Legal Practice | 法律实践

2023-06-15
202306/040

Inside this issue:

Is the use of an overseas email server equivalent to the domestic party exporting personal data?

Case Introduction：

Suppose a German company *A*, with affiliate entity in China *a*. For the consideration of unified company management and marketing, employees of all affiliated entities of company *A* use a unified mailbox service system, for example: user@A.com . In addition, the mailbox server of company *A* is built in Germany. When the employees in *a* use the mailbox service whose server is set up in Germany, will it cause the domestic party exporting personal data?

As we know, when sending an email, even if the email title and body are blank, the email addresses (personal information[1]) of the receiver and sender are naturally included in the email transmission. The sending and receiving principle of an email might be simply illustrated as follows: when you send an email, firstly, the composed email is sent to your mailbox server through your mailbox client, such as Outlook, after encryption, and then forwarded to the recipient's mailbox server through certain procedures, and then forwarded to the recipient's client by the recipient's mailbox server through the mail protocols, allowing the recipient to download and read the emails from the sender.

Data Transfer Fact Analysis：

If we look at the scenario that employee *b* of company *a* in China uses enterprise mailbox to complete his work, *b* writes an email and clicks send, no matter the recipient is *c* in the same office in China, or the Chinese distributor *d* downstream of the supply chain, or the leader *e* of the parent company in Germany, the packet written by *b* containing personal information (email addresses of the sender and receiver) will be transferred to the mailbox server of company *A* in Germany first. Due to the limitation of space, this article will not address the forwarding of the email from the sender's email server to the recipient's email server. In other words, when *b* sends the email, **the personal information (email addresses) of the natural person in China has been transmitted across the border during the process from the client to the sender's email server.**

Legal Analysis：

In this process, Company *a* acts as the personal information handler, the Chinese employee *b* serves as the trustee entrusted by *a* to process the data, and company *A* is the overseas recipient.

According to Article 38 of the Personal Information Protection Law of P.R.C. ("PIPL"), if a handler of personal information needs to provide personal information outside the People's Republic of China for business purposes, one of the following conditions shall apply.

(A) in accordance with the provisions of Article 40 of the PIPL, passing a safety assessment organized by the Cyberspace Administration of China;

(B) in accordance with the provisions of the cyberspace administrations, undergoing a personal information protection certification by a qualified institution;

(C) in accordance with the standard contract formulated by the Cyberspace Administration of China, concluding with the overseas recipient the Standard Contract.

(D) Other conditions stipulated by laws, administrative regulations or the cyberspace administrations.

To sum up, when an enterprise utilizes the mail system of the parent company, if the mailbox server is located outside of China, each mail delivery raises the issue of the domestic party exporting personal data. And according to the PIPL, when personal information crosses the border, the personal information handler should choose one of the following methods - security assessment, personal information protection certification, or standard contract - to ensure compliance with personal information cross-border transmission, to their actual scenario.

On a practical level, for most SMEs, data outbound transfer security assessments are generally not triggered (the threshold is high). Comparatively, standard contracts are more efficient and convenient than personal information protection certification, with lower compliance costs; it is sufficient to prepare a standard contract and file the standard contract and personal information protection impact assessment report for registration with the relevant provincial cyberspace administration.

The Measures for Standard Contract for Outbound Transfer of Personal Information ("Measure"), has been effective since June 1, 2023. For personal information outbound transfer activities conducted after the effective date of the Measure, the activities shall be carried out only after all compliance steps have been completed. For companies that have already conducted personal information outbound transfer activities before the Measure came into effect, the Measure provides for a six-month grace period (until November 30,2023) for rectification.

Therefore, relevant companies should fulfill their personal information outbound transfer compliance obligations in accordance with the provisions of the PIPL as soon as possible in order to mitigate unnecessary compliance risks.

[1] Personal information is all kinds of information relating to identified or identifiable natural persons recorded electronically or by other means, excluding information after anonymization processing." Personal Information Protection Law of P.R.C., Article 4.
In addition, email addresses that are associated with accounts that contain sensitive personal data, such as medical information or financial data, may be considered sensitive personal information.

L'utilisation d'un serveur de messagerie électronique situé à l'étranger donne-t-elle nécessairement lieu à une exportation de données à caractère personnel par le pays envoyeur ?

