)，登入治安警察局FTP伺服器接收“外地僱員及聘用僱主系統”資料，兩者資料庫的資料建立聯繫，屬上述法律定義的“個人資料互聯”處理方式。

根據《個人資料保護法》第22條規定，“資料的互聯”屬須預先監控的處理個人資料方式。根據第9條規定：法律規定或具組織性質的規章性規定未規定的個人資料的互聯，須由負責處理個人資料實體或與其共同負責的實體根據第22條第1款的規定向本辦公室提出申請並取得許可。個人資料的互聯應符合法律或章程規定的目的和負責處理個人資料的實體的正當利益；不得導致歧視或削減資料當事人的權利、自由和保障；須有適當的安全措施及考慮需互聯的資料的種類。

根據勞工事務局提供的資料，以“互聯”方式處理“外地僱員及聘用僱主系統”資料的目的為“公佈聘用外勞企業的實體名單；監管企業使用外勞的狀況；研究及制定有關外勞政策；協助人力資源辦公室就

¹ 聘用僱主資料包括僱用外地勞工的公司或企業資料及聘請家庭傭工的自然人僱主資料，《個人資料保護法》僅保護自然人的個人資料，而公司或企業的資料則不適用。換言之，公司或企業的資料不適用該法律規定。

企業編號與治安警察局的企業編號作對應。”

根據第22/2001號行政法規（《治安警察局的組織與運作》）第2條及第3條規定，治安警察局負責管制非法移民及負責出入境工作，擔負有關人士出入境之一切任務。同一行政法規第30條規定，治安警察局出入境事務廳依法發出外地僱員身分辨別證；組織僱主及外地僱員之紀錄，並保持其最新資料。根據第24/2004號行政法規（《勞工事務局的組織及運作》）第1條及第2條規定，勞工事務局是負責協助制定及執行勞動、就業、職業安全健康及職業培訓政策的澳門特別行政區公共部門，尤其負責促進對勞動、就業、職業安全健康及職業培訓的社會環境的分析及研究，以便在澳門特別行政區的社會及經濟政策總方針內訂定勞動政策的措施；執行並跟進與勞動關係及勞動條件有關的行政或立法措施，以及促進與澳門特別行政區內、外的公共部門、公共或私人實體在勞動範疇內的交流及合作。另外，同一行政法規第7條第3款（五）項及第17/2004號行政法規（禁止非法規章）第7條規定，勞工事務局負責監察非法工作情況。

勞工事務局為公佈聘用外勞企業的實體名單；監管企業使用外勞的狀況；研究及制定有關外勞政策；協助人力資源辦公室就企業編號與治安警察局的企業編號作對應，以執行法定職責，需瞭解外地僱員及聘用僱主資料，具正當性要求治安警察局提供“外地僱員及聘用僱主系統”資料。勞工事務局處理該等資料的正當性符合《個人資料保護法》第6條第（四）項規定，屬於履行具公共利益的任務及行使公共當局的權力。

為使勞工事務局瞭解“外地僱員及聘用僱主系統”資料，以方便該局跟進有關工作，加快行政效率，治安警察局與勞工事務局“互聯”處理“外地僱員及聘用僱主系統”資料，符合《個人資料保護法》第5條1款（二）項的規定，對資料的處理沒有偏離收集資料的目的，“互聯”的建立是為維護正當的公共利益，有關資料的處理方式符合負責處理個人資料的實體的正當利益。

關於“互聯”不允許任何歧視或削減資料當事人的權利、自由及保障方面。就本申請而言，勞工事務局透過“互聯”方式查閱治安警察局“外地僱員及聘用僱主系統”資料，目的是簡化行政程序，即時接收已更新的外地僱員及聘用僱主資料，“互聯”資料的處理與資料原來的收集目的相符，不存在歧視當事人權利。

就“互聯”須有適當的安全措施方面，勞工事務局透過政府內部網絡Informac與治安警察局“互聯”處理“外地僱員及聘用僱主系統”資料，根據行政暨公職局提供的資料，Informac網絡屬封閉式網



絡，供各公共部門連接對方部門的系統或服務，連接Informac網絡系統的主要方式是以光纖專線、DDN專線及VPN登入。此外，根據勞工事務局提供的資料，該局需輸入用戶名稱及密碼登入治安警察局FTP伺服器接收有關資料，勞工事務局的系統只有獲授權人士可以查閱及使用相關資料，且系統設有密碼保護。

綜上所述，本辦公室根據《個人資料保護法》第9條及第22條1款(三)項的規定，許可勞工事務局與治安警察局基於上述所指的目的，且在保障資料安全處理及不削減當事人權利的情况下，“互聯”處理“外地僱員及聘用僱主系統”。

主任

陳海帆

2009年5月27日

Autorização n.º 04/A/2009/GPDP

Tradução

Assunto: Pedido da Direcção dos Serviços para os Assuntos Laborais (DSAL) relativo ao tratamento, por meio de “interconexão”, de dados contidos no “Sistema sobre os Trabalhadores Não Residentes e os seus Empregadores” da Polícia de Segurança Pública (PSP)

A DSAL solicitou, ao GPDP, autorização de “interconexão de dados pessoais” para poder efectuar o tratamento, através de “interconexão”, de dados guardados no “Sistema sobre os Trabalhadores Não Residentes e os seus Empregadores”, da PSP, que confirmou o pedido no seu ofício.

A DSAL pediu autorização para efectuar, através de “interconexão”, o tratamento dos seguintes dados, contidos no “Sistema sobre os Trabalhadores Não Residentes e os seus Empregadores” da PSP: nome, sexo, data de nascimento, nacionalidade, título de identificação do trabalhador não residente (cartão azul), número e prazo válido do título, país ou região de origem do documento, número e tipo do passaporte, categoria do trabalhador (técnico/não técnico/de interesse individual), profissão, continuidade do trabalho (dias), todos estes dados relativos ao trabalhador não-residente, bem como número, nome, morada e número de telefone do empregador, número do contrato e prazo de vigência do mesmo. Segundo o estipulado na alínea 1) do n.º 1 do artigo 4.º da Lei n.º 8/2005, Lei da Protecção de Dados Pessoais, os dados dos trabalhadores não residentes e dos seus empregadores¹ (que empregam os trabalhadores em nome pessoal), acima referidos, são dados relativos a pessoas identificadas, estando, por isso, e de acordo com o artigo 3.º da mesma lei, o tratamento dos mesmos sujeito à Lei da Protecção de Dados Pessoais.

O artigo 4.º da Lei da Protecção de Dados Pessoais estipula na alínea 10) do n.º 1 que a “interconexão de dados se refere à forma de tratamento que consiste na possibilidade de relacionamento dos dados de um ficheiro com os dados de outro ou outros ficheiros mantidos por outro ou outros responsáveis, ou mantidos pelo mesmo responsável com outra finalidade”. A DSAL acede, através do Informac, intranet do governo, ao servidor FTP da PSP para receber os dados do “Sistema sobre os Trabalhadores Não Residentes e os seus Empregadores”, pelo que o relacionamento dos dois ficheiros para o tratamento de dados configura “interconexão de dados pessoais”, definida e regulada pela lei acima citada.

A “interconexão de dados” é a forma de tratamento de dados sob o controlo prévio, prevista no artigo 22.º da Lei da Protecção de Dados Pessoais. O artigo 9.º da mesma lei estipula que a interconexão de dados pessoais que não esteja prevista em disposição legal ou disposição regulamentar de natureza orgânica, está sujeita a autorização do GPDP, solicitada pelo responsável ou em conjunto pelos

1. Os dados dos empregadores incluem os das companhias ou empresas que recrutam trabalhadores não residentes e as pessoas singulares que recrutam trabalhadores domésticos. A Lei da Protecção de Dados Pessoais protege apenas os dados pessoais de pessoas singulares, mas não das companhias ou empresas, isto é, os dados das companhias ou empresas não estão abrangidos pelas disposições previstas na referida lei.



respectivos responsáveis do tratamento, nos termos previstos no n.º 1 do artigo 22.º. A interconexão de dados pessoais deve ser adequada à prossecução das finalidades legais ou estatutárias e de interesses legítimos dos responsáveis pelos tratamentos, não devendo implicar a discriminação ou diminuição dos direitos, liberdades e garantias dos titulares dos dados, sendo também rodeada de adequadas medidas de segurança e tido em conta o tipo de dados objecto da interconexão. De acordo com as informações prestadas pela DSAL o tratamento de dados, através de interconexão, dos “trabalhadores não residentes e os seus empregadores” tem a finalidade de divulgar os nomes das entidades patronais que contratam trabalhadores não residentes, supervisionar a situação de recrutamento dos mesmos por parte de empresas, estudar e elaborar políticas relativas aos trabalhadores não residentes, bem como prestar apoio ao Gabinete para os Recursos Humanos para proceder a uma comparação e indagar da correspondência dos números das empresas encontradas neste e na PSP.

Segundo o estipulado nos artigos 2.º e 3.º do Regulamento Administrativo n.º 22/2001 (Organização e funcionamento do Corpo de Polícia de Segurança Pública), a PSP é responsável pelo controlo da imigração ilegal e pelo serviço de migração, desempenhando todas as missões relacionadas com os movimentos migratórios das pessoas. De acordo com o previsto no artigo 30.º, do mesmo Regulamento, aos Serviços de Migração compete emitir títulos de identificação de trabalhadores não residentes bem como organizar e manter actualizado o registo de empregadores e trabalhadores não residentes. Os artigos 1.º e 2.º do Regulamento Administrativo n.º 24/2004 (Orgânica e Funcionamento da Direcção dos Serviços para os Assuntos Laborais), a DSAL é o serviço público da Região Administrativa Especial de Macau incumbido de coadjuvar na implementação e execução das políticas de trabalho, emprego, segurança e saúde ocupacional e formação profissional, nomeadamente, promover a análise e o estudo do meio social do trabalho, do emprego, da segurança e saúde ocupacional e da formação profissional, com vista à definição de medidas de política do trabalho, no quadro das linhas gerais da política social e económica da Região Administrativa Especial de Macau; assegurar a execução e o acompanhamento das medidas administrativas ou legislativas no que respeita às relações e condições de trabalho; e promover o intercâmbio e a colaboração, no domínio do trabalho, com serviços públicos ou entidades públicas ou privadas da Região Administrativa Especial de Macau ou do exterior. Além disso, segundo o estipulado na alínea 5) do n.º 3 do artigo 7.º do mesmo Regulamento Administrativo e no artigo 7.º do Regulamento Administrativo n.º 17/2004 (Regulamento sobre a Proibição do Trabalho Ilegal) a DSAL é responsável pela fiscalização das situações de trabalho ilegal.

