2020威科先行系列实务指引

数据全球化与隐私保护指引

环球律师事务所 GLOBAL LAW OFFICE SINCE 1979

Wolters Kluwer | 威科先行®

环球律师事务所
GLOBAL LAW OFFICE
SINCE 1979

总 序

承载一百八十年的专业服务品质，立足中国法律服务市场的需求。2020年，本着以精品内容持续服务法律市场的愿景，威科先行法律信息库推出的“威科先行实务指引”系列内容，特邀持续耕耘法律实务领域且成绩卓越的律师及团队为作者进行深度撰写。本年度“ 威科先行实务指引”系列品牌内容将聚焦网络安全、金融、反商业贿赂、劳动法四大领域，受邀作者团队将从多维视角出发进行内容撰写，落地成册，汇集成法律实务领域的智慧指引，赋能中国法律实务人士。

环球律师事务所
GLOBAL LAW OFFICE

关于我们

中国首家律师事务所：环球律师事务所由中国国际贸易促进委员会在 1979 年创建，是中国改革开放后成立的第一家律师事务所。经过四十多年来的不懈努力和发展，我们已成为中国律师业中最优秀的大型综合性律师事务所之一。

中国最优秀的大型综合性律师事务所之一：自成立伊始，我们即确立了“以国际化的视野、国际化的团队、国际化的质量服务于国内外客户”的宗旨，这使我们虽置身于多变的全球经济形势之中，却始终能够保持不变的业界领先地位。我们连续多年被众多的国内外权威法律评级机构评选为顶级的中国律师事务所之一，包括《钱伯斯》《法律 500 强》《亚洲法律杂志》等。

专业而卓越的律师团队：我们的律师均毕业于国内外一流的法学院，其中多数律师拥有法学硕士及以上的学历，部分合伙人还拥有美国、英国、澳大利亚、瑞士、新西兰、香港等地的律师执业资格。我们的律师团队拥有出色的执业背景，许多律师还曾就职于法院、国内外顶级律所或行业领先的企业与机构。

综合的一站式法律服务：我们能够为来自广泛行业的国内外客户，提供跨业务领域综合的一站式法律服务。我们深耕的行业包括但不限于银行、金融、保险、证券、投资、贸易、能源、矿业、化工、钢铁、制造业、交通运输、基础及公共设施、生命科学及医疗、电信、传媒、高科技、文娱体育、房地产、酒店休闲、餐饮、大消费等众多的细分领域。

开创性的问题解决能力：我们的律师能够将精湛的法律专业技术和丰富的商业知识结合起来，采用务实且富有建设性的综合法律方案，解决复杂多变的各类问题。我们保持领先的专业创新能力，善于富有创造性地设计交易结构和细节。在过去的四十多年来，我们凭借对法律的深刻理解和运用，创造性地完成了许多堪称“中国第一例”的项目和案件。

客户至上的服务理念：四十多年来，我们凭借精湛的法律知识、丰富的执业经验、高度的敬业精神以及良好的职业道德，向国内外客户展示和证明了我们的价值，同时也赢得了国内外客户的信赖。在未来的日子里，我们将继续凭借我们独到的优势助力国内外客户取得更为持久和长远的成功。

作者简介：

孟洁

孟洁为环球律师事务所常驻北京的合伙人。主要执业领域为网络安全、个人信息保护、互联网、电商合规、反腐败反商业贿赂合规。孟律师曾在诺基亚等世界五百强跨国公司和知名律师事务所工作超过十余年，担任知名人工智能独角兽公司总法律顾问、DPO。曾经及目前服务于大型跨国公司及知名互联网企业、车企、IoT、电信、云服务、人工智能、金融、医疗领域企业进行境内 / 境外的数据合规体系建设与数据合规专项，总结出不少可落地的实操方法论，颇受客户好评。她是国际隐私保护协会中国区联席主席，被 Legal 500评为“2020年度 TMT 领域特别推荐律师”、被全国律协评为全国千名涉外专家律师。孟律师曾经翻译过美国、欧盟、印度、巴西、俄罗斯等国的数据保护法案，并在各大期刊、公号发表过数百篇专业文章、著作，例如有《SDK 安全与合规白皮书》V1.0版与 V2.0版，《个性化展示安全与合规报告》等。

KOH Kok Shen（许国盛）

KOH Kok Shen 为环球律师事务所资深顾问，拥有通信、计算机、金融服务领域商业与合规领域的超过20年的丰富经验，并且熟悉美国合规法律与司法部实践，他对于跨文化之间的法律合规问题及合作深有心得。KOH Kok Shen 律师曾任迪堡有限公司的亚太合规负责人以及诺基亚有限公司亚太区法律顾问，并富有多年领导商业谈判的经验。KOH Kok Shen 律师具有英国和新加坡职业资格。KOH Kok Shen 律师自2005年开始于中国居住，在此之前，他在新加坡为互联网公司以及互联网、IT 行业初创企业提供了多年法律服务。

王程

王程为环球律师事务所的专业律师，主要执业领域为数据合规、知识产权与争议解决事宜，曾先后就职于花旗银行法务部、于美国纽约担任争议解决律师。王律师为纽约州执业律师、美国纽约北区联邦法院执业律师。王程律师本科毕业于上海外国语大学，具有法学与文学双学位，研究生毕业于美国 Emory 大学法学院。

陈子谦

陈子谦为北京市环球律师事务所的律师助理，主要执业领域网络安全与数据合规、个人信息隐私保护等领域。陈子谦曾在出门问问信息科技有限公司实习，负责数据合规方面的法律研究，包括欧盟 GDPR、美国 CCPA 和亚太地区法律及标准等；发表专业文章数篇；参与企业隐私保护、数据合规方案落地；协助审核、起草并翻译相关合同及文件。陈律师本科毕业于西南政法大学法学院，可以使用中文和英文工作。

张淑怡

张淑怡为北京市环球律师事务所的律师助理，主要执业领域为网络安全与数据合规、个人信息隐私保护等领域，发表关于数据保护法律法规分析的文章多篇。张淑怡本科毕业于外交学院，研究生毕业于英国爱丁堡大学法学院。

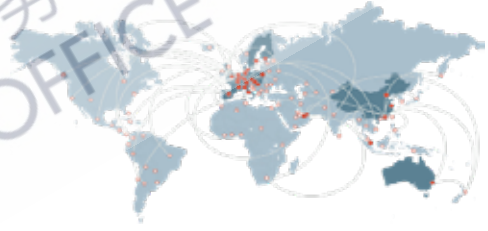
致谢：

特别感谢以下人员对本指引所做的各方面的支持与贡献：刘淑珺、殷坤、史筱唯、刘心怡、叶欧仪、王若菡

Bird & Bird

鸿鹄律师事务所

鸿鹄律师事务所是一家真正的国际化律所，其团队围绕客户的需求而组建。我们热情而又务实，了解客户所需，帮助客户实现真正的商业优势。



万事万物皆有关联

鸿鹄现有 1350 多名律师和法律从业人员，在全球设有 29 个办公室，擅长运用领先的专业知识提供全方位的法律服务，所涉领域包括商事、公司、欧盟与竞争、知识产权、争议解决、劳动法、金融、以及房地产。

鸿鹄成功的关键在于行业专注性。本所客户的业务基础是技术和无形资产，众多客户在规范市场运营。为了更好地满足客户需求，我们不断深入了解重要行业，包括汽车、航空与国防、能源与公用事业、金融服务、医疗保健与生命科学、零售与消费品、媒体、娱乐与体育、信息技术与通信。

我们跟随客户的业务变化调整自身：本所近日成立了专门的技术与通信行业团队，这就是听取客户意见的直接成果，帮助我们成功地在行业发展中占得先机。

国际视野

鸿鹄在世界各地的主要商业中心都建立了办公室：

- 欧洲： 阿姆斯特丹、布拉迪斯拉发、布鲁塞尔、布达佩斯、哥本哈根、杜塞尔多夫、法兰克福、海牙、汉堡、赫尔辛基、伦敦、卢森堡、里昂、马德里、米兰、慕尼黑、巴黎、布拉格、罗马、斯德哥尔摩、华沙
- 中东与亚洲： 阿布扎比、北京、迪拜、香港、上海、新加坡、悉尼
- 北美：旧金山

本所是唯一一家在丹麦、芬兰和瑞典设立办公室的国际律师事务所，因此本所对寻求在北欧地区投资的企业而言是一个理想的选择。此外，本所与非洲、印度、日本和俄罗斯的当地律所建立了广泛的合作关系，使本所的业务版图延伸至其他重要法域。近期我们在旧金山开设了代表处，为我们的美国客户除美国之外的法律服务需求提供支持。

卓越的客户服务

鸿鹄是一家真正意义上的国际律所：我们共享相同的目标、会计制度和利润池，因为我们承诺在适当的地点安排适当的律师为客户提供服务。鸿鹄律师事务所有着开放、灵活的企业文化，力求提高反应速度，尽快帮助客户解决所面临的商业压力。为客户提供卓越的服务永远是我们的头等大事，无论客户如何定义卓越。

深入的行业知识

- 在每个行业相关的法律和监管框架都拥有法律专知。
- 由众多在相关行业拥有数十年经验的顾问提供务实而具有商业意识的服务。

中国业务联系人

储开泰 – 中国管理合伙人

ted.chwu@twobirds.com

专家顾问：

Ruth Boardman
合伙人，伦敦
ruth.boardman@twobirds.com

陈曼珊（Michelle Chan）
合伙人，香港
michelle.chan@twobirds.com

Hamish Fraser
合伙人，悉尼
hamish.fraser@twobirds.com

Ariane Mole
合伙人，法国
ariane.mole@twobirds.com

Dr. Fabian Niemann
合伙人，德国
fabian.niemann@twobirds.com

Jeremy Tan
合伙人，新加坡
jeremy.tan@twobirds.com

Lupe Sampedro
合伙人，伦敦
lupe.sampedro@twobirds.com

Berend Van Der Eijk
律师，荷兰
berend.vandereijk@twobirds.com

余绚雯（Clarice Yue）
法律顾问，香港
clarice.yue@twobirds.com

Lisa Vanderwal
法律顾问，悉尼
lisa.vanderwal@twobirds.com

Dr. Lena El-Malak
律师，阿聯酋
lena.elmalak@twobirds.com

Dr. Natallia Karniyevich
律师，德国
natallia.karniyevich@twobirds.com

Chester Lim
律师，新加坡
chester.lim@twobirds.com

Willy Mikalef
律师，法国
willy.mikalef@twobirds.com

柯恬恬（Tiantian Ke）
律师，上海
tiantian.ke@twobirds.com

Ester Vidal
律师，西班牙
ester.vidal@twobirds.com

NISHIMURA & ASAHI

关于西村朝日律师事务所

一流律师事务所强强联手，结成综合性律师事务所不断成长。西村朝日律师事务所通过整合多家专业性强、综合实力过硬的律师事务所，逐步形成了现有的组织结构。充分发挥各自的优势，在经验和专业技巧上形成互补，整体上实现知识扩充和机动性强化，从而更加全面灵活地应对各种社会经济结构与法律制度的变化。

律师人数超过 600 名，日本规模最大。西村朝日律师事务所的日本律师及外国律师人数超过 600 名，若包括税务师、专利商标代理人、律师助理和职员在内，总人数已超过 1,600 名。团队成员分别具备各领域的专业技能，可覆盖不同法律领域，不断提升律师事务所的综合实力。

顺应不断变化的全球化时代潮流，搭建稳如磐石的业务网络。作为国际法务领域的专家，迄今为止，西村朝日律师事务所已在欧美及世界各国建立了业务网络。2010 年起，伴随日本企业进军新的海外市场的战略，西村朝日律师事务所在亚洲及世界各国开设了办公网点。同时，西村朝日律师事务所与当地实力雄厚的律师事务所建立密切的合作关系，结合各国法律及国情，为客户提供完善的法律服务。此外，通过增加日本国内办公网点数量，为日本各地企业进军海外市场提供支援服务。目前，西村朝日已建立起灵活支持各种全球业务的运营体制。

个人信息与隐私 / 大数据领域

随着 IT 化的发展，对于包括个人数据在内的所谓大数据的利用，越来越受到国内外企业的关注。另一方面，由于这种个人信息的利用会给个人带来不安或不适，所以保护个人信息的重要性也日益增加。不仅日本，欧洲等世界各国的保护个人信息的法律及规定也在不断完善。西村朝日律师事务所基于国内外相关管制的最新信息，对金融、医疗、IT 领域等各行业的各种情况下的个人信息的利用，进行多角度／战略性的分析，提供实务性的法律咨询。此外，在应对个人信息泄露、侵犯隐私等事故中，也拥有丰富经验。开展国际业务的企业，在出现境外或者跨国的问题时，西村朝日律师事务所将与相关国家的律师合作进行对应。

西村朝日 - 数据隐私团队联系人：
河合优子（合伙人）
y_kawai@jurists.co.jp

目 录

前言

OECD《保护个人数据隐私和跨境流动准则》提出了促进贸易流通同时，鼓励数据自由流动（除特殊情况外），以达到各方利益的平衡，并由此制定了跨境数据流动的共同标准以改进全球隐私法规的“交互性”。《跨太平洋合作伙伴全面进步协议》着重强调了数据必须伴随商品和服务的自由贸易而自由流动。在如今数字信息时代，随着“数字化经济”概念的提出，全球贸易与经济一体化的步伐不断加快，“一带一路”战略稳步前行，互联互通的网络打开了中国与世界更加紧密相联的新格局。数据，毋庸置疑地成为了驱动未来经济增长和效率提升的核心资产，已与“石油、矿产、天然气”等共同成为了新生产力的要素。

我们不难发现，跨国收购、出海投资、跨境电商与售后服务、跨境支付与物流、全球版 App 发行等场景高密度出现，这些都依赖于来自世界各地的数据进行分析、计算与决策。大型跨国企业更以统一化运营的方式管理其国际业务与来自全球的员工，更多服务会通过本地采购或统一外包给境外第三方组织提供来实现，全球化数据中心的布署与第三国云计算服务合作伙伴的参与，为跨境数据流动提供了支持与帮助。与此同时，人们对于隐私和数据保护的认知也在逐步提高。在欧洲《通用数据保护条例》（“GDPR”）生效以后，各国隐私和数据保护的立法也迅速且蓬勃地发展起来。

《数据全球化与隐私保护指引》（“本指引”）共分为四大部分，以国内企业出海为视角，分别介绍了目前企业在数据全球化现象中面临的挑战与机遇、中国企业在进行出海业务应当如何开展前期规划（包括对数据出境要求梳理、出境数据的盘点、准备合同与评估、完成特殊审批并选定目标国家等）、全球重点目标国家及地区的数据与隐私保护法律解读，以及区域间各数据跨境流动体系的概述，以为中国企业“走出去”提供数据与隐私方面的实践性合规指引。

从本指引可见，虽然大部分国家和地区的法律在很大程度上受到了 GDPR 的启发，与 GDPR 的体例趋于一致，但也有些国家和地区采取了不同的立法态度以满足其国内的特殊需求。除了特殊数据需进行本地化不谈，原则上各国和地区都允许跨境数据传输，只是一些国家和地区因其国情不同，会设置不同的数据跨境传输条件：有的是以允许数据出境为原则，特殊类型数据不得出境；有的是以禁止数据出境为原则，但允许在符合例外条件下出境。

为了能够让中国企业在“走出去‘发展和国外企业’走进来”中国国门后，提前了解各国隐私保护法律与监管政策，避免在本土开展业务时或扩展全球业务时“水土不服”，我们撰写本指引以提供资讯。同时，我们也期待不同国家与地区之间可以致力于建构一个全面的、有高度的、多边参与的数据隐私合作框架，更有力地探讨不同法域在隐私保护法律法规上的可融合性和各国执行层面上的一致性。只有这样，才能更加促进数字经济在和谐的框架内有序且充分的流通，确保在国家安全的基础上达到多边共赢。我国《个人信息保护法（草案）》第十二条所述，“国家应积极参与个人信息保护国际规则的制定，促进国际交流与合作，推动与其他国家、地区与国际间组织的个人信息保护规则、标准的互认”。如果能为学界、立法界多贡献素材，也是本指引的写作初衷之一。

望得到同行及各界朋友的不吝指正，并感恩您与我们一路相伴！

孟洁
2020 年 11 月 8 日凌晨
写于北京华贸写字楼一座
(Email: mengjie@glo.com.cn)

第一部分
数据全球化
——企业的挑战与机遇

一、发展趋势

在数字社会与信息时代中，数据已经毋庸置疑地成为了驱动未来经济增长和经济效率的核心资产，同时人们对于隐私和数据保护的认识也在逐步提高。

欧洲数据保护法律的基石 - 《通用数据保护条例》（以下简称为“ GDPR”）的生效，不仅改变了欧洲，还成为了在全球范围内对于隐私和数据保护领域的立法参考，规划了全球的立法形态。紧随着欧盟，美国、中国、印度、东南亚和许多其他地区都出现了一股在隐私和数据保护方面的立法风潮。一些法律在很大程度上受到了 GDPR 的启发，同时也与 GDPR 的规范内容趋于一致，而其他地区则采取了不同的方式以满足其国家内部的需要。

随着全球隐私和数据保护制度的发展，我们不难发现各个国家地区在法律层面上出现了共同的特征，包括更广泛的管辖地域和域外效力、强化的执法或制裁条款、对数据主体权利的更有力保护、以及对国家和网络空间之主权意识的不断增强。在未来几年中，隐私和数据保护法有望继续成为最活跃、发展最快的法律领域之一。

二、企业面临的挑战

随着全球隐私和数据保护法律法规的迅猛发展，几乎所有企业都在努力有效地解决多方面广泛的与数据生命周期相关的监管和操作风险，包括在数据的收集、使用、共享和披露以及其他数据处理时的风险。以下是企业面临的一些主要挑战。

1. 在全球范围内，对于企业来说并没有“一体化”的数据保护合规方法。 尽管最近在隐私保护和数据保护制度领域的更新在一定程度上受到了 GDPR 的启发，但是出于地区间差异的考量，仅仅靠遵守 GDPR 是不足以形成全球化通用的合规策略的。即使在欧洲各个国家间，GDPR 也没有完全统一规则 - 它允许欧盟成员国就某些数据保护事宜自行立法。 达到此类国家特定的克减规定是可行的，但企业应准备好应对日益严格的当地要求。

2. 跨境数据传输面临越来越大的困难。尽管数据跨境的自由流通对企业、消费者和国家经济都有好处，但许多国家还是选择为数据的跨境流转设置障碍，例如禁止或限制某些或全部数据出口的数据本地化要求。因此，企业应充分了解其业务运营所在地区适用的数据出境法律法规。

3. 数据隐私法律方面的执法行动成为热点。 不遵守隐私和数据保护的法律法规可能会给机构组织造成一系列损害性后果，包括巨额罚款、声誉受损、客户信任度下降、损失消费者或员工、被个体起讼等等。此外，严重的数据泄露行为可能会很大程度上影响企业的成功、持续性运营。

4. 新兴技术和创新可能会遇到来自隐私和数据保护法律层面的挑战。 当难以确定新技术带来的确切影响时，新技术与隐私及数据保护法之间就会处于剑拔弩张的状态。对于企业而言，找到一个能够符合数据隐私合规要求的途径来开发和使用新技术是具有挑战性的。

为了帮助企业了解不同司法管辖区之间的各种隐私和数据保护要求，我们撰写了本数据全球化和隐私保护指引以供参考。

在以下各节中，本指引将介绍一些不同国家地区的隐私和数据保护制度，包括：

- 欧洲（英国、德国、法国、荷兰和西班牙）
- 北美（美国、加拿大）
- 亚洲（日本、中国、中国香港、新加坡、马来群岛、泰国、印度、阿拉伯联合酋长国、沙特阿拉伯）以及
- 大洋洲（澳大利亚和新西兰）。

对于每个地区，我们将简要介绍在隐私和数据保护方面公司经常问到的典型问题，即：

- 该国家地区的数据保护法律体系如何?
- 由谁负责相关法律的监督和执行?
- 相关法律会如何适用于公司?
- 数据保护原则是什么?
- 公司可以依循什么法律依据?