Introduction du cas :

Supposons qu'une société allemande, *A*, possède une filiale, *a*, en Chine. Pour des raisons de gestion uniformisé et de marketing, les employés de toutes les filiales de la société *A* utilisent un système de messagerie unique, par exemple : user@A.com . Par ailleurs, le serveur de messagerie électronique de la société *A* est installé en Allemagne. Lorsque les employés de l'entreprise *a* utilisent le service de messagerie mis en place en Allemagne, cela entraîne-t-il l'exportation de données à caractère personnel par le pays envoyeur ?
Nous savons que lorsque vous envoyez un e-mail, même si le sujet et le contenu du mail sont vides, l'adresse e-mail (informations personnelles[1]) du destinataire et de l'expéditeur est automatiquement incluse dans la transmission du message. Le principe d'envoi et de réception d'un courrier électronique peut être illustré comme ceci : lorsque vous envoyez un e-mail, celui-ci est d'abord envoyé, après cryptage, à votre serveur de messagerie par l'intermédiaire de votre boîte mail, par exemple Outlook, puis transmis au serveur de messagerie du destinataire par le biais de certaines procédures, et enfin envoyé à la boîte mail du destinataire depuis son serveur par l'intermédiaire de protocoles, permettant à celui-ci de télécharger et de lire le mail de l'expéditeur.

Analyse des faits relatifs au transfert de données :

Si l'on considère le scénario suivant : l'employé *b* de l'entreprise *a* en Chine utilise la boîte mail de l'entreprise pour effectuer son travail, *b* écrit un e-mail et clique sur envoyer, peu importe que le destinataire soit *c* dans le même bureau en Chine, ou le distributeur chinois *d* en aval de la chaîne d'approvisionnement, ou le dirigeant *e* de la société mère en Allemagne, le message écrit par *b* contenant des informations personnelles (adresses e-mail de l'expéditeur et du destinataire) sera d'abord transféré vers le serveur de la boîte mail de l'entreprise *A* en Allemagne. Pour des raisons d'espace, cet article n'abordera pas le transfert du mail du serveur de messagerie de l'expéditeur vers le serveur de messagerie du destinataire. En d'autres termes, lorsque *b* envoie un mail, **les informations personnelles (adresses électroniques) d'une personne physique ont été transmises de l'autre côté de la frontière au cours du processus de transmission entre la boite mail de l'envoyeur et le serveur de messagerie de l'expéditeur.**

Analyse juridique

Dans ce processus, la société *a* fait office de responsable du traitement des informations personnelles, l'employé chinois *b* agit en tant que mandataire chargé par *a* de traiter les données, et la société *A* est le destinataire à l'étranger.

Selon l'Article 38 de la loi sur la protection des informations personnelles de la République populaire de Chine (en anglais *the Personal Information Protection Law of P.R.C.* ou "*PIPL*"), si un responsable du traitement des informations personnelles doit envoyer des données personnelles en dehors de la République populaire de Chine à des fins professionnelles, l'une des conditions suivantes devra s'appliquer.

(A) Réussir une évaluation de sécurité organisée par la *Cyberspace Administration of China*, l'administration chinoise du cyberespace, et ce conformément aux dispositions de l'Article 40 de la *PIPL*.

(B) Se soumettre à une certification de protection des informations personnelles par une institution qualifiée conformément aux dispositions de la *Cyberspace Administration of China.*

(C) Conclure avec le destinataire étranger un contrat standard d'exportation de données personnelles (appelé *Standard Contract),* et ce conformément au *Standard Contract* formulé par la *Cyberspace Administration of China*.

(D) Autres conditions stipulées par les lois, les règlements administratifs ou la *Cyberspace Administration of China*.

En résumé, lorsqu'une entreprise utilise le système de messagerie de la société mère, si le serveur de la boîte mail est situé en dehors de la Chine, chaque envoi de message soulèvera un problème d'exportation de données à caractère personnel. Selon la *PIPL*, lorsque des informations personnelles franchissent la frontière, les responsables du traitement des données personnelles ont l'obligation d'opter pour l'une des

méthodes suivantes - l'évaluation de la sécurité, la certification de la protection des informations personnelles ou le *Standard Contract* - afin de garantir la conformité de la transmission transfrontalière des informations personnelles, en fonction du cas de figure rencontré.

