ABeam Consulting®

Build Beyond As One.

中国个人信息保护和网络安全相关法律法规的趋势与应对

Trends and Responses in Personal Information Protection and Cybersecurity-Related Laws in China

2025.08

引言

在数字化时代背景下，网络安全与个人信息保护已成为社会关注的重点领域。随着互联网技术的广泛应用，线上活动日益频繁，相关数据处理需求显著增长。当前全球范围内网络威胁形态持续演变，各国正通过立法手段加强风险防控。

中国也不例外，随着《网络安全法》等法律法规的逐步完善，企业必须遵守相关法律法规要求。

本报告首先概述主要国家·组织在网络安全与个人信息保护相关法律法规制度的现状与特点。特别聚焦欧盟、美国及日本，具体解析各国·组织如何通过法律法规制度保护个人信息并强化网络安全。

其次，在对照主要国家·组织异同点的基础上，概述中国网络安全与个人信息保护法律法规体系的现状与特征。

最后，基于ABeam多年的实践经验，系统性地阐述企业合规应对流程，并提出全球化视角下的解决方案。

我们希望本报告能够深化各界对网络安全与个人信息保护的认知，为企业及个人采取合规措施提供有效指引。

目录

第一章

主要国家·组织个人信息保护和网络安全相关法律法规概要

1.1 主要国家·组织的法律法规动态

近年来，全球个人信息保护和网络安全的法律法规不断发展。特别是，随着数字化的进步，保护个人信息和网络安全的重要性日益增加。

在欧盟， 通用数据保护条例 (GDPR) 自 2018 年实施以来已成为全球数据保护标准之一。

在美国，各州的隐私保护法不尽相同。《加州消费者隐私法》(CCPA) 及其修订版《加州隐私权法》(CPRA) 创建了与 GDPR 类似的法律法规，并为消费者提供了更大的数据透明度和控制权。

在亚洲地区，个人信息保护相关的法律法规监管也在不断加强。日本于2022年修订了《个人信息保护法》，新规强化了数据泄露时的报告义务，并进一步保障个人权利。

在中国，从2017年《网络安全法》施行以来，《数据安全法》、《个人信息保护法》等相关法律法规和指南相继出台。

后续内容中，我们将就这些主要国家·组织的法律法规的要点进行阐述。

欧盟[1]
● 2016年：网络与信息系统安全指令(NIS 指令)
● 2018年：通用数据保护条例(GDPR)
● 2023年：NIS2指令

美国[2]
● 2018年：加州消费者隐私法(CCPA)
● 2022年：关键基础设施网络事件报告法(CIRCIA)
● 2023年：加州隐私权法(CPRA)

日本[3]
● 2005年：个人信息保护法
● 2015年：网络安全基本法

[1]. 概要整理自：https://eur-lex.europa.eu/

[2]. 概要整理自：https://oag.ca.gov/ 和https://www.federalregister.gov/

[3]. 概要整理自：https://laws.e-gov.go.jp/

1.2 欧盟相关法律法规概要

个人信息保护

欧盟出台了多项旨在保护个人信息并加强数字时代网络安全的法律法规，特别重要的是2018年正式生效的《通用数据保护条例》(General Data Protection Regulation，简称GDPR)。除了加强个人权利外，它还为企业明确了广泛的适用范围和对违法行为的严厉处罚规定。

此外， GDPR 也对其他国家的法律法规体系产生了深远影响。

【GDPR概要[1]】

适用范围	• 它不仅适用于在欧盟境内开展业务的企业，也适用于所有使用或处理欧盟公民个人信息的企业。因此，欧盟以外的企业也将受到GDPR的约束。
个人数据的定义	• 与已识别或可识别个人相关的任何信息。在许多情况下，cookie等数字数据也被认为属于此类。
个人权利	• 它强化了数据主体(个人)的权利，明确规定了数据访问权、更正权、删除权(“被遗忘权”)、数据可移植权。
数据出境	• 原则上不允许将个人数据带出(转移)至欧盟以外的地区。数据转移需要严格遵守“数据跨境传输规则”。
处罚	• 违反GDPR的罚款非常高，最高可达年营业额的4%或2000万欧元，以较高者为准。

[1]. 概要整理自：https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1743906443998

1.2 欧盟相关法律法规概要

网络安全

欧盟也注重加强网络安全，2016年欧盟发布了《网络与信息系统安全指令》(The Directive on Security of Network and Information Systems，简称NIS 指令)，旨在加强关键基础设施的安全，提高其抵御网络攻击的能力。尽管NIS指令为加强欧盟国家的安全做出了贡献，但数字化的快速发展以及各国之间对策水平的差异，会使一些成员国更容易受到网络威胁，从而使整个欧盟面临风险。为了规避这些风险，修订后的NIS2指令于2023年生效，欧盟成员国需要在2024年10月之前将该指令纳入其国内相关法律法规体系。

企业也须遵照该指令采取高度安全措施，发生违规行为将被处以高额罚款。

【NIS2指令概要[1]】

对象	• 在欧盟境内提供服务的基础设施实体和重要实体。 • 基础设施实体：能源、交通、银行、金融市场基础设施、医疗保健、饮用水、数字基础设施等。 • 重要实体：邮政/快递、化工、食品、制造业等。
必要的安全措施	• 相关实体必须采取全方位的灾难应对措施。 • 系统安全政策、突发事件对应计划、业务可持续性计划、供应链安全对策、培训、准入管理步骤等。
报告义务	• 当发生重大突发事件时，必须在24小时内发出早期警告，并在一个月内向当局提交最终报告书。 • 当局有权对基础设施实体进行监管，包括突击检查和记录调查。
处罚	• 基础设施实体：最高1000万欧元或该实体全球年营业额的2%的罚款，以较高者为准。 • 重要实体：最高700万欧元或该实体全球年营业额的1.4%的罚款，以较高者为准。

