PSCI PHARMACEUTICAL SUPPLY CHAIN INITIATIVE

Building responsible supply chains

全球数据保护和隐私态势

薛梓源

网络安全及科技风险服务领导合伙人

德勤中国

议程

GDPR及近期趋势

亚太隐私保护法规

中国数据保护和隐私法规

演讲者介绍

- **薛梓源**
- 合伙人，风险咨询 – 网络风险
- 网络安全及科技风险服务领导合伙人
- 德勤中国

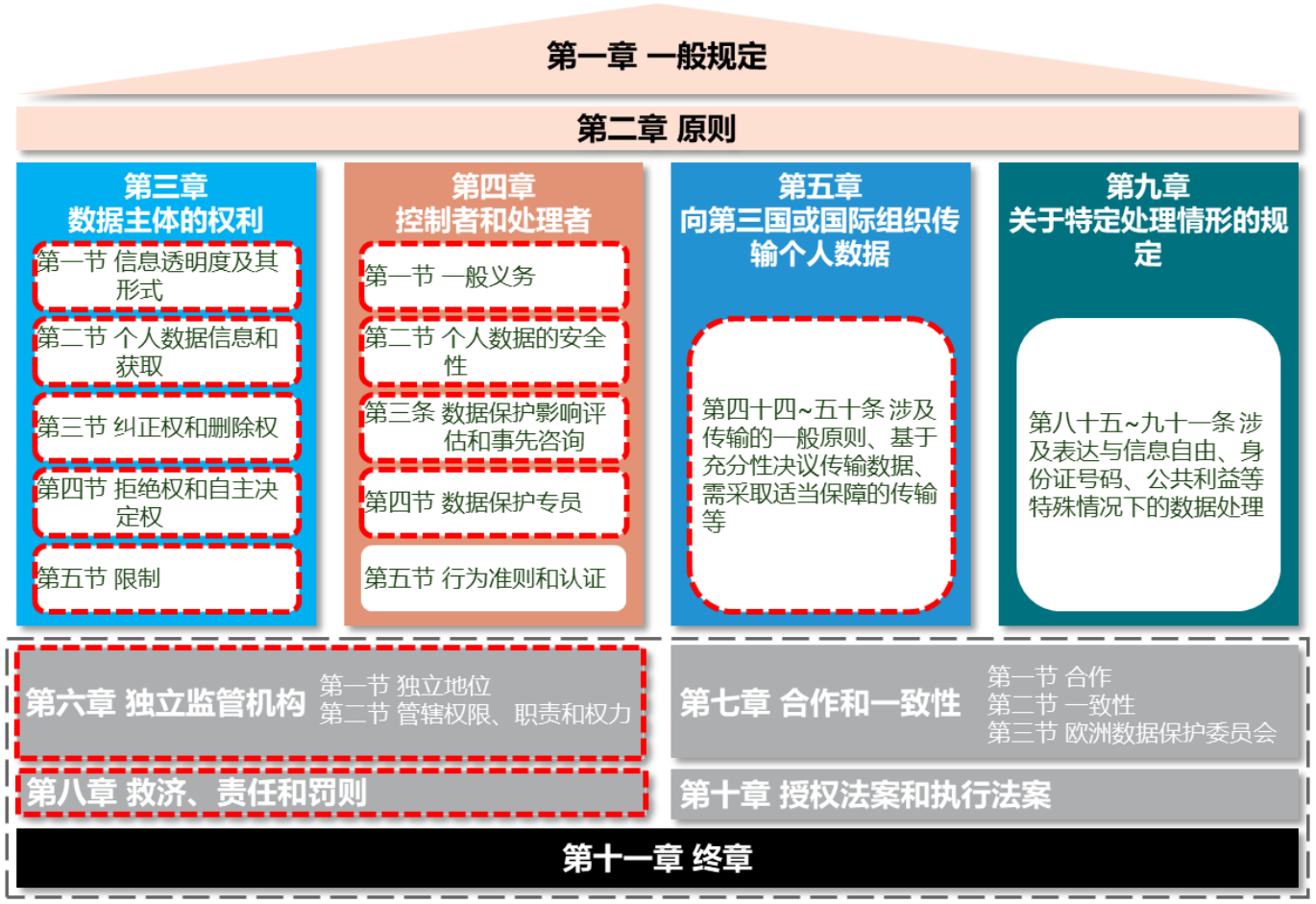
- Tel: +86 10 8520 7315
- Email: tonxue@deloitte.com.cn

