# 亚太经合

## 组织隐私框架

CSA GCR cloud security GREATER CHINA REGION alliance ®

# 致谢

## 中文版翻译说明

《亚太经合组织隐私框架(2015)》由云安全联盟(CSA GCR)数据安全工作组下属个人数据安全专题组负责组织翻译。

## 翻译审校工作专家：

组长：高巍

组员：薛琨，张明敏，廖聪城，王贵宗

在此感谢以上参与该文档的翻译审校工作的专家及工作人员。如译文有不妥当之处，敬请读者联系 CSA 数据安全工作组给与雅正!

联系邮箱：info@c-csa.cn；
云安全联盟大中华区
2021 年 8 月 8 日
云安全联盟 CSA 公众号

# 亚太经合组织隐私框架 (2015)

## 目录

## 亚太经合组织隐私框架 (2015)

## 前言

亚太经合组织成员经济体认识到数字经济的巨大潜力，将继续扩大商业机会，降低成本，提高效率，改善生活质量，并促进小企业更多地参与全球商业。 一个在经济体内部和外部保护隐私的框架，来确保个人信息区域性转移利于消费者、企业和政府。 部长们已经签署亚太经合组织隐私框架，认识到制定有效的隐私保护措施的重要性，以避免信息流动的障碍，确保亚太经合组织地区持续的贸易和经济增长。

## 第一章．序言

1. 亚太经合组织各经济体认识到，在保持亚太地区各经济体之间以及各贸易伙伴之间信息流动的同时，保护信息隐私的重要性。 正如亚太经合组织各国部长在批准 1998 年《电子商务行动蓝图》时承认的那样，如果没有政府和企业的合作，就无法实现电子商务的潜力，"制定和实施技术和政策，来建立对安全、可靠的通信、信息和交付系统的信任和信心，并解决包括隐私在内的问题..."。 消费者对在线交易、信息网络和个人信息管理的隐私和安全的信任和信心，对于使成员经济体获得电子商务的好处和参与当今信息驱动的经济至关重要。 亚太经合组织经济体认识到，提高消费者信心和确保电子商务和创新的增长,一个关键部分是在尊重国内法律和法规、适用于信息隐私保护的国际框架，并加强亚太地区的信息安全的同时，通过合作来促进有效的信息隐私保护和亚太地区的信息自由流动。

2. 与互联网和其他信息网络相连的信息和通信技术，包括移动技术，使人们有可能从世界任何地方收集、储存和访问信息。 这些技术为个人、政府、企业和整个社会带来了社会和经济效益，包括增加消费者选择、市场扩张、生产力、教育、通信和产品创新。 然而，尽管这些技术使收集、分析和使用大量信息变得更容易和更便宜，但它们的设计和使用方式往往使这些活动无法被个人察觉。 个人

可能更难对其个人信息保持一定程度的控制。 结果是个人担心他们的信息被使用和滥用可能产生的有害后果。 因此，有必要在线上和线下的情况下推动和执行遵守道德的和值得信赖的信息实践，以加强个人和企业的信心。

3. 由于技术和信息流性质的变化，商业运营和消费者的期望已经发生了重大转变：企业和其他组织现在需要每天 24 小时同时输入和获取数据，以满足商业、客户和社会需求，并提供高效和具有成本效益的服务。不必要地限制这种信息流动或给它带来负担的监管体系，会对全球商业、经济和个人产生不利影响。 因此，在推动和执行道德信息实践的过程中，也有必要制定考虑到全球环境中的这些现实情况的保护隐私的体系。

4. 亚太经合组织经济体赞同基于原则的亚太经合组织隐私框架，认为它是鼓励发展适当的隐私保护措施和确保亚太地区信息自由流动的重要工具。

5. 该框架旨在促进整个亚太地区的电子商务，与经合组织《保护隐私和个人数据跨境流动指南》（经合组织指南）的核心价值一致，并重申了隐私对个人和信息社会的价值。该框架的上一版本（2005 年）是以经合组织指南（1980 年）为蓝本的，该指南在当时代表了关于什么是公平和值得信赖的个人信息处理的国际共识。更新后的《框架》（2015 年）借鉴了《经合组织指南》（2013 年）[1]中的概念，并适当考虑了亚太经合组织地区不同的法律特点和背景。

6. 该框架特别指出在保持信息流动的同时保护隐私的重要性，以及与亚太经合组织成员经济体特别相关的问题。 其实用和独特的方法是将注意力集中在一致的而非完全相同的隐私保护上。 通过这样的方式，它力求使隐私与商业和社会需求及商业利益相协调，同时，对成员经济体内部存在的文化和其他多样性给予适当的承认。

[1] www.oecd.org/internet/ieconomy/privacy-guidelines.htm

7. 本框架旨在为亚太经合组织经济体的企业和政府实体提供明确的指导和方向，说明常见的隐私问题以及隐私问题对合法商业行为和政府职能的影响。 它通过强调现代消费者的合理隐私期望来做到这一点。 企业和成员经济体应以符合本框架所列原则的方式，尊重个人的隐私利益。