A DSAL precisa de conhecer, para cumprir as suas atribuições conferidas pela lei, os dados dos trabalhadores não residentes e dos seus empregadores a fim de divulgar os nomes das entidades que contratam trabalhadores não residentes, supervisionar a situação de recrutamento dos mesmos por parte de empresas, estudar e elaborar políticas relativas aos trabalhadores não residentes, bem como prestar apoio ao Gabinete para os Recursos Humanos para averiguar da correspondência dos números das empresas respectivamente encontrados neste e na PSP. Assim, considera-se legítimo o pedido à PSP dos dados contidos no “Sistema sobre os Trabalhadores Não Residentes e os seus Empregadores”. Deste modo, a DSAL, para a execução da missão de interesse público e o exercício de poderes de autoridade pública, tem legitimidade para proceder ao tratamento dos dados, anteriormente mencionados, no âmbito da alínea 4) do artigo 6.º da Lei da Protecção de Dados Pessoais.

O acesso da DSAL ao “Sistema sobre os Trabalhadores Não Residentes e os seus Empregadores” tem como objectivo acompanhar

os respectivos trabalhos e melhorar a eficácia administrativa, observando o tratamento, junto da PSP, pela “interconexão”, de dados dos “trabalhadores não residentes e dos seus empregadores”, o estipulado na alínea 2) do n.º 1 do artigo 5.º da Lei da Protecção de Dados Pessoais. Tal tratamento é compatível com a finalidade de recolha de dados e o relacionamento por “interconexão” visa salvaguardar os legítimos interesses públicos, correspondendo a forma do tratamento dos dados aos interesses legítimos da entidade responsável pelo tratamento dos mesmos.

No aspecto de que a interconexão não deverá implicar a discriminação ou diminuição dos direitos, liberdades e garantias dos titulares dos dados, a DSAL tem, no presente pedido, como objectivo receber, pelo acesso, via interconexão, ao “Sistema sobre os Trabalhadores Não Residentes e os seus Empregadores” da PSP, os respectivos dados mais actualizados e simplificar o processo administrativo, sendo o tratamento por interconexão compatível com a finalidade de recolha dos dados, não implicando a discriminação ou desrespeito pelos direitos dos titulares.

Quanto às adequadas medidas de segurança de interconexão, a DSAL estabelece, via *Informac*, intranet do governo, a interconexão com o “Sistema sobre os Trabalhadores Não Residentes e os seus Empregadores” da PSP. Segundo as informações prestadas pela Direcção dos Serviços de Administração e Função Pública, o *Informac* é um sistema de Intranet fechado que possibilita o relacionamento do ficheiro ou dos serviços de uma autoridade pública com os mesmos de outra, sendo interligado, principalmente, por fibras ópticas e linhas DDN e acessível apenas através da introdução do código VPN. Além disso, as informações prestadas pela DSAL comprovam que esta poderá ter acesso, com entrada do código do utilizador e da senha, ao servidor FTP da PSP e receber os respectivos dados que serão consultados e utilizados apenas pelos funcionários da DSAL autorizados para tal e serão protegidos com a senha.

Pelo exposto, o GPDP autoriza, no âmbito do artigo 9.º e da alínea 3) do n.º 1 do artigo 22.º da Lei da Protecção de Dados Pessoais, a DSAL e a PSP a estabelecerem, com o objectivo referido e sob a condição de garantir a segurança do tratamento dos dados e não implicar a diminuição dos direitos dos seus titulares, a interconexão para efectuar o tratamento dos dados contidos no “Sistema sobre os Trabalhadores Não Residentes e os seus Empregadores”.

Aos 27 de Maio de 2009

A Coordenadora
Chan Hoi Fan



第05/A/2009/GPDP號許可

事由：A公司申請以“互聯”方式轉移僱員資料予位於美國母公司之“全球人力資源資訊系統”

A公司就以“互聯”方式轉移僱員資料予位於美國母公司之“全球人力資源資訊系統”一事，向本辦公室申請“個人資料互聯”許可。

A公司申請以“互聯”方式轉移予美國母公司的僱員資料包括：姓名、地址、身份證明文件號碼及副本、年齡/出生日期、性別、國籍、婚姻狀況、子女姓名、相片、聯絡方法、收入、與福利津貼相關事項的管理資料、受益人及受撫養人的身份識別資料、緊急事故的聯絡人資料、個人履歷、學歷及專業資格、語言能力及程度、與報酬相關的資料、職業活動資料、納稅人編號、僱員使用公司信用卡所生的開支帳目資料、公司車輛資料、醫療保險資料、出勤記錄、培訓及工作評價資料、職業及個人發展計劃資料、後續發展規劃、內部安全出入及許可資料。

根據第8/2005號法律（《個人資料保護法》）第4條第1款第（一）項規定，個人資料是指某個身份已確定或身份可確定的自然人有關的任何資訊，包括聲音和影像。故上述所指僱員使用A公司信用卡所生的開支帳目資料及該公司之車輛資料，是以A公司之身份作識別，不屬僱員之個人資料。除上述兩種資料類別外，其他申請資料與身份已確定的僱員相關，為個人資料之範疇，故根據《個人資料保護法》第3條規定，對僱員個人資料之處理受該法律所規範。

根據《個人資料保護法》第4條第1款第（十）項規定：“資料的互聯是指一個資料庫的資料與其他一個或多個負責實體的一個或多個資料庫的資料的聯繫、或同一負責實體但目的不同的資料庫的資料聯繫的處理方式。”A公司為位於美國母公司國際集團之其中一個成員，其與所屬集團位於美國的伺服器建立了資料處理聯繫，透過集團的內聯網系統將其僱員之個人資料轉移予母公司之“全球人力資源資訊系統”，以便A公司之僱員資料與其所屬集團之“全球人力資源資訊系統”建立資料聯繫，藉此將該等資料提供予國際集團之所有成員或其他在業務的正常程序下需要獲取有關係統資料的第三者使用，上述處理方式令A公司的僱員資料庫與母公司的“全球人力資源資訊系統”的資料庫建立了資料聯繫，屬上述法律規定的“個人資料互聯”情況。

根據《個人資料保護法》第22條規定，“資料的互聯”屬須預先監控的處理個人資料方式，須經本辦公室許可。其中同一法律第9條第1款規定：法律規定或具組織性質的規章性規定未規定的個人資料的互

聯，須由負責處理個人資料實體或與其共同負責的實體根據第22條第1款的規定向本辦公室提出申請並取得許可。同條第2款規定：“個人資料的互聯應符合法律或章程規定的目的和負責處理個人資料的實體的正當利益；不得導致歧視或削減資料當事人的權利、自由和保障；須有適當的安全措施；考慮需互聯的資料的種類。”

根據A公司提供的資料，其將所有之僱員資料透過“互聯”方式轉移予位於美國母公司之“全球人力資源資訊系統”，主要是便於集團的國際人力資源部門能集中處理所屬集團成員之人力資源，以統一政策及確保集團所有成員能獲得相同的培訓及晉升的機會。換言之，A公司基於母公司之全球人力資源管理目的，與母公司就僱員資料之處理建立“互聯”，符合A公司處理僱員資料之正當利益。而A公司基於全球人力資源行政管理目的與母公司建立“資料互聯”的資料處理方式，亦與A公司收集其僱員個人資料作行政管理之目的相同，符合《個人資料保護法》第5條第1款(二)項的規定，對僱員資料處理沒有偏離有關目的。

就“個人資料互聯”的建立不能導致歧視或削減資料當事人的權利、自由及保障方面。A公司與母公司“互聯”處理僱員資料，主要是基於集團對所屬成員之僱員進行全球性人力資源管理需要，為集團旗下僱員提供平等的培訓和晉升機會，有關的資料處理方式不存在歧視當事人的權利、自由和保障。

關於A公司以“互聯”方式轉移僱員資料予位於美國母公司的“全球人力資源資訊系統”之資料處理的安全措施方面。根據A公司根據的資料，“全球人力資源資訊系統”的伺服器由母公司負責管理，系統內資料的存取及傳遞都經由集團之內聯網系統進行，而非透過互聯網。母公司有本身之資訊安全系統，並有採取適當的技術及組織措施確保個人資料處理的機密性、完整性和有效使用性，防止資料遭受意外及非法的破壞或意外遺失、變更、未獲許可之披露或獲取，以及阻止使用其他不法之處理。資訊安全系統主要設有存取權限控制(Access Controls)、保安事故應對程序(Security Incident Procedures)及審計追蹤(Audit Controls)等措施，具體包括：對系統用戶進行身份驗證，並設定相適應的存取權限；培訓員工遵守及履行資訊安全政策；偵測任何對系統的潛在和實質入侵或攻擊，並作出處理，以減低保安事故所產生的影響；對於緊急的偶發事故（如自然災害、系統故障等），設有資料備份及意外復原計劃；檢測資訊系統的活動，並記錄成日誌及報告。另外，A公司與母公司就僱員資料的處理，簽定了資料保護協議(Data Protection Agreement)，規範對方履行個人資料保護義務。



綜上所述，本辦公室根據《個人資料保護法》第9條及第22條1款(三)項的規定，許可A公司與美國母公司基於上述所指的目的，且在保障資料安全處理及不削減當事人權利的情況下，與美國母公司之“全球人力資源資訊系統”“互聯”處理僱員資料。

主任

陳海帆

2009年7月2日

Autorização n.º 05/A/2009/GPDP

Tradução

Assunto: Pedido da empresa A relativo à transferência, via interconexão, de dados pessoais dos seus funcionários para o Sistema informático de recursos humanos globais, instalado na sede da empresa, nos EUA

A empresa A solicitou, ao GPDP, autorização de “interconexão de dados pessoais” para transferir, via “interconexão”, os dados pessoais dos seus funcionários para o Sistema informático de recursos humanos globais, instalado na sede da empresa, nos EUA.

Os dados dos funcionários que a empresa A pediu para transferir, através de “interconexão”, para a sede nos EUA incluem: nome, morada, número e cópia do documento de identidade, idade/data de nascimento, sexo, nacionalidade, estado civil, nomes dos filhos, fotografia, contactos, rendimento, informações de gestão relacionadas com os benefícios e subsídios, dados de identidade dos beneficiários e elementos do agregado familiar, contacto em caso de acidentes ou emergência, curriculum vitae, habilitação e formação profissional, competência e nível linguísticos, informações relativas ao salário e às actividades profissionais, número do contribuinte, informações sobre as despesas gastas por funcionários com o cartão de crédito da empresa, informações sobre veículos da empresa, informações sobre seguros médicos, registo de assiduidades, formação e avaliação do desempenho no emprego, informação sobre profissão e desenvolvimento pessoal, plano do desenvolvimento pessoal contínuo e informações da segurança interna em relação a entradas e saídas e respectivas autorizações.

Nos termos da alínea 1) do n.º 1 do artigo 4.º da Lei n.º 8/2005, Lei da Protecção de Dados Pessoais, os dados pessoais referem-se a qualquer informação relativa a uma pessoa singular identificada ou identificável, incluindo som e imagem, pelo que as informações sobre as despesas gastas por funcionários com o cartão de crédito da empresa e sobre veículos da empresa, acima referidas, são dados que identificam a empresa, não sendo os dados pessoais dos funcionários. Os outros dados, excepto as duas categorias das informações referidas, são os relativos aos funcionários identificados, estando, no âmbito do artigo 3.º da Lei da Protecção de Dados Pessoais, o tratamento dos mesmos sujeito a esta lei.