- 薛梓源先生具有超过二十五的风险咨询服务经验，他专长的业务领域包括信息安全管理、数据安全与隐私保护、安全系统实施和运维服务。作为合伙人，薛先生丰富的行业经验和专业知识涵盖了高科技、医疗健康、制造等行业。作为网络安全领域领军人物，薛先生目前是德勤大中国地区网络安全和科技风险负责人，团队覆盖中国大陆和港澳地区，合伙人和总监人员超过30人，提供全程的安全规划，安全加固，安全监控和应急响应服务。

GDPR及近期趋势

GDPR简介

通用数据保护条例（GDPR）是欧盟法律中针对所有欧盟个人的数据保护和隐私法规。 GDPR的主要目标是恢复个体对个人数据的控制，并简化欧盟内部国际业务的通用规范。



- 灰框所示部分为对监管机构的要求
- 为GDPR项目实施过程中的主要关注重点内容

GDPR的10个重要要求

1 **删除权**
- 必须立即答复请求
- 如果数据公开，需通知有关第三方

2 **数据可移植性**
- 以结构化、常用且机器可读的格式接收个人数据
- 将个人数据传输到另一个控制者

3 **数据保护影响评估（DPIA）**
- 对设想的处理操作和目的进行描述
- 评估风险并考虑解决这些风险的措施

4 **监管机构权力范围更广**
- 处以罚款（年营业额的2%-4%）
- 授权和咨询的权力
- 暂停国际数据传输

5 **隐私设计和默认数据保护**
- 从每个处理活动的计划开始就嵌入隐私
- 在个人数据的整个生命周期中进行评估

6 **文件记录要求增加**
- 控制者和处理者的文件编制必须对监管机构可用
- 维护处理活动的书面记录

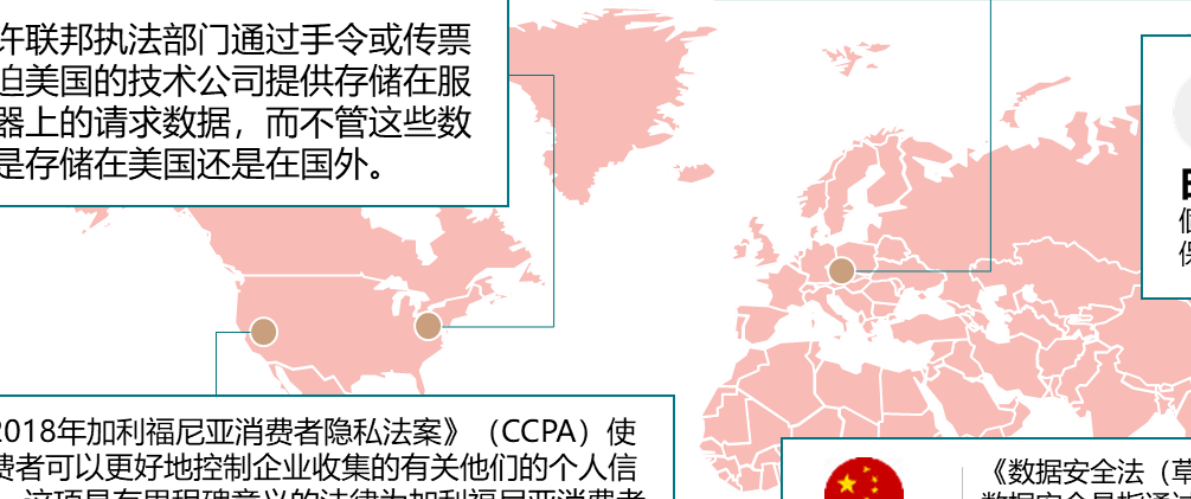
7 **指定数据保护官（DPO）**
- 独立，直接向最高管理层报告
- 告知和建议，监控合规性，和作为监管机构的联络点