8. 该框架的制定和更新是基于以下几点的重要性：

- 对个人信息实施适当的隐私保护，特别是避免个人信息被入侵和滥用的有害后果。
- 信息的自由流动对贸易，以及对发达和发展中市场经济体的经济和社会增长的重要性。
- 使在亚太经合组织成员经济体中收集、访问、使用或处理数据的全球公司能够在其组织内制定和实施统一的方法，以便在全球范围内获取和使用个人信息。
- 赋予隐私执法机构权力，以履行其保护个人隐私的任务。
- 推进国际和区域机制，包括亚太经合组织跨境隐私规则（CBPR）系统，以促进和实施隐私保护，并保持亚太经合组织经济体之间以及与其贸易伙伴之间信息流动的连续性。
- 鼓励各组织对其控制下的所有个人信息负责。
- 促进该框架、及其实施措施（如 CPEA 和 CBPR 体系）与其他地区的隐私做法之间的互操作性。

## 第二章 范围

亚太经合组织隐私框架第二章的目的是明确这些原则的涵盖范围。

| 核心定义 | 释义 |
| --- | --- |
| 9. 个人信息是指关于已识别或可识别个人的任何信息。 | 9. 该框架旨在适用于关于在世自然人而非法人的信息。 该框架适用于个人信息，即可以用来识别个人的信 |

息。 它还包括一些不能单独满足此条件的信息，这些信息不能单独满足此条件，但是与其他信息放在一起将可以识别一个人。 例如，某些类型的元数据经过汇总，可以揭示个人信息，并可以洞悉个人的行为，社交关系，私人偏好和身份。

10. 个人信息控制者是指控制个人信息的收集、持有、处理、使用、披露或转让的个人或组织。它包括指示另一个人或组织代表他或她收集、持有、处理、使用、转让或披露个人信息的人或组织，但不包括按照另一个人或组织的指示执行这些职能的人或组织。它也不包括收集、持有、处理或使用与个体、家庭或家族事务有关的个人信息的个人。

10. 该框架适用于公共和私营部门中控制个人信息的收集、持有、处理、使用、转移或披露的个人或组织。就本框架而言，如果一个人或组织指示另一个人或组织代表其收集、持有、使用、处理、转移或披露个人信息，则发出指示的人或组织是个人信息控制者，并负责确保遵守原则。个体通常会出于个人、家庭或家族的目的而收集、持有和使用个人信息。例如，他们经常保存地址簿和电话清单，或编写家庭通讯。本框架无意涵盖此类个人、家庭或家居活动。

11. 公开可用的信息是指个人在知情的情况下向公众提供或允许提供的有关个人的信息，或从以下方面合法获得和获取的信息。

a) 向公众提供的政府记录。

b) 新闻报道；或

c) 法律要求向公众提供的信息。

11. 该框架对可公开可用的信息的适用性有限。尤其是在信息已经公开的情况下，如果个人信息控制者不直接从有关个人那里收集信息，那么通知和选择要求往往是多余的。公开可用的信息可能包含在向公众提供的政府记录中，如有权投票的人

的登记册，或新闻媒体广播或发布的新闻项目中。

**补充定义**

12. **CBPR 体系**是 APEC 跨境隐私规则体系的缩写。[2]

12. 亚太经合组织领导人于 2011 年批准的亚太经合组织跨境隐私规则体系是一个基于自愿的问责制的方案，以促进亚太经合组织经济体之间尊重隐私的个人信息流动。它有四个主要组成部分。
    - 为成为 CBPR 体系责任机构设定标准。
    - 信息控制者被认可的责任机构认证为符合亚太经合组织 CBPR 体系的程序。
    - 评估标准，供认可的责任机构在审查信息控制者是否符合 CBPR 体系要求时使用；以及
    - 通过认可的责任机构提供的投诉程序，执行 CBPR 体系要求的安排，并由作为 CPEA 参与者的隐私执法机构（PEA）提供支持。

13. **CPEA** 是亚太经合组织跨境隐私执法安排的缩写，它是一个实用的多边机制，通过建立一个框架，使隐私执法机构能够在跨境隐私执法方

13. CPEA 是一个多边机制，使亚太经合组织地区的隐私执法机构能够在隐私法的跨境执法方面进行合作。亚太经合组织成员经济体的任何隐

[2] 更多信息请参考：www.cbprs.org

面进行合作，在这个框架下，当局可以在自愿的基础上分享信息，并以某些方式请求和提供协助。[3]

私执法机构都可以参加。CPEA 的目的是

- 促进亚太经合组织成员经济体的隐私执法机构之间的信息共享。
- 提供机制以促进隐私执法机构之间在执行隐私法方面的有效跨境合作；以及
- 鼓励与亚太经合组织地区以外的隐私执法机构分享信息和进行隐私调查和执法的合作。