D'un point de vue pratique, pour la plupart des PME, une évaluation de la sécurité des transferts de données sortantes n'est généralement pas nécessaire (à l'exception de cas particulier). En comparaison, un *Standard Contract* est plus efficace et plus pratique qu'une certification de protection des informations personnelles, avec des coûts de mise en conformité moins élevés, il suffit de préparer un *Standard Contract* et de le déposer, avec le rapport d'évaluation de l'impact sur la protection des informations personnelles, afin de les enregistrer auprès de la *Cyberspace Administration of China* de votre province.

Les *Mesures Relatives au Standard Contract pour les Transferts Sortants de Données à Caractère Personnelles* (dites "*Mesures*") sont entrées en vigueur depuis le 1er juin 2023. Les activités de transmission de données personnelles vers l'étranger menées après la date d'entrée en vigueur des *Mesures* ne peuvent être effectuées qu'une fois que toutes les étapes de mise en conformité ont été franchies. Pour les entreprises qui ont déjà mené des activités d'exportation de données personnelles avant la date d'entrée en vigueur des *Mesures*, un délai supplémentaire de 6 mois (jusqu'au 30 novembre 2023) a été accordé afin procéder à la mise en conformité.

Par conséquent, les entreprises concernées devront s'acquitter de leurs obligations de mise en conformité en matière de d'exportation de données personnelles, et ce dès que possible, conformément aux dispositions de la *PIPL*, afin de limiter les risques inutiles en matière de conformité.

[1] Les informations personnelles sont tous les types de données relatives à des personnes physiques identifiées ou identifiables, recueillies électroniquement ou par d'autres moyens, à l'exclusion des informations après traitement sous forme anonyme". Loi sur la protection des informations personnelles de la R.P.C., Article 4 (*PIPL*).

En outre, les adresses électroniques associées à des comptes contenant des données personnelles sensibles, telles que des informations médicales ou financières, peuvent être considérées comme des informations personnelles sensibles.

使用境外邮箱服务器是否一定会引起个人信息跨境传输？

案例引入：

假设某德国公司*A*，在中国境内存在关联实体*a*。出于公司统一管理和市场推广方面的考量，*A*公司的各关联实体员工均使用统一的邮箱服务系统，例：user@A.com。此外，*A*公司的邮箱服务器搭建在德国境内。当*a*公司的员工在使用服务器搭建在德国的邮箱服务时，是否会引起个人信息跨境传输呢？

我们知道，在发送一份电子邮件时，即使邮件标题、正文都空白，但收发件人的邮件地址（个人信息[1]）天然包含在邮件传输中。而一封电子邮件的收发原理，可以简单理解如下：在你发送一份电子邮件时，首先写好的电子邮件经过加密通过你的邮箱客户端，如Outlook,发送到你的邮箱服务器，再经过一系列程序转发到收件人的邮箱服务器，再由收件人的邮箱服务器通过邮件协议转发到收件人的客户端，这样收件人就可以下载阅读来自发件人的邮件。

数据传输事实分析：

如果代入*a*公司中国员工*b*使用企业邮箱完成工作的场景来看，*b*写好一封邮件点击发送，不论收件人是同一中国办公室的*c*,还是供应链下游的中国经销商*d*,亦或是德国母公司的领导*e*，*b*写好的这封包含个人信息（收发件人邮箱地址）的数据包都会首先传输到位于德国境内*A*公司的邮箱服务器上，因篇幅所限，本篇文章先不考虑邮件从发件人的邮箱服务器转发至收件人的邮箱服务器的问题。即，*b*的这份邮件，**在从客户端到发件人的邮箱服务器这一过程中，已经出现了中国境内的自然人的个人信息（邮箱地址）跨境传输的现象。**

法律分析：

在这一过程中，个人信息处理者为*a*,中国员工*b*为受*a*委托处理数据的受托人，而*A*公司为境外接收方。

根据《个人信息保护法》（“个保法”）第三十八条的规定，个人信息处理者因业务等需要，确需向中华人民共和国境外提供个人信息的，应当具备下列条件之一：

（一）依照本法第四十条的规定通过国家网信部门组织的安全评估；

（二）按照国家网信部门的规定经专业机构进行个人信息保护认证；

（三）按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务；

（四）法律、行政法规或者国家网信部门规定的其他条件。

综上所述，企业在使用母公司的邮件系统时，若邮箱服务器在境外，每次的邮件发送都会引起个人信息跨境问题。而根据个保法，个人信息跨境时个人信息处理者应当根据自己的实际情况从安全评估、个人信息保护认证、标准合同中选择一种方式来开展个人信息跨境传输合规安排。