[1].概要整理自：https://www.nis-2-directive.com/NIS_2_Directive_Articles.html

1.3 美国相关法律法规概要

个人信息保护

《加州消费者隐私法》(California Consumer Privacy Act，简称CCPA) 于2018年经加州议会通过，成为美国首部综合性州级个人信息保护立法。2020年，《加州隐私权法案》 (California Privacy Rights Act，简称CPRA) 通过，作为 CCPA的修正和补充版本，于2023年正式生效。

其他州也陆续制定符合各自特点的隐私相关法律法规，纳入CCPA和欧盟GDPR的要素。

在联邦政府层面，《美国数据隐私保护法》(American Data Privacy and Protection Act，简称ADPPA)在2022年首次通过了众议院能源和商业委员会的表决，国民们都很期待该法能够正式立法通过。

【CPRA概要[1]】

适用范围	• 在加州开展业务且满足特定条件(例如年总营业额超过2500万美元)的营利性企业/组织。这意味着注册地在加州以外的企业也将受到CPRA的约束。
个人信息定义	• 识别或可以直接/间接与特定消费者或家庭合理关联的信息。在许多情况下，cookie等数字数据也被认为属于此类。
个人权利	• 消费者权利包括知情权、个人信息删除权、个人情报买卖或共享的拒绝权、未成年人个人信息使用的许可权、更正权等。
数据出境	• 没有直接或单独规范数据跨境传输的规定。
处罚	• 每次违规行为最高可处以2,500美元的罚款(涉及16岁以下人士个人信息的故意/违规行为可处以7,500美元的罚款)。此外，每次事故消费者可获得最高750美元的赔偿权利，这意味着赔偿金额的总额可能很高。

[1].概要整理自：https://www.caprivacy.org/cpra-text/

1.3 美国相关法律法规概要

网络安全

在网络安全方面，《关键基础设施网络事件报告法》(Cyber Incident Reporting for Critical Infrastructure Act of 2022，简称CIRCIA)于2022年经美国总统签署生效。该法案通过建立强制报告机制，强化政府与私营部门在网络威胁情报共享和协同防御方面的合作。随后，2024年，美国网络安全和基础设施安全局(Cybersecurity and Infrastructure Security Agency，简称CISA)公布了CIRCIA相关的实施草案(征求意见稿)。如果获得通过，该草案将要求16个关键基础设施领域的众多企业采取应对措施，包括化学工业、通信、金融服务、食品与农业、能源、信息技术和医疗等。目前，该草案最终版仍在制定中。

【CIRCIA相关的实施草案概要[1]】

※尚未实施

对象	• 在关键基础设施领域超出规定规模企业标准的美国国内的实体。 • 关键基础设施：包括 化学工业、通信、金融服务、食品与农业、能源、信息技术、医疗等。
必要的安全措施	• 需要记录突发事件发生时报告所需的数据。 (一)与威胁行为者的互动(邮件、聊天等) (二)可疑的网络流量、文件、登录信息等。 (三)操作系统版本、补丁级别、配置设置等。
报告义务	• 必须在发现可报告事件后72小时内，或遭网络勒索支付赎金后24小时内向当局报告。
处罚	• 当局有权对对象实体进行信息提供或传唤要求。虚假报告可处以罚款或最高五年监禁(在与恐怖主义相关的案件中最高可判处八年监禁)。

[1].概要整理自：https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements

1.4 日本相关法律法规概要

个人信息保护

日本《个人信息保护法》(Act on the Protection of Personal Information，简称APPI)旨在确保个人信息得到妥善处理，同时保护个人权益。该法于2003年制定，2005年全面实施。此后，为了应对数字技术和全球化的进步，进行了多次修订。目前，每3年对实施情况进行一次审查，必要时进行修订。

【个人信息保护法(APPI)概要[1]】

适用范围	• 使用日本公民的个人信息、个人关联信息或化名、匿名处理后的个人信息提供商品或服务的企业/机构。该法同样适用在国外使用日本公民个人信息的情形。
个人信息定义	• 与生存个体相关的信息，可通过姓名、出生日期或其他可用来识别特定个人的信息。还包括可以识别个人身份的代码，例如指纹和ID号码。与个人信息相关联cookie等数字数据也被视为适用对象。
个人权利	• 规定了个人信息的披露、更正、暂停使用和删除的要求权。
数据出境	• 经本人同意，可以传输给国外的第三方。但可以自由传输至欧盟等已获得与日本同等级别的个人信息保护体系认证的国家和地区。
处罚	• 如有违反，个人将被处以最高一年的监禁或最高100万日元的罚款。企业将被处以最高1亿日元的罚款。

[1].概要整理自：https://laws.e-gov.go.jp/law/415AC0000000057

1.4 日本相关法律法规概要

网络安全

为应对日益频繁且复杂化的网络攻击，日本于2015年实施了《网络安全基本法》。该法规定设立政府网络安全战略本部并制定网络安全战略，要求中央政府、地方政府及关键基础设施运营商等主体切实强化网络安全防护措施。

然而，与欧盟和美国相比，日本在关键基础设施运营商的具体安全义务规定及违规处罚机制尚存完善空间，相关法律法规体系的强化仍处于持续研讨阶段。

【网络安全基本法概要[1]】

对象	• 国家政府、地方公共组织、关键社会基础运营商、网络相关运营商等。 • 关键基础设施：电力、燃气、化工、航空、铁路、信息通信、金融、医疗等。
必要的安全措施	• 关键基础设施运营商需要自主推动网络安全标准制定、演练与培训、信息共享等工作。
报告义务	• 该法本身没有任何规定要求关键基础设施运营商或其他实体进行报告的义务。报告将根据各领域的单独指南进行规范。
处罚	• 如果网络安全委员会的相关人员泄露机密，将被判处一年以下有期徒刑或50万日元以下罚款。关于企业对网络安全措施不完备的处罚，本法并无直接规定。