14. **隐私执法机构**是指负责执行隐私法的任何公共机构，该机构有权进行调查和/或履行执法程序。

14. 隐私执法机构是一个公共机构，负责执行亚太经合组织经济体的隐私法。它将有权力进行调查和/或履行执法程序。一个经济体可以有一个以上的隐私执法机构。

15. **隐私法**是指亚太经合组织成员经济体的法律和法规，其执行具有保护符合亚太经合组织隐私框架的个人信息的效果。

15. 亚太经合组织成员经济体的隐私法有各种不同的形式。有些是一般性的隐私或数据保护法规，而其他的一些则采取部分的方法，涵盖特定领域，如信用报告或健康信息。在某些情况下，相关的法律规定包含在涉及电信或消费者保护等问题的更广泛的法律中。就本定义而言，

[3] CPEA的正式名称是 "亚太经合组织跨国界隐私执法合作安排"。更多信息请访问：www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx

这些法律被称为什么并不重要：重要的是法律的效果。

16. **PRP 体系**是 APEC 处理者隐私认可体系的缩写。

16. PRP 体系描述了处理者必须满足的基准要求，以便得到亚太经合组织认可的责任机构的认可，并就处理者的隐私政策和做法提供保证。PRP 体系帮助个人信息处理者证明他们有能力有效履行个人信息控制者的与处理个人信息有关的隐私责任义务。

**适用**

17. 考虑到每个成员经济体在社会、文化、经济和法律背景方面的差异，在实施这些原则时应具有灵活性。

17. 虽然亚太经合组织内的所有法律和实践的完全相同对电子商务来说并不是必须的，但亚太经合组织各经济体对隐私保护采取兼容的方法将大大促进国际商务和隐私执法合作。尽管如此，本框架认识到还需要考虑到各经济体之间的社会、文化和其他差异。

18. 本框架第三部分所包含的这些原则的例外情况，包括与国家主权、国家安全、公共安全和公共政策有关的，应该

a) 对满足与例外情况有关的目标来说是有限的和相称的；并且

b) (i) 向公众公布；或

18. 在国内实施本框架的经济体可采取适合其特定国情的适当例外。

在承认政府尊重隐私的重要性的同时，本框架无意阻碍为保护国家安全、公共安全、国家主权或实现其他重要公共政策目标而采取的法律

(ii) 根据法律规定。

授权的政府行动。尽管如此，成员经济体应努力确保这些活动对个人和组织的权利、责任和合法利益的影响尽可能地有限。

## 第三章 亚太经合组织信息隐私原则

19. 信息隐私原则应作为一个整体来看待和解释，而不是孤立看待特定的原则，因为它们之间存在着密切的相互关系。[4]

| 原则 | 释义 |
| --- | --- |
| **I. 预防伤害** | |
| 20. 认识到个人对隐私的合法期望，个人信息的保护应防止这种信息被滥用。此外，认识到滥用个人信息可能造成伤害的风险，具体义务应考虑到这种风险，补救措施应与收集、使用和转让个人信息所产生伤害的可能性和严重程度相称。 | 20. 本原则承认，本框架的主要目标之一是防止个人信息的滥用和随之而来的对个人的伤害。因此，隐私保护措施包括自律工作、教育和宣传活动、法律、法规和执法机制，应防止错误地收集和滥用个人信息对个人造成的伤害。<br><br>因此，组织控制措施应防止错误收集或滥用个人信息造成的伤害，并应与收集、使用或转移个人信息所 |

[4] 各项原则之间在语言使用上可能存在一些小的差异（例如，在原则中如何描述个人信息的使用）。在未来的修订项目中，如果将原则的措辞纳入其范围，可能会有效地统一语言。同时，除非上下文另有说明，个人信息的 "使用 "应被视为包括个人信息的收集、持有、处理、使用、披露或转让。

威胁的任何伤害的可能性和严重性相称。

如果发生了影响个人信息的重大安全漏洞，向隐私执法机构和/或有关个人发出通知可能有助于减少对有关个人造成有害后果的风险。[5]

## II. 声明

21. 个人信息控制者应就其在个人信息方面的做法和政策提供清晰和易于理解的声明，其中应包括
    a) 正在收集个人信息的事实；
    b) 收集个人信息的目的；
    c) 可能向哪些类型的人或组织披露个人信息；
    d) 个人信息控制者的身份和位置，包括如何就其做法和对个人信息的处理与他们联系的信息；
    e) 个人信息控制者为个人提供的限制使用和披露，以及访问和纠正其个人信息的选择和方法。

22. 应采取一切合理可行的步骤，确保在收集个人信息之前或之时提供此类通知。否则，这种通知应在实际可行的情况下尽快提供。

21. – 23. 本原则旨在确保个人能够知道收集了他们的哪些信息，以及这些信息将被用于何种目的。通过提供通知，个人信息控制者可以使个人在与该组织的互动中做出更明智的决定。

