欧盟GDPR探析

构建合规的桥梁

-By BlueDog

有 智 慧 ，有 信 任 ，让 数 据 更 安 全

www.angeek.com.cn

目录

01 合规的背景与呼声

合规的背景与呼声

GDPR全称General Data Protection Regulation-欧盟《通用数据保护条例》（下称“GDPR”）于2018年5月25日正式生效。GDPR全文共10章99条263页。GDPR给欧盟的数据安全带来了全面制度改革，其核心目标是将个人数据保护深度嵌入组织运营，真正将抽象的保护理论转化为实实在在的行为实践。对于企业而言，小至隐私政策、业务流程，大到信息技术系统、战略布局，无一不需要重新审视规划。

为什么有了1995年的《个人数据保护指令》，还要出台GDPR呢?

1995年的《个人数据保护指令》（下称《指令》）共34个简单条文的适用范围取决于**属地因素**，要么机构的成立地在欧盟，要么利用了欧盟境内的设备进行了个人数据的处理活动（仅仅是传输通道除外）GDPR不仅考虑属地因素，还增加了**属人因素**。

受GDPR约束的机构有哪些呢?

一是成立地在欧盟的机构
二是成立地在欧盟以外的机构:只要其在提供产品或者服务的过程中（不论是否收费）处理了欧盟境内个体的个人数据，将同样适用于GDPR。
三是服务对象为欧盟境内的用户。

GDPR是一部针对个人数据保护的条例，那什么是个人数据呢

个人数据，也称为个人信息，是指任何指向一个已识别或可识别的自然人（“数据主体”）的信息。可识别的自然人能够被直接或间接地识别，尤其是通过参照诸如**姓名、身份证号码、定位数据、在线身份识别这类标识，或者是通过参照针对该自然人一个或多个如物理、生理、遗传、心理、经济、文化或社会身份的要素。**值得注意的是根据用户画像可以确定某一类人的信息也是属于个人数据哦。

合规的背景与呼声-为何企业需要关注GDPR

2018 年是数据保护具有里程碑意义的年份。自 2018 年 5 月 25 日欧盟《通用数据保护条款》生效以来，深刻影响欧盟乃至全球范围内个人数据
保护和数字经济发展态势。许多国家已采用或计划采用 GDPR 数据保护标准进行本国数据保护立
法或完善工作，从而导致全球数据保护立法规则进一步融合。

GDPR 生效以来，三大主体（监管机构、数据主体、数据控制者）对数据保护的重视程度不断提升。

www.angeek.com.cn

1.法律义务：GDPR是欧盟的法律规定，适用于所有处理欧盟公民数据的组织，无论该组织是否在欧盟境内。违反GDPR的企业可能面临重大的法律后果。

2.巨额罚款：GDPR规定，违反其条例的企业可能面临的罚款高达其全球年营业额的4%或2000万欧元（以较高者为准）。

3.品牌和声誉：数据泄露或不遵守数据保护法规可能会严重损害企业的品牌和声誉。消费者越来越关心其个人数据的使用和保护，对此不负责任的企业可能会失去客户的信任。

4.消费者权利：GDPR强调了个人的数据权利，如访问权、更正权、删除权等。企业必须确保消费者可以轻松地行使这些权利。

5.数据管理和治理：GDPR鼓励企业对其数据进行更好的管理和治理，这不仅可以提高数据安全性，还可以提高企业的运营效率。

6.竞争优势：对于那些确保数据安全并尊重消费者隐私的企业，这可以成为其竞争优势。消费者可能更倾向于选择那些他们认为会保护其数据的企业。

7.供应链要求：即使某企业可能不直接受GDPR的约束，其业务合作伙伴可能会要求它符合GDPR的要求，以确保整个供应链的合规性。

安几网安
ANGeek C.S.

02

GDPR：定义与愿景

GDPR的定义

2018 年 5 月 25 日生效的《通用数据保护条例》(GDPR) 是欧盟一项全面的数据隐私法律，为个人数据的收集、处理、存储和传输建立了一个框架。它要求以安全的方式处理所有个人数据，并包括对不遵守这些要求的企业的罚款和处罚。它还为个人提供了一些有关其个人数据的权利。

最纯正获取：https://gdpr-info.eu/

法规 (欧盟) 2016/679

	欧盟法规
标题	关于在处理个人资料和在转移这些数据方面保护自然人的法规，以及废除指令95/46/EC (数据保护指令)
通过机构	欧洲议会和欧盟理事会
日志记录	L119,2016年5月4日,p. 1–88[1]
	历史
推出日期	2016年4月14日
生效日期	2018年5月25日
	准备文本
委员会建议	COM/2012/010 final – 2012/0010(COD)
	相关法规
代替条文	数据保护指令

通用数据保护条例

- 第一章（第 1 条至第 4 条）
  一般规定
- 第二章（第 5 条至第 11 条）
  原则
- 第三章（第十二至二十三条）
  数据主体的权利
- 第 4 章（第 24 – 43 条）
  控制器和处理器
- 第五章（第四十四至五十条）
  将个人数据传输至第三国或国际组织
- 第六章（第 51 至 59 条）
  独立监管机构
- 第七章（第 60 – 76 条）
  合作与一致性
- 第 8 章（第 77 – 84 条）
  补救措施、责任和处罚
- 第九章（第85-91条）
  有关具体处理情况的规定
- 第 10 章（第 92 – 93 条）
  授权行为和实施行为
- 第 11 章（第 94 – 99 条）
  最后条款

GDPR的愿景（ Lawfulness, fairness, and transparency）

The first principle of GDPR states that organizations should always adhere to the laws. Organizations must mention in their privacy policy what data they are collecting and for what purpose.