[1].概要整理自：https://laws.e-gov.go.jp/law/426AC1000000104

1.5 小结

近年来，随着网络攻击风险的增加和数据保护意识的增强，主要国家·组织正积极推进相关法律法规制度的制定与修订，相关商业主体须即使采取合规措施。其中，欧盟以严苛的监管规则和高额处罚著称，其立法实践对全球数据保护制度产生显著影响。

基于上述国际立法动态，我们将在下一章节解读中国在个人信息保护及网络安全领域的核心法律法规框架。

个人信息保护相关法律法规要点汇总

	欧盟 (GDPR)	美国 (CPRA)	日本 (APPI)
数据出境	原则上禁止 (或遵守相关规则进行)	无规定	经本人同意即可 (与日本个人信息保护制度水平同等或更高的国家和地区之间可自由转移)
处罚	大额罚款	大额罚款	罚款和监禁 (力度低于美国与欧盟)

网络安全相关法律法规要点汇总

	欧盟 (NIS2指令)	美国 (CIRCIA新规草案) ※尚未实施	日本 (网络安全基本法)
报告义务	重大网络安全事件发生后 24小时内发布早期预警等	重大网络安全事件发生后 72小时内进行报告等	没有规定报告义务
处罚	大额罚款	罚款或5年以下监禁等	小额罚款 或一年以下监禁等

第二章

中国个人信息保护和网络安全相关法律法规概要

2.1 中国相关法律法规动态

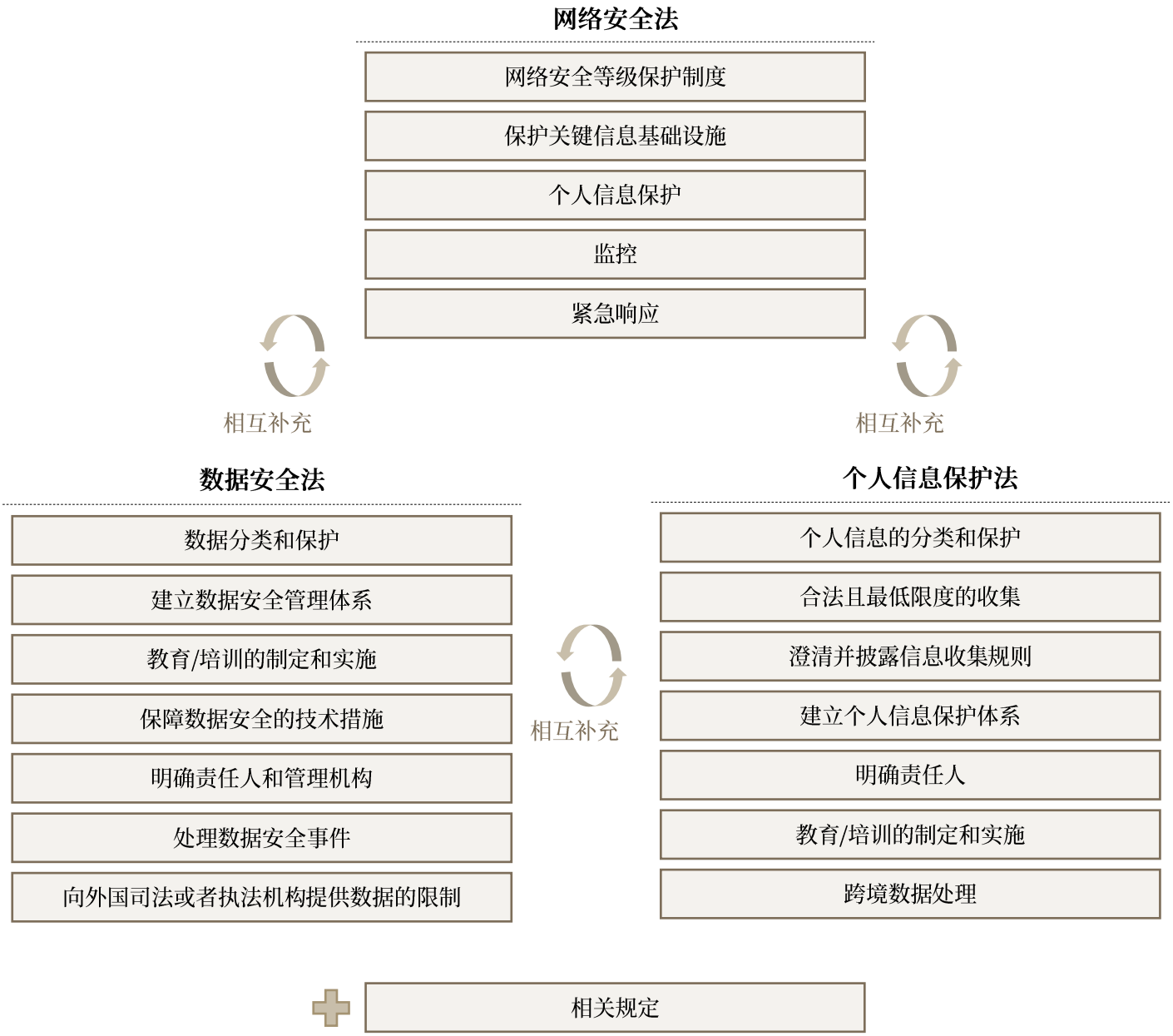
中国为应对伴随着数字化社会的发展而产生的风险，很早就开始制定网络安全和个人信息保护方面的法律法规。具体而言，迄今已颁布了三部主要的信息安全相关法律，首先是2017年的《网络安全法》，以及随后颁布的《数据安全法》和《个人信息保护法》。此外，相关法律法规也在逐步公布并执行，并要求企业遵守这些法律法规。