根据收集个人信息的背景，可以使用各种方法提供通知。例如，遵守本原则的一个常见方法是，个人信息控制者在其网站上发布通知。如果组织在离线情况下与个人接触，如当面或通过电话，可以使用张贴或书面通知或电话脚本。在其他情况下，例如在内部网站或员工手册中放置通知可能是合适的。在移动环境下发出通知存在着实际的挑战。为了在小屏幕上提供通知，个

[5] 请参考下文第 54 条。

| | |
|---|---|
| 23.个人信息控制者提供有关收集和使用公开信息的通知可能不合适。 | 人信息控制者可能要考虑标准通知、图标或其他措施的价值。<br><br>各组织应在收集有关个人的信息时或之前通知他们。同时，该原则也承认，在某些情况下，在收集信息时或之前发出通知是不可行的，例如，在某些情况下，数字技术会在潜在客户主动联系时自动收集信息，如使用 cookies 时经常出现的情况。<br><br>另外，如果个人信息不是直接从个人获得的，而是从第三方获得的，那么在收集信息时或之前发出通知可能是不可行的。例如，当保险公司为了提供医疗保险服务而从雇主那里收集雇员的信息时，保险公司在收集雇员的个人信息时或之前发出通知可能是不可行的。<br><br>此外，在有些情况下，没有必要提供通知，例如在收集和使用公开的信息，或商业联系信息和其他专业信息，以确定个人在商业环境中的专业身份。例如，如果一个人在商业关系中把他或她的名片给了另一个人，那么这个人不会期望得到关于为预期的商业目的收集和正常使 |

用该信息的通知。

除此以外，如果与某人在同一公司工作的同事向该公司的潜在客户提供该人的业务联系信息，该人不会期望得到有关该信息的转让或预期使用的通知。

**III. 收集限制**

24. 个人信息的收集应限于与收集目的相关的信息，任何此类信息应通过合法和公平的方式获得，并在适当情况下通知有关个人或征得其同意。

24. 本原则根据收集个人信息的目的来限制个人信息的收集。个人信息的收集应与此类目的相关，而实现此类目的的必要性和相称性可能是确定相关内容的因素。

该原则还规定，收集方法必须是合法的和公平的。因此，在许多经济体中，以虚假手段获取个人信息（例如，一个组织利用网络钓鱼、电话营销或借口电子邮件来欺诈性地将自己伪装成另一家公司，以欺骗消费者并诱使他们披露其信用卡号码、银行账户信息或其他敏感个人信息）可能被认为是非法的。因此，即使在那些没有明确法律禁止这些特定的收款方式的经济体，它们也可能被认为是不公平的收款方

式。

该原则还承认，在某些情况下，向个人提供通知或获得个人同意是不合适的。例如，在爆发食物中毒的情况下，相关卫生部门在没有通知个人或获得个人同意的情况下，从餐馆收集顾客的个人信息，以告知他们潜在的健康风险，是合适的。

## IV. 个人信息的使用

25. 所收集的个人信息应仅用于实现收集的目的和其他兼容或相关的目的，但以下情况除外。
    a) 得到个人信息被收集者的同意；
    b) 为提供个人要求的服务或产品所必需；或
    c) 根据法律和其他法律文书、公告和具有法律效力的声明的授权。

25. 本原则将个人信息的使用限制在满足收集目的和其他兼容或相关目的。在本原则中，"个人信息的使用 "包括个人信息的转让或披露。

本原则的应用需要考虑个人信息的性质、收集的背景、个人的期望和信息的预期用途。在确定某一目的是否与所述目的相一致或相关时，基本标准是扩展的使用是否源于或促进这些目的。例如，为 "兼容或相关的目的 "使用个人信息将扩展到以下事项：创建和使用中央数据库，以有效和高效的方式管理人事；由第三方处理雇员的工资单；或者，使用一个组织收集的信息，

以授予信贷，随后收集欠该组织的债务。

## V. 选择

26. 在适当的情况下，应向个人提供明确、突出、易懂、可获得和负担得起的机制，以行使对其个人信息的收集、使用和披露的选择。个人信息控制者在收集公开信息时可能不适合提供这些机制。

26. 选择原则的一般目的是确保个人在收集、使用、转移和披露其个人信息方面拥有选择权。无论选择是以电子方式、书面方式还是其他方式传达，关于这种选择的通知都应该措辞明确，并清楚、醒目地显示出来。

行使选择权的机制应该是个人可以使用和负担得起的。容易获得和方便是应该考虑的因素。

当一个组织提供有关行使选择权的现有机制的信息时，应考虑对信息及其传达方式进行调整，以使其对特定的个人群体更加 "容易理解"（例如，如果信息是针对儿童的，则以适合其年龄的方式提供相关语言的解释）。

本原则还通过 "在适当的情况下 " 这一引言承认，在某些情况下，没

有必要提供一个行使选择的机制。

在许多情况下，在收集可公开获得的信息时，提供一个行使选择权的机制是不必要的，也是不实际的。例如，当从公共记录或报纸上收集个人的姓名和地址时，没有必要提供一个机制来行使选择权。