8 **数据画像限制**
- 不受制于评估健康、工作表现、个人喜好和经济状况的自动处理方式的权利

9 **同意的要求**
- 在收集前自由给出
- 具体而明确
- 随时可撤销

10 **向数据保护机构发出违规通知，并与数据主体进行沟通**
- 无延迟地通知监管机构（最长72小时）
- 报告性质、后果和补救措施

后GDPR时代国家隐私法规的发展趋势



美国
CLOUD
法案

《澄清境外合法使用数据法案》

允许联邦执法部门通过手令或传票强迫美国的技术公司提供存储在服务器上的请求数据，而不管这些数据是存储在美国还是在国外。

EU CLOUD COC

欧盟云行为准则基于GDPR提出了明确的要求和建议的程序，以提高云服务中的数据保护水平。

日本
個人情報保護法

个人信息保护法（APPI）

日本已于2017年底与欧盟就GDPR的相应规定进行了协商。2018年7月17日，双方确定彼此的法律和法规具有适当的保护。

美国
《加利福尼亚消费者隐私法案》（CCPA）

《2018年加利福尼亚消费者隐私法案》（CCPA）使消费者可以更好地控制企业收集的有关他们的个人信息。 这项具有里程碑意义的法律为加利福尼亚消费者确保了新的隐私权，其中包括：

- 了解企业收集的个人信息以及如何使用和共享个人信息的权利；
- 删除从其中收集的个人信息的权利（有一些例外）；
- 拒绝出售其个人信息的权利； 和
- 行使CCPA权利的非歧视权。

中国
数据安全法（草案）

《数据安全法（草案）》将数据定义为任何电子或非电子形式的信息记录。数据安全是指通过采取必要的措施来确保数据得到有效保护和合法使用并持续处于安全状态的能力。国家坚持维护数据安全，平等促进数据开发利用，通过数据开发利用和产业发展促进数据安全，通过数据安全保证数据开发利用和产业发展。

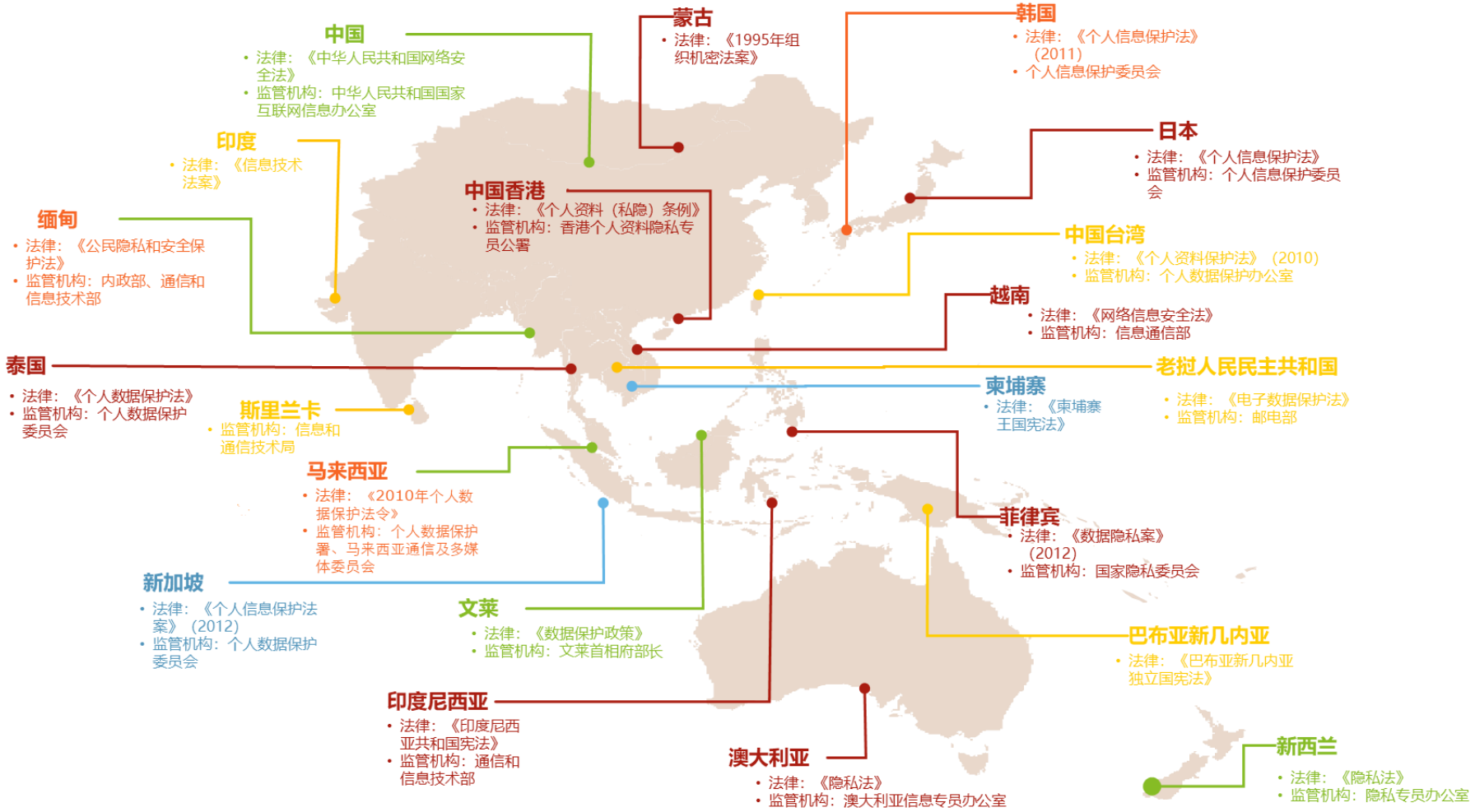
《数据安全法（草案）》要求，数据保护应基于数据在经济和社会发展中的重要性，并且如果对数据进行篡改、破坏、泄漏或非法获取或使用，将会损害国家安全、公共利益或公民和组织的合法权益。基于危害程度对数据进行分类和保护。重要数据的处理者应设立数据安全官员和管理机构，履行相应的数据安全保护职责，并采取必要的安全措施，否则应承担相应的法律责任。