Purpose limitation data should be collected for specific purposes. Organizations need to mention the objectives behind collecting data and delete it once the target is achieved.

Data minimization

Organizations need not collect unnecessary and irrelevant data. They are allowed to collect, process, or hold the minimum amount of data required to fulfill their purposes.

Accuracy

Organizations must take necessary steps to ensure that personal information is accurate and not misleading. Any misleading or incorrect information should be erased as soon as discovered.

Storage limitation

Organizations need not store personal data for a more extended period. Data should be reviewed frequently and erased if it is not required anymore.

Integrity and confidentiality

The integrity and confidentiality principle ensures that organizations take adequate measures to protect consumers' data and privacy. This principle is also known as the security principle.

GDPR 的首要原则指出，组织应始终遵守法律。组织必须在其隐私政策中提及他们正在收集哪些数据以及出于什么目的。

目的限制数据应为特定目的而收集。组织需要提及收集数据背后的目标，并在目标实现后将其删除。

数据最小化

组织不需要收集不必要和不相关的数据。他们被允许收集、处理或保存实现其目的所需的最少量数据。

准确性

组织必须采取必要措施确保个人信息准确且不具有误导性。任何误导性或不正确的信息一经发现应立即删除。

存储限制

组织不需要更长时间地存储个人数据。应经常检查数据，如果不再需要则将其删除。

诚信和保密

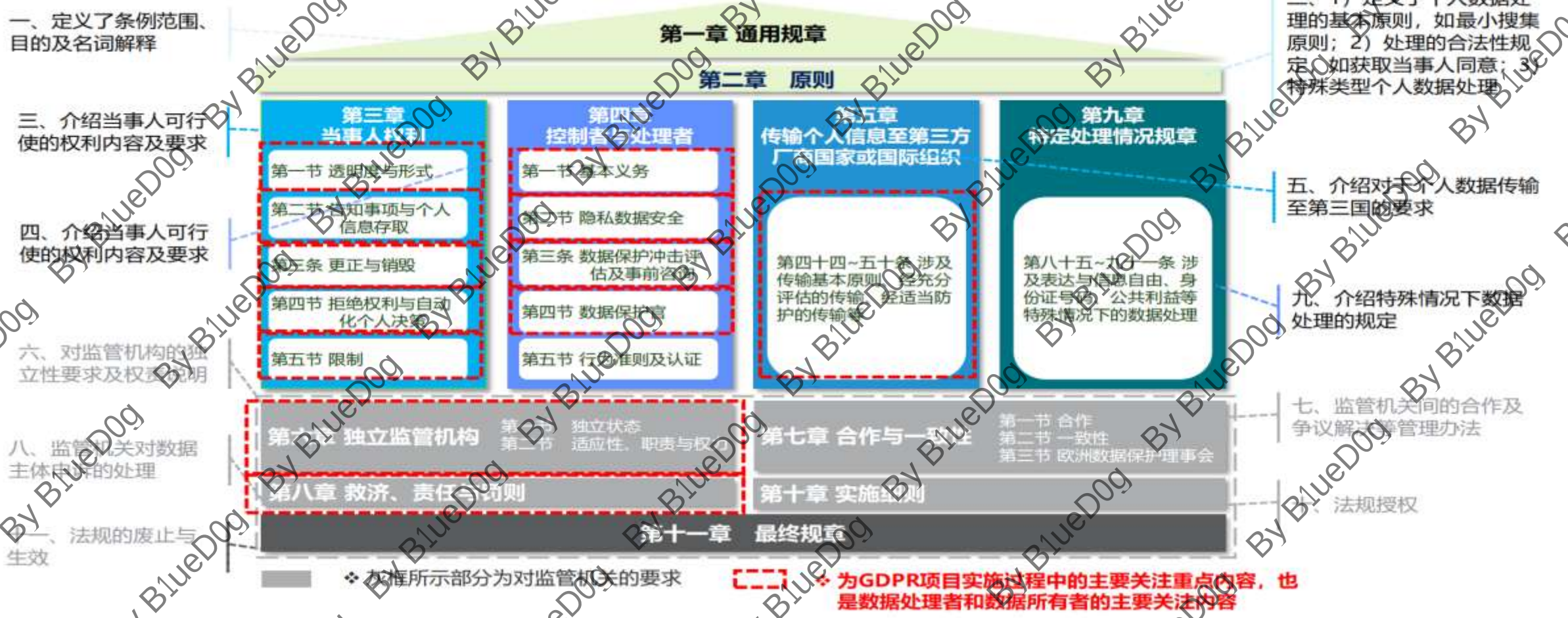
完整性和保密性原则确保组织采取适当的措施来保护消费者的数据和隐私。该原则也称为安全原则。

安几网安
ANGeek C.S.