在特定和有限的情况下，在收集、使用、转让或披露其他类型的信息时，提供一个行使选择权的机制是没有必要或不可行的。

例如，当商业联系信息或其他能识别个人职业身份的专业信息在商业背景下被交换时，提供一个行使选择权的机制通常是不切实际或不必要的，因为在这些情况下，个人会期望他们的信息以这种方式被使用。

此外，在某些情况下，当雇主为就业目的使用其雇员的个人信息时，提供一个行使选择权的机制是不可行的。例如，如果一个组织决定集中管理人力资源信息，就不应该要求该组织在从事这种活动之前向其

雇员提供一个行使选择的机制。

## VI. 个人信息的完整性

27. 个人信息应准确、完整，并在使用目的的必要范围内保持最新。

27. 本原则认为，个人信息控制者有义务保持记录的准确性和完整性，并在必要时对其进行更新以实现使用目的。根据不准确、不完整或过时的信息做出关于个人的决定可能不符合个人或组织的利益。

## VII. 安全保障措施

28. 个人信息控制者应以适当的保障措施来保护他们所持有的个人信息，以防止风险，如个人信息的丢失或未经授权的访问，或未经授权的破坏、使用、修改或披露信息或其他滥用行为。这类保障措施应与受到威胁的可能性和严重性、信息的敏感性和持有信息的背景相称，并应定期审查和重新评估。

28. 本原则承认，个人信息被委托给他人的个人有权期望他们的信息得到合理的安全保障措施的保护。

## VIII. 访问和更正

29. 个人应该能够

29. – 31. 获取和更正个人信息的能

a) 从个人信息控制者那里得到确认，即个人信息控制者是否持有关于他们的个人信息。
b) 在提供充分的身份证明后，向他们传达有关他们的个人信息。
   i. 在一个合理的时间内。
   ii. 收费（如果有的话）不过分。
   iii. 以合理的方式；iv. 以普遍可以理解的形式；和。
c) 对与他们有关的个人信息的准确性提出质疑，并在可能和适当的情况下，要求纠正、完成、修改或删除这些信息。

30. 应提供这种查阅和纠正的机会，除非在以下情况下。
   i. 这样做的负担或费用将是不合理的，或与有关案件中个人隐私的风险不相称；
   ii. 由于法律或安全原因或为了保护机密商业信息，该信息不应披露；或
   iii. 个人以外的其他人的信息隐私将受到侵犯。

31. 如果(a)或(b)项下的请求或(c)项下的质疑被拒绝，应向个人提供原因，并能够对这种拒绝提出质疑。

力，虽然被普遍认为是隐私保护的一个核心方面，但并不是一项绝对的权利。

本原则包括获取信息的具体条件，包括与时间、费用以及提供信息的方式和形式有关的条件。在这些领域中，什么被认为是合理的，将因情况不同而不同，例如信息处理活动的性质。访问权也将受到安全要求的制约，这些要求排除了直接访问信息的可能性，并要求在提供访问权之前提供充分的身份证明。

访问必须以合理的方式和形式提供。合理的方式应包括组织和个人之间的正常互动方法。例如，如果交易或请求中涉及计算机，而个人的电子邮件地址是可用的，电子邮件将被视为提供信息的 "合理方式"。与个人进行过交易的组织可以合理地期望以类似于以前与所述个人交流时使用的形式，或以该组织内部使用和可用的形式回答请求，但不应理解为需要单独的语言翻译或将代码转换为文本。

一个组织为回应获取信息的请求而提供的个人信息的副本和该组织使用的任何代码解释都应该是容易理解的。这一义务不包括将计算机语

言（如机器可读指令、源代码或目标代码）转换为文本。然而，如果一个代码代表一个特定的含义，个人信息控制者必须向个人解释该代码的含义。例如，如果该组织持有的个人信息包括个人的年龄范围，并由一个特定的代码表示（例如，"1 "表示 18-25 岁，"2 "表示 "26-35 岁，等等），那么在向个人提供这种代码时，该组织应向个人解释该代码代表什么年龄范围。

如果个人要求获取他或她的信息，应以目前持有的语言提供该信息。如果信息所使用的语言与最初收集的语言不同，并且如果个人要求以该原始语言提供信息，如果个人支付翻译费用，组织应以原始语言提供信息。

提供获取和更正信息的能力的程序细节可能因信息的性质和其他利益而不同。由于这个原因，在某些情况下，改变、压制或删除记录可能是不可能的、不可行的或不必要的。

与获取信息的基本性质相一致，各组织应始终真诚地努力提供信息。例如，如果某些信息需要保护，并且可以很容易地与其他被要求查阅

的信息分开，该组织应该编辑受保护的信息并提供其他信息。

然而，在某些情况下，各组织可能有必要拒绝获取和更正信息的要求，本原则规定了必须满足的条件，以使这种拒绝被认为是可以接受的，其中包括。要求对个人信息控制者构成不合理的费用或负担的情况，例如，当要求访问的性质是重复的或无理取闹的时候；提供信息将构成违法或损害安全的情况；或者，为了保护一个组织已经采取措施防止披露的商业机密信息，有必要进行披露，而披露将有利于市场上的竞争者，例如特定的计算机或建模程序。