生命科学和健康行业中的GDPR罚款

国家	日期	罚款（欧元）	控制者/处理者	所引用法条	概要
德国	2019-10-30	14,500,000	Deutsche Wohnen SE	Art. 5 GDPR, Art. 25 GDPR	该公司使用了一个归档系统来存储租户的个人数据，但该系统没有提供删除不再需要的数据的可能性。存储租户的个人数据并不检查是否允许存储或甚至是否需要存储。这涉及到有关租户个人和财务状况的数据，例如工资表、自我披露表、就业和培训合同的摘录、税收、社会保障和健康保险数据以及银行对账单。
荷兰	2019-10-31	900,000	UWV	Art. 32 GDPR	由于UWV（荷兰雇员保险服务提供商-“ Uitvoeringsinstituut Werknemersverzekeringen”）在访问在线雇主门户时未使用多因素身份验证，因此安全性不足。 雇主以及健康和安全服务部门能够在记录缺勤的系统中收集和显示员工的健康数据。
英国	2019-12-17	320,000	Doorstep Dispensaree Ltd. (Pharmacy)	Art. 32 GDPR	该公司已在建筑物背面未密封的容器中存储了约500,000个文档，其中包含姓名、地址、出生日期、NHS编号以及医疗信息和处方，但未能有效保护这些文档，导致文档受到水的损害。
德国	2019	294,000	Unknown	Art. 5 GDPR	一家公司因“不必要地长时间”存储和保留人事档案以及在人员选择过程中“过度”收集数据而被罚款294,000欧元，在此期间还要求提供健康数据。
挪威	2020-02-26	73,600	Rælingen Municipality	Art. 5 (1) f) GDPR, Art. 32 GDPR	在Showbie数字学习平台中处理了15名肢体和精神残疾儿童的健康信息，在学校与其家庭之间传递了与健康有关的个人信息。 Datatilsynet发现，在使用该应用程序之前，没有进行必要的风险评估、隐私影响评估或测试，并且登录该应用程序时缺乏安全性，导致可以访问小组中其他学生的信息。