- 如何定义个人数据?
- 何种情况下公司会被认为是控制者，何种情况下是处理者?
- 数据主体有哪些权利?
- 隐私声明中应提供哪些信息?
- 公司应注意哪些直接营销法律法规?
- 对于数据共享和处理有哪些要求?
- 对儿童数据是否有特殊保护?
- 公司应采取什么措施来确保实现问责制?
- 在数据泄露方面是否由通知的要求?
- 跨境数据传输规则是什么?
- 国家地区如何执行数据隐私法律?

第二部分
我国企业出海的前期规划

一、企业出海的数据合规思路

《网络安全法》作为现阶段网络安全领域的核心法律，仅针对关键信息基础设施运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据的出境行为做出了限制规定，而对于“一般性”的网络运营者并未做出明确的限制规定，其他现行的法律及行政法规也仅针对部分特殊行业的数据出境行为进行限制。

从各项法规和 / 或国家标准的征求意见稿中，我们不难发现，国家对于数据出境的规制态度趋于严格。但整体来看，通过明确合理的规定，在确保网络空间主权、国家安全、数据安全、法人及个人合法权益不受侵害的前提下，保证数据有序且安全的自由流通。近期出台的《数据安全法（草案）》也证明了这一点，第一、二条明确了促进数据开发利用，但因境外组织、个人开展数据活动损害到国家安全、公共利益或者公民、组织合法权益的，将被依法追究法律责任。这一规定体现了既鼓励数据流通又维护国家安全和数据主权的立法宗旨，赋予《草案》必要的域外适用效力。2020 年 10 月发布的《个人信息保护法（草案）》第三条第二款亦明确规定，在以向境内自然人提供产品或者服务为目的，或分析、评估境内自然人的行为时，适用该法。

因此，和其他国家相比，数据出境在现阶段中国法律体系下并不属于一个绝对禁止或者难以实现的业务场景，企业在履行相应的合规义务后仍可以顺利完成数据出境。企业在规划数据出境工作前应当重点注意以下要点。

1. 明确公司业务类型与收集的数据情况

1.1 本地化储存

根据《网络安全法》第三十七条的规定，关键基础设施运营者应当在中国境内存储在境内运营收集和产生的个人信息和重要数据，且仅当出于业务需要时，经相关监管机关评估后方可出境。《个人信息保护法（草案）》第四十条关于关键信息基础设施运营者的规定与《网络安全法》第三十七条规定基本一致，但提高了数据本地化的门槛，即个人信息达到一定数量的也需要境内存储。具体数量级有待于网信部门出台进一步的细则要求。

若公司符合关键信息基础设施运营者的标准，且经过评估后确认数据的出境为“确需提供”的情况，则同时需要将开展的安全自评估保存两年并上报行业主管部门。因此，企业应提前做好相应安排，及时对业务进行评估，明确自身是否属于“关键基础设施运营者”，以确保自身数据出境的合规性。而作为一般性的网络运营者，根据近期出台的一系列征求意见稿等文件，根据具体拟需出境的数据类型事先履行评估流程。但与关键基础设施运营者不同的是，一般性的网络运营者仅在满足部分特殊情况的前提下，需经监管机关评估，比如说《个人信息保护法（草案）》如果拟出境的是个人信息的，需要关注个人信息的数量，如果达到了国家网信部门规定的一定数量的，就需要将在中华人民共和国境内收集和产生的个人信息存储在境内，确需向境外提供的，应当通过网信部门组织的安全评估。虽然《个人信息保护法（草案）》以及其他一些部门规章和国家标准还在征求意见尚未生效，暂时不具有法律约束效力，但在一定程度上代表了立法机关对于数据出境问题的规制态度，将来也很有可能依照目前的规制内容直接生效适用，因此建议企业尽早落实数据出境的评估制度。

1.2 数据类型

根据《中华人民共和国保守国家秘密法》等法律法规、国家标准的规定，并非所有数据都可出境且部分数据的出境有一定限制。为了保证出海业务的顺利进行，企业在数据出境前的规划中应当充分考虑出境的业务场景、出境数据类型以及各类数据在出境时是否会受到限制等问题，以避免在数据出境时遭遇阻碍、违反相关法律法规等情况，减少不必要的损失。

1.2.1 存在限制出境的数据类型

	相关法律法规	数据类型	数据出境的限制
1.	《中华人民共和国保守国家秘密法》	国家秘密类数据	禁止出境
2.	《地图管理条例》	地图数据	服务器须设在境内
3.	《征信业管理条例》	征信机构在中国境内采集的信息	征信机构在中国境内采集的信息的整理、保存和加工，应当在中国境内进行。
4.	《中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知》	个人金融数据	在中国境内收集的个人金融信息的储存、处理和分析应当在中国境内进行。 除法律法规及中国人民银行另有规定外，银行业金融机构不得向境外提供境内个人金融信息。

5.	《网络预约出租汽车经营服务管理暂行办法》（2019 年修正）	个人信息及业务生成的数据	个人信息和生成的业务数据，应当在中国内地存储和使用，保存期限不少于 2 年，除法律法规另有规定外，上述信息和数据不得外流。
7.	《人口健康信息管理办法》	人口健康信息	责任单位不得将人口健康信息在境外的服务器中存储，不得托管、租赁在境外的服务器。
8.	《人类遗传资源管理暂行办法》	人类遗传资源	未经许可，任何单位和个人不得擅自采集、收集、买卖、出口、出境或以其他形式对外提供重要遗传家系和特定地区遗传资源。
9.	《国家健康医疗大数据标准、安全和服务管理办法（试行）》	健康医疗大数据	应当存储在境内安全可信的服务器上，因业务需要确需向境外提供的，应当按照相关法律法规及有关要求进行安全评估审核。
10.	《邮件快件实名收寄管理办法》	实名收寄活动中收集和产生的用户信息和重要数据	在中华人民共和国境内实名收寄活动中收集和产生的用户信息和重要数据应当在境内存储。
11.	《证券基金经营机构信息技术管理办法》 《外商投资期货公司管理办法》 《私募投资基金服务业务管理办法（试行）》 《关于加强在境外发行证券与上市相关保密和档案管理工作的规定》	客户信息及业务资料数据 在境外发行证券与上市过程中，提供相关证券服务的证券公司、证券服务机构在境内形成的工作底稿等档案	除法律法规和中国证监会另有规定外，证券基金经营机构不得允许或者配合其他机构、个人截取、留存客户信息，不得以任何方式向其他机构、个人提供客户信息。 外商投资期货公司交易、结算、风险控制等信息系统的核心服务器以及记录、存储客户信息的数据设备，应当设置在中国境内。 在境外发行证券与上市过程中，提供相关证券服务的证券公司、证券服务机构在境内形成的工作底稿等档案应当存放在境内。

1.2.2 个人信息出境

1.2.2.1 个人信息主体的授权同意

个人信息出境需要遵循个人信息主体授权同意的基本原则。《网络安全法》规定，网络运营者在“使用”个人信息主体的个人信息时，应当获得其授权同意。而“使用”包括“跨境传输”的行为，因此，对于未获得个人信息主体同意的数据，不得出境。《个人信息与重要数据出境安全评估办法（征求意见稿）》进一步对此做出了明确解释，“个人信息出境，应向个人信息主体说明数据出境的目的、范围、内容、接收方及接收方所在的国家或地区，并经其同意。未成年人个人信息出境须经其监护人同意。”此处的同意代指明示的同意，即需要个人信息主体通过书面、口头等方式主动做出纸质或电子形式的声明，或者自主做出肯定性动作，对其个人信息进行特定处理做出明确授权。《数据出境安全评估指南（征求意见稿）》也对于实践中构成有效同意的场景

做出了列举，包括拨打国际及漫游电话、发送国际电子邮件、进行国际即时通信等。《个人信息保护法（草案）》规定了企业向中华人民共和国境外提供个人信息的，应当向个人告知接收方的身份、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使权利的方式，并取得个人信息主体的单独同意，即应当由个人在充分知情的前提下，自愿、明确地作出意思表示。需要通过强提示，让个人信息主体充分知悉风险，经过审慎地思考并通过主动勾选或者签署等肯定性的动作，作出充分的意思表示，而不得通过概括授权的方式代替。

如果无法获得个人信息主体同意的，在某些特定场景（例如：危及公民生命财产安全等紧急情况的）下也可以将个人信息传输出境，但一般来讲这种例外情形在企业的日常经营中发生的概率较小，企业如需将个人信息传输出境的，还是应该先征得个人信息主体的同意。

除获取个人信息主体的同意外，企业还需要注意，个人信息的出境也应获得国家相关部门的批准，详情请参阅下文第 1.2.2.3 节所述。

1.2.2.2 完备且全面的合同

除同意外，与数据接收方之间签署合作协议应当是个人信息顺利出境的第二个核心要素。企业需要通过合同对数据接收方的权利和义务做出明确规定，基于此保障个人信息的安全，维护个人信息主体及企业自身的合法权益。

首先，企业在合同中需要特别注意明确企业与接收方在本次合作中分别承担的角色，这不仅关系到后续数据安全事件中的责任分配，更是对于影响着企业制定内部政策及保护措施等重要环节。

企业与数据接收方之间既有可能是数据控制者与委托处理者的关系，也有可能是共同数据控制者的关系，需要根据具体的数据收集处理场景进行分析并通过合同进行明确。根据《信息安全技术 个人信息安全规范》第 3.4 条，个人信息控制者是“有能力决定个人信息处理目的、方式等的组织或个人”。因此，判断企业与数据接收者之间角色关系的核心要点在于确认数据接收方对数据使用目的及方式是否拥有自主权。当双方关系为“共同控制者”时，数据接收者对于数据的收集、使用等都拥有自决性，在获取后也不需要根据企业的指令进行销毁或者交还数据。一些数据接收方会出于后续业务发展、数据变现的考虑而要求获得“共同数据控者”的身份。企业应考虑业务需求，具体出境的个人信息类型等对此进行判断与评估。

在确定了双方分别承担的角色后，企业应当重点参考《个人信息出境安全评估办法（征求意见稿）》的具体规定，该办法除了要求企业在合同中明确出境的信息目的、个人信息类型等基本情况外，还对个人信息主体的救济途径、接收方及提供方的责任义务、接收方所在国家的法律环境是否合适等诸多方面做出了具体且明确的规定。企业在与境外接收方签署合同时，应当重点注意涉及上述规定的合同条款。

如个人信息主体有要求，企业还应当提供此合同的复印件，此合同也将作为监管机关进行安全评估的重点参考文件，建议企业提高对此类合同的重视程度并详细完善各项条款。

1.2.2.3 省级网信部门进行个人信息安全影响评估

根据《个人信息出境安全评估办法（征求意见稿）》的规定，个人信息出境前，网络运营者应当向所在地省级网信部门申报个人信息出境安全评估。省级网信部门的评估已经成为了个人信息出境的前置程序，只有在省级网信部门评估同意后方可出境。

因此，建议企业在进行数据出境之前应当事先对出境行为进行安全自评估，发现潜在风险并及时整改，以提高主管机关评估的通过率。

是否获得个人信息主体同意也应属于评估的一项内容，因此，企业可以在确认已获得个人信息主体同意的情况下开展安全影响评估流程。其中，企业应当重点评估以下内容：

- 是否制定数据出境计划
- 是否符合国家有关法律法规和政策规定。
- 合同条款是否能够充分保障个人信息主体合法权益。
- 合同能否得到有效执行。
- 企业自身或接收者是否有损害个人信息主体合法权益的历史、是否发生过重大网络安全事件。
- 企业获得个人信息是否合法、正当。

如果个人信息被获准出境，企业应当建立个人信息出境记录并且至少保存 5 年。同时，企业应在每年 12 月 31 日前将本年度个人信息出境情况、合同履行情况等报所在地省级网信部门。

值得注意的是，《个人信息保护法（草案）》避免了一刀切式的要求，借鉴 GDPR 中关于 SCC、认证的相关规定，规定了网信办组织评估、专业机构进行个人信息保护认证、与境外接收方订立合同这三种情况。企业因业务需要，确需向中华人民共和国境外提供个人信息的，应当至少具备上述任何一项条件。《个人信息保护法（草案）》对此作出的调整有利于促进数据在不同法域间的流通，也为企业进行正常商业贸易下的个人信息出境提供了更多选择。

《个人信息保护法（草案）》的公布标志着中国在个人信息保护方面的一大步，尽管《个人信息保护法（草案）》目前正处于征求意见稿阶段，但依然体现了目前国家对于个人信息保护的监管趋势，同时鉴于《个人信息保护法（草案）》所规定的高昂违法成本，建议企业尽早进行自查，注重进行安全影响评估、制定内部管理制度、做好对个人信息进行分级分类和加密存储等安全措施、记录处理活动、制定应急预案、定期进行审计和培训演练，发挥内部能动性和外部机构优势，定制一套综合全面、可持续的数据出境合规体系。

1.2.3 重要数据出境

1.2.3.1 重要数据的识别

根据《数据安全管理办法（征求意见稿）》，重要数据是指一旦泄露可能直接影响国家安全、经济安全、社会稳定、公共健康和安全的数据，如未公开的政府信息，大面积人口、基因健康、地理、矿产资源等数据。重要数据一般不包括企业生产经营和内部管理信息、个人信息等。《数据出境安全评估指南》的附录 A 中对重要数据的类型作出了详细列举，也可以作为公司判断重要数据的主要参考依据。

1.2.3.2 安全自评估

重要数据出境前的安全影响评估不同于个人信息，企业应在数据出境前自行组织进行安全评估，并对评估结果负责。在评估过程中应当重点注意以下评估要点：

- 数据出境的合法性、正当性及必要性；
- 涉及个人信息情况，包括个人信息的数量、范围、类型、敏感程度，以及个人信息主体是否同意其个人信息出境等；
- 涉及重要数据情况，包括重要数据的数量、范围、类型及其敏感程度等；
- 数据接收方的安全保护措施、能力和水平，以及所在国家和地区的网络安全环境等；
- 数据出境及再转移后被泄露、毁损、篡改、滥用等风险；
- 数据出境及出境数据汇聚可能对国家安全、社会公共利益、个人合法利益带来的风险。

企业在完成自评估后，应当将自评估报告留存至少两年，且每年至少进行一次数据出境安全影响评估并及时将评估情况报行业主管或监管部门。此外，需注意的是，虽然重要数据出境与个人信息出境不同，其出境不是必须请主管机关评估的请主管机关评估，但是根据《数据安全管理办法（征求意见稿）》第二十八条的规定，公司向境外提供重要数据前，应当评估可能带来的安全风险，并报经行业主管监管部门同意；行业主管监管部门不明确的，应经省级网信部门批准。因此，可以看出，中国在数据出境方面加大了主管机关的控制权，秉持在合法、有序的基础上进行数据流通的规制原则。

1.2.3.3 报请主管机关评估

在某些特殊情况下，例如涉及的数据量级过于庞大、数据类型过于敏感以及其他可能危害国家安全和社会公共利益的情况时，仅进行企业自评估已经不足以满足合理的安全期待，此时需要报请行业主管机关进行评估，由国家网信部门、行业主管部门确定主管部门评估范围，制定主管部门评估方案，并成立主管部门评估工作组，并最后形成主管部门评估报告。专家委员会将结合主管部门评估报告和安全自评估报告进行审议并给出是否同意数据出境的建议。最后，国家网信部门、行业主管部门根据专家委员会建议做出决定。

在此情况下，企业应当事先进行完善且全面的安全自评估，根据评估结果完成整改，在确保各项

评估指标已经基本符合要求的前提下，再报请主管机关进行评估，提高评估通过的概率。

2. 合理选择出海目标国

对于企业而言，在选择数据出境目标国家之前需要进行综合考量与仔细分析。目标国家的选择需要评估多个方面的因素，例如客户群体的需求、数据出境的成本以及企业自身运营的便利性等。除上述商业考量之外，另外一个不可忽略的重要因素则是中国法律法规以及国家标准对于数据出境的规定。

正在征求意见过程中的《信息安全技术 数据出境安全评估指南（征求意见稿）》（以下简称“《数据出境安全评估指南》”）细化了数据出境安全的要求，为涉及跨境数据传输的企业与机构提供了更为详细的指引。其中第 5.2.6 条对于数据出境的目标国家做出了规定，明确了数据出境安全评估的要点应当包括“数据接收方所在国家或地区的政治法律环境”。

2.1 目标国家评估标准

《数据出境安全评估指南》进一步区分了个人数据与重要数据出境目标国家的评估要求。当出境的客体是个人数据时，该条规定要求企业对数据接收方所在国家或地区的以下方面做出评估：

- 该国家或地区现行个人数据保护法律法规或标准情况，与我国现行个人数据保护法律法规或标准提供的保护水平相比较的差异性；
- 该国家或地区加入的区域性或全球性的个人信息保护方面的机制，以及其做出的具有约束力的承诺；
- 该国家或地区落实个人信息保护的机制，如是否具有特定的执法或监督机构、行业自律机制以及为数据主体提供的行政或司法救济渠道等。

当出境的客体是属于《数据安全评估指南》附录 A 中所规定的重要数据[1]时，除上述三个方面外，相关政府部门还被要求针对以下接收方所在国家或地区以下方面做出评估：

- 该国家或地区在数据安全方面的现行法律法规、标准情况；

1 即，相关组织、机构和个人在境内收集、产生的不涉及国家秘密，但与国家安全、经济发展以及公共利益密切相关的数据（包括原始数据和衍生数据），一旦未经授权披露、丢失、滥用、篡改或销毁，或汇聚、整合、分析后，可能造成以下后果的数据应被认定为重要数据：
a) 危害国家安全、国防利益，破坏国际关系；
b) 损害国家财产、社会公共利益和个人合法利益；
c) 影响国家预防和打击经济与军事间谍、政治渗透、有组织犯罪等；
d) 影响行政机关依法调查处理违法、渎职或涉嫌违法、渎职行为；
e) 干扰政府部门依法开展监督、管理、检查、审计等行政活动，妨碍政府部门履行职责；
f) 危害国家关键基础设施、关键信息基础设施、政府系统信息系统安全；
g) 影响或危害国家经济秩序和金融安全；
h) 可分析出国家秘密或敏感信息；
i) 影响或危害国家政治、国土、军事、经济、文化、社会、科技、信息、生态、资源、核设施等其它国家安全事项。

- 该国家或地区落实数据安全的机制，如网络安全或数据安全方面的主管机构、司法机制、行业自律机制等；

- 该国家或地区政府（包括其执法、国防、国家安全等部门）调取数据的法律权力；

- 该国家或地区与其他国家或地区间有关数据流通、共享等方面的双边或多边协定。

2.2 评估结果

根据《数据安全评估指南》附录 B 中第 B.3.3 条的规定，接收方所在国家或地区的政治法律在评估中会根据其具体情况被划分为高、中、低三个保障能力等级，并被作为评估接收方所在国家或地区总体安全风险级别的依据。

而接收方所在国家或地区总体安全风险的级别也可能会对数据最终能否出境的结果产生较大影响，因此，企业在选定数据出境的目标国家前，除从商业角度进行分析外，还应当对该国数据保护方面的政治与法律情况做出分析，确保目标国家的数据安全风险处于可控的范围内，从而使数据出境能够顺利进行。如果风险不处于可控范围内，则说明该目标国家对于数据安全方面的保护措施不足。如企业仍坚持将该国家选为数据出境的目标国家，则有可能遭受数据安全事故带来的损失，甚至也会有可能招致相关政府部门的行政处罚。

3. 熟悉目标国家或地区法律法规 / 监管条例、司法判例与合同要求

当数据出境通过上述层层评估与审核，确认满足数据出境要求后，企业应注意这并非数据流转周期的终点。此时的合规应同时重点关注目标国家在个人信息与隐私保护领域的法律 / 法规、司法判例与合同要求，以确保数据在目标国家的保存、处理、共享、转让等符合相应的监管要求。