"商业机密信息 "是指一个组织已采取措施防止披露的信息，如果这种披露会促使市场上的竞争者使用或利用该信息损害该组织的商业利益，从而造成重大经济损失。一个组织使用的特定计算机程序或业务流程，该程序或业务流程的细节可能是机密商业信息。如果机密的商业信息可以很容易地与其他被要求查阅的信息分开，组织应编辑机密的商业信息，并提供非机密的信息，只要这些信息构成有关个人的个人信息。在无法将个人信息与商

业机密信息分开的情况下，以及在批准获取信息会暴露该组织自身的上述商业机密信息，或会暴露另一组织的商业机密信息，且该组织负有保密义务的情况下，该组织可以拒绝或限制获取。

当一个组织以上述理由拒绝获取信息的请求时，该组织应向个人解释其做出这一决定的原因，并提供如何质疑这一拒绝的信息。如果这种解释会违反法律或司法命令，则不期望该组织提供这种解释。

**IX.问责制**

32. 个人信息控制者应负责遵守使上述原则生效的措施。当个人信息被转移给另一个人或组织时，无论是在国内还是国际上，个人信息控制者都应获得个人的同意，或尽职尽责，并采取合理措施，确保接收者或组织将按照这些原则保护信息。

32. 高效和具有成本效益的商业模式往往需要在不同地点的不同类型的组织之间进行信息转移，而且关系各不相同。在转移信息时，个人信息控制者应负责确保接收者在未获得同意的情况下按照这些原则保护信息。因此，信息控制者应采取合理措施，确保信息在被转移后能按照这些原则得到保护。

在某些情况下，这种尽职调查可能是不切实际或不可能的，例如，当个人信息控制者和被披露信息的第三方之间没有持续的关系。在这种情况下，个人信息控制者可以选择

使用其他手段，如获得同意，以确保信息得到符合这些原则的保护。然而，在国内法律要求披露的情况下，个人信息控制者将被免除任何尽职调查或同意的义务。

个人信息控制者帮助确保对其持有的个人信息负责的一个有用手段是制定一个隐私管理计划。[6]

## 第四章 实施

33. 第四部分为成员经济体提供有关实施亚太经合组织隐私框架的指引。第一部分着重于成员经济体在国内实施该框架时应考虑的措施，而第二部分则列出整个亚太经合组织实施该框架的跨境要素的安排。

### A. 国内实施指南

34. 成员经济体在考虑采取旨在国内实施亚太经合组织隐私框架的措施时，应考虑到以下基本概念：

#### I. 使隐私保护和信息流动的利益最大化

35. 个人信息的收集、持有、处理、使用、转移和披露的方式应能保护个人隐私，并使个人和经济体能够从境内和跨境的信息流动中获得最大利益。

36. 因此，作为建立或审查其隐私保护以落实亚太经合组织隐私框架的一部分，成员经济体应采取一切合理和适当的步骤，以确定和消除不必要的信息流动障碍，并避免产生任何此类障碍。

[6] 请参考下文第 43-45 条。

## II. 落实亚太经合组织隐私框架

37. 为落实本框架并确保对个人的隐私保护，有几种选择，包括立法、行政、行业自律或这些政策工具的组合。在实践中，本框架旨在以灵活的方式实施，以适应各种执法模式，包括通过隐私执法机构、多机构执法机构、指定行业机构组织、法院和法庭，或成员经济体认为适当的上述组合。

38. 各成员经济体实施本框架的方式往往不同。个别成员经济体可能决定，不同的信息隐私原则需要不同的国内实施方式。无论在特定情况下采取什么方法，总的目标应该是在亚太经合组织地区发展兼容的隐私保护方法，并尊重个别经济体的要求。

39. 亚太经合组织经济体应采取非歧视性做法，落实本框架的原则，并保护个人免受发生在该成员经济体管辖范围内的隐私侵犯。例如，成员经济体应确保实施本框架保护措施的法律或其他方法，不妨碍生活在其他经济体的个人从这些保护措施中受益。

40. 政府机构和其他利益相关者之间的协调对于确定加强隐私而不对国家安全、公共安全和其他公共政策目标造成障碍的方法很重要。

41. 成员经济体应考虑建立和维护隐私执法机构。应向已成立的隐私执法机构提供必要的管理、资源和技术支持，以有效行使其权力，并在客观、公正和一致的基础上作出决定。

42. 隐私执法机构可能会发现，对选定的监督工作采用基于风险管理的方法是有益的。在允许的情况下，根据侵犯隐私采取或建议采取的行动可能造成的伤害的可能性和严重程度来确定其执法工作的优先次序。[7]