亚太隐私保护法规

亚太隐私法规一览


中国
• 法律：《中华人民共和国网络安全法》
• 监管机构：中华人民共和国国家互联网信息办公室
蒙古
• 法律：《1995年组织机密法案》
韩国
• 法律：《个人信息保护法》（2011）
• 个人信息保护委员会
印度
• 法律：《信息技术法案》
日本
• 法律：《个人信息保护法》
• 监管机构：个人信息保护委员会
中国香港
• 法律：《个人资料（私隐）条例》
• 监管机构：香港个人资料隐私专员公署
缅甸
• 法律：《公民隐私和安全保护法》
• 监管机构：内政部、通信和信息技术部
中国台湾
• 法律：《个人资料保护法》（2010）
• 监管机构：个人数据保护办公室
越南
• 法律：《网络信息安全法》
• 监管机构：信息通信部
泰国
• 法律：《个人数据保护法》
• 监管机构：个人数据保护委员会
老挝人民民主共和国
• 法律：《电子数据保护法》
• 监管机构：邮电部
柬埔寨
• 法律：《柬埔寨王国宪法》
斯里兰卡
• 监管机构：信息和通信技术局
马来西亚
• 法律：《2010年个人数据保护法令》
• 监管机构：个人数据保护署、马来西亚通信及多媒体委员会
菲律宾
• 法律：《数据隐私案》（2012）
• 监管机构：国家隐私委员会
新加坡
• 法律：《个人信息保护法案》（2012）
• 监管机构：个人数据保护委员会
文莱
• 法律：《数据保护政策》
• 监管机构：文莱首相府部长
巴布亚新几内亚
• 法律：《巴布亚新几内亚独立国宪法》
印度尼西亚
• 法律：《印度尼西亚共和国宪法》
• 监管机构：通信和信息技术部
澳大利亚
• 法律：《隐私法》
• 监管机构：澳大利亚信息专员办公室
新西兰
• 法律：《隐私法》
• 监管机构：隐私专员办公室

亚太各国隐私法特点

	知情权	访问权	修正权	擦除权	限制处理权	数据可携权	反对权	自动化决策和用户画像相关权利	强制性数据泄露通知
澳大利亚	✓	✓	✓	✗	✗	✗	✗	✗	✓
中国	✓	✗	✓	✓	✗	✗	✗	✗	✓
中国香港	✓	✓	✓	✓	✓	✗	✓	✗	自愿通知
印度	✓	✓	✓	✓	✓	✗	✓	✗	自愿通知
印度尼西亚	✓	✓	✓	✓	✗	✗	✓	✗	✓
日本	✓	✓	✓	✓	✓	✗	✓	✓	✓
马来西亚	✓	✓	✓	✓	✓	✗	✓	✗	✗
新西兰	✓	✓	✓	✗	✗	✗	✓	✗	自愿通知
新加坡	✓	✓	✓	✗	✗	✗	✓	✗	自愿通知
韩国	✓	✓	✓	✓	✓	✗	✓	✗	✓
泰国	✓	✓	✗	✓	✓	✓	✓	✗	✓

中国数据保护和隐私法规

中国市场的数字化转型带来合规性挑战

1. “互联网”与“业务”的深度融合

背景

1. 对行业进步的需求
2. 大数据、云计算、人工智能和其他技术的驱动
3. 中国对“互联网+商业”的支持和鼓励

影响

行业领先公司不断寻求变化和突破

2. 越来越多的监管关注

背景

1. 公司将不可避免地收集、使用和处理用户的个人信息
2. 管理和技术上的新漏洞将给数字化转型中的公司带来越来越多的挑战

担忧

1. 如何平衡行业发展与合规要求之间的关系
2. 在保护用户个人信息和隐私安全的前提下，如何充分利用业务数据的价值

中国网络安全合规要求

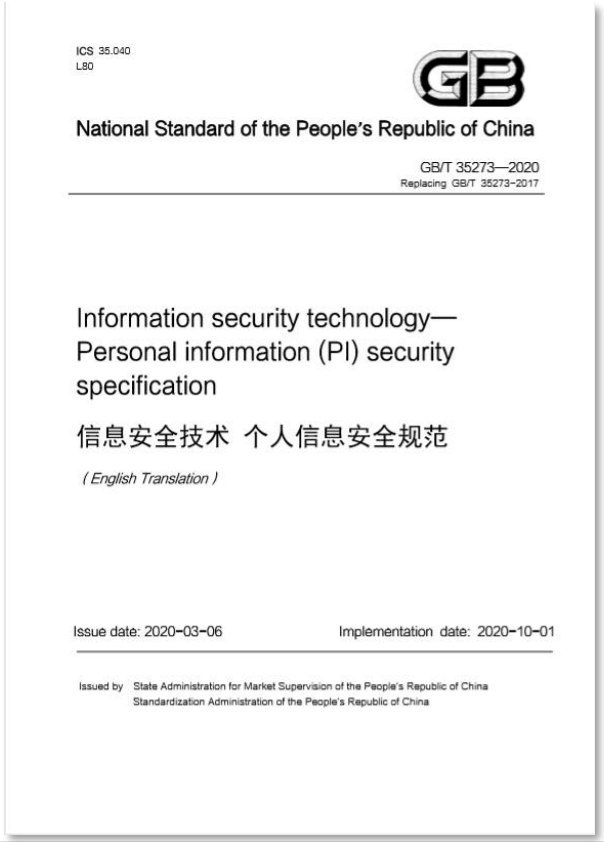
中国政府希望提高网络空间安全性和个人隐私保护的成熟度，依据《中华人民共和国网络安全法》（CCSL）逐步发布了一系列法律、法规和标准。 由于篇幅所限，下面仅列出部分政策、法规或标准：

