SQUIRE PATTON BOGGS

通用数据保护条例（GDPR）对亚太区的影响
What Are the Implications of the GDPR in Asia Pacific?

什么是GDPR
The New Law

《通用数据保护条例》（GDPR）是欧盟于近期通过的严格的新法规，旨在保护欧盟居民隐私。

The European Union (EU) has recently adopted the General Data Protection Regulation (GDPR), stringent new legislation to protect the privacy of EU residents.

适用范围
Who is Covered?

该法规不仅将对那些在欧洲开设子公司或分支机构的企业造成影响，而且还会波及将欧盟客户或其商业运营行为作为业务目标的公司。

This law will affect not only companies with European subsidiaries, but also companies that target EU customers or their behavior.

GDPR是有关收集和保存数据方式的监管条例（无论保存数据的服务器所在何地）。所以即使您所在企业的服务器位于亚洲，只要其中存储有任何欧盟消费者的信息，您都应该注意并分析这一新法规的适用情况。

The GDPR applies to regulate how such data is collected and kept, no matter where the servers that hold the data are located. So, if your server sits in Asia but holds any EU employee or consumer information, you should analyze the application of this new law.

违规风险
What is the Risk?

对违反GDPR 的罚款规定从2018年5月25日开始实施，其金额可能高达 2000万欧元或4% 的全球销售收入，以高者为准。值得注意的是，除了来自政府的监管调查和处罚之外，GDPR还允许个人提起集体诉讼，而这就有可能会升级并导致政府的监管调查（我们已经注意到一些由正在准备发起诉讼的原告团体所提出的信息收集要求）。基于这些理由，我们认为该监管条例及处罚措施对企业所造成影响的速度将远超其他新颁布的监管法律。

Failure to follow the GDPR can lead to fines of up to €20 million or 4% of global revenue, whichever is higher, once the penalty phase begins on May 25, 2018. Besides the governmental regulatory investigations and fines, class action suits are allowed for individuals, which can escalate to a regulatory investigation. We are already seeing requests for information from plaintiff's groups in preparation of this.

For these reasons, we believe that the impact of these regulations and fines will be felt much more quickly than other new regulatory laws.

对策
What to Do

尽管距GDPR的正式实施还有一段时间，但预先准备工作的重要性不容忽视。根据我们的估计，企业可能需要一年或一年以上的时间来进行这些准备工作，主要是对遵守GDPR所必须采取的应对和变革措施进行评估和执行，这些准备工作包括：

It is important for companies to prepare in advance for the GDPR. Despite the time available before the penalty phase, we believe it may take companies a year or more for preparation to assess and implement the changes needed to comply. Below is an overview of the projects that your team should consider to implement.

- 初步尽职调查 -- 启动信息收集工作，并评估企业需要采取哪些步骤来遵守GDPR的要求 。

  Preliminary Due Diligence – Start gathering information and assessing what steps your organization needs to take to become GDPR compliant.

- 数据配置 -- GDPR要求企业对其数据处理活动进行详细记录。因此企业需要对内部和外部的数据流动情况进行审查和配置，并同时确保采用了适当的传输机制。

  Data Mapping – The GDPR requires organizations to keep detailed records of their data processing activities. Review and map your internal and external data flows and ensure appropriate transfer mechanisms are in place.

- 经由双方同意的数据运用及自动处理（包括性能分析）-- GDPR 不但使获得有效同意的难度增大，而且对包括性能分析在内的自动化处理的运用规定了限制条款或额外义务。因而企业应对所有的数据处理活动进行审查并确保遵守该条例。

  Consent-Based Data Uses, Automated Processing, Including Profiling – The GDPR makes it harder to obtain valid consent and contains restrictions/additional obligations relating to the use of automated processing including profiling. All processing activities should be reviewed and made to conform with the regulation.

- 保密和隐私 -- GDPR规定，隐私声明必须使用简单和明确的语言，并且内容必须简明易懂且易于获得。因而您的企业可能需要在所有的隐私声明中添加新的内容。同时，企业还需要对隐私声明、同意书和处理流程加以审查并作出相应修订。

Privacy Notices and Consents – Under the GDPR privacy notices must be concise, intelligible and easily accessible using clear and plain language. Additional content may be required to be inserted into all privacy notices. Privacy notices, consent forms and processes should be reviewed and amended accordingly.

- 个人权利 —— GDPR 不但对现有的个人权利范围进行了扩充，还引入了新的权利。因而企业应该建立起确保个人能够有效行使其权利的规程。

Individuals Rights – The GDPR extends existing rights and introduces new rights for individuals. Organizations must put in place procedures allowing individuals to effectively exercise their rights.

- 设计隐私、默认隐私和数据质量 —— 对GDPR的合规和遵守必须纳入与个人数据使用相关的所有处理进程和应用程序中。GDPR 还对数据保存和数据质量（如准确性）等作出了严格的规定。因而企业应据此对已经存在的相关程序加以审查和修改，否则就有必要重新开发和规范化程序。

Privacy by Design, Privacy by Default and Data Quality – Compliance with the GDPR must be embedded into all processes and applications which involve the use of personal data. The GDPR also contains strict rules on data retention and data quality, such as accuracy. Procedures should be reviewed and amended, if existing, or developed and formalized, as necessary.

- 数据分享 —— GDPR对数据处理器加诸了直接责任，并对管理数据处理器的数据控制器（包括对协议中的规定条款）作出了更加严格的规定。 GDPR 的规定还包括了针对联合数据控制器的新义务。因而，企业应对现有的处理器协议以及控制器到控制器协定和相关条款进行审查和更新。

Data Sharing – Direct liability is imposed on data processors, and stricter requirements are imposed on data controllers engaging data processors, including incorporating prescribed clauses in agreements. The GDPR also contains new obligations for joint data controllers. Processor agreements and controller-to-controller agreements/clauses should be reviewed and updated.