03

GDPR的关键组成部分

GDPR的关键组成部分



04

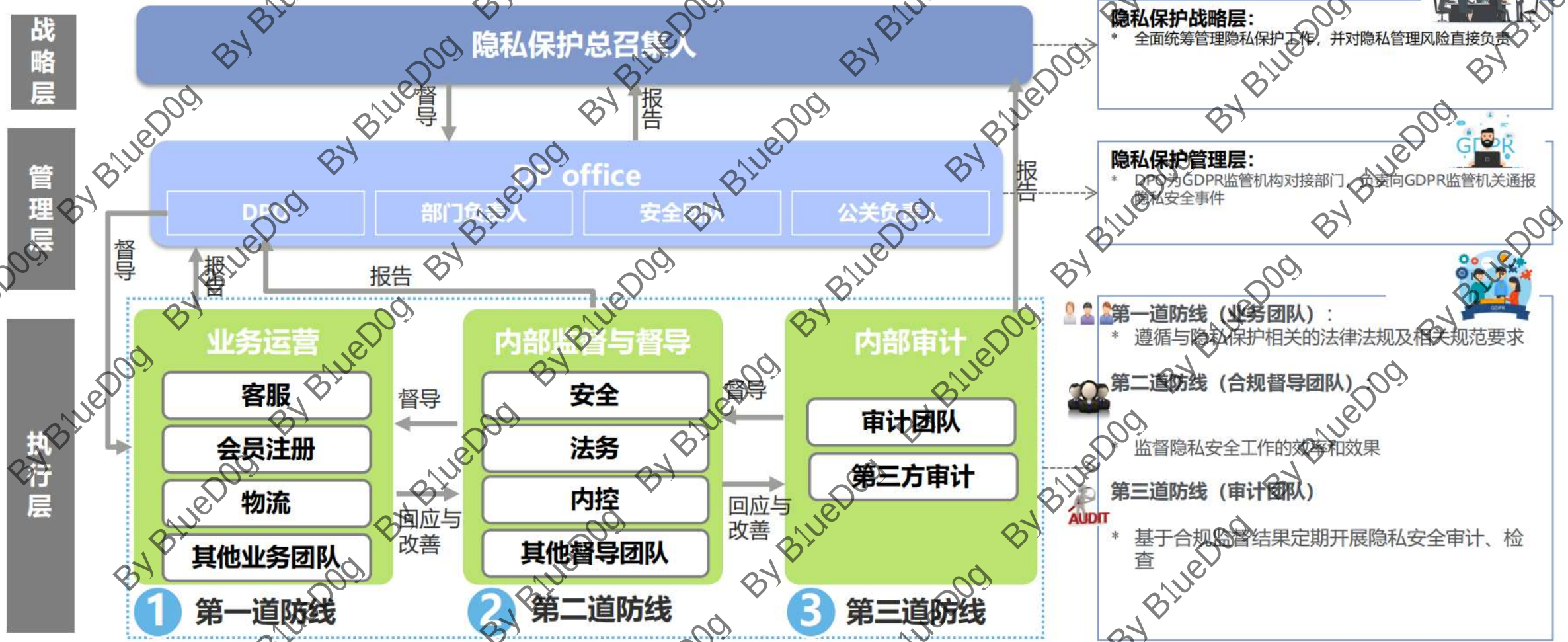
企 业 如 何 确 保 合 规

GDPR合规应对


GDPR《一般数据保护条例》
当事人权利
同意和告知
默认的隐私保护（PBD）
第三方服务提供商管理
数据安全与处理活动记录
信息泄漏通知
隐私保护影响评估（DPIA）
数据保护官（DPO）
跨境数据传输
救济、责任与罚则
隐私保护体系框架
隐私数据收集同意告知机制
隐私保护影响评估机制
默认的隐私保护设计管理机制
当事人权利行使机制
第三方供应商安全管理机制
隐私数据跨境传输机制
隐私事件应变处理机制
• GDPR实施指南
✓ wp259-_rev.01：同意
✓ Wp251：自动化决策和用户画像
✓ Wp250：个人数据泄露通知
✓ WP248：隐私保护影响评估
✓ WP243：数据保护官
✓ WP242 _rev.01:数据可携权
隐私数据管理
应对方案
隐私数据收集同意告知机制
• 评估收集的目的及合法性；
• 设计隐私声明告知和同意方式
• 调整/优化系统和产品功能
隐私保护影响评估机制
• 确定DPIA执行时机和执行范围
• 开展隐私影响评估
• 制定和落实风险改善建议和计划
默认的隐私保护设计管理机制
• 系统/产品开发的需求分析阶段嵌入适用隐私保护需求或
• 系统/产品开发的测试阶段验证隐私保护需求的实现。
当事人权利行使机制
• 落实隐私权行使流程
• 设置权利请求受理、处理岗位
• 调整/优化系统及产品功能
• 加强第三方供应商管理，协同处理权利请求
第三方供应商安全管理机制
• 对受委托的第三方单位开展隐私保护评估
• 合同管理
• 管理第三方单位对个人数据的访问、处理
隐私数据跨境传输机制
• 确定隐私数据跨境涉及的业务场景及接受方；
分析适用的合法跨境传输依据
• 签署标准合同条款（SCC）或
• 申请有约束力的公司规则(BCRS)
隐私事件应急处理机制
• 落实和优化应急处理流程
• 加强与主管机关的关系
定期开展应急演练
• 加强员工隐私安全培训
持续的隐私安全评估和检查
跨部门团队协同合作（包括业务、安全、法务、系统团队、大数据团队、产品和服务开发等）

隐私管理的组织架构

GDPR的合规落地，涉及到从**产品界面到后端数据库、再到制度流程**的全面排查和改造，需要跨部门团队协同合作。为了确保组织隐私保护体系的持续有效运行，组织需要**设置隐私保护架构和岗位**，以便在高级管理层的领导下，有效地推动隐私保护工作的落地和优化。



安几网安
ANGeek C.S.