部分网络安全合规要求

立法趋势

2020年3月6日 发布
2020年10月1日 正式生效

GB/T 35273-2020



ICS 35.040
L80

National Standard of the People's Republic of China

GB/T 35273—2020
Replacing GB/T 35273-2017

Information security technology—
Personal information (PI) security
specification

信息安全技术 个人信息安全规范

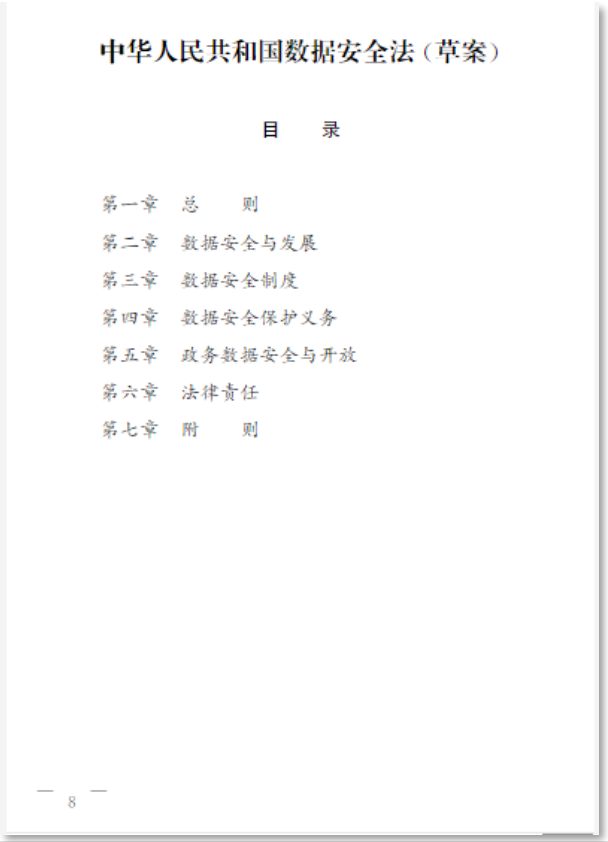
(English Translation)

Issue date: 2020-03-06 Implementation date: 2020-10-01

Issued by State Administration for Market Supervision of the People's Republic of China
Standardization Administration of the People's Republic of China