在数字经济与大数据的浪潮下，各国都在积极探索监管路径，以确保数据在实现其商业价值的同时不损害个人信息主体的各项权利。境内企业进行数据出海的目标国家主要集中在欧盟、美国及亚太地区，而这三个辖区也先后推出了针对数据方面的安全保护法案，例如，欧盟《通用数据保护条例》（“GDPR“）以及 EDPB 出台的各项意见及指南，通过整体且统一的保护标准构建起了欧盟数据保护新的法律体系；而美国虽然目前尚未在联邦层面制定统一的数据隐私保护法，但是已经通过在各个分散领域的法规中对某些特殊类型的信息及行业作出了针对性规定，如针对儿童保护方面的 COPPA 法案、针对医疗领域的 HIPAA 法案等，此外，单独针对个人信息与隐私保护的法案也已经在美国各州层面开始推进和落实，如美国的《加利福尼亚州消费者隐私法案》（“CCPA”），通过消费者保护的角度对于个人信息的收集与处理做出规定，明确了数据保护规则和相关主体义务。而亚太地区各国家也都普遍重视个人信息保护与隐私安全问题并出台了相应的法案进行约束，如韩国的《个人信息保护法案》（“PIPA”）、印度《个人数据保护法案》（“PDPB”）等。

企业一旦违反上述法案，将会承担较为严重的法律责任及后果，建议企业应当事先密切关注目标国家的个人信息保护法律法规与政策，并在数据出境后合法合规地完成后续处理流程，减少不必要的商业损失。具体可参考本指引其余章节对于不同国家 / 地区个人信息保护法律法规的阐述与

分析。

二、总结

1. 建立基准

综上所述，我们可以看到数据出境需要经过一系列的仔细考量与评估。企业首先应对于出海业务涉及的业务及数据进行梳理，确定目标国家。其次，需对于数据出境的目的进行评估，确认数据出境的合法性、正当性与必要性。然后，企业应起草数据出境计划并进行数据安全自评估，在适用的情况下还需通过国家网信部门与行业主管部门的评估。当满足所有数据出境的要求后，企业应注意明确自身在数据收集处理中的角色，对数据采取有效保护措施，并同时推进在目标国家的数据合规工作，以确保数据安全并减少不必要的违规处罚。

因此，建议企业针对数据出境的整体流程建立一套完善的合规流程及制度文件，包括在线协议、自评估流程模板、企业内部安全保护制度、数据跨境传输合作协议模板等内容，以形成规范化的数据出境流程制度，定期完成评估及报送的义务，保障数据在安全可控且合法合规的情况下进行跨境流通。

2. 追踪与调整

企业需要注意的是，达到数据出境的合规要求是一个持续动态的过程，在建立了完善的数据出境合规体系后，还需要对法律法规的更新情况、数据出境的数据类型、目的、接收方等的变更情况、安全保护措施是否能够与时俱进、数据接收方的安全保护能力、目标国的法律法规及政治环境变更情况等诸多方面进行长期且密切的关注和监测。一旦发生变化，应当及时根据相关法律法规的要求进行处理，以确保数据出境的风险始终处于可控的范围内。

第三部分
全球数据与隐私保护

一、欧洲

1. GDPR 概述

1.1 概述

1.1.1 法律体系

自 2018 年 5 月 25 日起生效的欧盟《通用数据保护条例》（“GDPR”）[2]，是欧盟通过的一项法律，其性质为条例（Regulation）。GDPR 通过并生效后，取代了欧盟《数据保护指令》（Data Protection Directive）[3] 以及所有成员国的数据保护法，对欧盟所有成员国发生直接的、统一的、首要的效力。但是，在很多场合（例如，履行法律义务，执行公共事务，处理员工数据等），GDPR 允许或要求成员国就数据保护事宜进行立法。

除 GDPR 之外，其他法规对欧盟制度下的企业也很重要，例如，1）《电子隐私指令》（e-Privacy Directive）[4] 及其修订，该指令适用于电子通信行业中的个人数据处理，以及 2）适用于刑事执法机关出于执法目的而处理个人数据的《数据保护执法指令》（Law Enforcement Directive）[5]。

2 Regulation (EU) 2016/679。

3 Directive 95/46/EC。

4 Directive 2002/58/EC。

5 Directive (EU) 2016/680。

1.1.2 监管机构

每个欧盟成员国的本地数据保护机构（“DPA”）继续存在并执行数据保护法，其在 GDPR 中被称为监管机构。欧盟数据保护委员会（“EDPB”）是一个独立的欧盟机构，负责发布指南并就与 GDPR 相关的事项提供建议。欧盟数据保护委员会同样需要确保其数据保护成员机构之间的一致性；必须就数据保护机构进行的特定活动发表意见，并且在机构间发生争议时，扮演争议解决的角色。所有欧盟成员国的数据保护机构均参与到欧盟数据保护委员会的各方各面。欧洲经济区（EEA）国家（挪威，冰岛和列支敦士登）的数据保护机构的参与程度则比较有限。欧盟数据保护专员公署（“EDPS”）也是欧盟数据保护委员会的成员。欧盟数据保护专员公署负责监督欧盟机构中数据保护规则的应用。

1.1.3 实体和地域范围

a) 实体范围

GDPR 适用于 i）全部或部分通过自动化手段进行的个人数据处理 , 或 ii）通过自动化手段以外的其他方式进行的、构成或旨在构成归档系统的数据处理，但以下情况除外：

- 超出欧盟法律范围之外（例如，有关国家安全的活动）；
- 与欧盟共同的外交和安全政策有关；
- 有权机关出于执行刑罚的目的而执行的（另有指令适用该种情形）；
- 由欧盟机构执行的（另有条例适用该种情形）；
- 自然人实施的作为“纯粹个人或家庭活动”进行的个人数据处理。（GDPR 第 2 条）。

b) 地域范围

GDPR 可以通过两种方式适用于组织：

- 营业地标准：GDPR 适用于在欧洲经济区设立“营业地”，且在其营业地的“活动范围内”进行个人数据处理的组织。（GDPR 第 3 条第 1 款）。
- 针对性标准或监控标准：在非欧洲经济区建立的组织中，对欧洲经济区个人的下列数据处理活动将受 GDPR 的约束：

- 为其“提供商品或服务”（无论是否需要支付对价）；或者
- 在“监控”其在欧洲经济区中的行为。（GDPR 第 3 条第 2 款）。

欧盟数据保护委员会明确指出：1）组织机构打算提供商品或服务的意图应该显而易见（例如，在其网站上使用欧洲经济区语言或欧洲经济区货币），并且 2）“监控”意味着数据控制者通过这样做以达到其目的（例如行为广告和内容的地理定位，通过 cookies 进行在线跟踪和设备指纹识别）。不论组织是否有意图监控欧洲经济区中的某个个体，监控标准均适用。

1.1.4 数据处理原则

GDPR 规定了七项数据处理原则，即 1）合法性、合理性和透明性；2）目的限制；3）数据最小化；4）准确性；5）有限存储；6）完整性与保密性以及 7）可问责性。可问责性原则是一项新增原则，它要求组织负责并能够证明数据的合规性（GDPR 第 5 条）。有关可问责性原则的进一步分析，请参阅下面的第 8 节“可问责性”。

1.1.5 数据处理的合法依据

为了符合 GDPR 有关处理个人数据的规定，数据控制者必须确保每项目中的数据处理行为都具有合法依据：

- 数据主体同意。同意必须是明确的、知情的、可区分的、可撤销的和细化的以及其他自愿同意——换言之，不论数据主体是否同意或撤回其同意，都不会产生任何不利后果。

- 出于履行与数据主体之间的合同或采取措施筹备该合同的必要。数据处理必须出于与数据主体签订或履行合同之必要。

- 出于遵守成员国或欧盟法律项下法定义务之必要。法律义务不一定是成文的，但应在可预见的适用范围内清晰而精确。

- 出于维护数据主体或其他人的重大利益但数据主体无法给予同意时之必要，例如，紧急处理，灾难应对。

- 出于公共利益或在行使被授予控制者的官方权限时执行任务之必要。

- 出于合法利益目的之必要。对于数据控制者而言，这可能是最灵活的法律依据，例如为直接营销目的或防止欺诈进行数据处理。数据控制者必须确定他们所追求的是什么“利益”；确保这是合法的；并确保与处理过程对个人的影响相平衡。此合法利益评估应记录在案。（GDPR 第 6 条）。

1.2 重要定义

1.2.1 个人数据和特殊类别个人数据

“个人数据”被定义为“任何与已识别或可识别的自然人相关的信息”；一个人可通过多种方式被识别，诸如姓名、身份编号、地址数据、网上标识等。（GDPR 第 4 条第 1 款）。

特殊类别个人数据包括：种族或族裔出身，政治观点，宗教或哲学信仰，工会成员身份，关于健康或性生活和性取向的数据，遗传数据，及用于惟一识别身份的生物特征数据。（GDPR 第 9 条第 1 款）。此外，处理与刑事诉讼和定罪有关的个人数据也受到类似特殊类别个人数据的限制。GDPR 仅允许在某些特定列出的例外情况下，对特殊类别个人数据进行处理，例如基于明确同意，基于欧盟或成员国法律下的就业、社会安全以及社会保障等。

1.2.2 数据控制者和数据处理者

数据控制者指的是“决定——不论是单独决定还是共同决定——个人数据处理目的与方式的自然人或法人、公共机构、代理机构或其他实体”。（GDPR 第 4 条第 7 款）。

数据处理者指的是“代表数据控制者处理个人数据的实体”。雇员不是数据处理者。（GDPR 第 4 条第 8 款）。

有关数据控制者和处理者之间关系的更多讨论，请参见下面的第六节“数据共享和处理”。

1.3 数据主体权利

GDPR 极大扩展了数据主体对相关个人数据的权利，包括：

- 知情权和访问权（例如，获取副本）；
- 更正错误个人数据的权利；
- 擦除不符合 GDPR 要求（例如，不再需要处理；个人撤回同意；非法处理等）的个人数据的权利；
- 数据携带权，即数据主体有权获得其提供给控制者的相关个人数据，且其接收的个人数据应当是经整理的、普遍使用的和机器可读的，并且当数据处理是 1）是通过自动化方式进行的，或 2）基于同意或履行合同，数据主体有权无障碍地将此类数据从其提供给的控制者那里传输给另一个控制者（在技术可行的情况下）；
- 当处理过程存在问题时（例如，对个人数据的准确性有争议或个人已反对处理等）限制数据处理的权利；
- 反对特定类型处理的权利，包括直接营销（绝对权利），基于合法利益或公共任务以及研究或统计目的的处理。
- 如果涉及到对数据主体具有法律效力或类似重大影响的完全自动化的决策（包括用户画像），则数据主体具有不受该决定约束的其他权利。
- 向数据保护机构（DPA）进行投诉的权利。

控制者必须遵守“不应无故拖延”以及“最迟应在一个月内提供信息”，不过该期限有一定的可能性可以延长，并且在某些情况下，数据主体行使权利的请求可能受到限制（例如，访问权不应对其他权利产生不利影响，包括知识产权保护和商业秘密等；为了行使表达自由和信息自由的权利或遵守法律义务，擦除权则不适用等）。此外，控制者在响应数据主体的请求时不可收取费用。

1.4 隐私声明

隐私声明（通常也称为隐私政策）是一项应给予数据主体的信息通知，以实现其知情权并确保处理的透明性。GDPR 要求对于向数据主体提供的广泛信息，控制者应当“以一种简洁、透明、易懂和容易获取的形式，以清晰和平白的语言来提供；对于针对儿童的任何信息，尤其应当如此”，包括：

- 控制者的身份与详细联系方式；
- 处理的目的，以及处理的合法基础；
- 处理特殊类别数据时，应明确合法依据；
- 个人数据的接收者或者接收者的类型；
- 在欧盟以外进行数据传输的详情；
- 数据存储期限（如无法提供，则需要提供设定该期限的标准）；
- 数据主体权利；
- 提供个人数据是一项法定的还是合同的要求，以及没有提供此类数据可能会造成的后果；
- 是否存在任何自动化决策，以及在存在的情形下，对于涉及的逻辑、包括此类处理对于数据主体的重要性和预期后果的信息；和
- 如果收集的是间接数据，则还需要提供信息类别和信息来源。（GDPR 第 13 和 14 条）。

1.5 直接营销

合法依据：同意和合法利益是 GDPR 中最有可能用来判断直接营销合法性的法律依据。对于通过电子邮件进行的直接营销而言，欧盟《电子隐私指令》要求几乎所有类型的电子营销都必须有获取数据主体的“选择同意”（opt-in）。但是，“在销售产品或提供服务的情况下”，该邮件可能可采用“选择退出”（opt-out）机制，但是该机制须遵循有关直接营销的其他限制条件。如果该直接营销基于 Cookie，或包含在公共电子通信服务上使用的设备上进行存储信息或检索信息的其他技术，则也需要对此获取同意。因此，在线行为广告需要获得同意。

反对权：根据 GDPR，数据主体有绝对权利反对为了直接营销而处理相关个人数据，或反对和此类直接营销相关的用户画像，该权利必须“让数据主体明确知晓，且应当与其他信息区分开来，清晰地告知数据主体”。

1.6 数据共享与处理

GDPR 对控制者在委托数据处理者中施加了高度的谨慎义务。处理者的处理应受书面合同约束，该合同应载明一系列信息（例如，所处理的数据和处理的时间）和义务（例如，发生个人数据泄露时的协助义务，采取适当技术和组织措施以及审计协助义务）。这也适用于处理者进一步委托分包的情况（GDPR 第 28 条）。控制者还必须核查处理者履行其义务的能力。

GDPR 也对共同控制关系提出了要求，即两个或更多控制者共同确定处理的目的与方法。为符合 GDPR 的规定，共同控制者必须在内部之间安排各自的职责，尤其是涉及到行使数据主体权利和向个人提供透明性信息。该安排必须阐明各方在数据主体方面的职责和责任，且数据主体应当可以了解有关该安排的基本信息。（GDPR 第 26 条）。

1.7 儿童隐私保护

GDPR 做出了许多针对儿童的规定。例如，如果一个组织直接向儿童提供信息社会服务（广义而言，在线服务），并且如果是基于同意这一合法依据而处理儿童数据，那么该组织必须获得其父母的同意。在这种情况下的儿童指的是未满 16 周岁的人（但成员国可依法规定年龄低至 13 周岁）；给儿童的信息通知必须采取儿童友好的方式；处理儿童数据可能会需要进行数据保护影响评估等。在后述的情形下，儿童是指任何未满 18 周岁的人。

1.8 可问责性

1.8.1 通过设计的数据保护和默认的数据保护

要求控制者采取适当的技术和组织措施（例如假名），旨在实施数据保护原则，并整合保障数据主体权利的保障措施（“通过设计的隐私保护”）；并确保在默认情况下，仅处理为特定目的所需的个人数据（“默认情况下的隐私保护”）。（GDPR 第 25 条）。

1.8.2 数据保护影响评估（DPIA）

DPIA 是一种评估，组织机构可以通过该评估确定并减少因数据处理活动而给个人带来的风险。GDPR 要求组织机构在开始任何“高风险”处理活动之前，要进行数据保护影响评估，例如涉及系统性和广泛性的处理活动（例如用户画像），决策对个人产生法律 / 重大影响的地方，以及通过闭路电视监控系统 CCTV 对公共区域进行系统性的监控。如果此类风险无法减轻并保持较高水平，则控制者应在处理前向监管机构进行咨询（GDPR 第 35-36 条）。各成员国的数据保护监管机构已发布其所规定的需进行数据保护影响评估的活动清单。

1.8.3 数据处理活动记录

控制者应保留处理活动的记录，该记录需包括法定提供的信息，例如数据处理的类型、目的等。数据处理者也应当保留其所代表数据控制者进行的各类处理活动的记录。尽管 GDPR 规定该项要求不适用于雇员少于 250 人的组织机构，但是此项例外不适用于处理刑事犯罪或特殊类别个人数据。（GDPR 第 30 条）。

1.8.4 数据保护官（DPO）和 GDPR 代表

如果控制者或处理者的核心活动包含对某种特殊类型个人数据的大规模处理和对定罪和违法相关的个人数据的处理以及对数据主体进行大规模性的常规和系统监控，则 GDPR 要求组织机构委任一名数据保护官。数据保护官必须具有充分的专业素质，具有独立性，得到充足的支持和资源。如果数据保护官履行其他任务，则她或他对此必须没有相关的利益冲突。数据保护官的委任必须在总体上向数据保护机构公开。数据保护官的作用是提供信息 / 咨询，监督合规性并充当数据保护机构的单一联系人。（GDPR 第 37-39 条）。

此外，位于欧洲经济区以外但根据针对性 / 监控标准受 GDPR 约束的组织，必须任命一个位于欧洲经济区的“GDPR 代表”。GDPR 代表充当欧洲经济区的联络点，处理来自数据主体和数据保护机构的请求，并帮助维护数据处理的记录。（GDPR 第 27、30 条）。

1.9 安全和数据泄露通知

GDPR 将个人数据泄露定义为“由于违反安全政策而导致传输、储存或其他处理中的个人数据被意外或非法损毁、丢失、更改或未经同意而被公开或访问”。如果发生个人数据泄露，则控制者应在知悉该信息后立即（在可行的情况下，至迟在 72 小时内）将其告知给主管监管机构，除非个人数据泄露对于数据主体“不太可能”会带来风险；如果泄露可能给数据主体的权利和自由带来高风险，则控制者必须通知他们。处理者在知悉个人数据泄露后必须立即向控制者报告。此外，GDPR 要求数据控制者必须留存内部违规记录。（GDPR 第 33-34 条）。

1.10 跨境数据传输

请参见下文第四部分：区域间数据跨境流动体系中的（一）欧盟部分。

1.11 执法

GDPR 建立了两级行政罚款制度。对于某些违规行为，主管监管机构可以对组织处以最高 1000 万欧元或其全球年营业额 2%的罚款（以较高者为准）；对于 GDPR 中最严重的侵权行为，监管机构可处以最高 2000 万欧元或组织机构全球年度营业额的 4%的罚款（以较高者为准）。在某些成员国，违反数据保护法规也可能导致刑事制裁。

此外，个人有权向主管数据保护机构提出投诉，有权寻求有效的司法救济，并有权就违反 GDPR 造成的物质或非物质损害向相关控制者或处理者要求获得补偿。

2. 英国

2.1 概述

2.1.1 法律体系

在本指引起草之日，与英国仍是欧盟成员国的情况一样，GDPR 在英国境内依然可以被直接适用。在英国，《2018 数据保护法案》（以下简称“DPA 2018”）已在国会通过，被用于替代《1998 数据保护法案》并对 GDPR 做出具有英国特色的细节补充，例如，有关特定种类的数据处理的规定，以及引入对于特定事项的豁免（例如言论自由）。除此之外，DPA 2018 还包含了额外的条款以确保执行《欧盟关于知识产权的执法指令》、覆盖对情报机关处理个人数据的行为以及覆盖欧盟法律范围之外处理个人数据的行为。

英国脱欧提示：尽管英国已于 2020 年 1 月 31 日正式脱离欧盟，在脱欧过渡期结束之前（即 2020 年 12 月 31 日之前）GDPR 在英国直接适用。在过渡期结束之后，根据《2018 脱离欧盟法案》的规定，GDPR 将会被纳入英国的法律体系中，并被称为“英国 GDPR”。GDPR 与 DPA 2018 将会得到相应的修订（例如，从其中删去欧洲委员会的相关表述）。

2.1.2 监管机构

信息专员（Information Commissioner）是负责数据保护的独立监管机构，其背后有信息专员办公室（Information Commissioner’s Office，以下简称“ICO”）支持其工作。

不同于一般情况的是，ICO 要求所有在英国设立的控制者需要缴纳年注册费，以登记其处理个人数据。此项要求也存在一些豁免情况，可以登陆 https://ico.org.uk/for-organisations/data-protection-fee/ 查看更多信息。