De acordo com o estipulado na alínea 10) do n.º 1 do artigo 4.º da Lei da Protecção de Dados Pessoais, a “interconexão de dados é uma forma de tratamento que consiste na possibilidade de relacionamento dos dados de um ficheiro com os dados de um ficheiro ou ficheiros mantidos por outro ou outros responsáveis, ou mantidos pelo mesmo responsável com outra finalidade”. A empresa A, como um dos membros do grupo internacional, sediado nos EUA, estabeleceu o relacionamento de tratamento de dados com o servidor da sede nos EUA e pretende transferir, através da intranet do grupo, os dados pessoais dos seus funcionários para o Sistema informático de recursos humanos globais, ali instalado, a fim de facilitar o acesso aos dados de todos os funcionários do grupo, ou de terceiros que necessitem consultá-los no decurso do processo normal dos negócios da empresa. Tal forma de tratamento permite relacionar o ficheiro de dados pessoais dos funcionários da empresa A com o da sua sede nos EUA, instalado no Sistema informático de recursos humanos globais, o que configura a “interconexão de dados pessoais” sujeita à lei acima referida.



Segundo o previsto no artigo 22.º da Lei da Protecção de Dados Pessoais, a “interconexão de dados”, como a forma de tratamento de dados pessoais sob o controlo prévio, está sujeita à autorização do GPDP. O artigo 9.º da mesma lei estipula que a interconexão de dados pessoais que não esteja prevista em disposição legal ou disposição regulamentar de natureza orgânica está sujeita a autorização do GPDP, solicitada pelo responsável ou em conjunto pelos correspondentes responsáveis pelo tratamento, nos termos previstos no n.º 1 do artigo 22.º. O n.º 2 do mesmo artigo estipula que a interconexão de dados pessoais deve ser adequada à prossecução das finalidades legais ou estatutárias e de interesses legítimos dos responsáveis pelo tratamento, não implicando, contudo, discriminação ou diminuição dos direitos, liberdades e garantias dos titulares dos dados; devendo ser rodeada de adequadas medidas de segurança e ter em conta o tipo de dados objecto de interconexão.

Segundo as informações fornecidas pela empresa A, a transferência, via interconexão, dos dados pessoais de todos os funcionários para o Sistema informático de recursos humanos globais, da sede da empresa nos EUA, tem como objectivo principal facilitar a gestão centralizada de todos os recursos humanos por parte do departamento dos recursos humanos internacionais do grupo, a fim de uniformizar as políticas e garantir que todos os seus funcionários tenham iguais oportunidades de formação e promoção. Isto é, a “interconexão”, a estabelecer por parte da empresa A, baseada na necessidade da gestão dos recursos humanos globais da sede da empresa, corresponde aos interesses legítimos da empresa A no tratamento de dados dos seus funcionários. A forma do tratamento de dados pessoais da empresa A, por meio da “interconexão de dados pessoais” com a sua sede, com vista à gestão administrativa dos recursos humanos globais, é, também, adequada à finalidade de recolha de dados pessoais dos seus funcionários para a gestão administrativa, sendo compatível com a finalidade do tratamento de dados dos seus funcionários, prevista no 2) do n.º 1 do artigo 5.º da Lei da Protecção de Dados Pessoais.

No aspecto de que a interconexão não deverá implicar a discriminação ou diminuição dos direitos, liberdades e garantias dos titulares dos dados, a empresa A e a sua sede efectuem, via “interconexão”, o tratamento de dados dos funcionários com vista a responder à necessidade da gestão dos recursos humanos globais e proporcionar aos seus funcionários iguais oportunidades de formação e promoção, pelo que a referida forma do tratamento de dados não implica a discriminação dos direitos, liberdades e garantias dos titulares dos mesmos.

No que respeita às medidas de segurança do tratamento de dados pessoais a serem transferidos, via “interconexão”, pela empresa A, ao Sistema informático de recursos humanos globais da sua sede nos EUA, segundo as informações prestadas pela empresa A, a gestão do servidor do Sistema informático de recursos humanos globais é da responsabilidade da sede, sendo a captação e conservação dos dados do sistema feitas via intranet do grupo, mas não via Internet. A sede dispõe de sistema de segurança informática e aplica medidas técnicas e organizativas adequadas para assegurar a confidencialidade, integridade e eficiência do tratamento dos dados e prevenir a destruição, acidental ou ilícita, a perda acidental, a rectificação, a divulgação ou o acesso não autorizados, bem como qualquer outro tipo de tratamento ilícito. A segurança do sistema informático é garantida, nomeadamente, através do controlo do acesso, procedimento contra incidentes de segurança e controlo de auditoria, entre outras, incluindo, designadamente: verificação do nome do utilizador do sistema e os respectivos limites de captação e conservação; formação dos funcionários para observação e cumprimento das políticas de segurança informática; detecção e reacção a acessos ilegais ou ataques, prováveis e reais, ao sistema, a fim de minimizar o impacto

resultante de incidentes de segurança; capacidade de disponibilizar, no caso de incidentes tais como calamidades naturais ou obstáculos do sistema, urgentes e acidentais, a cópia dos dados e planos de recuperação dos mesmos; vigilância das actividades do sistema dos dados, a serem registadas no diário e relatório. Além disso, a empresa A e a sua sede assinaram o Acordo de Protecção de Dados que regula os deveres da protecção de dados pessoais a cumprir por ambas as partes.

Pelo exposto, o GPDP autoriza, no âmbito do artigo 9.º e da alínea 3) do n.º 1 do artigo 22.º da Lei da Protecção de Dados Pessoais, a empresa A e a sua sede nos EUA a estabelecerem, com o objectivo referido e sob a condição de garantir a segurança do tratamento dos dados e não implicar a diminuição dos direitos dos seus titulares, a interconexão com o Sistema informático de recursos humanos globais para efectuar o tratamento dos dados dos funcionários.

Aos 2 de Julho de 2009

A Coordenadora
Chan Hoi Fan



第06/A/2009/GPDP號許可

事由：A銀行（設於澳門的分行）申請與B銀行（設於中國上海的總行）“互聯”處理其客戶及僱員資料

A銀行就以專線方式傳送客戶及僱員資料予B銀行一事，向本辦公室申請“個人資料互聯”許可。

A銀行申請與B銀行“互聯”處理客戶及僱員個人資料，其中客戶資料包括：身份證明文件號碼、姓名、年齡/出生日期、性別、國籍、聯絡方法、銀行帳戶號碼及交易資料¹。而具體的僱員資料則包括：身份證明文件號碼、姓名、年齡/出生日期、性別、國籍及學歷。根據第8/2005號法律（《個人資料保護法》）第4條第1款(一)項規定，上述資料屬與身份已確定客戶及僱員相關的資訊，為個人資料範疇，根據同一法律第3條規定，對客戶及僱員個人資料的處理受該法律規範。

根據《個人資料保護法》第4條第1款(十)項規定：“資料的互聯是指一個資料庫的資料與其他一個或多個負責實體的一個或多個資料庫的資料的聯繫、或同一負責實體但目的不同的資料庫的資料聯繫的處理方式。”A銀行以專線方式將客戶及僱員的個人資料轉移至B銀行之電腦伺服器，由設於B銀行的數據中心及災備中心負責對該等資料進行管理、存儲及備份等，有關的處理方式令A銀行之客戶及僱員資料庫與B銀行相關的資料庫建立聯繫，屬上述法律規定之“個人資料互聯”。

根據《個人資料保護法》第22條規定，“資料的互聯”屬須預先監控的處理個人資料方式，須經本辦公室許可。其中同一法律第9條第1款規定：法律規定或具組織性質的規章性規定未規定的個人資料的互聯，須由負責處理個人資料實體或與其共同負責的實體根據第22條第1款的規定向本辦公室提出申請並取得許可。同條第2款規定：個人資料的互聯應符合法律或章程規定的目的和負責處理個人資料的實體的正當利益；不得導致歧視或削減資料當事人的權利、自由和保障；須有適當的安全措施；考慮需互聯的資料的種類。

A銀行是B銀行在澳門特別行政區設立之分行。根據A銀行提供的資料，A銀行向B銀行提供僱員資料的目的是基於人力資源管理需要，以便由總行記錄分行的人力資源狀況。向B銀行提供客戶資料則基於總行對分行之業務管理及內部控制管理需要，因B銀行之稽核部會按需要定期抽取A銀行之客戶資料/數據進

¹ 交易資料是指客戶所進行交易的金額、日期、賬戶結餘等電子數據。

行審查。故A銀行透過“互聯”方式將有關僱員及客戶資料轉移到設於B銀行之電腦伺服器系統，以便於總行根據上述目的使用有關的資料。且根據第32/93/M號法令（《金融體系法律制度》）第79條第1款d)項規定“信用機構為減少風險及增加經營活動之安全而組織相互提供資訊系統之可能性”，屬於銀行保密義務的例外情況。故A銀行與B銀行“互聯”處理客戶的資料數據，有助總行集中管理集團銀行業務，屬經營正當銀行業務而使用有關的資訊系統，符合上述法令的規定。換言之，B銀行基於業務及人力資源管理需要之目的，以“互聯”方式處理A銀行的客戶及僱員資料，有關的處理方式符合A銀行的正當利益。而就客戶及僱員資料以“互聯”方式處理亦符合《個人資料保護法》第5條第1款(二)項規定，沒有偏離A銀行收集相關資料的目的。

關於建立“個人資料互聯”不得導致歧視或削減資料當事人的權利、自由和保障方面。A銀行以“互聯”方式轉移客戶及僱員資料予B銀行，目的在於使總行有效地集中管理集團客戶資料以及記錄分行人力資源狀況，有關“個人資料互聯”的建立與A銀行處理其客戶及僱員資料的目的相符，在資料處理方面不存在歧視當事人的權利。

關於A銀行以“互聯”方式轉移客戶及僱員的個人資料予B銀行須有的適當安全措施方面。根據A銀行提供的資料，其透過專線與B銀行直接進行資料傳遞，資料之傳送並經加密碼處理，保障傳遞過程中資料的安全性及機密性，以阻外界不法入侵。負責管理及儲存A銀行資料的總行數據中心，系統設有適當的技術及組織措施保障資料處理的保密性、準確性及完整性，分別包括：操作員及受權人員須輸入密碼才能開系統，且密碼由另一獨立系統分開管理；系統操作員所作的任一操作結果需交予覆核人員檢查，故使用及備份資料都需由兩個或以上人員利用密碼控制完成；A銀行定期從數據中心系統抽取客戶交易資料進行核對，保證數據庫資料的準確及完整性；除攝錄監控外，數據中心並裝置了嚴密程度不同的門禁系統，嚴格控制進出入情況等。B銀行並設有災備中心，制定出一系列災難備份措施，以保障數據中心業務運作的持續性。

綜上所述，本辦公室根據《個人資料保護法》第9條及第22條1款(三)項的規定，許可A銀行與B銀行基於上述所指的目的，且在保障資料安全處理及不削減當事人的權利的情況下，“互聯”處理客戶及僱員資料。

主任

陳海帆

2009年7月24日



Autorização n.º 06/A/2009/GPDP

Tradução

Assunto: Pedido do Banco A (sucursal em Macau) relativo ao tratamento, via “interconexão” com o Banco B (sede situada em Xangai), de dados dos seus clientes e funcionários.