05

GDPR下的教训

标GDPR的罚款&执法

目前，**GDPR 罚款总额已超过40亿欧元**。这些数字表明了我们对维护数据保护法规的持续承诺，并突显了不合规所带来的日益严重的财务后果。

迄今为止 20 项最大的 GDPR 罚款:
https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/

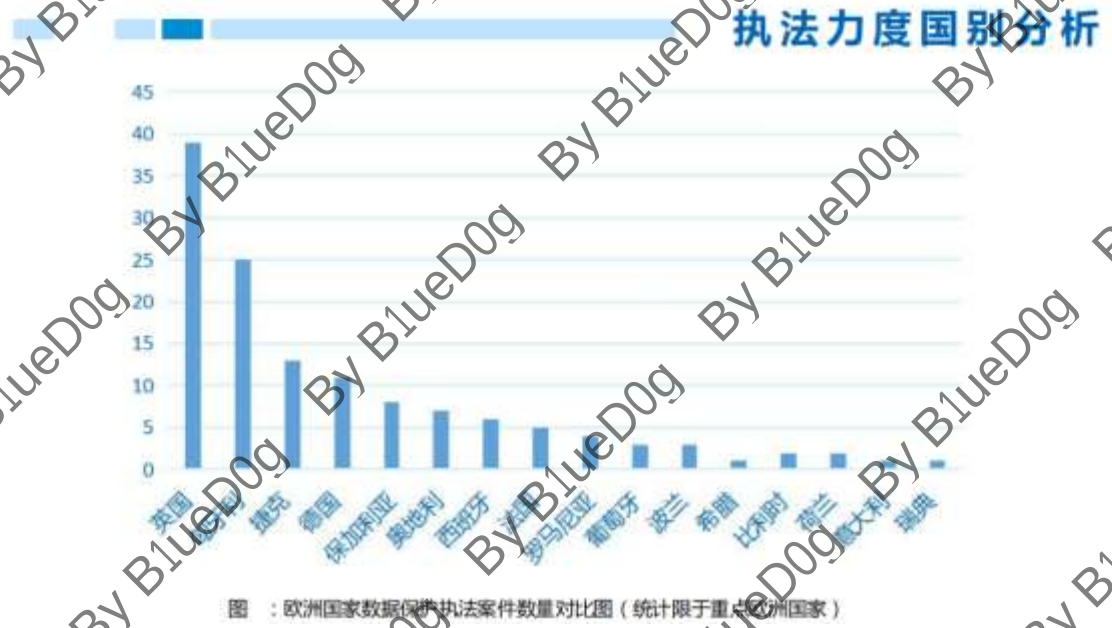


图 ：欧洲国家数据保护执法案件数量对比图（统计限于重点欧洲国家）

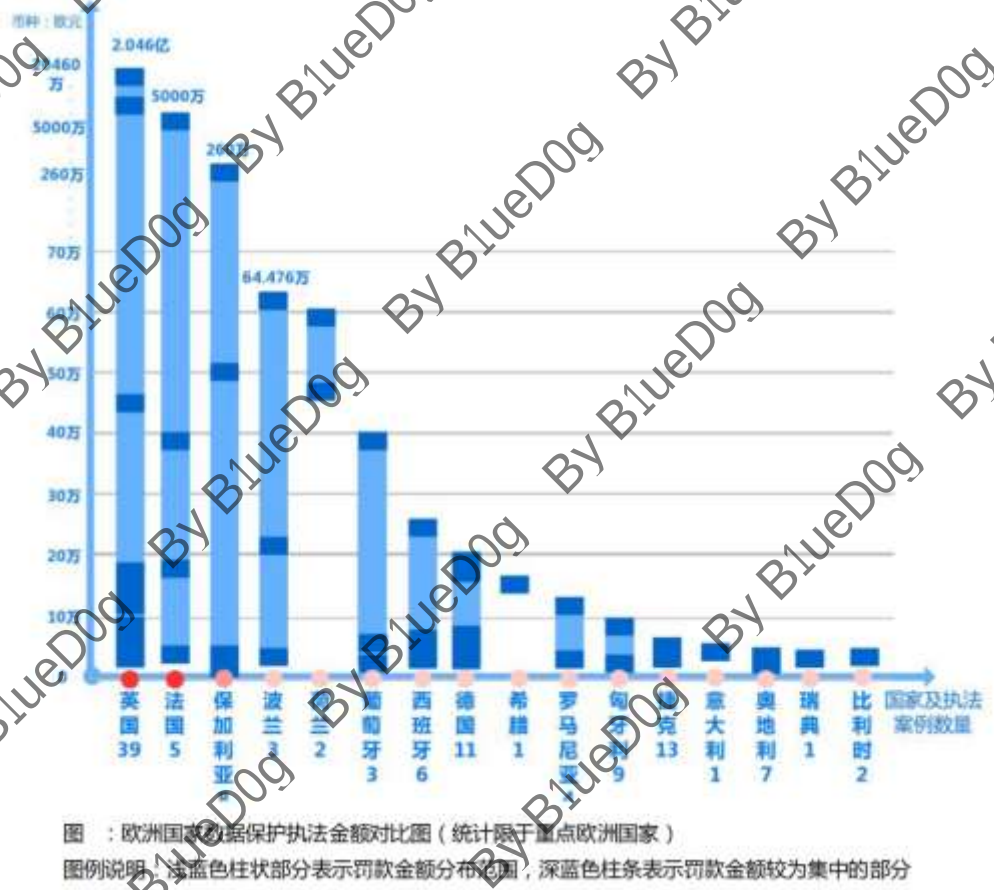
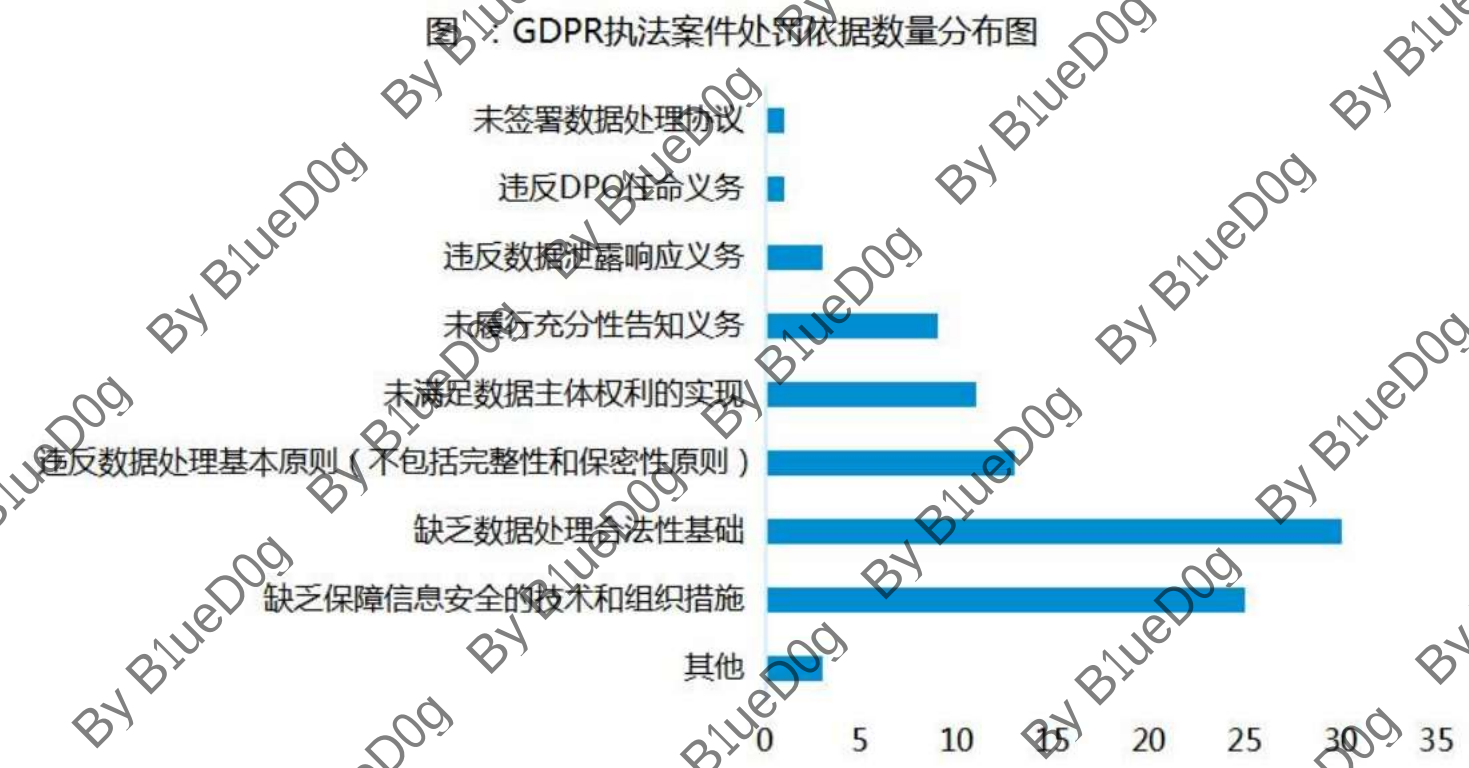