主要法律法规完善动态

2017年6月1日	《网络安全法》 为网络安全治理铺平道路
2020年1月1日	《密码法》 规范密码应用和管理
2021年9月1日	《数据安全法》 加强国家数据安全保障能力
2021年11月1日	《个人信息保护法》 加速个人信息保护合法化
2022年9月1日	《数据出境安全评估办法》 规范个人信息和重要数据的跨境处理
2023年6月1日	《个人信息出境标准合同办法》 提供个人信息跨境的标准化合同措施
2024年3月22日	《促进和规范数据跨境流动规定》 放宽个人信息跨境传输的程序要求
2024年9月14日	《敏感个人信息识别指南》 提供识别敏感个人信息的指南及具体示例
2025年1月1日	《网络数据安全管理条例》 明确基于数据安全相关三部法律应遵守的具体规定

2.2 三大基本法律概要

三部信息安全相关主要法律分别规定了重要数据和个人信息的保护、安全管理制度的建立，但各法内容有重叠之处，相互补充。此外，基于各法律的实施指南等相关规定也在陆续实施。因此，各企业需要了解三部法律及相关规定的具体内容，并采取综合应对措施。



2.3 网络安全法概要

为了应对网络攻击的增加以及由此产生的日趋复杂的网络和系统管理的需求，《网络安全法》于2017年6月1日起施行。该法旨在保障网络空间安全，维护国家安全和社会公共利益。《网络安全法》是一部重要立法，要求企业根据系统的重要程度，从管理和技术两个层面采取综合措施，确保网络安全，维护国家安全和社会公共利益。

企业应当遵守该法的规定，并采取适当措施加强网络安全。

【网络安全法概要】

对象	• 在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。
必要的 安全措施	• 网络运营者应当按照网络安全等级保护制度的要求，履行安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改 。
报告义务	• 发现网络产品或服务存在安全缺陷等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。 • 关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。 等
处罚	• 违法行为将根据其严重程度予以处罚。 严重的将被处以高额罚款。相关业务也有可能被暂停。

2.4 网络安全等级保护制度

该体系从“受侵害的客体”和“对客体侵害程度”两个角度对信息系统的安全等级进行评估，分为5个等级，并要求根据每个等级采取适当的安全措施。

【等级的判断标准[1]】

受侵害的客体	对客体侵害程度		
	一般损害	严重损害	特别严重的损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序和公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

【等级保护响应流程[1]】

[1]. 概要整理自《GB/T 22240—2020 信息安全技术 网络安全等级保护定级指南》和《GB/T 28449-2018 信息安全技术 网络安全等级保护测评过程指南》

2.5 个人信息保护法概要

作为中国首部全面规范个人信息保护的专门法律，《中华人民共和国个人信息保护法》于2021年11月1日正式施行。该法系统构建了涵盖个人信息收集、使用、存储、共享等全生命周期的规则体系，强化了个人在信息处理活动中的权利保障。

【个人信息保护法概要】

适用范围	• 在中华人民共和国境内处理自然人个人信息的活动，适用本法。 • 在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动，有下列情形之一的，也适用本法： (一)以向境内自然人提供产品或者服务为目的； (二)分析、评估境内自然人的行为； (三)法律、行政法规规定的其他情形。
个人信息定义	• 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。 • 个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。
个人权利	• 个人对其个人信息的处理享有知情权、决定权，有权限制或者拒绝他人对其个人信息进行处理；法律、行政法规另有规定的除外。 • 个人有权向个人信息处理者查阅、复制其个人信息；有本法第十八条第一款、第三十五条规定情形的除外。个人请求查阅、复制其个人信息的，个人信息处理者应当及时提供。 • 个人发现其个人信息不准确或者不完整的，有权请求个人信息处理者更正、补充。 • 个人有权要求个人信息处理者对其个人信息处理规则进行解释说明 • 自然人死亡的，其近亲属为了自身的合法、正当利益，可以对死者的相关个人信息行使本章规定的查阅、复制、更正、删除等权利；死者生前另有安排的除外。 等
数据出境	• 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。 中华人民共和国缔结或者参加的国际条约、协定对向中华人民共和国境外提供个人信息的条件等有规定的，可以按照其规定执行。 • 个人信息处理者应当采取必要措施，保障境外接收方处理个人信息的活动达到本法规定的个人信息保护标准。
惩罚	• 违反本法规定处理个人信息，或者处理个人信息未履行本法规定的个人信息保护义务的，由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务；拒不改正的，并处一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。 • 有前款规定的违法行为，情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。

2.6 数据出境监管

《个人信息保护法》的重要规定之一，是对个人信息跨境传输的规范。关于跨境数据监管，流程正在不断规范和完善，例如2022年起施行《数据出境安全评估办法》。根据跨境数据的内容和数量，所需的流程会有所不同，尤其外资企业需要明确其对企业的影响并采取适当的措施。

【数据跨境模式[1]】

例举跨境模式所需的程序		
跨境模式		所需程序
1	• 重要数据※出境 ※重要数据是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用等，可能危害国家安全、经济运行、社会稳定、公共健康和安全等的数据; 国家网信部门规定的其他需要申报数据出境安全评估的情形	应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估
2	• 关键信息基础设施运营者以外的数据处理者自当年1月1日起累计向境外提供**100万人以上个人信息**(不含敏感个人信息)或者**1万人以上敏感个人信息**	应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估
3	• 关键信息基础设施运营者以外的数据处理者自当年1月1日起累计向境外提供**10万人以上、不满100万人个人信息**(不含敏感个人信息)或者不满1万人敏感个人信息	应当依法与境外接收方订立个人信息出境标准合同或者通过个人信息保护认证
4	• 关键信息基础设施运营者以外的数据处理者自当年1月1日起累计向境外提供**个人信息**量(不含敏感个人信息)**少于10万人时** • 为了与个人签订并履行合同而向境外提供个人信息时(例如跨境购物、航空及酒店预订、签证手续等) • 依据依法制定的劳动规章制度及集体合同进行跨境人力资源管理，需向境外提供员工个人信息的　　等	数据出境时无需通知当局 (但依据个人信息保护法第55条规定，无论数量多少，均需进行个人信息保护影响评估)