O Banco A solicitou ao GPDP autorização de “interconexão de dados pessoais” para transferir, por cabos electrónicos exclusivos, os dados dos seus clientes e funcionários ao Banco B.

O pedido do Banco A para o tratamento, via “interconexão” com o Banco B, dos dados dos seus clientes e funcionários, dos quais, os dos clientes incluem: número do documento de identidade, nome, idade/data de nascimento, sexo, nacionalidade, contactos, número de conta bancária e dados das transacções bancárias, enquanto que os dos funcionários são, designadamente: número do documento de identidade, nome, idade/data de nascimento, sexo, nacionalidade e habilitações académicas. Segundo o estipulado na alínea 1) do n.º 1 do artigo 4.º da Lei n.º 8/2005 (Lei da Protecção de Dados Pessoais) os dados acima referidos são dados relativos a clientes e funcionários identificados, considerando-se, por isso, dados pessoais. Assim sendo, e de acordo com o artigo 3.º da mesma lei, o tratamento dos dados pessoais dos clientes e funcionários está sujeito à Lei da Protecção de Dados Pessoais.

O artigo 4.º da Lei da Protecção de Dados Pessoais estipula, na alínea 10) do n.º 1, que a “interconexão de dados” é uma “forma de tratamento que consiste na possibilidade de relacionamento dos dados de um ficheiro com os dados de um ficheiro ou ficheiros mantidos por outro ou outros responsáveis, ou mantidos pelo mesmo responsável com outra finalidade”. O Banco A efectua, por cabos electrónicos exclusivos, a transferência de dados pessoais dos seus clientes e funcionários ao servidor do Banco B, para que os centros de dados e de prevenção de contingências deste Banco possam proceder à gestão, conservação e cópia dos dados referidos, pelo que o relacionamento a estabelecer entre o ficheiro dos clientes e funcionários do Banco A e o do Banco B configura “interconexão de dados pessoais”, definida e regulada pela lei acima citada.

De acordo com o estipulado no artigo 22.º da Lei da Protecção de Dados Pessoais, a “interconexão de dados”, como forma de tratamento de dados pessoais sob o controlo prévio, está sujeita à autorização do GPDP. De acordo com o n.º 1 do artigo 9.º da mesma lei, a interconexão de dados pessoais que não esteja prevista em disposição legal ou disposição regulamentar de natureza orgânica está sujeita à autorização do GPDP, solicitada pelo responsável ou em conjunto pelos correspondentes responsáveis dos tratamentos, nos termos previstos no n.º 1 do artigo 22.º. O n.º 2 do mesmo artigo estipula que a interconexão de dados pessoais deve ser adequada à prossecução das finalidades legais ou estatutárias e de interesses legítimos dos responsáveis dos tratamentos; não devendo implicar a discriminação ou diminuição dos direitos, liberdades e garantias dos titulares dos dados; devendo ser rodeada de adequadas medidas de segurança; e ter em conta o tipo de dados objecto de interconexão.

O Banco A é sucursal do Banco B instalada na Região Administrativa Especial de Macau. O Banco A, segundo as informações por este prestadas, disponibiliza, devido à necessidade de gestão de recursos humanos, os dados dos seus funcionários ao Banco B para este poder registar os recursos humanos da respectiva sucursal, enquanto a disponibilidade de dados dos seus clientes ao Banco B é requerida pela gestão dos negócios bancários e pelo controlo interno, já que o Departamento de Inspeção do Banco B toma, periodicamente, dados dos clientes do Banco A para verificação. O Banco A efectua, via “interconexão”, a transferência dos dados dos seus funcionários e clientes ao servidor do Banco B para que este possa utilizá-los para o objectivo referido. Além disso, o estipulado na alínea d) do n.º 1 do artigo 79.º do Decreto-Lei n.º 32/93/M (Regime Jurídico do Sistema Financeiro) consigna: “A possibilidade de as instituições de crédito organizarem um sistema de informações recíprocas, com o fim de reduzir o risco e aumentar a segurança das operações”, constituindo os casos excepcionais quebra do sigilo bancário, pelo que a “interconexão” entre o Banco A e o Banco B, para o tratamento de dados dos clientes com recurso ao sistema informático, é resultante da necessidade da gestão centralizada do grupo bancário e dos seus negócios legítimos, estando a mesma prevista nas disposições legais acima referidas. Isto quer dizer que o Banco B efectua, através de “interconexão”, o tratamento de dados dos clientes e funcionários do Banco A devido à necessidade dos seus negócios bancários e da gestão dos recursos humanos, pelo que o tratamento de dados dos clientes e funcionários, via “interconexão”, é considerada necessária aos interesses legítimos do Banco A e compatível com a finalidade de recolha dos mesmos pelo Banco A, prevista no 2) do n.º 1 do artigo 5.º da Lei da Protecção de Dados Pessoais.

Em relação à discriminação ou diminuição dos direitos, liberdades e garantias dos titulares de dados, resultantes do estabelecimento de “interconexão de dados pessoais”, o Banco A efectua, via interconexão, a transferência de dados dos clientes e funcionários ao Banco B, com vista à centralização da gestão dos clientes e ao registo dos recursos humanos da sucursal do grupo bancário, sendo o estabelecimento de “interconexão de dados pessoais” compatível com a finalidade do tratamento de dados dos clientes e funcionários do Banco A, não implicando o tratamento dos referidos dados a discriminação dos direitos dos titulares dos mesmos.

Quanto às adequadas medidas de segurança requeridas pela transferência, via “interconexão”, de dados pessoais dos clientes e funcionários do Banco A para o Banco B as informações prestadas pelo Banco A indicam que os dados serão directamente transferidos, através de cabos electrónicos exclusivos, ao Banco B, estando a transferência sob o controlo de medidas de protecção a fim de assegurar a segurança e a confidencialidade dos dados durante o processo da transferência e prevenir o acesso ilegal. O sistema do centro de dados da sede, responsável pela gestão e conservação de dados do Banco A, dispõe de apropriadas medidas técnicas e orgânicas que asseguram a confidencialidade, precisão e integridade do tratamento de dados, incluindo, designadamente: os operadores e os indivíduos autorizados só podem ter acesso ao sistema depois de inserir os respectivos códigos, que são geridos por outro sistema independente; os resultados de qualquer operação a efectuar pelos operadores serão inspeccionados por outro verificador, pelo que o acesso e a cópia dos dados serão feitas por dois ou mais funcionários e através de códigos; o Banco A toma, periodicamente, dados do sistema do centro de dados para a verificação a fim de assegurar a precisão e a integridade dos dados do ficheiro; para além de videovigilância, o



centro de dados está protegido pelo sistema de segurança, a diferentes níveis, para o controlo rigoroso de entradas e saídas. O Banco B dispõe ainda do centro de prevenção de contingências e de respectivas medidas para as enfrentar com vista a garantir a continuidade do funcionamento do centro de dados.

Pelo exposto, o GPDP autoriza, no âmbito do artigo 9.º e da alínea 3) do n.º 1 do artigo 22.º da Lei da Protecção de Dados Pessoais, o Banco A a estabelecer, com o objectivo referido e sob a condição de garantir a segurança do tratamento dos dados e não implicar a diminuição dos direitos dos seus titulares, a “interconexão”, com o Banco B, para efectuar o tratamento de dados dos clientes e funcionários.

Aos 24 de Julho de 2009

A Coordenadora
Chan Hoi Fan

第07/A/2009/GPDP號許可

事由：關於勞工事務局申請與治安警察局、財政局及人力資源辦公室“互聯”處理其“職業介紹所查詢網頁”系統資料

勞工事務局就以“互聯”方式向治安警察局、財政局及人力資源辦公室提供其“職業介紹所查詢網頁”系統資料一事，向本辦公室申請“個人資料互聯”許可。

根據勞工事務局提供的資料，治安警察局、財政局及人力資源辦公室以“互聯”方式處理其“職業介紹所查詢網頁”系統資料包括：“職業介紹所行政執照持有人（倘屬法人或社團，則其經理、行政管理機關成員或領導人）的身份識別資料（自然人的證件及法人的商業登記證明掃描本）、執照上所載的資料（包括：執照編號、持牌姓名、持有證件類別及編號、執照生效及有效期、場所名稱、場所地址及特別條件）及財政局發出之M/1格式開業 / 更改申報表。”

而根據勞工事務局所提供的“職業介紹所查詢網頁”系統介面資料顯示，透過在該系統輸入職業介紹所的行政執照編號、成員姓名、電話、場所名稱、批示期間，可搜尋並查詢到符合要求的職業介紹所資料，包括識別資料及成員資料，識別資料有行政執照編號、執照類型、執照是否屬個人擁有、財政局檔案編號、首次申辦日期、首次批示日期、首次批准年份、首次簽發日期、有效日期、場所名稱、持有公司名稱、場所地址、電話、傳真、提供服務、勞工來源地及申請相關資料（申請日期、批示日期、申辦日期/局方取消、結果及商業登記文件檔）；成員資料則有名稱、證件類型、證件編號、是否股東、行政機關成員、職稱。而存於系統內之“商業登記文件檔”包括：職業介紹所行政執照掃描本¹、商業登記證明掃描本、營業稅一開業 / 更改申報表M/1格式掃描本、身份證明文件掃描本。

根據第8/2005號法律（《個人資料保護法》）第4條第1款（一）項之規定：“個人資料是指與某個身份已確定或身份可確定的自然人有關的任何資訊，包括聲音和影像，不管其性質如何或是否擁有載體”。“職業介紹所查詢網頁”系統內載有的職業介紹所識別資料及相關之行政執照掃描本，顧名思義是用作識別職業介紹所的身份，不屬於個人資料。另外，由於職業介紹所行政執照之申請人可為自然人、公

¹ 職業介紹所行政執照載有的資料包括：執照編號、執照持有人(包括公司、社團或自然人)資料、自然人執照持有人之身份證明文件類別及編號獲許可從事之服務、執照有效日期、場所名稱、場所地址、營業時間、特別條件及執照發出日期。

司或社團（見第32/94/M號法令第6條規定），當執照申請人為公司或社團時，其商業登記資料以及營業稅一開業 / 更改申報表M/1格式屬於公司及社團資料，非用作識別自然人的身份。因此，勞工事務局之“職業介紹所查詢網頁”系統以下的資料類別：職業介紹所的識別資料、職業介紹所行政執照掃描本、商業登記資料、營業稅一開業 / 更改申報表M/1格式資料（納稅人為公司或社團時），並不屬於自然人的個人資料，不適用《個人資料保護法》。