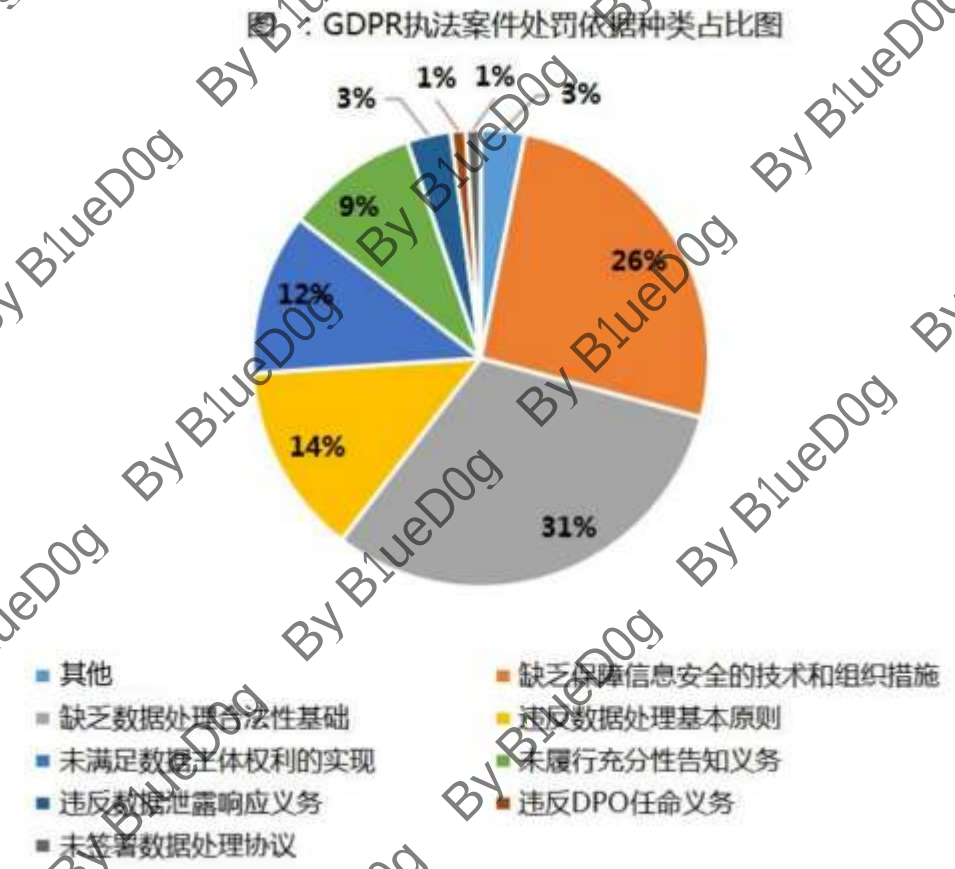
图 ：欧洲国家数据保护执法金额对比图（统计限于重点欧洲国家）

图例说明：浅蓝色柱状部分表示罚款金额分布范围，深蓝色柱条表示罚款金额较为集中的部分

图表数据来源:GDPR 执法案例精选白皮书

GDPR执法案例





图表数据来源:GDPR 执法案例精选白皮书

安几网安
ANGeek C.S.