[1]. 概要整理自《数据出境安全评估办法》及《促进和规范数据跨境流动规定》

2.7 基于信息安全相关法律法规的处罚与判例

违反信息安全相关法律法规可能会导致行政处罚和/或经法院判决的赔偿。以下列举关于违反《网络安全法》的典型案例，以及依据《个人信息保护法》境外适用条款对法国企业作出赔偿判决的司法实例。当跨国公司处理来自中国的个人信息时，不仅要遵守自己当地的法律法规，如GDPR，还要遵守中国相关法律法规。

《网络安全法》行政处罚案例(2024年8月) [1]

2023年11月至2024年7月，通辽市公安机关对通辽某热电公司进行了多次网络安全监察检查，并针对存在高危安全漏洞给予行政警告。但该公司并未采取有效整改措施，系统长期处于高危状态运行。由此，公安机关对该公司法定代表人A、网络安全员B分别处以1万元、5000元行政罚款。

个人信息保护法境外适用赔偿判例(2023年9月) [2]

中国原告C购买了一家法国公司经营的酒店的会员卡，并使用该公司的应用程序预订了缅甸的酒店。原告随后发现，其个人信息已被与该公司集团的多个外部地区和企业共享。虽然原告同意该公司在应用程序上跨多个国家共享个人信息的政策，但该政策对于提供服务的企业和地区范围规定不明确，原告认为个人信息被不当共享。因此，他起诉该公司违反个人信息保护法。法院认定被告未提供应有的信息、不当共享个人信息，判令其向原告书面道歉、删除个人信息，并赔偿2万元。

[1]. 概要整理自: https://baijiahao.baidu.com/s?id=1810625493255242736&wfr=spider&for=pc

[2]. 信息来源自:(2022)粤0192民初6486号民事判决书，https://www.meritsandtree.com/UpLoadFile/Files/2024/9/2/18249331e6e8f0be-b.pdf

2.8 在华日企合规经营关键举措

中国是世界上较早建立完善的系统安全和个人信息保护制度的国家。考虑到安全风险和商业趋势，相关法律法规的细化和补充也在持续进行。中国的法律法规与GDPR有许多相似之处，但也有中国独有的具体规定。因此，在欧盟合法的事情在中国可能是违法的，所以有必要对安全管理系统进行适当的本地化。

需要应对的相关法律法规事项涉及面广，要求企业在初期阶段就全面落实可能存在一定困难。企业首先要准确掌握自身现状，据此制定切实可行的应对措施与实施计划，继而循序渐进、扎实稳妥地推进落实。

若企业难以凭借自身资源准确评估现状或制定合规计划，借助专业咨询机构不失为明智之选。ABeam Consulting在该领域也拥有实务经验，下文将具体介绍相关服务案例。

【中国网络安全相关法律法规的核心合规要求】

系统安全视角
1) 信息系统自我安全评估 2) 各等级的安全措施
个人信息保护视角
1) 正确把握被使用的个人信息 2) 对于个人信息的收集和管理，遵守中国相关法律法规 3) 根据跨境个人信息的类型和数量采取恰当的流程及手续

第三章

中国相关法律法规的合规实务指南

3.1 中国相关法律法规的合规流程指引

在遵守中国网络安全相关法律法规时，首先需要正确把握现行制度及所持有数据的重要性(分类、是否含有个人信息、是否是跨境数据等)，进而明确现状与应有状态间的差距。制定解决问题的计划并实施措施，后续的持续评估及改进的PDCA流程也至关重要。

①现状调查	• 根据各项法律法规和准则对信息系统的管理和技术方面进行自我评估 • 对个人信息和其他数据的持有/管理状况进行自我评估
②明确现状与合规状态间的差距	• 梳理和罗列与中国法律法规制度存在的合规差异(问题)
③拟定规划	• 针对各项合规差距制定整改措施与时间节点，形成分阶段实施计划
④实施执行	• 严格遵循既定实施方案执行整改 • 推进信息系统安全等级保护备案工作，并依法完成个人信息跨境传输监管申报程序
⑤持续评估与改进	• 开展持续评估和改进流程，包括定期对员工进行培训

3.2 案例1 - 信息系统自我评估

许多在华外资企业虽然理解合规的必要性，但由于内部资源不足，对现状的掌握仍不充分。我们可协助这些企业进行自我安全评估，在满足等级保护的要求方面明确其当前的状况以及面临的挑战。

背景和问题	A公司是一家在中国开展业务的日本制造企业，其在本地和公共云上拥有多个业务系统。然而，由于缺乏足够的IT和法务部门，这些系统的管理状况尚未得到评估以确定其是否满足法律法规合规要求。
提供的解决方案	对A公司的主要系统进行了评估，以确定它们是否满足保护级别的管理和技术要求。具体列出了未满足要求的领域，并明确了应优先解决的事项。

评估观点(主要类别)[1]

管理要求	安全管理系统	技术要求	安全的物理环境
	安全管理组织		安全的通信网络
	安全管理人员		安全区域边界
	安全建设管理		安全计算环境
	安全运维管理		安全管理中心

[1]. 概要整理自《GB/T 22239-2019信息安全技术网络安全等级保护基本要求》

3.2 案例2 - 个人信息跨境评估

近年来，个人信息保护的定义以及获取、管理信息的要求逐渐明确和具体。特别是在将个人信息跨境转移到中国境外时，根据信息的内容和数量，流程会有所不同，因此各公司需要准确掌握自身的持有状况并采取适当的措施。我们利用我司的模板和评估标准对将要跨境的个人信息进行了评估。