除上述資料類別以外，其餘的“職業介紹所查詢網頁”系統資料，具體包括：職業介紹所行政執照的持有人（自然人）的姓名、證件類型及號碼、身份證明文件掃描本及營業稅一開業 / 更改申報表M/1格式掃描本，且包括職業介紹所行政執照由公司或社團持有時其代表人（經理、行政管理機關成員或領導人）的姓名、證件類型及號碼、身份證明文件掃描本。需適當說明的是，營業稅一開業 / 更改申報表M/1格式載有納稅人的識別資料，由於納稅人包括自然人及公司，如上段所述，公司或社團納稅人所申報的營業稅一開業 / 更改申報表M/1格式屬於其公司或社團資料，非屬個人資料，因此只有在自然人為其經營之職業介紹所申報營業稅一開業 / 更改申報表M/1格式，申報表上所載的自然人納稅人資料（包括納稅人編號、姓名、身份證明文件類型及編號、地址及聯絡電話），才屬於個人資料。故此，上述資料均與身份已確定的人士相關，符合《個人資料保護法》第4條第1款第(一)項規定之個人資料定義。根據《個人資料保護法》第3條規定，對有關個人資料之處理受該法律所規範。

根據《個人資料保護法》第4條第1款(十)項規定：“資料的互聯是指一個資料庫的資料與其他一個或多個負責實體的一個或多個資料庫的資料的聯繫、或同一負責實體但目的不同的資料庫的資料聯繫的處理方式。”治安警察局、財政局及人力資源辦公室透過行政暨公職局的Informac網絡連接勞工事務局之“職業介紹所查詢網頁”系統，實時查詢及取得該系統內職業介紹所行政執照持有人或持有機構的代表人的個人資料，令上述實體之間的資料庫建立了資料聯繫，屬上述法律定義的“個人資料互聯”處理方式。

根據《個人資料保護法》第22條規定，“資料的互聯”屬須預先監控的處理個人資料方式，須經本辦公室許可。其中同一法律第9條第1款規定：法律規定或具組織性質的規章性規定未規定的個人資料的互聯，須由負責處理個人資料實體或與其共同負責的實體根據第22條第1款的規定向本辦公室提出申請並取得許可。同條第2款規定：個人資料的互聯應符合法律或章程規定的目的和負責處理個人資料的實體的正當利益；不得導致歧視或削減資料當事人的權利、自由和保障；須有適當的安全措施；考慮需互聯的資料的種類。

根據勞工事務局提供的資料，其開放“職業介紹所查詢網頁”系統資料予治安警察局、財政局及人力資源辦公室使用，目的是：“根據第32/94/M號法令的規定，勞工事務局應將批准、修改或取消職業介紹所執照情況通知財政局及治安警察局，以及協助人力資源辦公室處理職業介紹所招聘及安排外地勞工工作的申請。”

關於治安警察局、財政局及人力資源辦公室是否具權限查閱及取得勞工事務局之“職業介紹所查詢網頁”系統資料，可考慮如下相關法規之規定：

- 根據第32/94/M號法令（《核准發出准照予職業介紹所之制度》）第2條規定，接受就業之提供、為求職人登錄、甄選人員、安排工作及招聘外地勞工為職業介紹所提供的業務範圍。根據同一法令第9、10及12條規定，職業介紹所執照之批給、續期、換發、修改及取消，屬勞工事務局局長之權限。其中第13條規定，勞工事務局應將與執照有關之通知，包括批准執照之請求、修改執照及取消執照通知財政局及治安警察局。
- 根據第22/2001號行政法規（《治安警察局的組織與運作》）第30條規定，治安警察局出入境事務廳依法發出外地勞工身分辨別證，使之續期或取消。根據第12/GM/88號批示第9條及第49/GM/88號批示第2條分別規定，人力資源辦公室對輸入外地勞工之申請作出許可批示後，須將卷宗送交治安警察局，以便該局決定是否許可名單中之勞工進入本地區並在本地區逗留。外地勞工在獲治安警察局發出身分辨別證（即“非本地勞工身份咭”）後，才可在本地區合法工作。
- 根據第30/99/M號法令（《訂定財政局新組織法》）第2條規定，財政局其中的職責包括：進行本地區之稅務管理，促進其與稅務法律之配合，執行稅務政策及在稅務及公共財政方面進行監察。故財政局具職責執行第15/77/M號法律核准之《營業稅章程》之相關規定，其中包括依照《營業稅章程》附表I規定的固定稅額徵收營業稅（見第4條規定），以及備有一本營業稅納稅人之登記冊，以記錄有關納稅人及其業務之資料，登記冊應載明認別納稅人及其業務所需之資料，以及載明與計算及結算營業稅有關之資料（見第19條規定）。為使財政局具條件履行《營業稅章程》規定之職責義務，《營業稅章程》第8條規定，凡擬從事任何工商業活動，最低限度在開業的可能日期三十天前，須由本人或其受權人向財政局遞交M/1格式申報書；且第32條規定，各公共機構均應與財政局合作以執行《營業稅章程》，尤其是有權限發出經濟活動准照之



實體機構，應將獲發准照之自然人或法人之身份資料告知財政局。

- 根據第116/2007號行政長官批示第3條至第5條規定，人力資源辦公室的職責為對澳門特別行政區勞動市場人力資源的變化作持續分析，以及執行處理聘用外地勞工申請的行政工作，人力資源辦公室為履行獲賦予的職責，可要求任何公共或私人實體，尤其是勞工事務局及社會保障基金提供審批聘用外地勞工的申請所需的資料。而人力資源辦公室根據第12/GM/88號批示之規定處理申請輸入外地勞工之行政手續，須審核提供外地勞動力的職業介紹所與輸入外地勞工之本澳企業訂立旨在使外地勞工在本澳工作的提供勞務合同（見第12/GM/88號批示第3條、第7條及第9條規定），當中涉及對職業介紹所所有否輸入外地勞動力資格的確認。

根據上述法律規定，治安警察局、財政局及人力資源辦公室處理勞工事務局之“職業介紹所查詢網頁”系統資料，為履行其法定職責所需，符合《個人資料保護法》第6條第(四)項規定的正當性條件，屬履行具公共利益的任務及行使公共當局的權力。

至於有關“個人資料互聯”處理方式是否符合相關法律所規定的目的和負責處理個人資料的實體的正當利益。根據第32/94/M號法令第13條及第116/2007號行政長官批示第五條規定，勞工事務局有義務與治安警察局、財政局及人力資源辦公室合作，向該等機關提供與其履行職責所需的“職業介紹所執照資料”，屬履行法律規定之義務，故“個人資料的互聯”處理並沒有偏離勞工事務局根據《個人資料保護法》第5條1款(二)項規定收集職業介紹所相關個人資料的目的，亦符合勞工事務局處理資料之正當利益。

關於“互聯”不得導致歧視或削減資料當事人的權利、自由及保障方面。勞工事務局透過“互聯”方式向治安警察局、財政局及人力資源辦公室提供“職業介紹所查詢網頁”系統資料，目的是履行法律規定之通告資料義務，而透過“互聯”方式能即時提供已更新的職業介紹所執照資料予上述部門，以加快行政手續之審批，不存在歧視當事人權利。

就“互聯”須有適當的安全措施方面，勞工事務局透過政府內部網絡Informac與治安警察局、財政局及人力資源辦公室“互聯”處理“職業介紹所查詢網頁”系統，根據行政暨公職局提供的資料，Informac網絡屬封閉式網絡，供各公共部門連接對方部門的系統或服務，連接Informac網絡系統的主要方式是以光纖專線、DDN專線及VPN登入。此外，根據勞工事務局提供的資料，登入“職業介紹所查詢網

頁”系統須輸入用戶名稱及密碼，並設定相應之存取權限；該局亦會對登入該系統的人員進行記錄，以及在儲存資料的位置進行上鎖。

綜上所述，本辦公室根據《個人資料保護法》第9條及第22條第1款第(三)項的規定，許可勞工事務局與治安警察局、財政局及人力資源辦公室基於上述所指的目的，且在保障資料安全處理及不削減當事人權利的情況下，“互聯”處理“職業介紹所查詢網頁”系統資料。

主任

陳海帆

2009年9月18日

Autorização n.º 07/A/2009/GPDP

Tradução

Assunto: Pedido da Direcção dos Serviços para os Assuntos Laborais (DSAL), relativo ao tratamento, por meio de “interconexão”, de dados contidos no seu sistema “website de consultas das agências de emprego”, junto da Polícia de Segurança Pública (PSP), da Direcção dos Serviços de Finanças (DSF) e do Gabinete para os Recursos Humanos (GRH)

A DSAL solicitou, ao GPDP, autorização de “interconexão de dados pessoais” para poder disponibilizar, via “interconexão”, os dados contidos no seu sistema “website de consultas das agências de emprego” à PSP, DSF e GRH.

Segundo as informações prestadas pela DSAL, os dados do seu sistema “website de consultas das agências de emprego” a serem tratados, via “interconexão”, pela PSP, DSF e GRH, compreendem: dados da identidade (documentos digitalizados de identidade de pessoa singular e de matrícula comercial de pessoa colectiva) do titular da licença administrativa de agência de emprego (do gerente, dos membros ou dos dirigentes do órgão de administração no caso de ser pessoa colectiva ou associação), dados registados no licenciamento que incluem: número da licença, nome do titular, tipo e número do documento, início e termo do prazo do licenciamento, nome e localização de agência e outras condições especiais) bem como a Declaração de Início de Actividade/Alterações (M/1), emitida pela DSF.

Os dados de interface do sistema “website de consultas das agências de emprego”, prestados pela DSAL, mostram que, com a introdução no sistema do número da licença administrativa, nome de membros, telefone, nome da localidade, prazo de licenciamento de determinada agência de emprego, se podem encontrar os dados da agência, incluindo os da respectiva identificação bem como dos seus membros. Os dados de identificação incluem número da licença administrativa, tipo da licença e se for individual o seu titular, número de cadastro na DSF, data do primeiro pedido, data do primeiro parecer, ano da primeira autorização, data da primeira emissão, data do prazo, nome da localidade, nome da companhia titular, endereço da localidade, números de telefone e de fax, serviços a prestar, país ou território de origem dos trabalhadores a recrutar bem como outros dados relativos ao pedido (data de pedido, data de parecer, data de pedido/cancelamento pela DSAL, resultados e documentos de matrícula comercial), enquanto os dados dos membros compreendem: nome, tipo do documento, número do documento, qualidade de se ser accionista ou membro do órgão de administração e funções. Os documentos de matrícula comercial, contidos no sistema, incluem cópia digitalizada da licença administrativa de agência de emprego¹, cópia digitalizada da matrícula comercial, cópia digitalizada da Contribuição Industrial – Declaração de Início de Actividade/Alterações (M/1) bem como a cópia digitalizada do documento de identidade.

1. Os dados contidos na licença administrativa de agência de emprego incluem: número da licença, dados do titular (sociedade, associação ou pessoa singular) da licença, tipo e número do documento de identidade do titular (pessoa singular) da licença, serviços autorizados, data de validade da licença, nome da localidade, endereços da localidade, horários de serviços, condições especial e data de emissão da licença.