从实操层面来说，对于大多数的中小企业，一般不会触发数据出境安全评估（门槛较高），而标准合同相比个人信息保护认证则更加高效便捷，合规成本较低；只需制备标准合同并对生效的标准合同和个人信息保护影响评估报告进行备案即可。

个人信息出境标准合同办法（“办法”）已于2023年6月1日起生效。对于办法生效后的个人信息出境活动，须在完成全部合规步骤之后才可开展个人信息出境活动。而对于在办法生效前已经开展个人信息出境活动的企业，办法则规定了6个月的整改宽限期（2023.11.30）。

因此，相关企业应尽快按照个保法的规定，完善个人信息跨境传输合规，以避免引发不必要的合规风险。

[1] “个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。”《个人信息保护法》，第四条。
此外电子邮件地址，如果与包含敏感个人数据的账户相关联，如医疗信息或财务数据等，那么该电子邮件地址可能被视为敏感个人信息。

Shanghai 上海

10F Jinmao Tower, 88 Century Avenue, Pudong New District, Shanghai City, PR China, 200121

上海市浦东新区世纪大道88号金茂大厦10楼

+86 21 5010 6580

Taicang 太仓

Room 1613B, German Centre, 319 Middle Zhenghe Road, Taicang City, Jiangsu Province, PR China, 215400

中国江苏省太仓市郑和中路319号兰德集团东亭大厦德国中心1613B

+86 512 5398 5389

shanghai@shaohe-lawfirm.com

www.shaohe-lawfirm.com

Your Contact 联系人

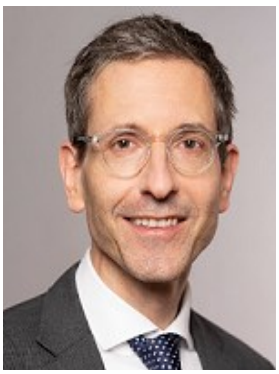
GAO Yuan | Associate 高媛 | 律师

+86 21 5010 7537

gao.yuan@shaohe-lawfirm.com

- Data Compliance 数据合规
- Corporate Governance 公司治理
- Compliance & Internal Investigations 合规和内部调查

Languages: Chinese, English, Italian 语言：中文、英文、意大利文



Philip Lazare | Foreign Counsel 李飞 | 顾问（德国）

+86 21 5010 6585

philip.lazare@shaohe-lawfirm.com

- Corporate/M&A 公司法和并购
- Data Compliance 数据合规
- Restructuring 重组
- Tax Law 税法

Languages: German, English 语言：英文、德文

About Shaohe Law Firm 关于劭合

Shaohe Law Firm is a full-service Chinese law firm with local expertise and global reach. Founded in 2007, Shaohe Law Firm has become one of the most trusted legal service providers for foreign, especially European, business in China.

- Shaohe Law Firm is a **PRC-licensed law firm**. We support clients in negotiations with Chinese counterparts, deal with government departments and represent clients in Chinese courts and arbitration.
- Shaohe Law Firm provides **full range of legal services** to foreign companies entering and developing in China.
- With more than 20 international and local lawyers, Shaohe Law Firm is one of the largest **German-speaking** laws firm in the country.
- As an independent law firm headquartered in Shanghai, we support you **all over China and cross borders**. We maintain a close cooperative relationship with other local firms in China and in other jurisdictions.

劭合律师事务所是一家在中国注册的律师事务所。我们拥有本地专业知识和全球视野。劭合律师事务所成立于2007年，目前已成为外资企业（特别是欧洲企业）在中国最信赖的法律服务提供者之一。

- 劭合律师事务所是一**家在中国注册的律师事务所**。我们代表客户与中国合作伙伴谈判，与政府部门进行磋商，同时也代理诉讼和仲裁。
- 劭合律师事务所帮助外资企业开拓中国市场以及在中国获得长久的发展提供**全方位的法律服务。**
- 劭合律师事务所拥有20多名中国律师和持其他国家执业许可的境外法律顾问，是全国**以德语为工作语言**的最大律师事务所之一。
- 作为一家总部位于上海的律所，我们可以为您提供**全国范围以及跨境**法律服务。我们与其他值得信赖的本土律所以及其他司法管辖领域的律所保持紧密的合作。

Welcome to follow our WeChat account where you will find the updated legal insights and news.

欢迎扫码关注我们的微信公众号，在这里您可以获取最新的法律资讯和新闻。