背景和问题	B公司是一家日本服务企业，其在中国的分支机构保存着员工和客户的个人信息，同时还将部分数据传输到日本总部用于业务目的。因尚未评估这些信息的管理是否符合法律法规要求，迫切需要进行验证。
提供的解决方案	我们使用我司的个人信息和管理现状的清单模板，对B公司计划要跨境的个人信息及其管理方法进行了评估。通过评估，明确了数据跨境方面需要实施的手续和管理问题，并制定了后续的对应计划。

个人信息示例[1]

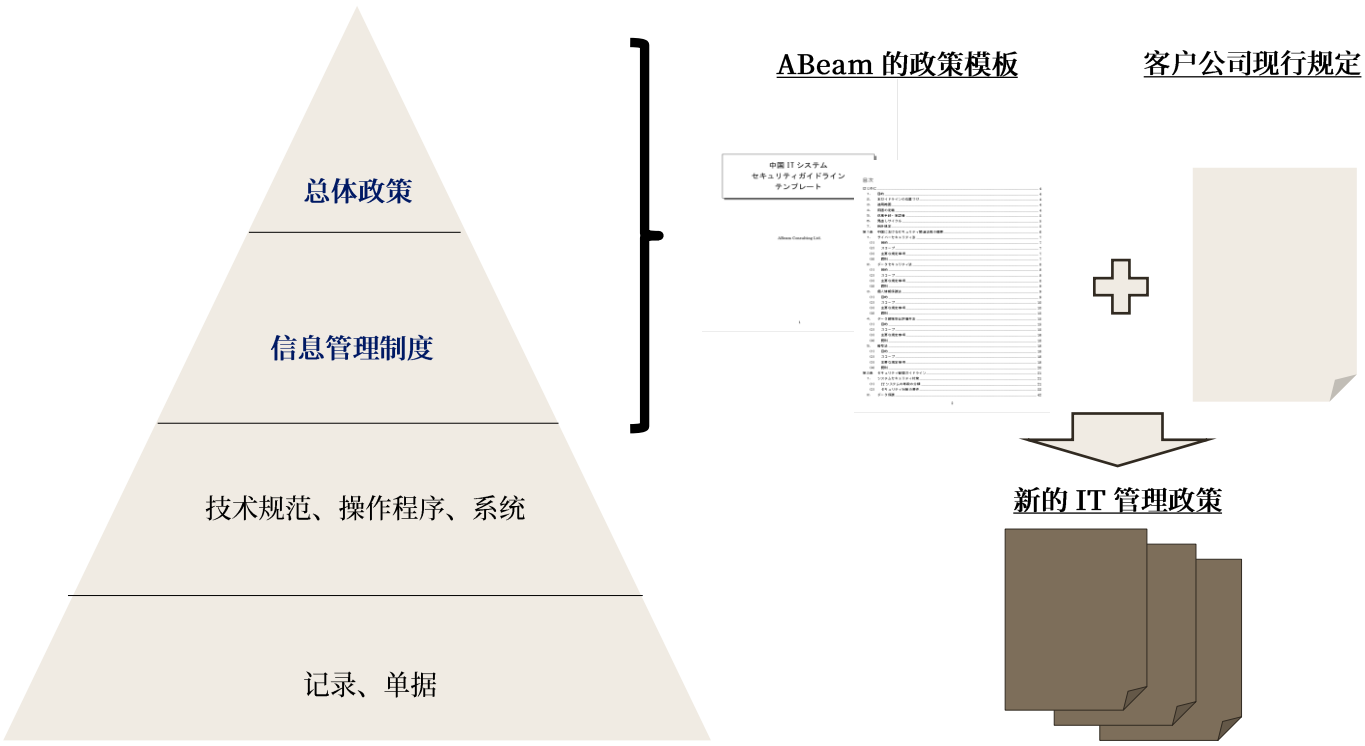
个人信息(示例)	种类举例
个人基本资料	个人姓名、生日、性别、民族、国籍、家庭关系、住址、个人电话号码、电子邮件地址等
个人身份信息	身份证、军官证、护照、驾驶证、工作证、出入证、社保卡、居住证等
个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等
网络身份标识信息	个人信息主体账号、IP 地址、个人数字证书等
个人健康生理信息	个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等，以及与个人身体健康状况相关的信息，如体重、身高、肺活量等
个人教育工作信息	个人职业、职位、工作单位、学历、学位、教育经历、工作经历、培训记录、成绩单等
个人财产信息	银行账户、鉴别信息口令 、存款信息(包括资金数量、支付收款记录等)、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑 换码等虚拟财产信息
个人通信信息	通信记录和内容、短信、彩信、电子邮件，以及描述个人通信的数据(通常称为元数据)等
联系人信息	通讯录、好友列表、群列表、电子邮件地址列表等
个人上网记录	指通过日志储存的个人信息主体操作记录，包括网站浏览记录、软件使用记录、点击记录、收藏列表等
个人常用设备信息	指包括硬件序列号、设备MAC 地址、软件列表、唯一设备识别码(如IMEI/Android ID/IDFA/OpenUDID/GUID/SIM 卡 IMSI 信息等)等在内的描述个人常用设备基本情况的信息
个人位置信息	包括行踪轨迹、精准定位信息、住宿信息、经纬度等
其他信息	婚史、宗教信仰、性取向、未公开的违法犯罪记录等

[1]. 概要整理自《GB/T 35273-202_信息安全技术个人信息安全规范》

3.2 案例3 – IT管理政策制定

为了达到等级保护的要求，首先需要正确制定内部IT管理政策，并按照政策实施具体的管理和技术措施。由于等级保护要求涉及面很广，我们基于符合等级保护要求的IT管理政策模板，协助各企业制定符合其需求的IT管理政策。