O artigo 4.º da Lei n.º 8/2005 (Lei da Protecção de Dados Pessoais) estipula, na alínea 1) do n.º 1, que os “dados pessoais” compreendem “qualquer informação, de qualquer natureza e independentemente do respectivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável.” Os dados de identificação de agências de emprego e as cópias digitalizadas das respectivas licenças, contidos no sistema “*website* de consultas das agências de emprego”, são, obviamente, os dados para identificar as agência de emprego, não se considerando, portanto, dados pessoais. Além disso, o requerente de licença administrativa de agência de emprego pode ser uma pessoa singular, uma sociedade ou uma associação (vide o artigo 6.º do Decreto-Lei n.º 32/94/M), pelo que, quando o requerente for uma sociedade ou uma associação, os seus dados de matrícula comercial e a Contribuição Industrial — Declaração de Início de Actividade/Alterações (M/1) são considerados como dados de uma sociedade ou uma associação, não servindo para identificar uma pessoa singular. Por isso, os dados contidos no sistema “*website* de consultas das agências de emprego” da DSAL, a saber: dados de identificação das agências de emprego, cópias digitalizadas da licença administrativa, dados de matrícula comercial, dados da Contribuição Industrial — Declaração de Início de Actividade/Alterações (M/1) (quando o contribuinte for uma sociedade ou uma associação) das agências de emprego, não são dados pessoais de pessoas singulares, não estando, portanto, sujeitos à Lei da Protecção de Dados Pessoais.

São considerados dados pessoais os restantes dados encontrados no sistema “*website* de consultas das agências de emprego”, designadamente: nome, tipo e número do documento, cópia digitalizada do documento de identidade e cópia digitalizada da Contribuição Industrial — Declaração de Início de Actividade /Alterações (M/1) do titular de agência de emprego (pessoa singular), nome, tipo e número do documento e cópia digitalizada do documento de identidade do representante (gerente, membro ou responsável do órgão de administração quando o titular da licença de agência de emprego for uma sociedade ou associação). É ainda de salientar que o contribuinte indicado na Contribuição Industrial — Declaração de Início de Actividade /Alterações (M/1), que contém dados de identificação do mesmo, pode ser pessoa singular ou colectiva. Quando o contribuinte for uma sociedade ou associação os dados contidos na Contribuição Industrial — Declaração de Início de Actividade /Alterações (M/1) não são dados pessoais, são, como o acima referido, dados de sociedade ou associação. Quando o contribuinte for pessoa singular, os dados constantes da Contribuição Industrial — Declaração de Início de Actividade /Alterações (M/1), a saber: número e nome de contribuinte, tipo e número do documento de identidade, morada e telefone, são, no âmbito da alínea 1) do n.º1 do artigo 4.º da Lei da Protecção de Dados Pessoais, dados pessoais relativos a pessoas identificadas, pelo que, o seu tratamento está sujeito a mesma Lei, de acordo com o seu artigo 3.º.

De acordo com a alínea 10) do n.º 1 do artigo 4.º da Lei da Protecção de Dados Pessoais “a “interconexão de dados refere-se a uma forma de tratamento que consiste na possibilidade de relacionamento dos dados de um ficheiro com os dados de outro ou outros ficheiros mantidos por outro ou outros responsáveis, ou mantidos pelo mesmo responsável com outra finalidade”. A PSP, a DSF e o GRH estabelecem, através da rede *Informac* da Direcção dos Serviços de Administração e Função Pública, o relacionamento com o sistema “*website* de consultas das agências de emprego” da DSAL, para efectuar consultas e obter dados pessoais de titulares de



licenças administrativas de agências de emprego ou de representantes de instituições titulares de licenças, contidos no referido sistema, pelo que o relacionamento estabelecido entre os ficheiros das entidades referidas configura “interconexão de dados pessoais”, definida e regulada pela lei acima citada.

A Lei da Protecção de Dados Pessoais estipula no artigo 22.º que a “interconexão de dados” é a forma de tratamento de dados pessoais sob o controlo prévio e necessita de autorização do GPDP. O n.º 1 do artigo 9.º da mesma lei estipula que a interconexão de dados pessoais que não esteja prevista em disposição legal ou disposição regulamentar de natureza orgânica, está sujeita a autorização do GPDP, solicitada pelo responsável ou, em conjunto, pelos respectivos responsáveis do tratamento, nos termos previstos no n.º 1 do artigo 22.º, acrescentando, ainda, o n.º 2 do mesmo artigo que a interconexão de dados pessoais deve ser adequada à prossecução das finalidades legais ou estatutárias e de interesses legítimos dos responsáveis pelos tratamentos, não devendo implicar a discriminação ou diminuição dos direitos, liberdades e garantias dos titulares dos dados, sendo também rodeada de adequadas medidas de segurança e tido em conta o tipo de dados objecto da interconexão.

De acordo com as informações prestadas pela DSAL, a abertura do seu sistema “*website* de consultas das agências de emprego” à PSP, DSF e GRH é resultante do estipulado no Decreto-Lei n.º 32/94/M que aponta no sentido de “a DSAL dever comunicar à DSF e à PSP o deferimento, alterações e cancelamento do pedido da licença de agências de emprego e apoiar o GRH para tratar os pedidos de agências de emprego de recrutar os trabalhadores não residentes, bem como prestar apoios ao GRH no tratamento de pedidos de recrutamento e colocação de trabalhadores não residentes por parte de agências de emprego”.

Para definir se a PSP, a DSF e o GRH possuem competências para consultar o sistema “*website* de consultas das agências de emprego” da DSAL, devem considerar-se as seguintes disposições legais:

- De acordo com o previsto no artigo 2.º do Decreto-Lei n.º 32/94/M, que regula o processo de licenciamento e as condições de funcionamento a que ficam sujeitas as agências de emprego, por actividade de agências de emprego, compreende-se a recepção de ofertas de emprego, inscrição de candidatos a emprego, selecção de pessoal, colocação, recrutamento de trabalhadores não residentes. Os artigos 9.º, 10.º e 12.º do mesmo Decreto-Lei estipulam que a concessão, renovação e substituição, alteração e cancelamento da licença das agências de emprego é da competência do director da DSAL, enquanto o artigo 13.º estabelece que o director da DSAL deve comunicar à DSF e à PSP o deferimento do pedido da licença e as alterações ou cancelamento da mesma.
- Segundo o previsto no artigo 30.º do Regulamento Administrativo n.º 22/2001 (Organização e funcionamento do Corpo de Polícia de Segurança Pública) o Serviço de Migração da PSP emite, renova e cancela, nos termos da lei, títulos de identificação de trabalhadores não residentes. O artigo 9.º do Despacho n.º 12/GM/88 e o artigo 2.º do Despacho n.º

49/GM/88 estipulam, respectivamente, que o GRH, depois de ter dado deferimento ao pedido de contratação de trabalhador não residente, deve remeter o processo à PSP para que esta decida sobre a autorização de entrada e permanência no território dos trabalhadores incluídos na lista do respectivo do pedido. Os trabalhadores não residentes só podem trabalhar, legalmente, no território depois de terem obtido o título de identificação de trabalhador não residente.

- Em conformidade com o previsto no artigo 2.º do Decreto-Lei n.º 30/99/M (Nova Lei Orgânica da Direcção dos Serviços de Finanças) as atribuições da DSF incluem: realizar a administração fiscal do território, promover a adequação das leis fiscais, executar a política fiscal e exercer a fiscalização nos domínios fiscal e das finanças públicas, pelo que a DSF é competente para executar as disposições estabelecidas no Regulamento da Contribuição Industrial, aprovado pela Lei n.º 15/77/M, que define a cobrança da contribuição industrial no âmbito das taxas fixas da Tabela Geral de Actividades que integra o mapa I anexo ao regulamento referido (vide o artigo 4.º do Regulamento) e a disponibilidade de um cadastro que deve conter os elementos necessários à identificação dos contribuintes e respectivas actividades, bem como os dados relevantes para o cálculo e liquidação da contribuição (vide o artigo 19.º do Regulamento). Para a DSF poder cumprir as suas atribuições, conferidas pelo Regulamento da Contribuição Industrial, o artigo 8.º deste Regulamento estipula que todo aquele que pretenda exercer qualquer actividade industrial ou comercial é obrigado a apresentar à DSF, por si ou seu procurador, a declaração M/1, com a antecedência mínima de 30 dias sobre a data provável do início da respectiva actividade, estabelecendo, ainda, o artigo 32.º que os serviços públicos do território devem colaborar com a DSF na observância deste Regulamento e as entidades a quem competir o licenciamento de qualquer tipo de actividade económica devem comunicar à DSF a identificação das pessoas singulares ou colectivas licenciadas.
- De acordo com os artigos 3.º a 5.º do Despacho do Chefe do Executivo n.º 116/2007, são atribuições do GRH analisar permanentemente a evolução dos recursos humanos no mercado de trabalho da Região Administrativa Especial de Macau e desempenhar as tarefas administrativas respeitantes aos pedidos de contratação de trabalhadores não residentes. Para o desempenho das atribuições que lhe estão conferidas, o GRH pode solicitar, a quaisquer entidades públicas ou privadas, designadamente à DSAL e ao Fundo de Segurança Social, as informações necessárias à apreciação dos pedidos de contratação de trabalhadores não residentes. No caso de pedidos de contratação de trabalhadores não residentes, através do recurso a empresas de Macau que contratam trabalhadores não residentes e agências de emprego que os fornecem, o GRH, no desempenho das tarefas administrativas respeitantes a estes pedidos e no âmbito do Despacho n.º 12/GM/88, deve verificar os contratos de prestação de serviços que visam a prestação de trabalho por parte de trabalhadores não residentes (vide os n.ºs 3, 7 e 9 do Despacho n.º 12/GM/88), incluindo a verificação de habilitação das agências de emprego para o fornecimento de trabalhadores não residentes.

De acordo com as disposições legais acima referidas, a PSP, DSF e GRH efectuem o tratamento de dados contidos no sistema



“*website* de consultas das agências de emprego” da DSAL para exercer as respectivas atribuições conferidas pela lei, e consignadas na alínea 4) do artigo 6.º da Lei da Protecção de Dados Pessoais: execução de uma missão de interesse público ou no exercício de poderes de autoridade pública, tendo, portanto, a legitimidade de tratamento de dados.

No aspecto de que o tratamento de dados, via “interconexão de dados pessoais”, deve ser adequado à prossecução das finalidades legais e de interesses legítimos dos responsáveis dos tratamentos, a DSAL tem obrigações de prestar, no âmbito do artigo 13.º do Decreto-Lei n.º 32/94/M e do artigo 5.º do Despacho do Chefe do Executivo n.º116/2007, a colaboração à PSP, DSF e GRH e disponibilizar-lhes, por força de obrigação legal, os “dados das licenças das agências de emprego” necessário ao desempenho das suas atribuições, pelo que a “interconexão de dados pessoais” é compatível com as finalidades de recolha de dados pessoais das agências de emprego por parte da DSAL, no âmbito da alínea 2) do n.º 1 do artigo 5.º da Lei da Protecção de Dados Pessoais, bem como com os interesses legítimos do tratamento de dados pela DSAL.