2.1.3 实体和地域范围

英国 GDPR 的域外效力与 GDPR 相似，包括营业地标准、市场指向或者监控标准。市场指向 / 监控标准适用于在英国没有营业地的组织。

2.1.4 数据处理原则

无特殊规定。

2.1.5 数据处理的合法依据

DPA 2018 中包括了允许对特定种类个人数据以及刑事犯罪相关数据处理的可见条款。该法案有长达 16 页的克减条款，包括对用于研究、欺诈预防与侦查、劳动法律事务等目的的特定种类数据的处理的情况。为了能适用大多数的可见情况，数据控制者必须制定并准备一份补充性“适当政策文件”，并在该文件中说明数据控制者将会如何遵守 GDPR 所规定的数据保留与销毁原则。

有关处理特定种类数据的额外信息也必须记录在处理活动的记录之中。

2.2 重要定义

无特殊规定。

2.3 数据主体权利

DPA 2018 对信用机构保留特别规定，要求其提供对信用文件的访问渠道。DPA 2018 也规定了个人权利的克减条款（例如，如果实现某个访问请求会使某人意识到自己正在被调查，这就会妨碍犯罪预防工作与刑事侦查工作）以及有关医疗卫生记录、社会工作记录、教育记录的访问请求的特别程序。

2.4 隐私声明

无特殊规定。

2.5 直接营销

《2003 隐私与电子通讯（欧洲委员会指令）条例》（以下简称“PECR”）（经修订）是英国用于执行欧盟《电子隐私指令》的法规。ICO 于 2020 年 1 月发布了直接营销的行为守则草案。如果公司有关人员同意、纵容或者管理疏忽过失违反了 PECR 有关直接营销的规定，则个人可能要为公司的违法行为承担责任。

2.6 数据共享与处理

无特殊规定。

2.7 儿童隐私保护

在英国，在同意的基础上向儿童提供的信息社会服务保护的相关规定适用于 13 岁以下的儿童。

在 2020 年 1 月，ICO 发布了有关适龄儿童使用的信息社会服务设计标准的操作规范草案。该规范草案目前正等待议会通过批准。这一草案有着较广的适用范围，并针对所有可能被 18 岁以下儿童访问使用的线上服务。

2.8 可问责性

a) 通过设计的数据保护和默认的数据保护

无特殊规定。

b) 数据保护影响评估（DPIA）

无特殊规定。

c) 数据处理活动记录

如果对特定种类数据的处理是依照 DPA 2018 中规定的克减情况所进行的，则通常要求将与此相关的额外信息记录在数据处理活动记录之中。详见上文第 1.8.3 条。

d) 数据保护官（DPO）和 GDPR 代表

关于 GDPR 代表的英国脱欧提示：在英国脱欧后，设立于英国之外，但由于市场指向 / 监控标准而受英国 GDPR 管辖的组织必须任命一名英国代表。

2.9 安全和数据泄露通知

无特殊规定。

2.10 跨境数据传输

脱欧提示：除非欧盟委员会授予英国“充分性认定”地位，否则英国将会在脱欧过渡期结束后会成为第三国。这意味着从欧洲经济区（EEA）向英国进行的数据传输行为需要通过实施替代性的安全措施以对数据进行保护，例如标准合同条款（SCC）。根据英国已经通过相应的次级立法，在脱欧过渡阶段结束后向 EEA 的数据传输是被认为有充足性保护的。但这些规定都是临时性的，可能会被修改。该法律还确认了以下内容：设立于英国境内的组织可继续使用标准合同条款，且可继续向被欧盟认定为采取了充分安全保护措施的国家传输个人数据。需要再次说明的是，这些规定都是临时性的。如果英国在未来决定对数据传输采取不同的规制措施，这些规定都有可能被修订。

2.11 执法

DPA 2018 中也创制了某些刑事犯罪行为（包括，为了不回应访问或携带权的请求而删除个人数据、在未获得控制者同意的情况下故意或过失地获得或披露个人数据、妨碍 ICO 搜查令的执行等）以及主要责任人员对于组织实施违法行为的责任。

3. 德国

3.1 概述

3.1.1 法律体系

使得新的《德国联邦数据保护法》（“FDPA”）生效的《德国数据保护修正案》于 2017 年 7 月 5 日通过，并于 2018 年 5 月 25 日生效。在该法中，德国立法者广泛使用了 GDPR 中的开放条款，并引入了一些补充条款，例如与特殊类别数据的处理和与指定数据保护官员相关的规则有关的规定。 此外，FDPA 还包含了实施《法律实施指令》的条款。

在联邦一级， 2019 年 11 月 20 日发布的第二部《德国数据保护修正案和实施法案》对 150 多项联邦法律（包括《信息自由法》、《电子政府法》、BSI- 法案、《社会保障法》等）进行了修改，以满足 GDPR 的要求。此外，各州还对其自身原有的法律做了更新。

3.1.2 监管机构

德国的联邦系统（由 16 个州组成的联邦）影响对数据保护的监督。数据保护监督由各州负责，但例外为电信和邮政公司由联邦政府监督，且联邦政府已将该任务分配给联邦数据保护专员。在大多数州，监督是由数据保护专员执行的。公司受对公司总部所在地区具有管辖权的机构的监督。

3.1.3 实体和地域范围

FDPA 适用于以下情况的私人实体：

a) 控制者或处理者在德国处理个人数据；

b) 数据处理活动是在控制者或处理者在德国实体的经营活动期间；或

c) 尽管控制者或处理者在欧盟或建立关联的 EEA 内没有实体，但向德国境内的个人提供商品或服务或者监控在德国个人的行为。

3.1.4 数据处理原则

无特殊规定。

3.1.5 数据处理的合法依据

德国的立法者广泛使用了 GDPR 中的开放条款，并加入了一些允许处理特殊类别的个人数据和雇员数据的条款，其中包括：

• 当处理员工数据对建立或进行雇佣关系所必需时，通常允许处理员工数据。FDPA 还对雇主 - 雇

佣关系中的同意做出进一步阐释。

- FDPA 还允许对敏感数据进行处理。如果处理是为了评估员工的工作能力、医疗诊断等目的而进行的，例如预防医学、提供健康或社会护理或治疗、或管理健康或社会护理系统和服务或根据数据主体与卫生专业人员签订的合同，且这些数据是由卫生专业人员或受专业保密义务约束或在其监督下处理的，则允许处理敏感数据。这些进一步的规定在实践中对活跃在医疗保健行业的公司发挥着重要作用。但是，只有当组织采取保护措施保护这些数据才有可能进行前述处理。

- FDPA 还允许在用于科学或历史研究和统计目的时，未经同意处理敏感数据，前提数据处理对于该等目的的实现是必需的，并且数据控制者处理这些数据的利益大大超过了数据主体不处理数据的利益。但是为了维护数据主体的利益，数据控制者必须采取“适当和具体的措施”。

此外，FDPA 还包括评分、信用检查和消费者贷款的规定，这些规定构成了德国信贷体系的基础。

3.2 重要定义

无特殊规定。

3.3 数据主体权利

FDPA 引入了对个人数据主体权利的减损条款，特别是包括以下内容：

- **向个人提供信息的义务：**在某些特殊情况下，如果控制者打算将个人数据进一步处理用于收集个人数据时持有的目的以外的目的，则 FDPA 免除控制者告知个人其权利的义务。例如，如果提供有关进一步使用的信息会干扰法律主张的确立、行使或辩护（前提是该个人对于该等信息方面没有更高的利益）。

- **访问数据的权利：**数据主体的访问权存在一项例外，即在进行科学研究时，如果数据对于科学研究所必需的，并且提供信息将需要耗费不成比例的成本。此外，FDPA 还规定了数据主体访问数据的权利的某些豁免，例如，此类数据被记录的原因仅仅是由于法律或法定要求不能删除这些数据或者仅用于监测数据保护或保护数据，且提供信息将需要耗费不成比例的成本，而已经采取适当的技术和组织措施使其不可能被用于其他处理目的。

- **删除权：**在非自动数据处理的情况下，如果不可能进行删除，或者由于特定的存储模式而涉及到不成比例的高工作量，并且数据主体对删除兴趣不大，则 FDPA 免除了控制者删除个人数据的义务。然而，在这种情况下，需要采取处理限制措施以代替删除措施。

3.4 隐私声明

无特殊规定。

3.5 直接营销

《反不正当竞争法》（Gesetz gegen den unlauteren Wettbewerb，UWG）中规定的直接营销规则是德国对欧盟电子隐私指令的执行规则。这些规则包含了公司在进行某些类型的直接营销（特别是促销性质的电子通信）时需要遵守的具体限制。即使直接营销不涉及个人数据，该等规则也适用（例如，如果向通用电子邮件账户发送营销通信，如 info@company.com）。需要注意的是，该等规则将在适当时候被处于拟议状态的《隐私和电子通信条例》所取代。

3.6 数据共享与处理

无特殊规定。

3.7 儿童隐私保护

德国对于处理信息社会服务相关的儿童个人数据的处理所设定的 16 岁门槛这一开放条款没有加以额外规定。

3.8 可问责性

a) 通过设计的数据保护和默认的数据保护

无特殊规定。

b) 数据保护影响评估（DPIA）

无特殊规定。

c) 数据处理活动记录

无特殊规定。

d) 数据保护官（DPO）和 GDPR 代表

与 GDPR 相比，德国语境下需要任命 DPO 的门槛要低得多。除 GDPR 要求外，控制者和处理者在符合以下要求时必须指定一名 DPO：（i）经常雇用至少 20 名处理个人数据自动处理的人员；或者，不管涉及个人数据处理的人数如何，（ii）数据处理行为必须进行 DPIA；或（iii）因商业原因、匿名传输或出于市场调查和民意调查的目的而处理与传输个人数据。

3.9 安全和数据泄露通知

无特殊规定。

3.10 跨境数据传输

无特殊规定。

3.11 执法

FDPA 规定了可能导致监禁或者罚款后果的刑事犯罪行为：

• 故意且未经授权，将大量个人的非公开的个人数据用于商业目的；

• 未经授权处理非公开的个人数据，以换取费用、个人或第三人获益或故意伤害他人；

• 欺诈性获取非公开的个人数据以换取费用、个人或第三人获益或故意伤害他人。

此外，在消费贷款方面，FDPA 对未能适当处理数据主体访问请求、未告知消费者或未能在规定时限内全面、正确地告知消费者的行为规定了行政罚款。

4. 法国

4.1 概述

4.1.1 法律体系

除直接适用 GDPR 外，法国的数据保护法律框架主要由 1978 年 1 月 6 日颁布的第 78-17 号《法国数据保护法案》及其实施令组成。法国于 2018 年 6 月 20 日颁布法律对《法国数据保护法案》进行了迄今为止的最后一次修正，修正的目的在于：

确保法国国内立法的特定条款与 GDPR 条款的表述相适应，以及对欧盟 2016/680 号法令进行转化，使得自然人在主管部门出于预防、调查、侦查、提起刑事诉讼或执行刑罚的目的处理其个人数据时，能够依据该法令得到保护。

法国于 2018 年 6 月 20 日颁布的法律的主要条款，其效力溯及至 2018 年 5 月 25 日 GDPR 生效之日。

法国为实施《法国数据保护法案》于 2005 年 10 月 20 日颁布的第 2005-1309 号法令，也于 2018 年 8 月 1 日由另一项法令（以下简称“法令”）进行了更正。

4.1.2 **监管机构**

The Commission Nationale de l’ Informatique et des Libertés（以下简称“ CNIL”）于 1978 年依法成立，是法国独立的数据保护监管机构。

在法国，数据控制者无需为登记个人信息处理事项支付年费。2018 年的法律废止了事先声明及授权制度。一直以来，事先授权的法律要求仅适用于非常有限的范围，即健康数据的处理事项（第九章第 54 条第三款）。

4.1.3 **实体和地域范围**

《法国数据保护法案》适用的地域范围与 GDPR 略有不同，该法案适用于数据控制者与数据处理者位于法国境内的情形，而不考虑数据处理是否在法国进行。

除此之外，针对 GDPR 允许成员国自行立法的领域，只要数据主体是法国居民，无论数据控制者是否位于法国，《法国数据保护法案》条款即适用。

4.1.4 **数据处理原则**

无特殊规定。

4.1.5 **数据处理的合法依据**

《法国数据保护法案》中引入了额外的克减规定，允许对特殊类别的个人数据进行数据处理。上述克减规定特别包括：

员工或主管部门进行的与生物识别信息相关的，为控制工作场所出入及应用程序访问权限所绝对必要的数据处理；

与再次使用判决和决定中出现的公共信息相关的数据处理，但前提是上述处理即没有重新识别有关人员的目的，也不会造成重新识别有关人员的效果；

根据 CNIL 公开发布的合理意见，进行公共研究所必需的数据处理。

4.2 重要定义

无特殊规定。

4.3 数据主体的权利

《法国数据保护法案》为数据主体规定了额外的数据保护权利。根据该法案，数据主体有权制定有关其个人数据事后管理的指令，以及未成年人享有一项特定的删除权（将在下文详细说明）。数据控制者有义务将上述权利告知数据主体。

4.4 隐私政策

无特殊规定。

4.5 直接营销

关于隐私和电子通信的欧盟第 2002/58/EC 号法令（以下简称“ePrivacy 法令”）对于法国的电子通信直接营销规则做出了规定。2004 年《法国数字经济信心法案》（以下简称“LCEN”）将上述规则纳入到了《法国邮政和电子通信法规》（以下简称“PECC”）中。

根据 PECC 第 L.34-5 条，“禁止使用未事先同意接受直接营销的个人、订阅者或用户的联系方式使用电子通信系统、传真机或电子邮件”。直接营销的概念非常广泛，涵盖了所有旨在直接或间接推销商品、服务，或提升商品或服务销售者形象的信息。

4.6 数据共享和数据处理

无特殊规定。

4.7 儿童隐私保护

基于同意，法国会为 15 周岁以下的儿童提供信息社会服务保护。

《法国数据保护法案》为未成年人提供了一项“被遗忘”的权利。根据数据主体的要求，如果数据主体为未成年人，数据控制者有义务通过提供信息社会服务尽快删除相关个人数据。如果数据控制者已经将个人数据传输至第三方数据控制者，则其应当采取合理的措施，将数据主体关于删除所有指向相关数据的链接、复制件或备份的主张告知该第三方。

如果在数据主体提出要求的一个月内，数据控制者拒绝回复或未做出回复，数据主体可将这一事项提交 CNIL，CNIL 将在三周内对该事项做出裁决。

4.8 可问责性

a) 通过设计的数据保护和默认的数据保护

无特殊规定。

b) 数据保护影响评估（DPIA）

无特殊规定。

c) 数据处理活动记录

无特殊规定。

d) 数据保护官（DPO）和 GDPR 代表

无特殊规定。

4.9 安全和数据泄露通知

无特殊规定。

4.10 跨境数据传输

无特殊规定。

4.11 执法

在法国，违反《法国数据保护法案》和 GDPR 中的特定条款会受到刑事处罚。例如，违反安全要求，非法收集个人信息，违反限制存储原则等。

5. 荷兰

5.1 概述

5.1.1 法律体系

截至本文撰写之日，《通用数据保护条例》在荷兰可被直接适用。除此之外，荷兰在 2018 年通过了《通用数据保护条例实施法》（Uitvoeringswet AVG，以下简称“《实施法》”），以替代原《荷兰数据保护法》并针对《通用数据保护条例》在荷兰的适用补充了细则，例如特殊种类数据处理细则、将监管主体正式化的细则，以及规定了对特定事项的豁免（如言论自由）。

5.1.2 监管机构

荷兰数据保护局（Autoriteit Persoonsgegevens）是依据《实施法》的规定所建立的负责数据保护的独立监管机构。尽管荷兰数据保护局也负责监管通过电子邮件营销、Cookies 以及类似技术所进行的个人信息处理，但必须指出的是，关于垃圾邮件和信息记录程序的规则由《荷兰电信法案》规范，并主要由荷兰消费者与市场管理局（Autoriteit Consument en Markt）监管。

5.1.3 实体和地域范围

《实施法》在地域范围方面的规定与 GDPR 相似：《实施法》在该方面的规定采取了“营业场所标准”（只要该组织在荷兰境内设有营业场所或分支机构，即受《实施法》管辖）以及“目标顾客或数据监测标准”（只要该组织的目标顾客群体位于荷兰境内、或其处理 / 监控的数据与荷兰相关，即受《实施法》管辖）。其中，“目标顾客或数据监测标准”适用于那些在荷兰没有设立营业场所或机构的组织。

5.1.4 数据处理原则

无特殊规定。

5.1.5 数据处理的合法依据

《实施法》也规定了针对特殊种类的个人数据以及刑事定罪数据方面的信息处理的额外克减规定。共计有 12 个克减条款，它们允许以研究、阻止与揭发诈骗、劳动法方面为目的的针对特定种类的个人数据处理。

5.2 重要定义

无特殊规定。

5.3 数据主体的权利

《实施法》对与自动决策以及学术、新闻以及艺术方面的个人数据使用有关的数据主体权利进行了特殊的规定。同时，《实施法》对数据主体个人权利的克减做出了相关规定（例如，如果允许访问特定数据的请求会向某些人泄密，从而妨碍犯罪预防或侦查）。该法也规定了科学研究方面的特殊条款以及对于金融机构数据泄露事件告知义务的豁免情形。

5.4 隐私声明

无特殊规定。

5.5 直接营销

前文所提及的《荷兰电信法案》是荷兰对于欧盟的《电子隐私指令》的具体适用规定。关于主动提供的电子通讯以及 Cookies 的法律规定主要由荷兰消费者和市场管理局负责监督执行，荷兰数据保护局则提供涉及个人数据处理方面的额外监管。近年来，荷兰数据保护局对于直接营销的监管愈加活跃，制定了关于垃圾邮件以及 Cookies 的处理意见，并积极对这些方面加以监管。消费者和市场管理局在这方面则显得没有那么积极。必须指出的是，正如消费者和市场管理局过去的监管情况所表明的，如果有违反《荷兰电信法案》中关于直接营销的规定的情况出现，相关个体可能需要为公司的管理行为承担相应的责任。

5.6 数据共享与处理

无特殊规定。

5.7 儿童隐私保护

基于同意，荷兰会为 16 周岁以下的儿童提供信息社会服务保护。

5.8 可问责性

a) 通过设计的数据保护和默认的数据保护

无特殊规定。

b) 数据保护影响评估（DPIA）

无特殊规定。

c) 数据处理活动记录

无特殊规定。

d) 数据保护官（DPO）及 GDPR 代表

无特殊规定。

5.9 安全和数据泄露通知

无特殊规定。

5.10 跨境数据传输

无特殊规定。

5.11 执法

无特殊规定。

环球律师事务所 GLOBAL LAW OFFICE SINCE 1979

6. 西班牙

6.1 概述

6.1.1 法律体系

GDPR 在西班牙有直接的效力。除了 GDPR 外，西班牙相关法律还包括：

- 补充和 / 或完善某些 GDPR 条款的《12 月 5 日关于个人数据保护和授予数字版权的组织法 3/2018》（“西班牙数据保护法”）；和
- 包含有关直接营销和 Cookie 要求的《7 月 11 日关于信息社会服务和电子商务的第 34/2002 号法律》（“ISS 法律”）。

除上述内容外，西班牙数据保护局（“AEPD”）也会发布与解释数据保护义务相关的指南和建议。

6.1.2 监管机构

AEPD 是西班牙独立的数据保护监管机构。 除 AEPD 之外，还有两个区域监管机构（加泰罗尼亚和巴斯克数据保护机构），负责处理由区域公共机构或执行公共区域职能的私人实体进行的处理活动。

6.1.3 实体和地域范围

西班牙《数据保护法》在实体范围上采取了与 GDPR 相似的方法，但《数据保护法》本身并未规定其自己的地域适用范围，但通常认为营业地标准、市场指向或监控标准同样适用。