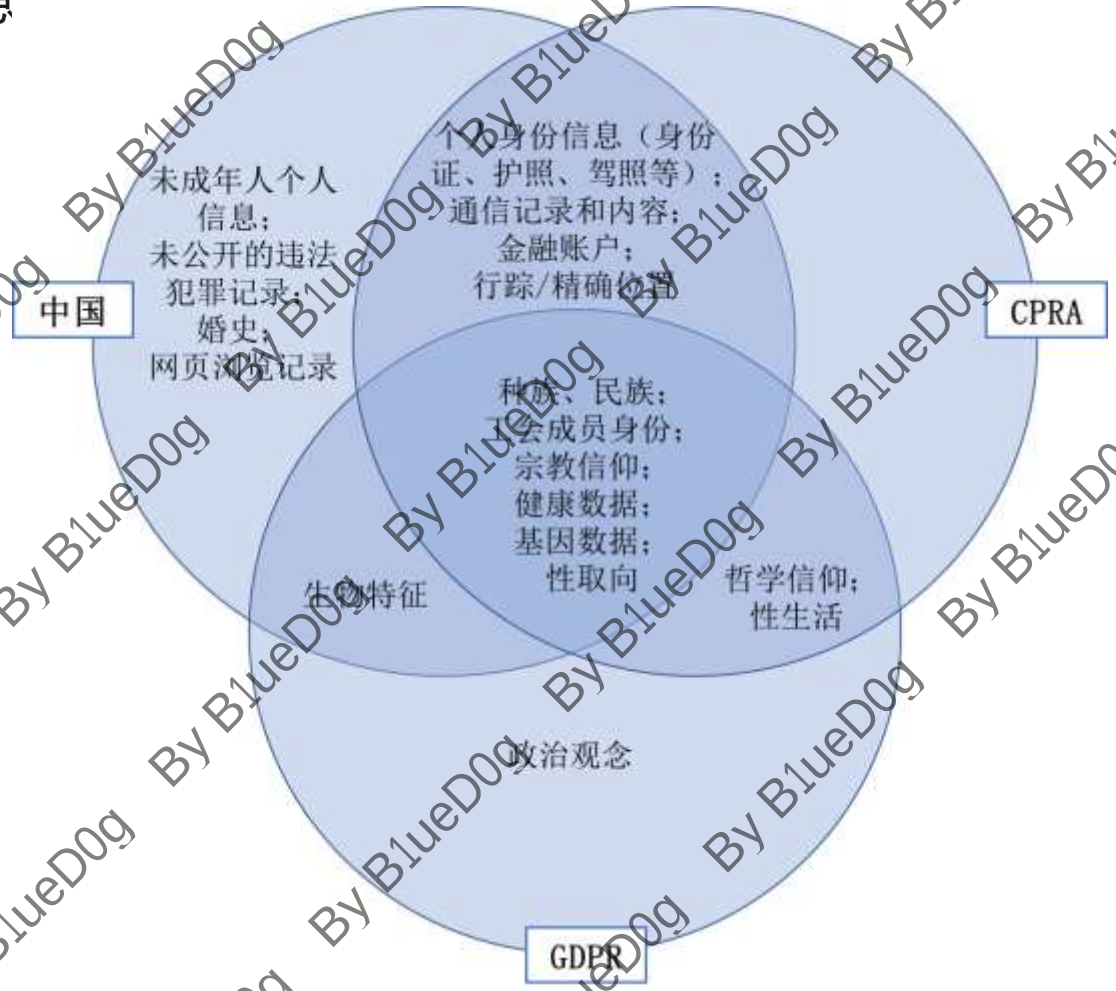
06

全球视野下的GPDR回响

个人信息的定义与分类

三部法律都区分了一般类型的个人信息和敏感个人信息

	GDPR	个保法	CCPA/CPRA
一般个人信息的定义及内涵	与已识别或可识别的自然人有关的信息		能够识别、关联、描述或能够合理地关联到消费者的信息
	排除： • 匿名化信息		排除： • 公开可得的信息 • 合法获得、真实的、引起公众关注的信息 • 去识别化信息 • 已汇总的信息



管辖范围

	GDPR	个保法	CCPA/CPRA
属地原则	在欧盟境内没有实体，但是由于数据处理行为与欧盟境内存在特定联系而受GDPR管辖。包括以下两种情形： • 针对欧盟境内信息主体提供产品或服务； • 在欧盟境内的监控行为。	在中国境内处理自然人个人信息的，适用个保法。 在境外处理中国境内个人信息的，也适用个保法，具体包括以下两种情形： • 以向境内自然人提供产品或者服务为目的； • 分析、评估境内自然人的行为； • 法律、行政法规规定的其他情形。	在加州开展“商业活动”的，受CCPA/CPRA约束。
属人原则	管辖数据控制者或处理者设立在欧盟境内的实体进行的对个人数据的处理行为，无论其处理行为是否发生在欧盟境内。 根据国际公法需要遵守GDPR的情形，例如欧盟成员国在境外的外交机构。	不适用	不适用

个人信息处理活动的范围

GDPR	个保法	CCPA/CPRA
收集，记录，组织，建构，存储，改编或修改，恢复，查询，使用，通过传输、分发方式进行披露或者其他使个人数据可被他人获得、排列或组合、限制、删除或销毁	收集、存储、使用、加工、传输、提供、公开、删除	收集、使用、存储、披露、出售、共享