背景和问题	日本制药公司C对其内部信息系统进行自我评估后发现，其IT管理政策不足以满足等级保护的要求。该公司在全国有多个分支机构，需要制定一套可在整个公司范围内应用的IT管理政策。
提供的解决方案	以我司符合等级保护要求的IT管理政策模板为基础，结合客户原有的内部规章制度内容，为C公司制定了符合等级保护要求的覆盖全公司范围的IT管理政策。

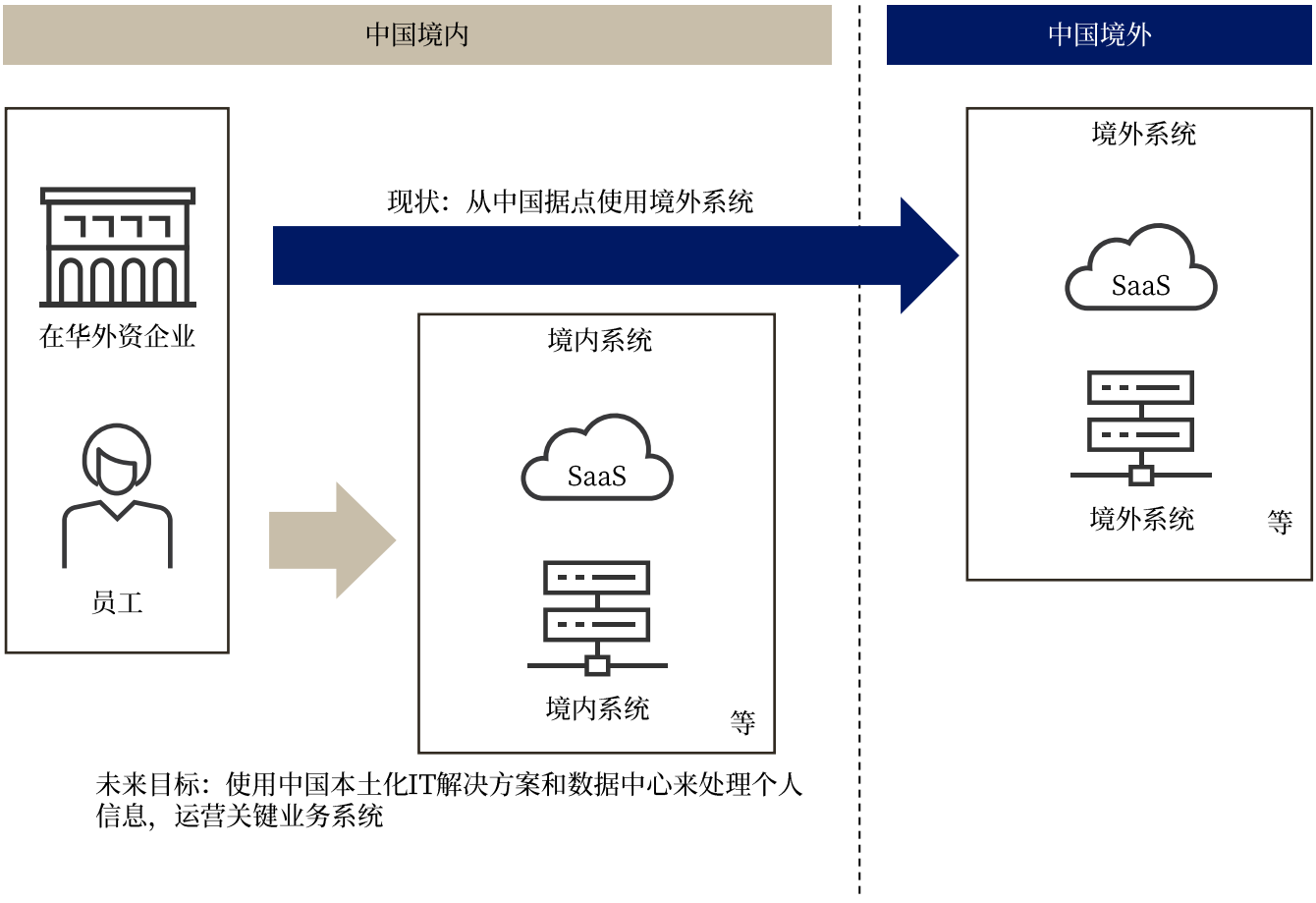


3.2 案例4 - 中国本土化IT解决方案应用构想制定

许多在华外资企业都使用其海外总部的系统。

然而，使用海外系统也存在个人信息保护、人工智能、半导体等法律法规风险。我们为希望将其关键业务系统切换为中国本地解决方案的客户提供计划制定服务。

背景和问题	D公司是一家在中国拥有多家工厂和办事处的日本制造企业，该公司使用日本总部和海外的SaaS来管理其核心业务和部分个人信息。虽然目前没有违反中国信息安全相关法律法规，但考虑到未来的风险和便利性，该公司正在考虑使用中国境内的系统。
提供的解决方案	充分活用我司ABeam Global Development Centre(Shanghai)(简称：GDC)的丰富知识和人才，制定了一整套将境外系统切换到中国境内系统的计划(架构、本土化解决方案的选定、系统实施成本和时间、日程等)。