6.1.4 数据处理原则

西班牙《数据保护法》规定了与数据存储原则有关的特定义务。 在完全删除个人数据之前（不论是出于该等数据对于实现特定目的不再必要还是数据主体提出了删除的请求），组织应将该等数据妥善封存额外一段时间，以便数据主体主张法律权利。根据西班牙《数据保护法》的规定，“妥善封存”是指除非监管机构要求或者行使或维护法律主张，任何人不得访问该等个人数据。被封存的数据也不能出于前述情况以外的目的进行处理。只有在封存期间届满后才能将个人数据完全销毁。

6.1.5 数据处理的合法依据

西班牙《数据保护法》对某些特殊类别的个人数据和刑事定罪数据的处理提出了若干具体规定。简而言之：

除非出于明确和合法的目的需要，数据主体的同意不足以用作处理与他有关的某些特殊类别的个

人数据。这意味着，“当（处理这些数据的）主要目的仅仅是确定数据主体的意识形态、工会成员、性取向、信仰或种族或族裔血统时”，受影响个人的同意不足以处理这些数据。这项规定的目的是避免歧视性情况（例如，防止个人因其种族血统而不被雇用）。

西班牙对犯罪数据的处理进行高度限制。这些信息只能用于预防、调查、侦查潜在的刑事犯罪，或者为了判断是否发生了刑事犯罪。这意味着对这类信息的处理大多限于主管当局和执法机构。此外，律师和大律师有权处理这些数据，以便为其客户提供服务。在任何其他情况下，只有在存有适用法律规定的情况下，才能处理这些信息。

6.2 重点定义

无特殊规定。

6.3 数据主体权利

无特殊规定。

6.4 隐私声明

无特殊规定。

6.5 直接营销

ISS 法律涵盖了欧盟《电子隐私指令》在西班牙的实施条款。该法律规定了包括通过电子手段进行直接营销所需满足的要求。

6.6 数据共享与处理

无特殊规定。

6.7 儿童隐私保护

在西班牙，只有征得年龄在 14 周岁以上的儿童的同意才能处理儿童个人数据。

6.8 可问责性

a) 通过设计的数据保护和默认的数据保护

无特殊规定。

b) 数据保护影响评估（DPIA）

无特殊规定。

c) 数据处理活动记录

无特殊规定。

d) 数据保护官（DPO）和 GDPR 代表

根据西班牙《数据保护法》规定，控制者和处理者应按照 GDPR 第 37（1）条的规定任命 DPO，但同时提供了可能负有该等义务的行业清单，以作举例。但如 AEPD 所确认的，该列表并不穷尽（即仅作为示例提供）。以下为所述行业清单：

- 官方专业协会和专业总理事会；
- 提供《西班牙受教育权法》所规定的规范学习的教育中心以及公立和私立大学；
- 按照《一般电信法》的规定，经营电子通信网络并提供电子通信服务的、将大规模处理个人数据的实体；
- 大规模开展数据主体的画像活动的信息社会服务提供商；
- 银行、信用合作社和官方信用协会；
- 私人金融信贷机构；
- 保险和再保险公司；
- 受股票市场法规约束的投资服务公司；
- 能源和天然气分销商和市场营销商；
- 负责信誉数据文件和防止欺诈数据文件的实体；
- 根据数据主体的偏好进行广告和商业研究活动或进行数据主体的画像活动的实体；
- 依法有义务保留患者病史的医疗机构（不包括自由职业者的医疗专业人员）；
- 执行有关个人的业务 / 信用报告的实体；
- 通过电子、信息、远距离传送或交互方式提供赌博和游戏服务的实体；
- 私人保安公司；和
- 处理未成年人的个人数据的体育联合会。

西班牙《数据保护法》没有关于任命 GDPR 代表的具体规定。

6.9 安全和数据泄露通知

无特殊规定。

6.10 跨境数据传输

无特殊规定。

6.11 执法

无特殊规定。

二、北美

1. 美国

1.1 概述

1.1.1 法律体系

联邦层面上，美国没有一部综合且全面的数据隐私保护法，而是以各部门的部门法调整不同领域的数据保护问题。例如，《格雷姆 - 里奇 - 比利雷法》（GLBA）通过对金融机构义务的规制以保护“消费者非公开个人信息”，《健康保险携带和责任法案》（HIPAA）适用于提供医疗服务的实体，保护“受保护的健康信息”，《公平信用报告法》（FCRA）要求消费者相关的金融机构采取合理的措施以维护信用信息的机密性、准确性和相关性。美国 1986 年的《电子通信隐私法（ECPA）》旨在保护通信产生、传输以及存储于计算机过程中的电报、口头以及电子的通信内容。ECPA 适用于电子邮件、电话沟通、电子存储的数据，同时也对触犯规定将造成的刑事以及民事责任作出了规定。需要特别提示的是，美国极重视儿童个人信息的保护，并制定了 COPPA 法案，从联邦层面确立了儿童个人信息保护的基本原则与要求，为各州立法提供了明确的导向与基础。

横向层面上，美国各州订立综合隐私立法的势头愈发强劲。全部 50 个州都提出了相关的法案，但是大部分还没有通过。目前，仅加利福尼亚、内华达和缅因三州正式通过了隐私法案。其中，具有地标意义的《加利福尼亚州消费者隐私法案》（CCPA）于 2020 年 1 月 1 日正式生效，被普遍认为是美国目前最为综合的数据和隐私保护立法。为了确保符合 CCPA 的规定，加州行政法官办公室已经批准了司法部发布的 CCPA 规定（CCPAR）并立即生效。该规定确定了合规流程以及行使权利的流程，同时也明确了针对法律规范的商业公司的重要透明度和可问责性机制。违反 CCPAR 即为违反 CCPA 并且适用 CCPA 中的救济手段。

1.1.2 监管机构

美国目前还没有一个绝对的数据保护监管机构。消费者保护机构（例如：联邦贸易委员会（FTC））有权制裁侵犯消费者隐私的行为并要求公司采取补救措施。《联邦贸易委员会法》第 5 部分禁止市场中出现不公平、欺骗或欺诈行为，公司不遵循隐私政策或相关立法的行为构成欺骗性行为，因此赋予 FTC 以这一领域内的执法权力。另外，FTC 是一系列联邦隐私法的主要执法机构，包括但不限于 GLBA，FCRA 和《儿童在线隐私保护法》（COPPA）。此外，其他的消费者保护机构（例如：联邦通信委员会）也有针对数据保护执法的权利。

对于如 CCPA 的州层面立法而言，各州的检察总长可能为其执法机构。

1.1.3 实体和地域范围

如其行为影响美国公民的隐私和数据权利，外国公司也可能受到美国法律的规制。

比如，2018 年 3 月通过的《澄清域外合法使用数据法》（即云法案）允许联邦执法机构通过许

可或传票的方式强制位于美国的技术公司提供服务器存储的被要求提供的数据，不论这些数据是存储在美国境内还是境外。美国司法部在云法案白皮书中称，位于外国的外国公司如在美国提供服务，与美国构成足够的联系，依联系的本质、质量和数量可能受到美国的管辖。[6]

由于美国没有一部统一的数据保护法，这部分将主要介绍 CCPA 的适用范围。

CCPA 适用于满足以下条件之一的企业：

1）年总收入超过 250 美元；

2）购买、接收、出售五万加州消费者、家庭或设备的个人信息；

3）年收入 50% 或以上来自于出售消费者个人信息。

适用 CCPA 的企业应当：

1. 通知消费者其被收集的个人信息类别以及相应的使用目的；

2. 根据消费者的要求删除其个人信息；

3. 向消费者披露关于该企业已收集的个人信息的特定信息；

4. 向消费者披露其个人信息是否已经被售卖或以其他方式分享给了其他主体；

5. 遵循消费者的不向第三方售卖其个人信息的请求；

6. 在售卖年龄小于 16 周岁的消费者的个人信息之前，征得确认授权；

7. 不因消费者行使其 CCPA 下的权利而歧视该消费者。

1.1.4 数据处理原则

虽然美国隐私法案几乎没有明确提出数据保护原则，FTC 颁布的《在瞬息万变的时代中保护消费者隐私：对企业和立法者的建议》（以下简称“FTC 指南”）认可了某些普适的原则。

数据安全 - 企业应对消费者数据提供合理程度的安全保护。

收集限制 – 公司应将数据收集限制在特定交易或消费者与企业关系的背景下、法律允许或授权的限度内进行。

存储限制 – 公司应对数据存储施加合理限制并在收集的合法目的达成后妥善处理数据。存储期限

6 美国司法部，提升世界范围内公共安全、隐私和法治水平：云法案的目的和影响白皮书，2019 年 4 月，第 8 页。

可以是灵活的，可根据数据类型与使用之间的关系确定。

数据准确性 – 公司应维持消费者数据的合理准确性，但是提升准确性的方法可以是灵活的，可根据数据的使用及敏感度确定。

透明度 – 公司应提高数据实践的透明度。

（i） 隐私政策应明确、简短、标准化以帮助消费者更好地理解并判断公司实践是否遵循隐私政策。

（ii）公司应对其掌握的数据进行合理的访问控制，访问限度应与数据敏感性和其使用的性质成比例。

（iii）所有利益相关者均应努力向消费者普及商业数据企业实践。

1.1.5 数据处理的合法依据

数据处理的合法依据并没有直接在美国立法中体现，但是普遍认为在企业收集前应通知，且基于消费者要求应披露有关个人数据收集、使用、保存、出售的信息。

在特殊情形下（如收集敏感数据或个人信息的使用与此前声称的内容有实质改变时），相关组织应获得信息主体肯定的明示同意。

1.2 重要定义

消费者 - CCPA 将消费者定义为“根据加州法规，属于加州居民的自然人”。CCPA 适用于所有加州居民，不论其是否为适用企业的消费者。因此，企业的员工或者供应商也可以成为消费者。

个人信息 - 个人信息的定义在各州及各个立法之间不是统一的。考虑到 CCPA 是目前生效的最完善的隐私法律，这一部分将援引 CCPA。

CCPA 中“个人信息”指能够直接或间接的识别、描述与特定的消费者或家庭相关或合理相关的信息。该法案对个人信息采取了枚举的方式，对于属于个人信息范围的字段以及不属于个人信息范围的字段都进行了举例说明。

家庭 - CCPAR 将“家庭”定义为一个或一群：

（1）居住在相同地址的人；

（2）共用由企业提供的共同设备或者相同服务的人；以及

（3）为企业识别为共用同一群体账户或单独识别符的人。

敏感个人信息 - 目前许多美国隐私相关法律中都没有“敏感个人信息”概念，其范围在不同的部门和州之间也存在较大的区别。加州一直处在美国隐私立法的领先地位，在新提出的《2020 年加州隐私权利和执行法案》（CPRA）中介绍了“敏感个人信息”的定义。

CPRA 中的“敏感个人信息”指，消费者的社会保障号码、驾照、州身份证、护照号；登录账号、金融账户、借记卡或信用卡号及使用卡片所需的安全或访问码、密码；访问账号的资格；精确地理位置；披露种族或民族出身的信息、商会会员；私人联系方式（企业为联系人的除外）；生物识别信息；健康、性取向相关信息；及为识别此类信息的目的所收集或分析的其他数据。

值得注意的是，CPRA 中的一些信息也同样包括在 CCPA 所提及的 14 种数据类型中。倘若企业因未遵守合理的安全义务而致使这些数据（结合了消费者的姓名）遭到了泄露，消费者将被允许提起诉讼。

FTC 认为，界定敏感个人信息的范围是很困难的且与个案的情况紧密相关[7]。然而，FTC 认可 CPRA 内容和儿童信息均属于敏感数据明确的范例。

数据控制者 - CCPA 并未使用此术语。然而，《华盛顿州隐私法案》认可“控制者”这一角色，并将其定义为独自或与他人一起决定个人数据处理目的和方式的自然人或法人。

数据处理者 - CCPA 并未使用此术语。然而，《华盛顿州隐私法案》认可“处理者”这一角色，并将其定义为代表控制者处理个人数据的自然人或法人。

第三方 - CCPAR 将“第三方类别”定义为与企业分享个人信息的第三方类型或分类，并提供了足够的特性描述以给消费者提供有价值的关于第三方类型的理解。第三方可能包括广告网络、网络服务提供商、数据分析提供商、政府机构、运营系统和平台、社交网络、以及数据经纪人。

1.3 数据主体权利

数据主体权利存在于特定的法案语境下，这部分将主要讨论 CCPA 赋予消费者的权利。根据 CCPA，消费者应有权要求收集消费者个人信息的企业向该消费者披露其已经收集的个人信息的种类和特定字段。CCPA 已经针对此权利下的信息范围和类型进行了定义。当收到经过验证的消费者请求后，企业应当立即采取手段免费向消费者披露和提供其要求的信息。

• **知情权** – 消费者有权知道企业收集哪些个人信息、是否将个人信息出售或披露及其接收者的身份。企业可以随时向消费者提供个人信息，但消费者不应在 12 个月内向企业要求提供两次以上的个人信息。CCPA 针对提供此类信息的方法和格式进行了进一步的规范。

• **选择退出的权利 –** 消费者有权拒绝出售自己的个人信息。

• **访问权 –** 消费者有权要求企业披露和提供其已经收集的个人信息种类以及特定类型的个人信息。

7 FTC 报告：线上行为报告的自我监管原则，第 55 页。

- **免受歧视的权利 –** 即使行使隐私权利，消费者仍有权以平等的价格享受平等的服务。

- **删除权 –** 消费者有权要求企业删除已经收集的个人信息。收到经过验证的消费者要求删除其个人信息请求的企业应当从记录中删除该消费者的个人信息，并要求服务提供方从他们的记录者删除该消费者的个人信息，CCPAR 第 3 条规定了关于遵循删除请求的更多细节（包括提交此类请求的方式）。

- **数据携带权 –** 消费者有权以一种便携及技术允许范围内方便使用的形式接收信息。

- **校验权：** CCPAR 提供了企业可以用于验证提交数据访问和删除请求的个人身份的两种方法。首先，如果企业运营了受密码保护的账户，则“可通过企业现有的验证消费者账户的身份方法来验证消费者的身份”，前提是符合 CCPA 的其他要求。其次，如果个人没有受密码保护的账户，则身份验证会较为复杂，并且受制于不同的标准，具体取决于请求的性质和待解决请求所涉的个人信息类型。

CCPAR 还详细说明了如何响应此类请求以及确认和响应此类请求时需要遵守的时间要求。在响应知情权的请求时，CCPAR 还规定了当企业不需要查找个人信息时必须满足的特定条件。CCPAR 还明确了发出此类请求时不得披露的信息类型，例如，财务账号、任何健康保险或医疗识别号、账号密码、安全问题和答案或唯一生物性识别数据。

1.4 隐私声明

鉴于没有一部联邦数据保护法，这部分将聚焦于加州的要求。

- **加州在线隐私保护法（CalOPPA）**要求通过互联网收集加利福尼亚州居民的个人可识别信息（PII）的商业网站或者在线服务的运营商（即所有者）在其网站或服务上显著公布隐私政策。（参见 Cal. Bus. & Prof. Code § 22575(a)）。

为了遵守 CalOPPA，隐私政策必须：

1. 识别通过网站或在线服务收集的 PII 的类别以及共享 PII 的第三方的类别；

2. 描述消费者可以查看并请求对其 PII 进行改变的方法（如有）；

3. 描述运营商在隐私政策发生重大变更时通知消费者的方式；

4. 清楚说明政策生效的时间；

5. 披露当运营者跨第三方网站或者在线服务收集 PII，则运营者如何响应 Web 浏览器“Do Not Track（DNT）”信号或者类似的机制；

6. 披露当消费者使用运营者的网站或在线服务时第三方是否可以收集个人可识别信息。

关于显著地披露隐私政策的要求，相关法规提出了在网站上使用图标、文字链接、超链接、封面以及在手机 App 内访问政策的要求（参见 Cal. Bus. & Prof. Code 22577(b)）。

• 为了遵守 CCPA：

企业必须在其在线的隐私政策中披露以下信息，并至少每 12 个月更新一次该信息：

（1）关于 CCPA 项下消费者权利的说明；

（2）过去 12 个月中收集的有关消费者的个人信息类别清单；

（3）链接至“请勿出售我的个人信息”的单独链接。

• CCPAR 就隐私政策作出了进一步的指导。例如：

（1）如何设计和放置隐私政策使之通俗易懂、易于阅读；

（2）如何确保政策可以被残疾的消费者合理访问；

（3）隐私政策中必须提供的信息；

（4）行使请求删除个人信息权的说明；

（5）行使退出出售个人信息权的说明；

（6）行使消费者隐私权利反歧视权的说明。

1.5 直接营销

美国对于直接营销行为进行了广泛的规制。

电子邮件 - 《2003 年关于对来自未经请求的商业及色情行为的攻击进行控制的法律》（反垃圾信息法）对于商业电子邮件信息进行规制。企业必须明确、清晰地解释接收方如何能够退出接收此类信息并及时响应退出请求。

短信 – 《电话消费者保护法案》要求发送自动化的营销或推销信息前应获得接收者的明确书面同意。

电话推销 – 国家层面上，《电话营销和消费者免受欺诈滥用法案》禁止营销者通过未经要求且合理消费者认为侵犯隐私的方式拨打推销电话。不同的法案施加了各种限制，如通话时间限制、禁止拨打名录、选择退出要求、强制披露、限制自动拨号机和预录制信息的使用等。

1.6 数据分享、数据处理和数据经纪

FTC 尚未发布过数据分享相关的指南，但是白宫在 2000 年发布了一份备忘录，为联邦政府部门间个人信息分享及隐私保护提供指引。该文件提出了通知、获取同意、限制再披露、数据准确性、安全性、数据最小化、可归责性及隐私影响评估的要求。虽然这一备忘录仅直接适用于《电脑匹配及隐私权法》和联邦政府机构，相关企业在其他背景下亦可以参考实践这些原则。

CCPA 中没有数据分享的专门条款，但是消费者有权要求企业披露个人信息分享中接受第三方的类别。

CCPA 将数据经纪人定义为“有意收集与第三方没有直接关系的消费者的个人信息并将其出售给第三方的企业”。加利福尼亚州关于数据经纪人的法律要求受到规制的数据经纪人需要向总检察长（Attorney General）注册并提供有关其行为的某些信息。消费者可以选择不出售其个人信息。但是，CCPA 中“个人信息”的定义不包括可从政府记录中合法获得的信息。

1.7 儿童隐私保护

美国国会于 1998 年 10 月通过 COPPA，FTC 后续颁布了其实施规则。COPPA 及其实施规则适用于提供线上服务（包括网站、广告和手机应用程序）时收集 13 岁以下儿童个人信息的行为。COPPA 的主旨是使家长掌控线上收集了哪些儿童的个人信息。总结而言，受规制的运营者要直接对家长履行告知义务、获取可证实的家长同意、允许家长审核收集的儿童个人信息、赋予家长撤回同意及要求删除儿童信息的权利。

除了 COPPA 的要求外，CCPAR 第五条针对涉及 16 岁以下的消费者制定了特别规则，包括与建立、记录以及遵从合理措施确定明确授权出售孩子个人信息的确是孩子的家长或者监护人。CCPAR 同样提供了确保同意是由孩子的父母或者监护人作出的方法。对于年龄在 13-15 岁之间的消费者，对于该等消费者个人信息的出售须采取主动选择进入方式以及日后选择退出的权利和程序。