[7] 参见预防伤害原则

## III. 隐私管理体系

43. 一个可操作的隐私管理方案将为个人信息控制者提供一个良好的基础，以证明它正在遵守实施本框架中的隐私保护措施。

44. 因此，成员经济体应考虑鼓励个人信息控制者为其控制的所有个人信息制定和实施隐私管理方案。隐私管理方案应

a) 适应个人信息控制者的结构和业务规模，以及其控制的个人信息的数量和敏感程度；

b) 在考虑到对个人存在潜在危害的风险评估的基础上，提供适当的保障措施；

c) 建立内部监督机制，并对查询和事件进行及时响应和反馈；

d) 由指定的负责人和受过适当培训的人员进行监督；

e) 在受到监督的同时应当定期更新该隐私管理方案。

45. 个人信息控制者应准备好在该经济体的主管隐私执法机构的要求下，或在其他适当实体的有效要求下，如根据 CBPR 制度或根据实施本框架的行业行为准则指定的问责机构，展示其隐私管理方案。

## IV. 促进实施保护隐私的技术措施

46. 技术措施可以通过补充和完善对隐私的法律保护，对国内隐私制度的整体有效性和影响作出重大贡献。因此，在考虑实施《框架》的方法时，成员经济体应促进并实施有助于保护隐私的技术措施。

47. 例如，成员经济体可以鼓励个人信息控制者充分利用现有的技术保障和措施。此外，他们可以促进研究和开发，鼓励进一步的隐私保护创新，并支持制定技术标准，将最佳隐私保护实践纳入系统工程。

## V. 公共教育和交流

48. 为使本框架产生实际效果，它必须为人们所了解并可获得。因此，成员经济体应

a) 宣传其隐私法律、并在国内安排如何为个人提供隐私保护的活动。

b) 开展活动，提高以下人士的认识

i 个人信息控制者了解本经济体的隐私保护要求和控制者的责任；

ii 个人信息处理者了解有助于有效履行个人信息控制者在处理个人信息方面的隐私义务的做法；

iii 个人了解他们如何报告违法行为以及如何寻求补救。

c) 鼓励或要求隐私执法机构和其他负责管理国内建立隐私保护的机构（例如，CBPR 制度的问责机构或为实施自律计划而建立的机构）酌情公开报告其活动情况。

## VI. 公私部门内部和部门之间的合作

49. 非政府实体的积极参与将有助于确保本框架的全部利益得以实现。因此，成员经济体应与相关的非政府利益相关者进行对话，包括那些代表公民、消费者和行业以及技术和学术界的非政府利益相关者，以获得关于隐私保护和信息流问题的投入，并寻求合作以推进本框架的目标。此外，尚未建立国内隐私保护制度的成员经济体在制定隐私保护措施时应充分注意非政府利益相关者的利益和需求。

50. 成员经济体应寻求非政府实体的合作，如代表公民和消费者的实体，以提高公众对隐私保护问题的认识。此外，成员经济体应鼓励这些实体积极参与促进和支持个人的隐私利益，例如，将投诉提交给隐私执法机构并公布这些投诉的结果。

51. 成员经济体应考虑制定战略，以反映出在政府机构间实施隐私保护的协调方法。

52. 成员经济体还应考虑在公共和私营部门以及非政府利益相关方之间开展协商和能力建设工作，例如，包括：

    a) 发展或支持组织内负责隐私保护的个人群体；

    b) 制作信息材料和安排经验分享活动。

## VII. 在个人隐私受到侵犯的情况下提供适当的补救措施

53. 成员国的隐私保护制度应包括对侵犯隐私行为的适当补救措施，其中可包括补救、阻止侵权行为继续发生的能力，以及其他补救措施。在确定对侵犯隐私行为的补救措施范围时，成员经济体应考虑到一些因素，包括：

    a) 该成员经济体提供隐私保护的特定制度（例如，立法执法权，其中可能包括个人诉诸法律的权利，行业自律，或各种制度的组合）；

    b) 拥有一系列与此类违法行为对个人造成的实际或潜在伤害程度相对应的补救措施的重要性。

54. 一个成员经济体应考虑鼓励或要求个人信息控制者在发现影响其控制的个人信息的重大安全漏洞时，酌情向隐私执法机构和/或其他相关机构发出通知。如果有理由相信该漏洞可能会影响到个人，在可行和合理的情况下，应鼓励或要求及时直接通知受影响的个人。