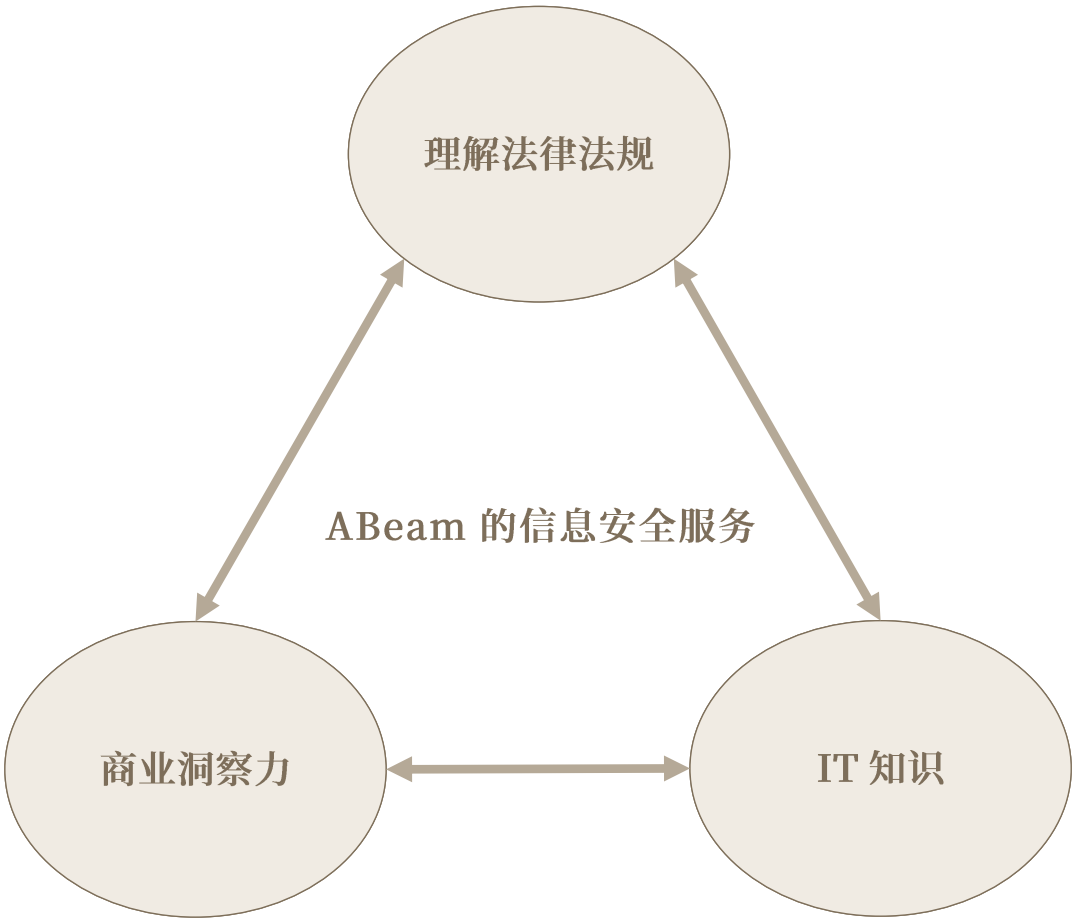
第四章

数字化时代下的风险管理：ABeam Consulting的职能与解决方案

在当今的数字社会中，信息安全和个人信息保护已经成为极其重要的问题。随着互联网的普及，我们的生活越来越依赖在线服务，处理的个人信息量也不断增加。在此情况下，网络攻击和数据泄露的风险不断增大，世界各国政府都在加强法律法规应对。

中国也不例外，企业也必须适当遵守相关法律法规。然而，法律法规和准则在不断补充和完善，单个公司仅使用其内部资源很难适时地跟上这些法律法规和准则。

作为一家综合性管理咨询公司，我们长期研究各国法律合规要求，并积累将法律法规要求融入企业运营与IT系统的实践经验。针对在华跨国企业，可提供包括合规现状评估、解决方案制定及持续改进建议在内的专业服务。在网络安全与数据合规领域，致力于为客户提供符合中国法律法规的专业支持。



关于ABeam Consulting

ABeam Consulting是一家综合性管理咨询公司，通过以亚洲为核心的全球网络，为各个国家和地区提供符合当地需求的全球化服务。我们拥有约8,800名专业顾问，在战略、BPR、IT、组织与人力资源、外包等领域具备深厚的专业知识和丰富经验，为金融、制造、零售、能源、信息通信、公共事业等行业的企业和组织提供全方位的咨询服务。作为企业可信赖的合作伙伴，ABeam Consulting致力于与客户共同创造新的未来，推动切实变革，助力企业和社会转型。

在中国市场，我们自2003年首次设立分支机构以来，已深耕二十余载。目前在上海、深圳、西安、大连、中国香港及中国台湾等地均设有分支机构，截至2024年7月，中国区员工规模已突破1,100人。

如对本报告内容感兴趣，欢迎随时垂询。我们将全力助力企业数字化转型与业务变革。

ABeam Consulting China

地址：上海市浦东新区陆家嘴环路479号71楼

TEL： +86-21-3303-9510

作者

小澤 繁树　　Ozawa　Shigeki

有关使用本报告的注意事项和免责声明

本报告基于2025年3月获得的信息发布，可能会因后续法律法规修订而发生信息滞后性。本报告系我司基于非法律专业立场编制，因信息来源、理解差异或客观局限，可能存在遗漏或偏差，仅供参考，我司不就其完整性、准确性承担任何责任。本报告不构成法律相关建议，也不构成法律相关建议的依据，如果您希望根据本报告中提供的信息采取任何行动，请务必根据您的实际情况寻求专业法律服务机构的建议。

在未经我司明确且正式的书面授权许可之前，任何个人、团体、组织或机构都严禁擅自对本报告进行任何形式的复制、转载或使用本报告的内容，否则，我司将依法依规追究其相应的法律责任。

对于因本报告或其内容所引起或与之相关的任何损害(包括但不限于直接、间接、附带、惩罚性损害及利润损失等)，无论该等损害系基于合同、成文法或侵权(含过失侵权)而产生，亦无论其是否已被或应被事先预见，我方概不承担任何责任。


ABeam Consulting®
Build Beyond As One.