1.8 可问责性

1.8.1 **通过设计的数据保护和默认的数据保护**

FTC 指南提出了设计数据保护的原则，明确企业应在开发产品和服务的各个阶段融入消费者隐私保护的思想。

FTC 还呼吁公司采取最佳实践方式，在商业数据实践中以保护隐私为“默认设置”。

1.8.2 **数据保护影响评估（DPIA）**

FTC 指南提出，公司内部应建立完整的数据管理体系以贯穿产品和服务的全生命周期。其中一项管理措施就是进行隐私风险评估以提高权责一致性，并帮助定位和解决隐私问题。

另外，《华盛顿州隐私法案》第 9 部分规定，在某些情形下（如为定向广告的目的处理个人数据、出售个人数据、处理敏感个人数据），公司必须开展并记录数据保护评估。

1.8.3 数据处理活动记录

总体而言，美国没有对数据处理行为进行记录的法定要求。然而如前述，华盛顿州要求企业在特定情形中记录数据保护评估过程。

1.8.4 数据保护官（DPO）和 GDPR 当地代表

美国法律基本不要求企业任命 DPO。但是存在一些例外，如 HIPAA 和马萨诸塞州法律要求企业任命个人或团体负责隐私和数据安全合规事宜。

1.9 安全和数据泄露通知

FTC 指南明确，数据安全是设计隐私保护的基础原则之一，企业必须为消费者数据提供合理安全保护。联邦和州法律如 GLBA 和《纽约州隐私法案》要求相关组织保障个人信息的机密性和安全性或合理保护个人信息免遭未授权的攻击。另外，FTC 还根据过去的执法案例为企业发布了一份针对数据安全的指引文件 [8]。

联邦法律和各州有各自的数据安全事件通知规则，如《HIPAA 安全事件通知规则》和《1997 年加利福尼亚州信息实践法案》。总体而言，相关机构应在合理期限内通知受影响的个人和监管机构。

加州规则进一步明确，数据安全事件通知应以书面形式和简洁易懂的语言做出，包含“发生了什么事件”、“涉及那些信息”、“企业正在采取的措施”、“消费者可以采取的措施”、“更多信息”等内容。

1.10 跨境数据传输

美国法律对于跨境数据传输鲜少有明确的限制，但是某些州对于政府合同和境外外包合同涉及美国境外的数据访问、保存和处理行为有一定规制。

值得关注的是，2020 年 7 月 16 日，欧洲法院判决欧盟 - 美国隐私盾机制未对数据主体提供欧盟法律要求的充分保护，因此无效。企业在开展美国和欧盟之间数据传输时不能再依赖于这一机制。

1.11 执法

自 2017 年 1 月上任以来，加利福尼亚州总检察长已获得了涵盖各种违法行为的和解和其他新禁令，包括不当披露个人信息、数据泄漏时未能通知监管机构和用户、不能保障合理的数据安全、不能充分保护或者非法披露敏感信息以及非法预装了会损害计算机安全性的软件。自执法开始，没有专门针对具体的产业或者部门开展执法。

最近两起被加利福尼亚州总检察长起诉的案件涉及个人信息和用药信息违反《不正当竞争法》和《商业与职业守则》。因此，企业应当意识到基本数据安全的不足，包括对访问包含敏感信息计

8 指引文件原文请参见：Available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

算机的控制、防止账户和密码被未经授权使用、更新安全工具以及充分记录和监控网络活动以检测恶意活动。企业还应当注意不要错误描述提供给消费者的安全类型和级别。

FTC 执法手段包括罚款、强制执行完善隐私和安全制度、禁止使用个人信息、要求企业赔偿消费者损失、删除非法获取的消费者信息等。

根据 FTC 发布的报告，FTC 于 2019 年提起 130 余起垃圾邮件和间谍软件和 80 余起一般隐私违法行为案件。最受关注的无疑是 Facebook 和剑桥分析案，Facebook 与 FTC 达成 50 亿美元罚款的和解协议。

1.12 立法趋势前瞻

受到 CCPA 的鼓舞，科技巨头和隐私拥护者一直呼吁美国通过一部联邦隐私法。国会中已有许多提案，如《消费者线上隐私权利法案》、《消费者数据隐私法案》、和《数据保护法案》。它们提出建立美国联邦隐私监管机构，行使执行全国数据规范的职能以保护美国人的隐私。

直至美国通过一部联邦隐私法，预计会有更多的州起草和讨论隐私法案。企业应当特别关注《纽约州隐私法案》、《华盛顿州隐私法案》和马塞诸塞州 120 号参议会提案。

2. 加拿大

2.1 概述

2.1.1 法律体系

加拿大主要的隐私立法为《联邦个人信息保护与电子文件法》（“PIPEDA”），阿尔伯塔、不列颠哥伦比亚、魁北克在各自管辖区内设立了与 PIPEDA 大体一致的独立隐私立法，上述立法统称为“加拿大隐私法”。除此之外，加拿大在反垃圾邮件[9]、广播电视、电信和电子文件领域设立了具有约束力的专门立法；加拿大大部分省都制定了单独的健康隐私立法，旨在保护医疗服务中所涉健康相关个人信息安全。

2.1.2 监管机构

加拿大隐私事务专员办公室（OPC）负责监督、执行相关的数据保护法。比如，加拿大的反垃圾邮件法（SC 2010 c 23，CASL）由加拿大的广播电台 - 电视及电信委员会、加拿大竞争局以及 OPC 负责管理。每个监管机构都针对 CASL 中不同的方面的要求和执法有管辖权。

2.1.3 实体和地域范围

PIPEDA 适用于在加拿大各省（阿尔伯塔、不列颠哥伦比亚和魁北克适用本省法律）商业活动中的个人信息收集、使用和披露。不同于 PIPEDA，不论该活动是否是商业性质的，阿尔伯塔、不列颠哥伦比亚和魁北克本省法律均适用，同时也适用于员工的个人信息。此外，PIPEDA 还适用于与联邦产业（例如银行、铁路、运河、航空公司和电信公司）运营相关的个人信息。

PIPEDA 中不包含特殊的地域管辖条款。但是，加拿大联邦法院认定，如果在加拿大和企业商业活动之间存在“真实且实质的联系”，那么即使该企业设立于其他管辖领域，PIPEDA 依然适用。可能影响到该联系建立的因素包括：终端用户所在地、网站内容来源、网站运营者所在地以及主机服务器所在地。

2.1.4 数据处理规则 / 标准

PIPEDA 规定了十项公平信息原则，其中包括责任承担原则，目的识别原则，同意原则，有限收集原则，有限使用、披露、存储原则，准确原则、安全保障原则、公开原则、个人访问原则以及合规性质疑原则。其他各省立法与此类似。

2.1.5 数据处理的合法依据 – PIPEDA 附表 1

机构只有在具有合理目的，且数据主体知情、同意的情况下才能收集、使用或披露个人信息。个

9 加拿大反垃圾邮件法（SC 2010 c 23，CASL）。除其他方面以外，CASl 规定了来自以及发往加拿大的商业电子信息（比如推销和市场营销信息），不论接收方是个体还是组织机构。除此以外，在商业电子信息方面，CASL 是选择加入机制。除非取得明示或默示同意，或者满足适用的例外情况，CASL 禁止发送商业电子信息。违反 CASL 规定的将受到高额罚款及其他严重后果（包括对主管人员和职员的延伸责任）。

人信息收集应当在该企业实现收集目的所需的范围内开展，并以公平、合法的方式进行。根据场景、拟进行的收集、使用、披露和信息的敏感程度，同意可以是明示或默示的。例如，在收集符合个人利益并且不能及时获得同意的情况下，或者可以合理期待征得个人同意会损害信息的可获得性并且对于调查违反协议或违反加拿大联邦或省法律有关目的而言收集是合理的情况下，个人信息的收集不需要征得同意。此外，PIPEDA 允许组织在某些情况下即使未获得同意也可以向其他组织披露个人信息。

2.2 重要定义

a) 个人数据 - 个人信息是指与一个可识别主体相关的信息。当有很大可能性个体能够通过个人信息的使用而被单独和与其他可用信息结合而识别到时，该信息一般被认为事“个人信息”。

敏感数据 - PIPEDA 或者省级关于数据保护的法律并没有规定“敏感数据”的定义。PIPEDA 指出，所有数据根据其内容情景都可被认为是敏感数据。

b) 数据控制者和数据处理者 - 加拿大隐私法没有定义数据控制者和处理者的概念，但是其使用的“机构”这一概念中包括了数据控制者和数据处理者。

2.3 数据主体权利

• 访问权 – PIPEDA 附表 1 第 4.9 条

如收到要求，机构应告知数据主体关于其个人信息的存在、使用和披露情况，并应允许其访问该信息。个人应有渠道对信息的准确性和完整性提出质疑，并适当修改该信息。

• 修改权 — PIPEDA 附表 1 第 4.9.5 条

当数据主体成功证明其个人信息不准确或不完整时，机构应当按其要求修改信息。根据受质疑信息的性质，修改方式包括更正、删除或增加信息。在适当情形下，应当将修改后的信息传输至对该信息有访问权的第三方。

• 投诉权 — PIPEDA 附表 1 第 4.10 条

数据主体应能够向一个或多个指定的机构合规负责人提出有关机构违反上述原则的质疑。

• 撤回同意权 — PIPEDA 附表 1 第 4.3.8 条

在遵守法律、合同限制并尽到合理通知的情况下，数据主体可以在任何时候撤回同意。机构应当告知数据主体撤回同意的含义。

2.4 隐私声明

PIPEDA 附表 1 第 4.8 条要求机构在个人信息管理方面公开其政策和实践情况，公开信息应当包括：隐私政策和投诉 / 问询渠道负责人的姓名、职称和地址，数据主体访问机构所持个人信息的渠道，机构收集个人信息的类型描述，以及该机构关联公司可获得的个人信息情况。

2.5 直接营销

加拿大反垃圾邮件法禁止未经明示或暗示同意，向个人发送、委托发送或允许发送非应邀的电子信息（包括文本、音频、语音或图片信息）。此外，上述非应邀信息中必须标识发件人、发件人联系方式，以及退订机制。

根据加拿大国家“禁止通话”清单及规则，除非获得消费者明示同意，电话营销员不得，且其客户应采取一切合理手段避免向登记在加拿大国家“禁止通话”清单上的号码进行电话营销。

加拿大没有设立针对邮件营销的特殊规则，但加拿大隐私法的一般要求适用。

2.6 数据共享与处理

根据加拿大隐私法，机构对其持有或保留的个人信息负责，包括已经转移至第三方进行处理的数据。在第三方处理数据时，机构应当通过合同或其他方式提供程度相当的保护。

根据 PIPEDA 规定，针对特定事项，加拿大隐私事务专员有权对各省间及跨境数据共享和披露做出安排。

2.7 儿童隐私保护

OPC 主张机构应当避免对儿童及目标儿童的网站进行追踪。OPC 建议，除例外情况外，收集、使用和披露低于 13 岁的儿童的个人信息，应当取得其父母或监护人的同意。13 岁以上但未达法定成年年龄的青少年可以做出有效力的同意，但要将其成熟程度纳入考虑范围内。

2.8 可问责性

a) 通过设计的数据保护和默认的数据保护

加拿大未针对隐私设计和隐私默认设置设立明确的条文规定，但 OPC 曾发布关于默认隐私设置的检验报告；此外，加拿大隐私法规定的一般原则，比如公开原则，与 GDPR 规定的隐私设计和默认原则相一致。

b) 数据保护影响评估

机构并不要求必须进行数据保护影响评估。加拿大财政委员会秘书处要求政府机构对涉及到个人信息产生、收集和处理的新设立或显著变更的项目或活动进行隐私影响评估。

c) 数据处理活动记录

无相关要求。

d) 数据保护官（DPO）

机构应当指派专人负责机构履行数据保护合规义务，加拿大通常将负责人称为“首席隐私官”或“隐私官”。

e）政策和程序

组织机构应当施行保护个人信息、接收和回复投诉及问询、以及培训员工的政策和程序。

2.9 安全和数据泄露通知

根据加拿大隐私法，安全保障措施应当保护个人信息，防止丢失、被盗、未经授权访问、披露、复制、使用或修改。无论个人信息以何种形式呈现，机构均应当予以保护。根据所收集信息的敏感程度、数量、分布、形式以及存储方式不同，机构应采取不同的保护措施。敏感程度更高的个人信息应当受到更高层次的保护。

对于阿尔伯塔来说，如果有合理理由认为机构所控制的个人信息发生了会对数据主体造成真实、显著危害的数据泄露事件，机构应当向 OPC 报告所有上述数据安全事件。除非法律有禁止性规定，机构应当通知将数据泄露事件告知受影响的数据主体，该通知内应包含特定信息。

根据 PIPEDA，如果能够合理认为违反安全保护措施会给个人带来造成重大伤害的真实风险，那么就必须向个人、OPC 进行通知。如果任何其他组织（例如其他组织、政府机构或政府机构的某一部门）能够降低可能因此遭受损害的风险或减轻损害，那么也应该向该其他组织进行通知。组织应当尽快进行通知。

在省一级，与健康信息有关的数据泄露也需要向个人通知或向该特定行业的相关监管进行报告。

2.10 跨境数据传输

一般来讲，加拿大允许将个人信息传输至境外的第三方数据处理者，但要求传输机构通过合同或其他方式确保境外第三方处理数据达到与加拿大水平相当的数据保护程度。

阿尔伯塔的规定更为具体，即如果机构使用加拿大境外的服务供应商收集、使用、披露或存储个人信息，那么该机构必须在其隐私政策和实践中明确说明上述数据活动的所在地，以及授权服务供应商代表机构进行上述数据活动的目的。

2.11 执法

OPC 作为监察机关，尚无权做出有拘束力的命令或罚款，但各省的隐私专员享有上述权力。如果个人违反 PIPEDA 下的数据泄露通知条款，如经由简易程序定罪，会受到不超过 $10,000 加拿大元的罚款；如经公诉程序定罪，会受到不超过 $100,000 加拿大元的罚款。

三、亚太

1. 日本

1.1 概述

1.1.1 法律体系

日本在隐私领域的主要立法为《个人信息保护法》。该法首次颁布于 2003 年，后分别于 2015 年 12 月和 2020 年 6 月修订 [10]。个人信息保护委员会（PPC）还就《个人信息保护法》的实施发布了大量指南。在特定领域（例如金融、医疗、劳动等领域），PPC 联合其他省厅共同颁布或由其他省厅单独颁布了一系列法规和指南。

1.1.2 监管机构

个人信息保护委员会（PPC）负责监督《个人信息保护法》的实施与执法情况。

1.1.3 实体和地域范围

《个人信息保护法》适用于日本所有处理个人信息的经营者，例如为经营目的提供个人信息数据库等。处理个人信息的经营者不包括中央政府、地方政府和其他行政机关。

《个人信息保护法》具有域外效力。根据《个人信息保护法》第 75 条，如果境外实体向日本公民提供商品或服务，尽管其在日本境外处理个人信息，但依然需要适用《个人信息保护法》中与处理个人信息的经营者相关的大多数条款。

此外，如果处理个人信息的目的属于《个人信息保护法》第 76 条规定的范围，那么《个人信息保护法》第 4 章中提到的关于处理个人信息的经营者的义务则并不适用于这些特殊类别的个人信息经营者。例如，广播机构、报纸出版商或其他新闻组织以供新闻报道之用而使用个人信息。

1.1.4 数据处理原则

《个人信息保护法》第 15 条（明确使用目的）、第 16 条（通过利用目的加以限制）及第 18 条（获取时对利用目的的通知等）的规定要求体现了个人信息处理目的的限制原则（即只能为特定目的而处理个人信息）。

1.1.5 数据处理的合法依据

根据《个人信息保护法》第 17 条（正当的获取），处理个人信息的经营者不得以欺骗或者其他不正当手段获取个人信息。

10 请注意本报告仅只包括《个人信息保护法》2020 年修改中今年 12 月实施的部分，并不包括 2020 年修改中 2022 年春季拟定实施的部分。

处理个人信息的经营者未经信息主体（指通过个人信息被识别的特定个人，下同）的事先同意，不得获取需要特别注意的个人信息，但有下列情形之一的除外：

（i）基于法律法规的；

（ii）保护人的生命、身体或者财产所需，但难以取得信息主体的同意的；

（iii）为加强公共卫生或促进儿童健康确有特殊需要，但难以取得信息主体同意的；

（iv）对国家机关、地方公共团体或受其委托者执行法令规定的事务需要提供协助，但有可能因取得信息主体的同意而对执行该事务造成障碍的；

（v）需要特别注意的个人信息被信息主体、国家机关、地方公共团体、《个人信息保护法》第 76 条第 1 款各项规定的主体及《个人信息保护委员会规则》规定的其他主体公开的；

（vi）内阁命令所规定的与前述每一项情况相似的其他情况。

1.2 重要定义

个人信息是指与在世个人相关并且可以识别特定个人（包括易于与其他信息进行结合从而识别特定的个人的信息）或包含个人识别码的信息。

个人识别码是指 a）已将特定个体的身体局部特征转换为供计算机使用的任何字符、字母、数字、符号或其他代码；或 b） 在向个人提供服务或商品时分配给个人的字符、字母、数字、符号或其他代码，或记录在发放给个人的卡片或其他文件上用来识别特定用户身份的字符、字母、数字、符号或其他代码。

需要特别注意的个人信息是指包括信息主体的种族、宗教、社会地位、病史、犯罪记录、因犯罪而遭受损害的事实，及内阁令规定的为避免信息主体带来不公平歧视、损害或其他不利影响而在处理时需要特别注意的个人信息。

数据控制者和数据处理者：《个人信息保护法》没有直接对数据控制者或数据处理者的概念做出规定，仅规定了处理个人信息的经营者的相关要求。关于处理个人信息的经营者定义请参见上文第 1.1.3 节实体和地域范围。

1.3 数据主体的权利

根据《个人信息保护法》第 27 条和第 28 条，信息主体可以要求处理个人信息的经营者向其告知使用目的，并且可要求处理个人信息的经营者披露其持有的个人信息中可以识别到该信息主体的个人信息。根据《个人信息保护法》第 29 条，如个人信息不正确，则信息主体可以要求处理个人信息的经营者更正、添加或删除其个人信息。根据《个人信息保护法》第 30 条第 1 款，如果个人信息的处理违反该法第 16 条或第 17 条，那么信息主体可以要求处理个人信息的经营者停止

使用或对其信息进行删除。第 30 条第 3 款也指出，若能够识别本人的持有的个人数据被处理个人信息的经营者违反第 23 条第一款或第 24 条的规定提供给了第三人的，则该个人信息主体可以请求个人信息处理业者停止将该持有的个人数据提供给第三人。

根据《个人信息保护法》第 31 条，当上述权利被处理个人信息的经营者拒绝时，其应当尽力向信息主体解释原因。

PPC 可依据《个人信息保护法》第 61 条，处理信息主体所提出投诉相关的必要调解事宜。

1.4 隐私声明

根据《个人信息保护法》第 27 条，隐私政策应当包括：

（i）处理个人信息的经营者的姓名或名称和地址，以及处理个人信息的经营者的代表人姓名（适用于公司实体）；

（ii） 所有个人数据的使用目的；

（iii） 向处理个人信息的经营者请求访问其所保存的个人信息的流程（包括应付的任何费用金额）；

（iv） 除前三项规定的内容外，内阁命令所规定的为确保适当处理个人信息的必要内容。

1.5 直接营销

直接营销受其他法律（例如《特定电子邮件传输管理法》和《特定商业交易法》）的管辖。

1.6 数据共享与处理

根据《个人信息保护法》第 23 条第（1）款，处理个人信息的经营者不得在未事先征得信息主体同意的情况下提供个人数据，但以下情况除外：

（i）基于法律法规的；

（ii）保护人的生命、身体或者财产所需，但难以取得信息主体的同意的；

（iii）为加强公共卫生或促进儿童健康确有特殊需要，但难以取得信息主体同意的；

（iv）对国家机关、地方公共团体或受其委托者执行法令规定的事务需要提供协助，但有可能因取得信息主体的同意而对执行该事务造成障碍的。

《个人信息保护法》下没有“处理者”的概念。尽管如此，根据第 23 条第（5）款，如果处理（a）个人信息的运营者将其获取的全部或部分个人数据委托给某一实体进行处理，（b）因合并或其他

事由而发生业务的承受，而导致该个人数据被提供给他人，或者（c）在将可与特定他人共同利用的个人数据提供给该特定他人时，已经事先将可共同利用这一事实和可共同利用的个人数据中的项目、共同利用的他人的范围、对利用主体的利用目的及该个人数据的管理负责的主体的姓名或名称通知给本人、或者置于本人容易知悉的状态，则该实体将不被视为第 23 条第（1）款的第三方并且该条规定的义务将不被适用。

1.7 儿童隐私保护

没有针对处理儿童个人信息的特殊规定。但是，请注意《个人信息保护法》第 17 条仍然适用于儿童个人信息的处理活动，不合规的手段可能会被认定为第 17 条下的“不正当手段”。因此，在实务中在获取儿童个人信息时，最好征得法定监护人的同意。

1.8 可问责性

a) 通过设计的数据保护和默认的数据保护

《个人信息保护法》未提及此概念。

b) 数据保护影响评估（DPIA）

《个人信息保护法》没有明确提及需要做数据保护影响评估，但根据《个人信息保护法》第 20 条，处理个人信息的经营者应当采取必需和恰当的措施确保信息安全。

c) 数据处理活动记录

《个人信息保护法》没有明确提及记录处理活动的义务。但是，根据第 40 条，PPC 可以对文件、记录和其他财产进行检查。此外，第 25 条和第 26 条要求处理个人信息的经营者在向第三方提供个人数据和从第三方接收个人信息时进行记录。

d) 数据保护官（DPO）

无相关要求，但根据 PPC 发布的指南，建议任命 DPO 是被建议采取的一种安全措施。

1.9 数据安全和数据泄露通知

根据个人信息保护委员会发布的《关于个人数据泄漏等事情发生时的应对》[11]，如发生了数据泄露，并且根据 PPC 发布的规则，有可能会损害个人权益，那么处理个人信息的经营者应当向 PPC 进行报告，并且联系涉及到的信息主体。

1.10 跨境数据传输

11 https://www.ppc.go.jp/files/pdf/iinkaikokuzi01.pdf.