2020年7月2日 发布征求意见稿

数据安全法草案



中华人民共和国数据安全法（草案）

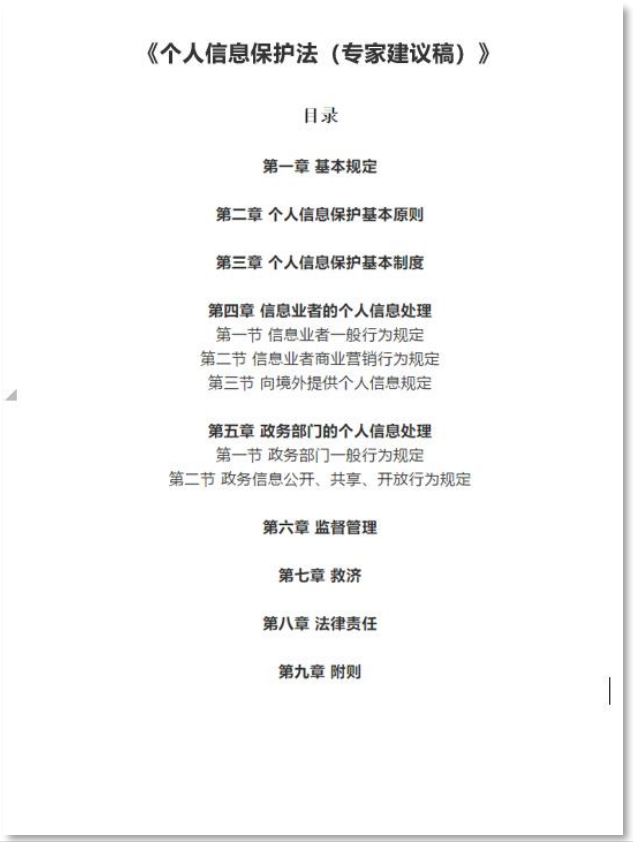
目 录

第一章 总 则
第二章 数据安全与发展
第三章 数据安全制度
第四章 数据安全保护义务
第五章 政务数据安全与开放
第六章 法律责任
第七章 附 则

— 8 —

2020年 正式进入立法进程

个人信息保护法



《个人信息保护法（专家建议稿）》

目录

第一章 基本规定

第二章 个人信息保护基本原则

第三章 个人信息保护基本制度

第四章 信息业者的个人信息处理
第一节 信息业者一般行为规定
第二节 信息业者商业营销行为规定
第三节 向境外提供个人信息规定

第五章 政务部门的个人信息处理
第一节 政务部门一般行为规定
第二节 政务信息公开、共享、开放行为规定

第六章 监督管理

第七章 救济

第八章 法律责任

第九章 附则

中方提出《全球数据安全倡议》

2020年9月8日上午，国务委员兼外长王毅在“抓住数字机遇，共谋合作发展”国际研讨会高级别会议上发表题为《坚守多边主义 倡导公平正义 携手合作共赢》的主旨讲话，提出《全球数据安全倡议》。

1. 各国应**以事实为依据**全面客观看待数据安全问题，积极维护全球信息技术产品和服务的**供应链开放、安全、稳定**。

2. 各国**反对**利用信息技术**破坏他国关键基础设施或窃取重要数据**，以及利用其从事**危害他国国家安全和社会公共利益**的行为。

3. 各国承诺采取措施防范、制止利用网络侵害个人信息的行为，**反对**滥用信息技术从事针对他国的**大规模监控、非法采集他国公民个人信息**。

4. 各国应**要求企业严格遵守所在国法律，不得要求**本国企业将境外产生、获取的数据存储在境内。

5. 各国应**尊重他国主权、司法管辖权和对数据的安全管理权**，未经他国法律允许不得直接向企业或个人调取位于他国的数据。

6. 各国如因打击犯罪等执法需要跨境调取数据，应**通过司法协助渠道或其他相关多双边协议解决**。国家间缔结跨境调取数据双边协议，**不得侵犯第三国司法主权和数据安全**。