No que respeita a que a “interconexão” não deverá implicar a discriminação ou diminuição dos direitos, liberdades e garantias dos titulares dos dados, a DSAL presta, através de “interconexão”, à PSP, DSF e GRH os dados contidos no sistema “*website* de consultas das agências de emprego” com vista ao cumprimento da obrigação legal de comunicação de dados. A disponibilidade, via “interconexão”, dos dados mais actualizados sobre as licenças das agências de emprego aos serviços referidos, para acelerar o processo de autorização administrativo, não implica a discriminação dos direitos dos titulares.

Quanto às adequadas medidas de segurança de interconexão, a DSAL estabelece, via *Informac*, intranet do governo, a interconexão com a PSP, DSF e GRH para efectuar o tratamento dos dados do sistema “*website* de consultas das agências de emprego”. Segundo as informações prestadas pela Direcção dos Serviços de Administração e Função Pública, o *Informac* é um sistema de Intranet fechado que possibilita o relacionamento do ficheiro dos serviços de uma autoridade pública com o mesmo de outras, sendo interligado, principalmente, por fibras ópticas e linhas DDN e acessível apenas através da introdução do código VPN. Além disso, as informações prestadas pela DSAL comprovam que o acesso ao sistema “*website* de consultas das agências de emprego” requer a entrada do código do utilizador e da senha e a autorização de consulta de informações. A DSAL procederá, igualmente, ao registo dos utilizadores que acedem ao sistema e guardará com dispositivos de fecho de segurança o local onde conserva os dados.

Pelo exposto, o GPDP autoriza, no âmbito do artigo 9.º e da alínea 3) do n.º 1 do artigo 22.º da Lei da Protecção de Dados Pessoais, a DSAL e a PSP, DSF e GRH a estabelecerem, com o objectivo referido e sob a condição de garantir a segurança do tratamento dos dados e não implicar a diminuição dos direitos dos seus titulares, a interconexão para efectuar o tratamento dos dados contidos no sistema “*website* de consultas das agências de emprego”.

Aos 18 de Setembro de 2009

A Coordenadora
Chan Hoi Fan

第08/A/2009/GPDP號許可

事由：關於行政暨公職局申請電子一站通資料庫與網上公職就業登記資料庫兩個內部資料庫“互聯”

行政暨公職局（下稱公職局）就其內部電子一站通資料庫（下稱ePass資料庫）以“互聯”方式向其另一內部資料庫，網上公職就業登記資料庫（下稱eJob資料庫）提供個人資料一事，向本辦公室申請“個人資料互聯”許可。

根據公職局提供的資料，ePass資料庫以“互聯”方式向eJob資料庫提供的資料包括：ePass用戶的通行帳戶編號（ePass編號）、身份證明文件種類及號碼、中葡文姓名、性別及出生日期。根據第8/2005號法律（《個人資料保護法》）第4條第1款（一）項之規定：“個人資料是指與某個身份已確定或身份可確定的自然人有關的任何資訊，包括聲音和影像，不管其性質如何以及是否擁有載體。”上述以“互聯”方式處理的資料為與身份已確定的自然人相關的資訊，屬於個人資料。根據《個人資料保護法》第3條規定，對有關個人資料之處理受該法律所規範。

根據《個人資料保護法》第4條第1款（十）項規定：“資料的互聯是指一個資料庫的資料與其他一個或多個負責實體的一個或多個資料庫的資料的聯繫、或同一負責實體但目的不同的資料庫的資料聯繫的處理方式。”根據公職局提供的資料，ePass資料庫及eJob資料庫為公職局兩個不同目的的內部資料庫，透過“ePass跨部門認證架構”進行資料互通。因此，上述處理使ePass資料庫及eJob資料庫建立聯繫，屬上述法律定義的“個人資料互聯”處理方式。

根據《個人資料保護法》第22條規定，“資料的互聯”屬須預先監控的處理個人資料方式，須經本辦公室許可。其中同一法律第9條第1款規定：法律規定或具組織性質的規章性規定未規定的個人資料的互聯，須由負責處理個人資料實體或與其共同負責的實體根據第22條第1款的規定向本辦公室提出申請並取得許可。同條第2款規定：個人資料的互聯應符合法律或章程規定的目的和負責處理個人資料的實體的正當利益；不得導致歧視或削減資料當事人的權利、自由和保障；須有適當的安全措施；考慮需互聯的資料的種類。

根據公職局提供的資料，ePass資料庫向eJob資料庫提供資料的目的是：“經ePass將個人資料傳送到本局人力資源廳的網上公職就業登記系統，以使用戶在進行新公職就業登記時，無需再次輸入相關資料，



以建立相關資料庫，從而達到便民的效果。”另一方面，用戶登入ePass帳戶後，可使用eJob服務，而毋須再次登入eJob帳戶。

根據第23/94/M號法令第7條第1款b)項規定，行政暨公職局人力資源廳之權限包括設立關於管理公共行政人力資源之資訊系統，並不斷使之保持最新資料。當用戶經ePass帳戶作新公職就業登記時，eJob資料庫取得ePass資料庫的個人資料，以建立有關的用戶資料，可使公職局人力資源廳更有效地履行其法定職責，符合《個人資料保護法》第6條第(四)項規定的正當性條件，屬履行具公共利益的任務及行使公共當局的權力。

至於有關“個人資料互聯”處理方式是否符合法律或章程規定的目的和負責處理個人資料的實體的正當利益。根據公職局提供的資料，電子一站通(ePass)是免費申請的電子服務通行帳戶，以使用戶處理及查詢其在不同部門內的資料及服務申請進度等，用戶可使用同一個ePass帳戶安全及有效地使用不同政府部門提供的ePass電子化服務，從而免除用戶為使用不同部門的電子服務而需申請不同登入帳戶。根據第23/94/M號法令第2條f)項及g)項規定，行政暨公職局之職責包括促進現代資訊技術在公共機關使用及普及，以及在技術上協調及輔助公共行政當局各資訊系統之發展及相互間之連接；促進、更新及確保公共行政當局共同資訊系統之接達及數據庫之存取。公職局為履行上述職責，建立ePass資料庫，以方便用戶使用不同部門提供的ePass電子化服務，而eJob資料庫以“互聯”方式取得及使用ePass資料庫的資料，是為了使ePass用戶作網上新公職就業登記時，無需再次輸入有關資料，以及用戶可使用ePass登記帳戶使用eJob服務，從而達到便民目的，故ePass資料庫與eJob資料庫以“互聯”方式建立聯繫符合《個人資料保護法》第5條1款(二)項規定，eJob資料庫處理資料沒有偏離ePass資料庫收集個人資料的目的。

關於“互聯”不得導致歧視或削減資料當事人的權利、自由及保障方面。上述“互聯”可免除ePass用戶作網上新公職就業登記時，需再次輸入資料，以及用戶可使用ePass登記帳戶使用eJob服務，目的為便民及完善政府部門的電子服務，且有關處理方式適用於所有使用eJob服務的ePass登記帳戶，對於用戶的使用條件及資格的設定並沒有出現不公平或歧視的情況，因此，在資料處理方面不存在歧視或削減資料當事人的權利、自由及保障。

就“互聯”須有適當的安全措施方面，根據公職局提供的資料，ePass資料庫及eJob資料庫的“互聯”經過一個密封的環境 — ePass跨部門認證架構進行，……能夠確保跨部門認證架構內資料的安全互通。

在“互聯”過程中，……個人資料在傳送時均被轉換為密碼，並在接收端經解密恢復其原初內容。另一方面，ePass帳戶包括登入名稱及密碼，所有ePass內的電子服務都需要用戶登入後才能使用，且用戶登入都會記錄在log內。ePass亦會參考公職局的資訊保安政策指引文件內的相關安全指引。

綜上所述，本辦公室根據《個人資料保護法》第9條及第22條第1款第(三)項的規定，許可行政暨公職局電子一站通(ePass)資料庫與網上公職就業登記(eJob)資料庫兩個內部資料庫，基於上述所指的目的，且在保障資料安全處理及不削減當事人權利的情况下，進行“互聯”處理。

主任

陳海帆

2009年9月25日



Autorização n.º 08/A/2009/GPDP

Tradução

Assunto: Pedido de autorização, da Direcção dos Serviços de Administração e Função Pública, para o estabelecimento de “interconexão” entre dois ficheiros internos, designadamente, o de Serviços Electrónicos e o de Bolsa de Registo de Emprego

A Direcção dos Serviços de Administração e Função Pública (adiante designada por SAFP) solicitou, ao GPDP, autorização de “interconexão de dados pessoais” para a transferência, via “interconexão”, de dados pessoais contidos no seu ficheiro de Serviços Electrónicos (adiante designado por ePass) para outro ficheiro, também dos SAFP, Bolsa de Registo de Emprego (adiante designado por eJob).

De acordo com as informações prestadas pelos SAFP, os dados a transferir, através de “interconexão”, do ficheiro ePass para o eJob incluem: número da conta comum do utente do ePass, tipo e número do documento de identidade, nomes em chinês e em português, sexo e data de nascimento. O artigo 4.º da Lei n.º 8/2005 (Lei da Protecção de Dados Pessoais) estipula na alínea 1) do n.º 1 que se entende por “dados pessoais” “qualquer informação, de qualquer natureza e independentemente do respectivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável”. Como os dados acima referidos, cujo tratamento será efectuado através de “interconexão”, dizem respeito a pessoas singulares identificadas, consideram-se, por isso, dados pessoais. Assim, de acordo com o artigo 3.º da Lei da Protecção de Dados Pessoais, o tratamento dos mesmos está sujeito a esta lei.

O artigo 4.º da Lei da Protecção de Dados Pessoais estipula, na alínea 10) do n.º 1, que a “interconexão de dados” é uma “forma de tratamento que consiste na possibilidade de relacionamento dos dados de um ficheiro com os dados de um ficheiro ou ficheiros mantidos por outro ou outros responsáveis, ou mantidos pelo mesmo responsável com outra finalidade”. Segundo informações prestadas pelos SAFP, tanto o ePass como o eJob são ficheiros internos dos SAFP, mas têm diferentes finalidades e interligam-se através da “estrutura de reconhecimento entre os diferentes Serviços”, pelo que o relacionamento a estabelecer entre os mesmos configura “interconexão de dados pessoais” definida e regulada pela lei acima referida.

De acordo com o estipulado no artigo 22.º da Lei da Protecção de Dados Pessoais, a “interconexão de dados”, como forma de tratamento de dados pessoais sob controlo prévio, está sujeita a autorização do GPDP. De acordo com o n.º 1 do artigo 9.º da mesma lei, a interconexão de dados pessoais que não esteja prevista em disposição legal ou disposição regulamentar de natureza orgânica está sujeita a autorização do GPDP, solicitada pelo responsável ou em conjunto pelos correspondentes responsáveis dos tratamentos, nos termos previstos no n.º 1 do artigo 22.º. O n.º 2 do mesmo artigo estipula que a interconexão de dados pessoais deve ser adequada à prossecução das finalidades legais ou estatutárias e de interesses legítimos dos responsáveis dos tratamentos; não devendo implicar a

discriminação ou diminuição dos direitos, liberdades e garantias dos titulares dos dados; devendo ser rodeada de adequadas medidas de segurança; e ter em conta o tipo de dados objecto de interconexão.