根据《个人信息保护法》第 24 条，如果处理个人信息的经营者向境外第三方提供个人信息，则应事先获得信息主体的同意，除非：

（1）第三方根据 PPC 发布的标准建立了必要的制度，能够采取与《个人信息保护法》同等的措施；或者

（2）根据 PPC 规定，该境外国家被认定为与日本具有相同标准的个人信息保护国。

1.11 执法

违反《个人信息保护法》最高可能被处 100 万日元的罚款，或两年以下有期徒刑。

2. 香港

2.1《个人数据（私隐）保护条例》概况

2.1.1 法律体系

《个人数据（私隐）保护条例》（第 486 章）（以下简称“PDPO”）对数据使用者使用个人数据的行为进行了规定。PDPO 规定了六条数据保护原则（DPPs）（详见下述第 2.1.4 条）以及其他对数据使用者的数据保护要求（例如直接营销方面的要求，详见下文第 2.5 条）。

个人资料私隐专员（以下简称“专员”）负责执行 PDPO 的规定。专员也认可虽 PDPO 未进行法律要求但自发的行为守则，可是不遵守该守则同样可能会导致专员采取调查，并在诉讼中做出对数据使用者不利的推定。

2.1.2 监管机构

香港个人资料私隐专员（PCPD）。

2.1.3 实体和地域范围

实体范围 - PDPO 适用于在香港对个人数据的收集、保留、处理以及使用。“数据处理”的定义包含了以自动化方法或其他方法对数据进行修订、扩增、删去或重新排列。而“使用”的定义则包含了对于个人数据的披露或者个人信息的传输。对于“个人数据”的定义详见第 2.2 部分 a 条。

地域范围 - PDPO 适用于在香港境内发生的或由位于香港的数据使用者控制的收集、持有、处理或使用个人数据的活动（对于“数据使用者”的定义详见第 2.2 部分 b 条）。PDPO 不具有域外效力。

2.1.4 数据保护原则

原则 1：收集个人数据的目的与方式

个人数据应当是为了直接与将会使用该数据的数据使用者的职能或活动有关的合法目的而收集。就该目的而言，数据应属足够但不超乎限度。数据使用者应当向数据主体知会特定的信息（详见下文 2.4 项）。

原则 2：个人数据的准确性以及保留期间

数据使用者应当确保个人数据的准确性，保留个人数据不得超过必要的时间。同时，应采取合同制约的方式要求参与处理的数据处理者遵守此项原则。

原则 3：个人数据的使用

除非已经获得数据主体的明确同意，数据使用者不能为了新目的而使用个人数据。

原则 4：个人数据的安全

为防止个人数据遭受未经授权或意外的访问、处理、删除，在特别考虑一些特定因素的情况下，数据使用者必须采取切实可行的措施保护个人数据。同时，应采取合同制约的方式要求参与处理的数据处理者遵守此项原则。

原则 5：信息须在一般情况下可提供

数据使用者须公开特定的信息，例如其有关个人数据的政策以及实务。

原则 6：对个人数据的访问

数据主体必须享有访问其个人数据的权利，以及更正其个人数据的权利。

2.1.5 数据处理的合法依据

PDPO 没有就个人数据的处理规定具体的“合法依据”。根据 PDPO 的规定，一般而言，使用个人数据不需要得到数据主体的同意，但前提是数据使用者遵守法律规定，告知数据主体相应的指定信息（详见第 2.4 部分）。一般来说，只有在个人数据被用于以下目的时，才需要获得数据主体的同意：(i) 直接营销 (ii) 新目的；和 (iii) 核对程序。也就是说，在需要数据主体同意的场景下，PDPO 也规定了特定的豁免情形（例如为了预防犯罪、为了统计以及科研、新闻以及卫生健康目的等）。

2.2 关键定义

a) 个人数据以及特殊类别个人数据

个人数据是指与在世的个人直接或间接相关、能从该数据直接或间接地确定个人的身份、且该数据的存在形式令予以查阅及处理是切实可行的任何数据。PDPO 下没有关于个人敏感数据的单独分类。

b) 使用者和处理者

数据使用者是指单独或连同其他人或与其他人共同控制数据的收集、持有、处理或使用的人。

数据处理者是指代他人处理个人数据、且不为本身的任何目的处理该数据的人。

2.3 数据主体的权利

PDPO 特别规定了两项数据主体的权利：

(a) 要求查阅数据的权利

数据主体有权要求查阅由数据使用者持有的属于数据主体的个人数据。

(b) 要求改正数据的权利

数据主体有权要求改正由数据使用者持有的属于数据主体的个人数据。

在收到上述两项要求的 40 天内，数据使用者必须遵循该要求进行相应处理，如无法做到，数据使用者则须回复该数据主体并说明原因（例如：需要更多时间）。

2.4 隐私政策

PDPO 下的原则 1 与原则 5 要求数据使用者向数据主体告知特定的信息，例如收集的个人数据类型、收集的目的、数据主体是否有义务提供该数据（如果有义务，需说明不提供的后果）、可能会收到数据的接受方类别、数据主体的数据访问权限以及更正权利以及相关联系人的具体信息。这些信息通常都涵盖在数据使用者向数据主体公开的隐私政策中。

2.5 直接营销

如果营销手段属于下列的情况，则该营销行为属于直接营销：

(a) 通过信函、传真、电子邮件或其他通讯方式，向指名特定人员发送信息或商品；或

(b) 致电特定人员。

在数据使用者将个人数据用于直接营销或将个人数据提供给他人用于其直接营销前，必须取得数据主体的明确同意。数据使用者同时必须告知数据主体相应的特定信息（例如何种个人数据会被用于直接营销、被营销的是何种商品或服务等）。

2.6 数据共享与处理

原则 1 要求数据使用者将可能的个人数据接收方类别告知数据主体。该接收方的类别应该清晰明确，以便一定合理程度上能够确定该接收者的情况。

在所有数据处理者参与的数据共享与处理的情况下，原则 2 与原则 4 要求数据使用者通过合同的方式去约束该数据处理者遵守 PDPO 规定的数据存储与安全要求。目前，PDPO 对于数据处理者与数据使用者间的协议并没有固定的模板或格式条款。

2.7 儿童隐私保护

关于未成年人的个人数据收集同样受到 PDPO 的总体规定的约束。需要特别注意的是，在涉及未

成年人的情况下，个人信息的收集必须是公平的、必要的且不超过合理限度。

当根据 PDPO 的规定需要征得同意的时候（例如为了一个新目的使用个人数据的时候），相关人员（即对未成年人负有监护义务的人）应能够代未成年人同意。但是，除非数据使用者有合理理由相信为了新目的使用个人数据对该未成年人明显有利的，否则数据使用者不能为了该新目的使用个人数据（即使相关人员已同意）。

PDPO 还规定免除香港警察或香港海关须经同意才能向与未成年人相关的个体披露该未成年人的个人数据的情形。

2.8 可问责性

a) 通过设计的数据保护和默认的数据保护

PDPO 并未对通过设计的数据保护和默认的数据保护提出法律要求。但是，这是由香港个人资料私隐专员建议的实践做法，特别是在推出新的信息技术以及通讯技术的时候。

b) 数据保护影响评估（DPIA）

在法律层面上，PDPO 并未要求实施数据保护影响评估。但是，个人资料私隐专员曾发表过关于隐私影响评估的资料册，并建议在特定情况下实施隐私影响评估（例如在处理大量个人数据，或采取危及隐私的技术时）。

c) 数据处理活动记录

无特殊规定。

d) 数据保护官（DPO）

无特殊规定。

2.9 安全和数据泄露通知

尽管个人资料私隐专员已建立了一个自愿性的线上数据泄露通知平台，并建议数据使用者在遇到此类情况将其作为适当的处理手段，但 PDPO 目前并未对数据安全和数据泄露通知做出任何要求。个人资料私隐专员也发布了不具有约束力的《资料外洩事故的处理及通报指引》。

2.10 跨境数据传输

PDPO 有关跨境个人数据传输的明确条款暂未生效。尽管如此，由于 PDPO 中“使用”一词的定义已包含“传输”，跨境数据传输仍受到 PDPO 中有关个人数据的一般规定的约束。

2.11 执法

个人资料私隐专员在处理当事人间有关个人数据的争端时，通常会采取和解的策略。对于情节严重的案件，个人资料隐私专员会进行调查，而后根据 PDPO 签发警告或执法通知。违反数据保护原则本身不构成刑事犯罪，但违反专员签发的执法通知则构成刑事犯罪，最高可罚款 50000 港币（大约 6400 美元）并处以 2 年监禁（首次犯罪）。除此之外，违反 PDPO 规定的直接营销规则也会构成刑事犯罪，最高可罚款 100 万港币（大约 128000 美元）并处以 5 年监禁。对于公开未经数据使用者同意而披露个人数据的罪行，最高可罚款 100 万港币（大约 128000 美元）并处以 5 年监禁。

3. 新加坡

3.1 概述

3.1.1 法律体系

新加坡适用的主要数据保护法律为《2012 年个人数据保护法案》（以下简称为“PDPA”）。除 PDPA 外，新加坡的数据保护规定还包括多个由新加坡数据保护委员会（以下简称为“PDPC”）所发布的综合或适用于特定领域的指导性文件。尽管这些指导性文件没有法律上的强制效力，但它们表明了 PDPC 会对 PDPA 进行解释并制定能适用于新加坡的个人数据处理的最佳处理方案。

3.1.2 监管机构

新加坡数据保护委员会负责执行《2012 年个人数据保护法案》的相关规定。

3.1.3 实体地域范围

a）实体范围

总的来说，PDPA 适用于对个人数据的处理（关于“个人数据”的定义，详见下文第 3.2.1 条），但不适用于以下情况：

- 以个人身份或家庭成员身份处理个人数据的自然人；
- 处理个人数据的是某个组织的职员，且该数据处理的行为发生于其履行其职务期间（需注意的是，这一情况下该组织仍应当遵守 PDPA 的规定）；
- 收集、使用、披露个人数据的是政府机构，或代政府机构行使职权的其他组织；
- 对于由自然人自己以非个人目的提供的，涉及自然人姓名、职务名称、工作地址、工作电邮地址、工作传真号码以及其他类似的自然人信息的商业联络信息处理。

此外，PDPA 第 2 节至第 6 节黎明了履行 PDPA 数据保护义务的例外情形。例如，如果个人数据是为了进行调查或者诉讼所必需的或者个人数据已公开，组织可以未经容易收集个人数据。

b）地域范围

PDPA 适用于任何在新加坡境内进行个人数据收集、使用以及披露活动的组织，包括那些设立于新加坡之外的组织。但是在实践中，如果需要针对某一组织适用 PDPA，则需要证明该组织与新加坡存在联系（例如于新加坡建立，或在新加坡设有分支机构）。

3.1.4 数据处理原则

PDPA 共规定了 9 条数据处理原则。各组织需要在处理个人数据时遵守这些原则。

- **同意义务：**在收集、使用或披露个人数据之前，各组织需要取得数据主体个人的授权同意。
- **目的限制义务：**仅在为实现一般人在该情况下认为合理的目的时，组织才可以收集、使用或披露自然人的个人数据。在可行的情况下，该目的应当告知相应的个人。
- **告知义务：**相关组织应在收集、使用、披露个人数据时或事先告知相应数据主体收集、使用、披露其个人数据的目的。
- **访问权限与更正义务：**在接到相关个人的请求后，相关组织应当向其提供其个人数据被使用和被披露的有关信息，或对相应个人数据中的错误缺漏之处进行补正。
- **准确性义务：**相关组织应当采取适当措施以保证其收集的个人数据是完整且准确的。
- **保护义务：**相关组织必须在其处理或控制个人数据期间采取适当的安全措施对个人数据进行保护，以防止个人数据遭受未经授权的访问、收集、使用、披露、复制、更改、处置或其他类似的风险威胁。
- **存储限制义务：**如果对于数据的存储对于商业目的的实现已不再是必需时，或如果对于个人数据的存储对实现收集个人资料的目的不再有用，则相关组织必须停止存储这些个人数据，或移除个人数据与特定个人的关联。
- **传输限制义务：**组织必须保证其向新加坡境外传输的个人数据能够获得与 PDPA 规定之下相同标准的保护。
- **可问责义务：**组织应当采取适当的措施以及政策以确保其行为符合 PDPA 所规定的义务，并向社会公开有关其政策与实际操作的信息。

根据书面合同的约定、被认为是“数据中介”且代另一组织、为了实现另一组织的目的对个人数据进行处理的组织（关于“数据中介”的定义详见下文第 3.2.2 部分）只需要遵守 PDPA 规定的保护义务以及存储限制义务。

3.1.5 数据处理的合法依据

组织在以下任意一个情形中均可收集、使用或披露个人数据：

- 已经从数据主体处取得明确同意，并满足以下条件：(i) 已向数据主体告知收集、使用、披露个人数据的目的且 (ii) 不能要求该数据主体对数据收集、使用、披露给予超出为数据主体提供产品或服务的必要限度的同意。
- 数据主体已被视为同意个人数据的收集、使用以及披露。这种情形只有在数据主体自愿向组织

就特定目提供个人数据时才适用。在该情形下，数据主体自愿提供个人数据的行为应当是合理的。

• PDPA 附表 2 至附表 4 中所规定的授权同意的例外情形。

3.2 重要定义

3.2.1 个人数据和特殊类别个人数据

个人数据定义为“无论真实与否，（a）可从该数据中识别个人；或者（b）结合该数据以及其他组织有权或有权访问的信息可识别该个人身份的数据”。

PDPA 中没有对“敏感个人数据”进行定义或针对特殊类别的个人数据的特定规则。然而，根据 PDPC 所发布的指引建议，对于具有敏感性质的个人数据采取更高级别的保护为良好实践的一种。

3.2.2 数据控制者和数据处理者

在 PDPA 中与“控制者”定义相似的表述是“组织”，包括“不论是否是根据新加坡法律成立或被承认的、但居住于新加坡或在新加坡有经营场所的组织、公司、合伙、法人团体、非法人组织或个人”。

在 PDPA 中与“处理者”定义相似的表述是“数据中介”。“数据中介”是指任何代另一组织对个人数据进行处理，且非被代理组织的员工的组织。

3.3 数据主体权利

根据 PDPA 的规定，作为个人数据主体具有以下权利：

• 访问读取其个人数据的权利；

• 更正其个人数据的权利；

• 撤回对其数据进行收集、使用、披露的同意的权利。

任何组织应在收到数据主体相关访问或更正请求后尽快实现这一请求（一般是在 30 天内完成，但也有可能延长这一时长）。如出现属于 PDPA 附表 5 以及附表 6 中所规定的例外情形，则组织没有义务响应数据主体的请求。组织可就数据主体的访问和更正请求收取适当的费用。

通常而言，组织必须在 10 天内实现来自数据主体撤回其对于收集、使用或披露个人数据的同意的请求。但该时长也有可能被延长。

目前，PDPA 正被修改以加入新的“数据携带权”。该权利是指组织在收到数据主体的请求后，应当以常用的机器可读格式向数据主体提供组织持有或控制的其个人数据。

3.4 隐私声明

PDPA 要求组织采取以下措施：(a) 将个人数据收集、使用、披露的目的告知所有数据主体；(b) 在接到数据主体的请求后，向数据主体提供能够回应有关个人数据的收集、使用以及披露的问题的员工工作联络方式。

在实践中，上述两项措施都应在收集、使用或披露个人数据前或当时通过隐私声明（或隐私政策）告知。

3.5 直接营销

电话营销行为（包括通过短信与传真进行营销）受到 PDPA 中的“禁止呼叫”（以下简称为“DNC”）条款规制。除非获得订阅者明确且不模糊的同意，或存在业务关系的情况以及满足其他要求下，组织才可将营销信息发至 DNC 数据库中所登记的新加坡电话号码。

通过电子邮件进行的营销则受到《垃圾信息控制法案》的管制。如果邮件内容符合《垃圾信息控制法案》中的有关规定、满足标签要求并提供了退订按钮，则未经请求的营销邮件可被发送至上述数据库中登记的电邮地址。如果组织收到来自个人的退订请求，则必须在收到该请求后的 10 个工作日内停止向该个人发送营销电子邮件。

需要注意的是，PDPC 已宣布相关计划，准备将 PDPA 中的 DNC 条款与《垃圾信息控制法案》进行合并。

3.6 数据共享与处理

组织仍然需要对数据中介代其处理的数据负责，就像这些数据是由该组织自己处理的一样。为实现这一目的，大多数组织都会与其数据中介签订数据处理协议，并力图履行其主要的 PDPA 义务，以保证数据中介对数据的处理符合 PDPA 的规定。

3.7 儿童隐私保护

PDPC 发布的没有法律约束力的指南规定了有关处理儿童个人数据的额外要求。PDPC 通常认为 13 岁以上的未成年人具有相应的行为能力，能够自主做出相应的同意。尽管如此，组织在判定授权是否有效时，仍然应当保证它能够令未成年人充分理解授权行为本身的性质以及授权所带来的相应后果。

PDPC 的指引亦建议组织在收集、使用、或披露未成年人的个人数据时应当采取预防措施（该预防措施的用词应当是清晰且易于理解的）。组织还应当采取额外的行动，特别是在错误的个人数据可能对未成年人造成严重后果时，对个人数据的准确性进行验证。

3.8 可问责性

3.8.1 通过设计的数据保护和默认的数据保护

PDPA 中并未对数据保护设计与默认数据保护做出明确的规定，但 PDPC 认为组织最好在开始进行任何形式的数据处理前制定适当的政策以及程序规则。为实现这一倡议，PDPC 出版了《信息与通讯技术系统的数据保护设计指引》。该指引将默认的数据保护纳入作为其总体原则之一。

3.8.2 数据保护影响评估（DPIA）

PDPA 并未强制要求组织进行 DPIA。但是，当组织正在对新系统或流程进行设计，或针对系统和流程进行重大改进时，PDPC 建议其进行 DPIA，否则可能会导致时间成本与工作量的增加。理想状态下，主导这一操作的人员应当是 DPO 或者项目主管。