个人信息处理主体及其义务

主体	GDPR		个保法	CCPA&CPRA
	数据控制者	数据处理者	个人信息处理者	企业
概念	单独或与他人共同确定个人数据处理的目的和方式的自然人、法人、公共权力机关、代理机构或其他机构。	代表数据控制者处理个人数据的自然人、法人、公共权力机关、代理机构或其他机构。	在个人信息处理活动中自主决定处理目的、处理方式的组织、个人。	在加利福尼亚州开展业务，收集消费者个人信息，或代表收集此类信息，并满足一定条件的实体，可以单独或与他人共同决定处理消费者个人信息的目的和方式。
义务	通知义务：包括收集信息前向信息主体告知处理的目的、方式等，以及发生数据泄露时的通知义务。			
	境外的个人信息处理者（GDPR：数据控制者和数据处理者）应当在境内设置代表人； 个人信息处理者（GDPR：数据控制者）开展特定的个人信息处理活动前应当进行个人信息保护影响评估。			无
	保存数据处理活动的记录。		无	无
	无	遵守与数据控制者之间的合同义务。	合规审计的义务	无

个人信息跨境传输

	GDPR	个保法
基本规则	GDPR 首先规定了一个充分保护水平认定的名单，向名单上的国家、地区或组织转移数据的，不需要采取特别的保障措施。 如果不在名单上，则需要根据GDPR的规定，采取适当的保障措施才能够进行个人信息的跨境转移。	满足下列四个条件之一的，可以向境外转移： • 通过国家网信部门组织的安全评估； • 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； • 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； • 法律、行政法规或者国家网信部门规定的其他条件。
特殊规则	除了上述两种基本规则外，GDPR还规定了两个特殊规则： 一是在存在有效国际协议的情况下，可以基于司法判决、行政决定等进行跨境传输； 二是在满足特定的条件后，即使缺乏充分保护认定以及适当的保障措施，也可以进行跨境转移。	对于存储于我国境内的个人信息，有以下两个规定： 一是按规定存储于我国境内的个人信息，确需向境外提供的，应当通过国家网信部门组织的安全评估。 二是境外的司法或者执法机构要求提供存储于我国境内的个人信息的，应当经主管机关批准。

安几网安
ANGeek C.S.

07

GDPR之旅：展望与期待

企业如何从现状迈向完全合规

- 具有价值创造模式的合规体系需要企业充分考虑团队的多样性，储备具有丰富经验的、可以设计、实施及不断完善合规体系进而实现对法律、合规、政策、声誉及道德层面风险管控的专业人才，进而确保创新资源的合理分配，确保创新的可量化性。
- 基于风险的业务流程，相应地设计和整合合规流程，打破部门各业务组之间的流程断点，在节省成本的同时实现信息实时交互、资源协同高效的业务处理模式。
- 通过合规科技提升预测和分析能力，同时提高洞察力，以帮助企业内部制定合适的合规计划，进一步做出具备战略性的决策。
- 强化对于供应商的沟通与管理，强化关键核心技术提供方资质与能力审核，综合前瞻性、可扩展性等因素开展多维度技术应用适配测试与安全评估。特别注意在供应商（以及他们所提供的解决方案）技术初试点之后的价值和应用能力。
- 价值创造模式的合规体系中的技术平台需实现通过多个风险领域帮助对合规及职业道德违规行为的预防及检测作出反应。