- 国际数据传输——GDPR对目前在欧洲经济区以外的个人数据传输必须有适当措施这一要求没有作出实质性的改变，但对违反行为的制裁力度大大增加。因而企业拥有合规机制的重要性和必要性也随之大大增加了。

International Data Transfers – The GDPR does not substantively change the current requirement to have adequate measures in place when transferring personal data outside the EEA, but the sanctions for non-compliance are substantially increased. It is now more important than ever that your organization has compliance mechanisms in place.

- 数据保护影响评估 (DPIAs) —— GDPR 要求企业在进行任何有关“高风险”的数据处理工作时执行 DPIA，并在某些情况下向监督机构咨询。因而企业应留心关注联合国世界车辆法规协调论坛(WP29)或关键成员国监督机构发布的指导文件，并在必要时审查和更新内部进程和程序，使之符合 DPIA 要求。

Data Protection Impact Assessments (DPIAs) – The GDPR requires businesses to carry out DPIAs in relation to any “high risk” data processing and to consult with the supervisory authority in certain circumstances. Organizations should look out for expected guidance from the WP29 or supervisory authorities from key Member States and, if necessary, review and update internal processes and procedures to conform with DPIA requirements.

- 数据安全和数据泄露管理流程——GDPR规定企业组织必须从技术层面和组织结构层面采取适当的数据安全保护措施，并且“在适当的情况下”采用GDPR所给出的具体措施。GDPR 还规定在任何情况下，企业组织都必须在72小时内毫不拖延地向监督机构汇报数据泄露事故，并将可能产生高风险的泄露事故信息通知受到影响的个人。有鉴于此，企业有必要对所需采用的数据安全保护措施进行深入了解，并在必要时对数据泄露管理流程进行修改以符合GDPR的要求 。

Data Security and Breach Management Process – Organizations must take appropriate technical and data security measures, including specific types of measures described in the GDPR, “where appropriate”. The GDPR also requires the reporting of data breaches to the supervisory authority without delay, and in any event within 72 hours, and to inform affected individuals about high risk breaches. It is important that businesses understand the required security measures and, if necessary, modify their breach management process to become GDPR compliant.

- 隐私治理 —— GDPR中规定了一项新的问责要求，即公司必须证明其遵守GDPR。在某些情况下，企业有必要任命一名数据保护官，而一套由适当的规章制度、员工培训及数据隐私意识所支持的公司治理结构是履行企业职责并证明其合规性的关键所在。企业必须在充分理解问责制要求的基础上对现有的规章制度进行审查、修改和补充以长期遵守。

Privacy Governance – The GDPR contains a new accountability requirement which requires a company to demonstrate its compliance with the GDPR. The appointment of a Data Protection Officer is mandatory in certain circumstances and a robust governance structure, supported by the appropriate policies and employee training and awareness, is critical to fulfilling the obligation to demonstrate compliance. Organizations must fully understand the accountability requirement and review, amend and supplement their existing policies to adhere to it.

Suggestion

建议

数据隐私保护一直以来都被顺理成章地作为一项技术问题来对待。然而，随着如今数据隐私及网络安全相关法律所覆盖的司法管辖区越来越广，企业将需要承担更多法律责任。

It may be natural to think of data privacy protection as mostly a technical issue. But as data privacy/cybersecurity laws start to move across borders, there are many legal obligations to be considered.

针对GDPR的准备工作是包含了多个步骤的复杂过程，其首要任务是对企业所收集的个人资料的具体情况以及存储地点进行评估。这不仅可以确定企业在GDPR合规方面存在哪些问题，还可以定义数据隐私法可能适用的其他司法管辖区（例如，中国、日本和卡塔尔最近颁布的新的法律条款或修订案都有可能对您所在企业的数据产生影响）。

Preparing for the GDPR, is a multi-step process that starts with an assessment of what personal data you collect and where it is stored. This can identify not only issues with GDPR compliance, but also other jurisdictions where data privacy laws may apply. For example, China, Japan and Qatar have recently enacted new laws/revisions that may impact your data.

由此看来，聘请一家拥有足够广泛的全球业务网络的法律顾问是十分必要的，因为企业将只需要与其一方进行合作就能够更有效地平衡潜在的冲突规则。根据对所收集的个人资料的评估结果，优秀的法律顾问能够与企业协商、研讨并确定最适合的解决方案，并通过与企业内部的IT 及信息安全团队或第三方技术解决方案供应商的紧密合作来实施这些方案。因此，我们建议您尽快采取行动，以尽早避免由于个人资料丢失所造成的天价处罚和由此带来的业务损失。

If your law firm is global enough, you will be able to work with one firm to more efficiently balance the potentially conflicting rules. Based on the assessment, a weighing of options should lead to creating the optimal business-friendly solution. A good firm should have the ability to help you implement those solutions, in cooperation with your IT/Information Security team or 3rd party technical solution vendor. The time to act is now in order to avoid the massive penalties and loss of business associated with lost personal data.

Contact / 联络人

Scott Warren
合伙人，东京分所
电话 +81 3 5774 1800
电邮 scott.warren@squirepb.com

詹智鹰
资深法律顾问，上海分所
电话 +86 21 6103 6356
电邮 olivia.zhan@squirepb.com

朱桔
高级法律顾问，上海分所
电话 +86 21 6103 6303
电邮 lindsay.zhu@squirepb.com

吴延华
法律顾问，北京分所
电话 +86 10 6589 3755
电邮 dean.wu@squirepb.com