7. 信息技术产品和服务供应企业**不得在产品和服务中设置后门**，非法获取用户数据、控制或操纵用户系统和设备。

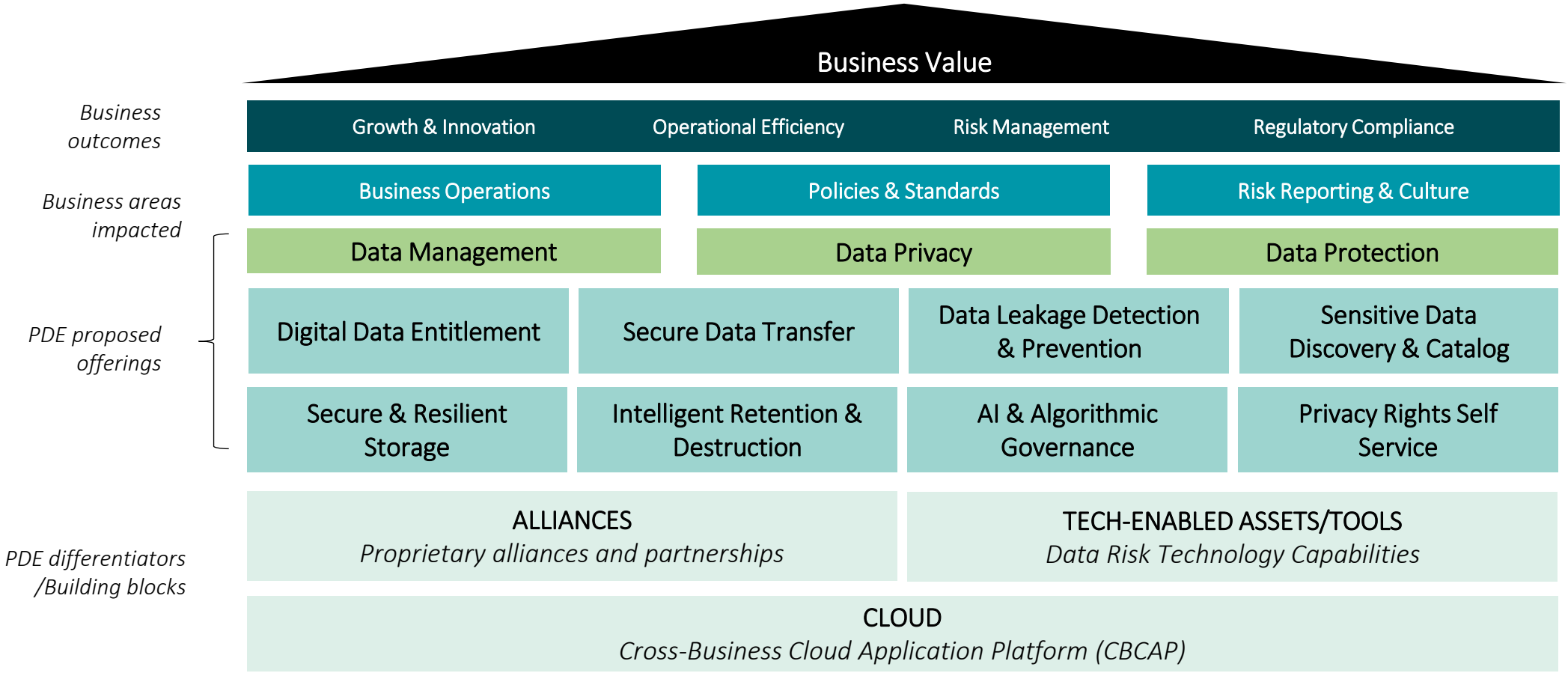
8. 信息技术企业**不得利用用户对产品依赖性谋取不正当利益，强迫用户升级系统或更新换代**。产品供应方承诺及时向合作伙伴及用户告知产品的安全缺陷或漏洞，并提出补救措施。

生命科学和健康行业中的常见场景

大数据技术的应用将推动医疗健康企业向精确医学的转变，将根据患者的病情选择相关的临床途径。 这种能力未来将基于收集患者信息和营销数据进行发展，以及使用在线和离线渠道对目标进行营销。

场景类别	信息特点	特征与案例	安全措施要点
个性化服务与管理	**业务要求**：必须准确识别个人 **信息内容**：包含完整准确的个人健康医疗信息 **信息接收与使用者**：可识别的个人、有审计、有保护隐私义务	针对个人的医疗服务、卫生健康服务，传染病管控等 **场景举例**：医院互联互通、远程医疗、健康传感数据管理、移动应用、商保对接	由于涉及个人标识信息，环境与接收人需要严格管控，需要高标准保证数据完整性和可用性
服务对象告知	**业务要求**：服务对象个人可识别，周边人不易识别 **信息内容**：部分个人可识别信息或代码，与其他信息内容分离，例如张XX、排队序号等 **信息接收与使用者**：不识别个人，局部小范围人群	在公开场合通知服务对象，例如门诊叫号、检查叫号、体检服务叫体检人等	个人信息需部分遮蔽，环境与接收人数量受到限制
管理、研究、教育与统计分析	**业务要求**：不需要识别个人 **信息内容**：一般人口信息、各类医疗、卫生服务信息 **信息接收与使用者**：不可识别	例如病例分析、各类病种分布统计、流行病研究、疾病队列研究等 **场景举例**：临床科研、医学健康教育、医疗/医疗研发	需要进行去标识化处理，通过协议或领地模式严格管控，需要确保数据的完整性和真实性

德勤的隐私和数据保护框架



薛梓源

Tonny XUE

北京 东城

扫一扫上面的二维码图案，加我微信

CONTACT

pscinitiative.org

info@pscinitiative.org

Annabel Buchan:
+55 (11) 94486 6315

PSCI

@PSCInitiative

WeChat

制药供应链组织PSCI

For more information about the PSCI please contact:

PSCI Secretariat
Carnstone Partners Ltd
Durham House
Durham House Street
London
WC2N 6HG

info@pscinitiative.org

+55 (11) 94486 6315

About the Secretariat
Carnstone Partners Ltd is an independent management consultancy, specialising in corporate responsibility and sustainability, with a long track record in running industry groups.

carnstone
partners ltd