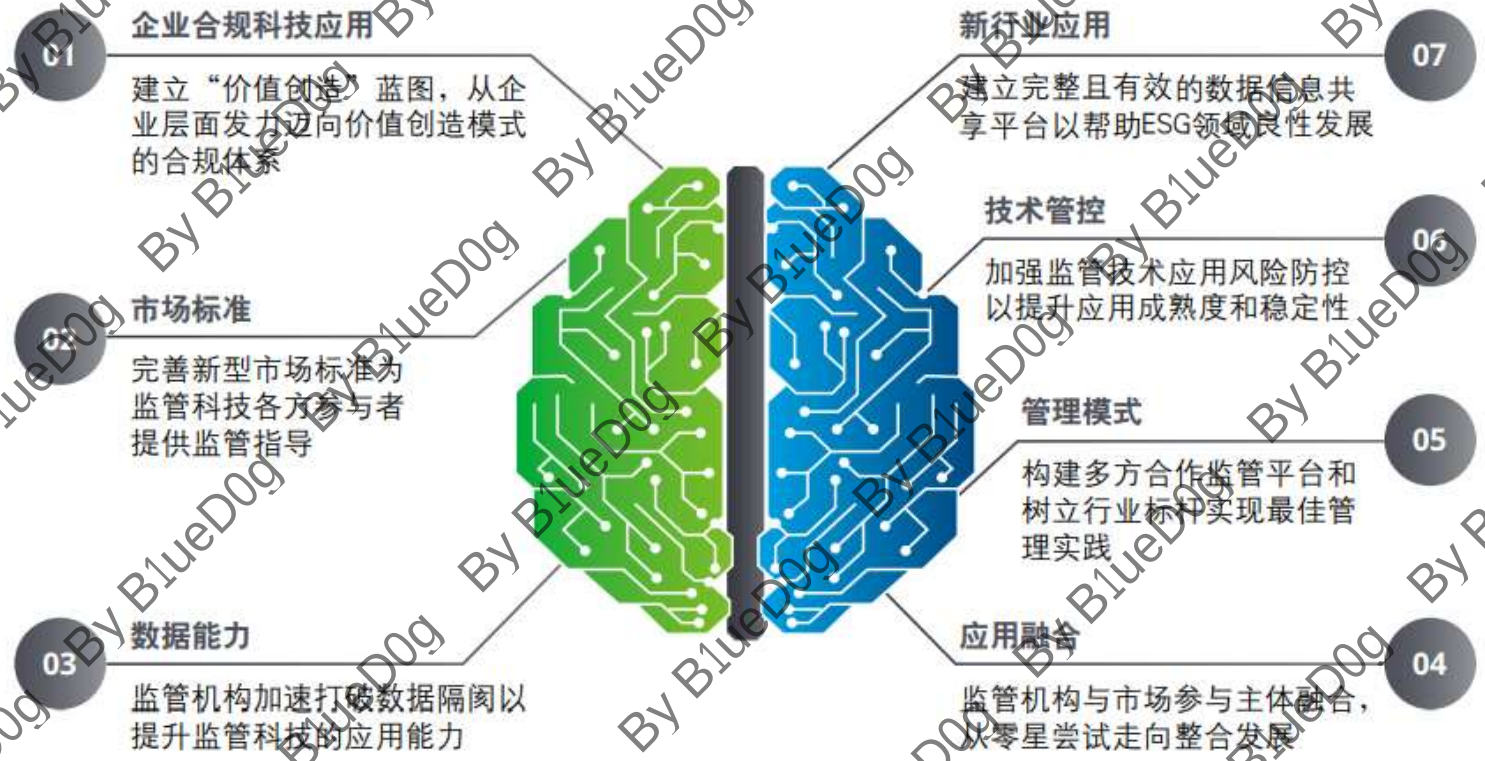
简单的来说：

首先，尽早确保取得企业管理层对现代化合规体系的认可。

此外，企业应建立跨职能、跨学科的团队

展望与期待

当前合规科技正处于发展阶段，监管政策的不断完善作为重要推动力，通过监管体系、发展模式和应用实践三个方面持续推动合规科技发展。在科技的推动下，企业合规将呈现出技术化、数字化、智能化的特点。与此同时，监管法规正逐渐从静态监管转向动态监管，从机构监管转向功能 监管，监管机构与被监管机构及相关利益方之间的交流与沟通不断加强，监管的包容性和有效性在实践中实现灵活、动态平衡。



来源：德勤研究

安几网安
ANGeek C.S.

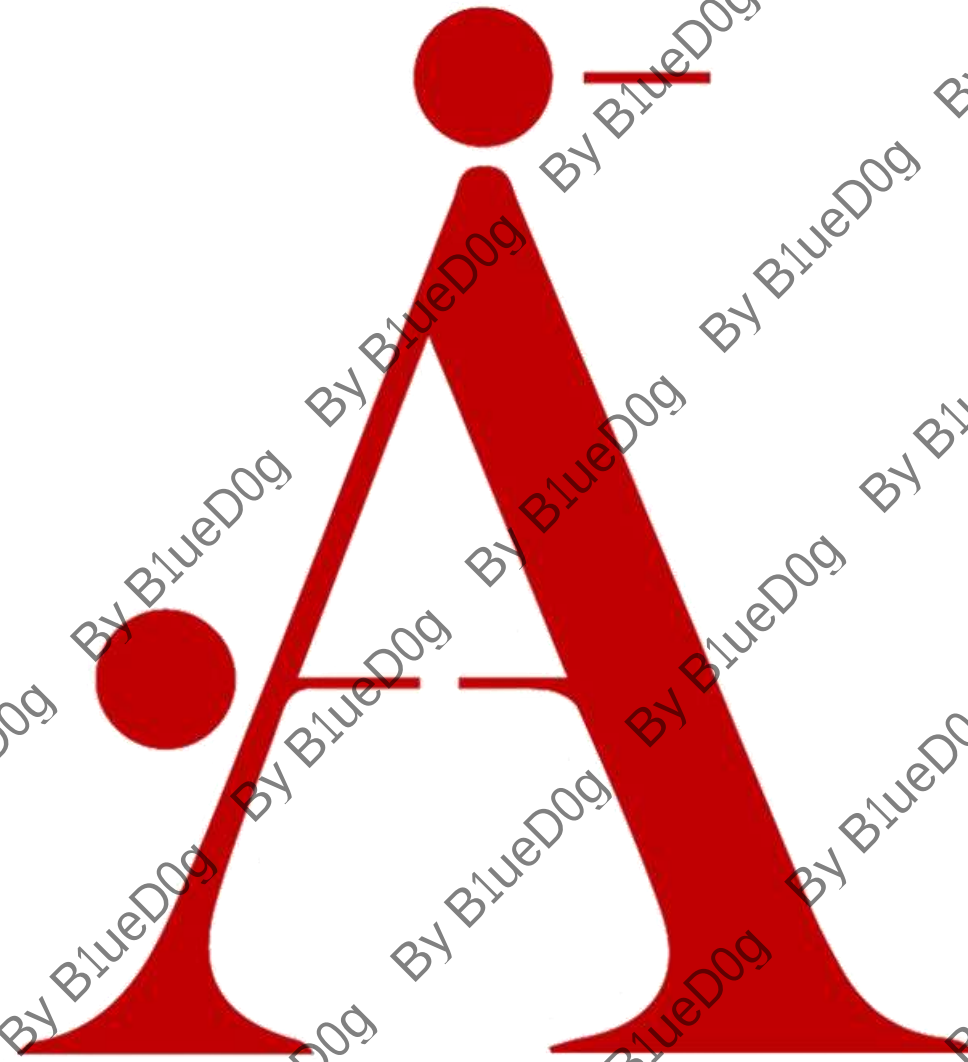
08

Q & A 和 资 源 提 供

Q&A和资源提供

您可以通过扫描左侧二维码获取本文及其他关于GDPR的资料

欢迎与我交流：B1ueD0g@duck.com



安几网安
NGeek C.S.

安几网安

期待更多交流

有 智 慧 ，有 信 任 ，让 数 据 更 安 全

安 几 网 安

www.angeek.com.cn