Segundo informações prestadas pelos SAFP, a transferência de dados do ficheiro ePass para o eJob tem como objectivo “disponibilizar os dados do ePass à Bolsa de Registo de Emprego, do Departamento de Recursos Humanos destes Serviços, para criar, de imediato, o respectivo ficheiro, sem necessidade de reintroduzir os respectivos dados, aquando de novo registo de emprego, facilitando, deste modo, aos cidadãos estes procedimentos”. Além disso, os utentes, depois de aceder à sua conta pessoal do ePass, podem ter acesso directamente aos serviços do eJob sem terem necessidade de efectuar novo login. De acordo com o previsto na alínea b) do n.º 1 do artigo 7.º do Decreto-Lei n.º 23/94/M compete ao Departamento de Recursos Humanos institucionalizar e manter permanentemente actualizado um sistema de informação para a gestão dos recursos humanos da Administração Pública. Quando um utente efectuar, através da sua conta pessoal no ePass, novo registo de emprego, o eJob poderá obter os respectivos dados pessoais existentes no ePass que poderão ser usados no eJob, o que permite ao Departamento de Recursos Humanos dos SAFP cumprir, de forma mais eficaz, as suas atribuições legais, tendo, portanto, legitimidade para o tratamento dos dados, para a execução da missão de interesse público e o exercício de poderes de autoridade pública, no âmbito da alínea 4) do artigo 6.º da Lei da Protecção de Dados Pessoais.

No que se refere a saber se a “interconexão de dados pessoais” é adequada à prossecução das finalidades legais ou estatutárias e de interesses legítimos dos responsáveis dos tratamentos, o ePass é, segundo as informações prestadas pelos SAFP, uma conta comum requerida gratuitamente para acesso aos serviços públicos e que permite ao utente tratar os respectivos dados registados nos diferentes Serviços e consultar o andamento dos respectivos requerimentos, etc. Os utentes podem utilizar, com segurança e eficácia, através da mesma conta ePass, os serviços prestados electronicamente por diferentes Serviços, evitando assim incómodos causados aos utentes que precisam de requerer, junto de diversos Serviços, contas de acesso para utilização dos respectivos serviços electrónicos ePass. De acordo com o estipulado nas alíneas f) e g) do artigo 2.º do Decreto-Lei n.º 23/94/M, as atribuições dos SAFP consistem em promover a utilização e a generalização das modernas tecnologias de informação nos serviços públicos, bem como coordenar e apoiar tecnicamente o desenvolvimento e interligação dos sistemas informáticos da Administração Pública; e promover, actualizar e assegurar o acesso aos sistemas de informação e bases de dados comuns à Administração Pública. Para o cumprimento das atribuições referidas os SAFP criaram o ficheiro ePass a fim de facilitar o acesso dos utentes aos serviços electrónicos prestados pelos diferentes Serviços. A obtenção e utilização dos dados do ficheiro ePass pelo eJob, via “interconexão”, visa dispensar a introdução repetida dos respectivos dados quando os utentes efectuarem, através das suas contas no ePass, novos registos de emprego, para além de permitir o acesso dos utentes aos serviços de eJob com a sua conta no ePass, facilitando o acesso dos cidadãos. Pelo exposto, conclui-se que o estabelecimento do relacionamento, via “interconexão”, entre os ficheiros ePass e eJob é adequado ao previsto no 2) do n.º 1 do artigo 5.º da Lei da Protecção de Dados Pessoais, sendo o tratamento de dados por parte do ficheiro eJob compatível com a finalidade de recolha dos dados pessoais para o ficheiro ePass.



No aspecto de que a “interconexão” não deverá implicar a discriminação ou diminuição dos direitos, liberdades e garantias dos titulares dos dados o estabelecimento da “interconexão” referida poderá evitar a introdução repetida dos respectivos dados por parte dos utentes registados no ePass, quando estes efectuarem novos registos de emprego, e permitir o acesso dos utentes aos serviços do eJob com as suas contas registadas no ePass, contribuindo, assim, para o aperfeiçoamento dos serviços electrónicos dos Serviços da Administração sendo este um procedimento benéfico para os cidadãos. Além disso, a forma de tratamento aplica-se a todas as contas registadas tanto no eJob como no ePass, não havendo desigualdade ou discriminação resultante das condições e qualificação de acesso, pelo que o tratamento dos dados não implica a discriminação ou diminuição dos direitos, liberdades e garantias dos titulares dos dados.

Relativamente à necessidade de adequadas medidas de segurança na “interconexão”, as informações prestadas pelos SAFP comprovam que a “interconexão” entre os ficheiros ePass e eJob é realizada através de um ambiente fechado chamado “ePass - estrutura de reconhecimento entre os diferentes Serviços” que assegura a segurança da transferência dos dados dentro de tal estrutura. No processo de “interconexão” os dados pessoais serão transmitidos sob forma codificada e decodificados no terminal de recepção. Além disso, todas as contas abertas no ePass requerem a inserção do nome do utente e a respectiva senha para acesso aos serviços electrónicos disponíveis no ePass e cada acesso de todos os utentes será registado no *log*. O ePass terá também em consideração as respectivas indicações encontradas no guia da política de segurança de informática dos SAFP.

Pelo exposto, o GPDP autoriza, no âmbito do artigo 9.º e da alínea 3) do n.º 1 do artigo 22.º da Lei da Protecção de Dados Pessoais, os SAFP a estabelecerem, com o objectivo referido e sob a condição de garantir a segurança do tratamento dos dados e não implicar a diminuição dos direitos dos seus titulares, a “interconexão” dos seus dois ficheiros, ePass e eJob, para efectuar o tratamento dos dados neles contidos.

Aos 25 de Setembro de 2009

A Coordenadora
Chan Hoi Fan

附註

第01/AV/2009/GPDP號許可

(補充第08/A/2008/GPDP號“互聯”許可)

事由：關於A銀行申請增加第08/A/2008/GPDP號“互聯”許可之客戶資料種類

本辦公室於2008年6月25日以第08/A/2008/GPDP號“互聯”許可批准A銀行以“互聯”方式將其“客戶個人資料”轉移予香港B銀行。

A銀行現向本辦公室申請增加第08/A/2008/GPDP號“互聯”許可中所列之“客戶資料”種類：客戶的身份證號碼及賬戶結餘資料。根據第8/2005號法律（《個人資料保護法》）第3條及第4條第1款第（一）項規定，有關的資料屬於身份已確定客戶的個人資料，對上述資料的處理受該法律所規範。

本申請涉及已登記“互聯”許可的個人資料種類的修改，根據《個人資料保護法》第24條第2款規定，須根據第21條和22條規定的程序進行。

本辦公室於第08/A/2008/GPDP號許可已對A銀行與香港B銀行“互聯”處理客戶個人資料的情況作出審核及批准，當中包括對“互聯”方式之認定、資料種類、目的、A銀行之正當利益、對資料當事人的權利、自由和保障是否構成影響以及資料處理之安全措施之審查。而A銀行是次申請僅涉及第08/A/2008/GPDP號許可“互聯”資料種類之增加，沒有偏離上述“互聯”許可所確認之目的：有關的客戶資料供銀行集團作資料查閱及備份用途。且其他事項亦與上述“互聯”許可已審核及批准之事項相同，故無須另外發出許可。

基於上述“互聯”資料種類之增加符合《個人資料保護法》第9條有關“互聯”之規定，本辦公室根據《個人資料保護法》第9條、第22條1款（三）項以及第24條第2款規定，以附註方式將下列內容加入第08/A/2008/GPDP號“互聯”許可，並成為該許可之組成部分，與該許可具同等之法律效力：

在“互聯”的個人資料種類中增加：客戶的身份證號碼及賬戶結餘資料。

主任

陳海帆

2009年4月15日



Tradução

Autorização Nota n.º 01/AV/2009/GPDP (Suplemento à Autorização n.º 08/A/2008/GPDP)

Assunto: Pedido do Banco A para acrescentar tipos de dados dos clientes à autorização de “interconexão” n.º 08/A/2008/GPDP

GPDP autorizou, em 25 de Junho de 2008, através da autorização n.º 08/A/2008/GPDP, o pedido do Banco A para transferir, via interconexão, “dados pessoais dos clientes” ao Banco B de Hong Kong.

O Banco A solicitou, em novo pedido ao GPDP, autorização para acrescentar, ao tipo de “dados dos clientes”, contidos na autorização de interconexão n.º 08/A/2008/GPDP, o número do bilhete de identidade e o saldo da conta dos clientes. De acordo com o artigo n.º 3 e a alínea 1) do n.º 1 do artigo 4.º da Lei n.º 8/2005 (Lei da Protecção de Dados Pessoais), os referidos dados são relativos a clientes identificados, estando, por isso, o seu tratamento sujeito à tutela da lei.

O presente pedido é referente à alteração do tipo de dados pessoais contidos na autorização de interconexão, sendo obrigatório observar, no âmbito do n.º 2 do artigo 24.º da Lei da Protecção de Dados Pessoais, os procedimentos previstos nos artigos 21.º e 22.º.

O GPDP verificou e autorizou, pela autorização n.º 08/A/2008/GPDP, o relacionamento, por interconexão, do Banco A com o Banco B de Hong Kong para tratamento de dados pessoais dos clientes, tendo verificado a forma de interconexão, os tipos de dados, as finalidades, os interesses legítimos do Banco A, o impacto nos direitos, liberdades e garantias dos titulares de dados, bem como as medidas de segurança para o referido tratamento. O presente pedido do Banco A refere-se, apenas, à adição de novos tipos de dados aos referidos na autorização de interconexão n.º 08/A/2008/GPDP, sendo compatível com a finalidade reconhecida na referida autorização de interconexão: os dados dos clientes servem para consulta e cópia, apenas do grupo bancário. Os restantes assuntos são idênticos aos já verificados e autorizados pela citada autorização de interconexão, pelo que é desnecessário emitir nova autorização.

Considerando que o aumento dos tipos de dados da interconexão referida, está no âmbito das disposições legais relativas à interconexão, previstas no artigo 9.º da Lei da Protecção de Dados Pessoais o GPDP, nos termos do artigo 9.º, da alínea 3) do n.º 1 do artigo 22.º e do n.º 2 do artigo 24.º, acrescenta, pela presente nota, à autorização de interconexão n.º 08/A/2008/GPDP o seguinte, passando a fazer parte integrante da mesma e com igual força jurídica:

Acrescentam-se aos tipos de dados pessoais da interconexão: o número do bilhete de identidade e o saldo da conta dos clientes.

Aos 15 de Abril de 2009

A Coordenadora
Chan Hoi Fan