## VIII. 亚太经合组织隐私框架的国内实施情况报告机制

55. 成员国应通过完成和定期更新信息隐私个人行动计划（IAP），向亚太经合组织通报该框架在国内的实施情况。

### B. 国际实施指南

56. 在处理亚太经合组织隐私保护框架的国际实施时，根据第四章 A. 国内实施指南部分的规定，成员经济体应考虑与保护个人信息隐私有关的以下几点：

### I. 成员经济体之间的信息共享

57. 鼓励成员经济体就对隐私保护有重大影响的事项进行分享、交流、调查和研究。

58. 鼓励各成员经济体在与隐私保护有关的问题上相互教育，分享和交流有关宣传、教育和培训计划的信息，以提高公众对隐私保护和遵守相关法律法规重要性的认识。

59. 鼓励成员经济体就调查违反隐私保护的各种技术和解决涉及此类违反行为的争端的监管战略分享经验，例如，包括投诉处理和替代争端解决机制。

60. 成员经济体应指定并向其他成员经济体公布其管辖范围内的公共机构，这些机构将负责促进各经济体之间在隐私保护方面的跨境合作和信息共享。

61. 成员经济体应鼓励制定具有国际度量的衡量标准，为有关隐私和个人信息流动的政策制定过程提供标准。

### II. 调查和执法方面的跨境合作

62. 考虑到现有的国际安排（包括 CPEA）和现有的或正在制定的自我监管或共同监管方法，并在国内法律和政策允许的范围内，成员经济体应扩大使用现有的合作

安排，并考虑在必要时制定额外的合作安排或程序，以促进隐私法执行方面的跨境合作。这种合作安排可以采取双边或多边安排的形式。

63. 对上段的解释是，成员经济体有权以遵守合作的请求不符合国内法律、政策或优先事项为由，或以资源限制为由，或以在有关调查中没有共同利益为由，拒绝或限制就特定调查或事项进行合作。

64. 在隐私法的民事执法中，跨境合作安排可包括以下方面：

a) 具备迅速、系统和有效地通知其他成员经济体的指定公共机构的调查或隐私执法行动的机制，同时这些调查或隐私执法行动针对的是不符合本框架规定的保护措施的行为，并且可能影响这些其他经济体的个人或个人信息控制者。

b) 具备有效分享必要信息的机制，以便在跨境隐私调查和执法案件中成功合作。

c) 具备在隐私执法案件中的调查协助机制。

d) 具备根据非法侵犯隐私的严重程度、所涉及的实际或潜在危害以及其他相关考虑，确定与其他经济体的公共当局合作的案件的优先次序的机制。

e) 采取措施，对根据合作安排交流的信息保持适当的保密性。

## III. 跨国界隐私机制

65. 亚太经合组织认识到在保持个人信息跨境自由流动的同时保护隐私的重要性，并鼓励成员经济体实施该框架，确保提供个人信息能够安全和负责任地流动的条件，例如通过使用 CBPR 制度。

66. 成员经济体将努力支持发展和承认或接受跨境隐私机制，供各组织在亚太经合组织区域内传输个人信息时使用，同时认识到各组织仍有责任遵守当地的隐私要求以及所有适用法律。此类机制应适用亚太经合组织信息隐私原则。

67. 为落实第 65 段，各成员经济体开发了 CBPR 制度[8]，该制度为参与经济体提供了一个实用的机制，以便在国际、跨境背景下实施亚太经合组织隐私框架，并为各组织提供了一种跨境转移个人信息的方式，使个人可以相信其个人信息的隐私得到保护。

68. 成员经济体与适当的利益相关者合作，开发了 PRP 制度，以补充 CBPR 制度，帮助个人信息处理者证明他们有能力且有效履行个人信息控制者在处理个人信息方面的义务。

## IV. 跨境传输

69. 一个成员经济体应避免[9]限制个人信息在其与另一个成员经济体之间的跨境流动，相关经济体应当(a)制定了实施本框架的立法或监管文书，或(b)存在足够的保障措施，包括有效的执法机制和个人信息控制者制定的适当措施（如 CBPR），以确保持续保护水平符合本框架和实施本框架的法律或政策。

70. 对个人信息跨境流动的任何限制都应与其转移所带来的风险相匹配，同时应考虑到个人信息的敏感性，以及跨境转移的目的和背景。

## V. 隐私框架之间的互操作性

71. 认识到个人信息的流动不会止于区域边界，各成员经济体应鼓励和支持制定国际合作安排，以促进使本框架产生实际效果的隐私制度或机制之间的互操作性。

[8] 2011 年领导人宣言指出，"我们将采取以下步骤，进一步开放市场和促进区域贸易。[……]实施亚太经合组织 CBPR，以减少信息流动的障碍，加强消费者隐私，并促进各区域数据隐私制度的互操作性。"(http://www.apec.org/Meeting-Papers/Leaders-Declarations/2011/2011_aelm.aspx)

[9] 跨境数据流动仍然受制于成员经济体适用的国内法律、法规以及国际协议和承诺。

72. 提高隐私框架的全球互操作性可以带来改善个人信息流动的好处，有助于确保当个人信息流向成员经济体之外时，隐私保护得到维持，并可以简化个人信息控制者和处理者的合规要求。全球互操作性还可以帮助个人在全球环境中维护其隐私权，并帮助当局改善跨境隐私执法的方式。

CSA GCR cloud security alliance GREATER CHINA REGION ®


官网：http：//c-csa.cn

微信号：csagcr

邮箱：info@c-csa.cn

电话：18024312752


CSA 大中华区公众号