3.8.3 数据处理活动记录

新加坡没有法律或规定要求保留对处理活动的记录。

3.8.4 数据保护官（DPO）和代表

新加坡提出了任命一名专门的数据保护官的法律义务。DPO 的工作联系方式应当向社会公开。

PDPA 中没有规定“代表”的概念（即：一个设立于新加坡之外的组织需要任命一名驻于新加坡的联系人以处理有关数据保护的事宜）。

3.9 安全和数据泄露通知

尽管目前 PDPA 并未对数据泄露通知做出强制性的规定，PDPC 仍然建议组织应当在数据泄露符合以下情形时尽快通知 PDPC（“尽快”是指组织认定数据泄露属于应当通知的类别后的 72 小时内）：

- 该数据泄露范围较大（即该数据泄露范围涉及 500 人或更多人的个人数据）；或
- 该数据泄露可能对相关的个人产生重大的伤害或影响。在这一情况下，PDPC 亦建议组织应当尽快通知收到影响的相关个人。

（以上二者统一称为“自愿数据泄露通知要求”）

尽管自愿数据泄露通知要求并不具有法律上的强制约束力，但在实践中，一旦数据泄露达到了需要进行通知的规模，大多数组织都会尝试像遵守强制规定一样去遵守这一要求。这是因为组织担心如果外界认为它没有遵守这一要求，其声誉就很有可能受到冲击，且顾客也会因此产生负面评价。另外，PDPC 也表明，它将会在决定是否就数据泄露针对组织采取措施时，把“没有进行数据泄漏通知”纳入考虑范围内。

同时，请注意 PDPA 目前正在修订中，以加入数据泄漏通知相关的强制性规定。在该机制下的通知的标准以及时间要求估计会与目前的自愿数据泄露通知要求相同。

3.10 跨境数据传输

PDPA 允许数据的跨境传输，但组织需要保证数据接收者的数据保护标准与 PDPA 的要求相当。这一相当性标准可根据以下的方式来实现：

- 组织与数据接收者签订数据处理协议，以要求接收者为个人数据提供与 PDPA 规定相当的数据保护标准；
- 证明个人数据将被转移到的国家 / 地区的适用法律提供了与 PDPA 规定相对应的数据保护标准；
- 取得数据主体对于传输的同意，该同意应当满足特定的条件。

3.11 执法

不遵守数据保护义务可能会导致以下后果：

- 最高 100 万新加坡元的罚款；
- PDPC 责令停止收集、使用或披露个人数据；
- PDPC 责令删除个人数据，和 / 或；
- PDPC 责令允许其或拒绝其对个人数据的访问或更改。
- PDPA 目前正在修订中，新规定将罚款的最高额提升至组织年度总营业额的 10%，或 100 万新加坡币（二者中取其高）。

除此之外，个人也有权向 PDPC 的主管部门进行投诉，以寻求有效的司法救济、获得禁止令或从组织处就该组织违反 PDPA 规定所造成的损失获得赔偿。

4. 马来西亚

4.1 概述

4.1.1 法律体系

马来西亚负责规制数据保护的主要法律是《2010 年个人数据保护法案》（以下简称为“PDPA”）。《2013 年数据保护规定》（以下简称为“PDP 规定”）对该法案进行了进一步补充。

4.1.2 监管机构

马来西亚的数据保护监管机构是“个人数据保护局”（以下简称为“JPJD”）。JPJD 隶属于马来西亚通讯及多媒体委员会。

4.1.3 实体地域范围

a）实体范围

PDPA 适用于对于个人数据的处理行为（“个人数据”的定义详见下文第 4.2.1 条），但不适用于由联邦或各州政府对于个人数据的处理。应当注意的是，JPJD 已提议对 PDPA 进行修改，使工作联系方式信息不再受到 PDPA 的管辖。

b）地域范围

PDPA 适用于符合以下情况的数据使用者：

- 数据使用者设立于马来西亚境内，且该个人数据是由该数据使用者、该数据使用者的员工或由与该数据使用者有关的人员进行处理的，无论该数据处理是否发生于该使用者设立地的范围内；
- 数据使用者并非设立于马来西亚境内，但使用马来西亚境内的设施对数据进行处理，本情况内的“处理”不包括以将数据中转通过马来西亚为目的的处理。

4.1.4 数据处理原则

PDPA 规定了 7 项相关组织在处理个人数据时需要遵守的数据处理原则：

- 总体原则：只有在数据主体同意，或可适用同意的例外的情况下，个人数据才能被处理；
- 通知和选择原则：数据使用者必须向数据主体书面告知；
- 披露原则：在数据主体不知情、没有获得数据主体同意的情况下，个人数据不能够被向第三方披露。

- 安全原则：数据使用者必须采取可行的措施，以避免个人数据遭受任何损失、滥用、修改，未经授权的或意外的访问、修改或灭失；

- 存储原则：为特定目的而处理的个人数据不得在实现该目的后仍被超时保留；

- 数据完整性原则：数据使用者须采取合理措施，以保证个人数据是准确完整的、不具有误导性且处在最新的状态；

- 访问原则：数据主体须被赋予访问数据使用者持有的其个人数据的权利，并能够更正不准确、不完整、具有误导性的、过时的个人数据。

4.1.5 数据处理的合法依据

只有在满足以下条件的情况下，个人数据才能被处理：数据主体给予了同意、数据是为了与数据使用者的活动有直接联系的合法目的而被处理的、数据的处理对于实现该目的是必要的且数据以一种适当且不过分的方式被处理。但是，在特定的情况下，个人数据的处理不需要来自数据主体的授权同意，包括：

- 为了履行与数据主体的合同，或与数据主体签订合同是必要的；

- 为了履行法律义务；

- 为了司法行政；

- 为了维护数据主体的重大利益；

- 为行使成文法赋予或规定的任何人享有的职能。

对于个人敏感数据只有在得到数据主体的明确同意，或在数据处理为了实现以下目的所必需的情况下才可被处理：

- 为了履行与劳动就业相关的权利或义务；

- 为了维护第三者的切身利益，且授权同意已经以合理的方式被取得（或已由数据主体提供授权同意）；

- 由专业医疗人员或具有保密义务的人员进行的医疗行为；

- 获取法律建议、行使法律权利、或为了诉讼程序需要；

- 为行使成文法赋予任何人的职能，以及其他通讯与多媒体部部长认为合适的目的。

4.2 重点定义

4.2.1 个人数据与特殊种类的个人数据

个人数据被定义为“任何在商业交易过程中（a）全部或部分被自动化处理用于该等目的；（b）被记录且记录的目的在于其被全部或部分地被该等设备所处理；或（c）该信息被记录作为档案系统的一部分，或记录的目的在于组成相关档案系统的一部分”。在以上的每一种情况中，个人数据都可以直接或间接地与一个数据主体相关，这一数据主体的身份可以从上述信息或数据使用者持有的信息中被确认。个人数据包含了所有个人敏感数据以及数据主体所表达的观点，但不包含根据《2010 年信用报告机构法案》由信用报告机构处理的有关信用报告的信息。

个人敏感数据是指“包含任何物理、精神健康或状况、政治见解、宗教信仰或其他本质上类似的信仰、由其实施或指控的任何犯罪行为或由部长根据公报公布的命令确定的任何其他个人数据”。

4.2.2 数据控制者与数据处理者

PDPA 中与“数据控制者”相似的概念是“数据使用者”。“数据使用者”是指单独或与他人共同处理数据、控制数据、授权他人处理个人数据的人，但以上定义范围不包括数据处理者。

数据处理者的定义为任何单独代表数据使用者处理个人数据，且非为处理者个人目的对个人数据进行处理的人；但该数据处理者不是数据使用者雇用的员工。

4.3 数据主体权利

根据 PDPA 的规定，数据主体有以下权利：

- 访问其个人数据的权利；
- 更正其个人数据的权利；
- 阻止其个人数据被用于直接营销的权利；
- 撤回对于收集、使用、披露其个人数据的同意的权利。

组织应当在接到访问或更正数据请求后的 21 日内实现该请求，尽管该期间有可能被延长。如果符合访问与更正义务的例外情形（例如，数据使用者并未被提供其需要的，用于查明与访问请求有关的个人数据的信息，或用于确定与更正请求相关的数据不准确、不完整、具有误导性或未更新），相关组织则没有必要响应访问数据或数据更正的请求。相关组织可以就处理访问数据或数据更正的申请收取适当的费用；最高费用的上线由 PDPA 下的附属规例进行了规定。

需要注意的是，JPJD 已提议对 PDPA 进行修改，以引入新的权利：数据携带权。在该项权利之下，作为数据主体的个人有权以一种结构性的、可机读的格式访问其个人数据文件，这种格式的个人

数据文件可以在不同的数据使用者之间传输，以便数据主体获取不同使用者的服务。

4.4 隐私声明

根据通知和选择原则，数据使用者必须向数据主体告知以下事项：

• 将会被数据使用者处理的个人数据的介绍以及数据来源；

• 处理个人数据的目的以及数据主体的权利；

• 可能作为数据披露对象的第三方的主体类型；

• 限制数据处理的选项与方式；

• 数据主体或数据处理者提供数据的行为是强制的还是自愿的；

• 未提供数据的后果。

该告知必须尽可能快地以英语及马来西亚语两种语言通知到数据主体。

4.5 直接营销

数据主体有权阻止其个人数据被用作直接营销。数据主体可以通过向数据使用者提交书面申请选择停止对其个人数据的处理或完全不开始对个人数据的处理。需要注意的是，JPJD 目前正在对适用于直接营销的法律进行审阅，相关建议包括设置一个“禁止呼叫”（DNC）数据库，并要求数据使用者实施相应措施，允许数据主体取消订阅线上服务。

4.6 数据共享与处理

在数据主体不知情且没有授权同意的情况下，个人数据不能被披露给第三方。但在以下情况下，个人数据可以在没有得到数据主体的授权同意的情况下被披露：

• 数据的披露对于预防或发现犯罪、进行调查是必需的；或数据是由法律要求或法院命令授权披露的。

• 数据处理者有合理的理由相信根据相关法律的规定，其有权对其他人披露个人数据。

• 数据处理者有合理的理由相信，如果数据主体了解披露个人数据的行为以及该披露行为的背景情况，数据主体会同意披露。

• 在由通信与多媒体部部长决定的情况下，数据的披露被认为是符合社会公共利益的。

但当数据处理的工作是由数据处理者进行时，数据使用者必须保证数据处理者已充分承诺会就数

据的处理提供相应的技术安全措施以及组织安全措施，并采取行动以确保其可以遵守这些措施。

4.7 儿童隐私保护

PDP 规定对于年龄在 18 岁以下的数据主体而言，相应的同意需要由父母、监护人或其他对数据主体有抚养监护职责的人做出。除此之外，法律上没有其他对儿童个人数据处理的特殊规定。

4.8 可问责性

a) 通过设计的数据保护和默认的数据保护

PDPA 中并未对数据保护设计以及默认数据保护做出明确的规定。但根据安全原则，数据使用者须采取切实可行的措施对个人数据进行保护，以免个人数据遭受任何形式的损失、滥用、修改以及未经授权或意外的访问、披露、篡改或灭失。当处理工作是由专门的数据处理者开展时，数据使用者必须确保该数据处理者在与数据处理相关的技术安全与组织安全措施方面提供充足的保障，并采取合理措施来遵守这些安全措施要求。

需要注意的是，JPJD 已经宣布发布关于数据使用者实施通过设计的数据保护的指引。

马来西亚并没有对实行数据保护影响评估做出法律上的要求。

c) 数据处理活动记录

数据使用者须对任何有关于正在处理、已经处理的个人数据的应用、告知、请求或其他方面的信息进行记录，并保留该记录。

d) 数据保护官（DPO）和代表

马来西亚法律并没有要求数据使用者任命数据保护官，但 JPJD 已宣布相应计划以修订 PDPA 以赋予数据使用者任命数据保护官的强制义务。

当数据使用者并非设立于马来西亚境内，但使用马来西亚境内的硬件设备处理个人数据时（仅将马来西亚作为数据中转站的处理行为除外），数据使用者需要任命一名位于马来西亚境内的代表。

4.9 安全和数据泄露通知

目前，马来西亚法律没有针对数据泄漏通知的强制要求。尽管如此，JPJD 已经宣布计划对 PDPA 进行修订，以加入针对数据泄漏通知的强制要求。

4.10 跨境数据传输

在以下情况中，数据使用者可以将个人数据传输至马来西亚境外：

- 境外地点位于通信与多媒体部部长的白名单中，并在公报中公布（但需要注意的是，截至目前为止未有公报公布的该等地点）；

- 数据主体已授权同意进行传输；

- 数据传输对于履行数据使用者和数据主体间所订立的合同是必需的；

- 数据传输对于履行数据使用者和第三方间的订立的合同是必需的，但该合同须满足以下条件：(i) 该合同是数据主体要求签订的，或 (ii) 该合同是为了实现数据主体的利益而签订的；

- 数据传输的目的在于协助法律诉讼的进行，取得法律意见，或建立、行使、保护法律权利；

- 数据使用者在一般情况下有合理的理由相信：(i) 该传输是为了避免或减轻对于数据主体的不利影响；(ii) 获取数据主体关于该传输的书面授权同意是不切实际的；(iii) 如果获取前述授权同意是可行的，数据主体在该情况下会进行该授权；

- 数据使用者已采取一切合理的措施并进行了尽调，以保证到达传输目的地的个人数据不会被以违反 PDPA 规定的方式被处理；

- 数据传输对于保护数据主体的切身利益而言是必须的；

- 在通信与多媒体部部长确定的情形下，出于公共利益考量，有必要进行数据传输的。

在实践中，马来西亚的大多数数据使用者都会将 “采取合理措施，进行尽调，保证数据不被违法处理”的情形作为向马来西亚之外的国家或地区传输个人数据的法律依据，并以此为基础与相应的数据接收者签订数据传输协议，确保数据不会被以违反 PDPA 规定的形式被处理。

4.11 执法

不遵守数据处理义务的行为可能会面临最高 50 万马来西亚令吉的罚款，和 / 或最高 3 年监禁。在违法行为发生时负责管理公司相应事务的人员也可能分别或与公司一同被起诉。

需要注意的是，JPJD 已宣布对 PDPA 的修订计划，以赋予数据主体就数据使用者违反 PDPA 向数据使用者提起民事诉讼的权利。

5. 泰国

5.1 概况

5.1.1 法律体系

在泰国主要规制数据保护的法律是《2019 年个人数据保护法案》（以下简称为“PDPA”）。需要注意的是，泰国政府已将 PDPA 中有关数据控制者和处理者的关键责任条款延迟至 2021 年 5 月 27 日生效。

5.1.2 监管机构

负责执行 PDPA 的监管机构是个人数据保护委员会（以下简称为“PDPC”）。

5.1.3 实体和地域范围

a) 实体范围

PDPA 适用于个人数据处理的相关情形（“个人数据”的定义详见下文第 5.2.1 条），但在以下方面不可适用：

- 数据收集者收集、使用或披露个人数据的目的在于个人利益或家庭活动；
- 具有维护国家安全职责的公共部门的相关行为，包括维护国家金融安全以及公共安全，例如与反洗钱、法医侦查科学以及网络安全等方面的责任义务；
- 在遵守职业道德或符合公共利益的情况下，自然人或法人仅以媒体活动、艺术或文学为目的使用或披露个人数据的行为；
- 众议院、参议院以及国会根据其职责与权力对于个人数据收集、使用或披露的行为；
- 在法律诉讼、法律执行以及财产保全程序中的法院审判及裁定以及相关官员的工作（包括按刑事诉讼程序进行的工作）的情况；
- 信用机构或其员工根据管理信用机构相关活动的法律对数据进行的处理。

b) 域外效力

PDPA 适用于在泰国境内有实体的数据控制者或处理者的处理活动。在下列情况中，PDPA 也适用于泰国境外的数据处理者或控制者对于数据的处理活动：

- 数据处理者或控制者向数据主体提供产品或服务，无论数据主体是否有为这些产品或服务付款；

或

• 监控位于泰国境内的数据主体的行为。

5.1.4 数据处理原则

PDPA 规定了八条相关组织需要在处理个人数据时遵守的数据处理原则：

• 个人数据的处理必须有合法依据。

• 个人数据收集的目的必须是具体、明确且合法的，且个人数据不得以与该目的不符的方式被处理。

• 对于处理的目的而言，个人数据必须是充分的、相关的，且应当被限制于与处理目的相关的范围内。

• 个人数据必须是准确的，且应当保持更新。

• 个人数据的存储时长不得超出必要的限度。

• 个人数据必须根据个人的权利进行处理。

• 个人数据的安全必须有保障。

• 个人数据不得被传输至无法提供充分的数据保护的第三国。

5.1.5 数据处理的合法依据

总的来说，除非数据主体给予授权同意，个人数据均不得被处理。然而，在以下情况下，个人数据可以在没有数据主体授权同意的情况下被处理：

• 处理的目的是准备历史记录文件或统计学研究；

• 处理的目的是保护个人的切身利益；

• 处理的目的是履行数据控制者与数据主体间必要的合同义务，或是响应签署合同前数据主体个人的要求；

• 为了履行数据控制者与公共利益有关的必要责任，数据处理是必须的；

• 处理是为了任何个人或法人（包括数据控制者自身）的合法权利；或

• 处理是为了履行数据控制者的法律责任。

- 只有在数据主体给予明确的授权同意的情况下，敏感个人数据才能被处理。在以下情况下，敏感个人数据也可以被处理：

- 在数据主体无法给予授权同意的情况下，为了预防或降低对于个人生命、身体健康的危险；

- 敏感个人数据的处理是在合法活动的过程中进行的，且有来自非营利组织的适当监督（例如具有政治、宗教或哲学上的目的的非营利组织）；

- 处理的数据与在获得数据主体的明确同意后向社会公开的信息相关；

- 数据处理对于法律请求而言是必须的；或

- 数据的处理符合法律的目的，其中包括公共卫生方面的公共利益，就业保护和某些研究目的。

5.2 重要定义

5.2.1 **个人数据与特别种类的个人数据**

个人数据的定义为：任何与某个个人相关的信息，且通过该信息可直接或间接识别改名个人的身份，但这不包括逝者的信息。

PDPA 没有使用“敏感个人数据”这一表述，但法律的确针对特别种类的敏感数据的处理提出了更高的要求。这些数据包括种族、政治观点、礼拜、宗教或哲学信仰、性行为、刑事犯罪记录、健康数据、残疾状况、工会成员信息、基因信息、生物特征数据、以及其他任何可能以相同方式影响数据主体的数据。PDPC 有可能在 PDPA 的附属法规中就此提供更加详细的指引。

5.2.2 **数据控制者和数据处理者**

数据控制者的定义为：有权力或义务做出有关个人数据收集、使用或披露的决定的自然人或法人。

数据处理者的定义为：根据数据控制者的指令，或代数据控制者进行个人数据的收集、使用或披露活动的自然人或法人，且该自然人或法人本身并非数据控制者。

PDPA 下的 “人”（person）被确定为“自然人”。

5.3 数据主体的权利

根据 PDPA 的规定，数据主体个人有以下权利：

- 访问个人数据的权利

- 要求数据控制者更正个人数据，以保证个人数据准确性、时效性、完整性以及不具有误导性的权利。

- 数据携带权，即数据主体有权以可读取、通常被自动工具使用的、可以自动方式被使用或披露的文件格式获得其个人数据文件；

- 反对个人数据收集、使用或披露的权利；

- 限制对其个人数据使用的权利。

在特定情况下，数据主体请求行使权利可能会遭到限制（例如，访问数据的权利或数据携带权不应破坏他人的权利或自由）。PDPC 有可能在 PDPA 的附属法规中提供有关数据主体权利的详细指引（包括回应数据主体请求适用的时间规定）。

5.4 隐私声明

在收集个人数据时或之前，必须告知或让相关数据主体知晓以下信息：

- 处理其个人数据的目的；

- 收集其个人数据是法律上的要求还是合同上的要求，或是合同成立的必要要求？同时数据主体应被告知其未成功提供这些数据所可能带来的后果；

- 数据控制者的身份以及详细联系方式。如适用，还应告知数据控制者的代表或数据保护官的身份以及详细联系方式；

- 数据主体的权利。

5.5 直接营销

根据 PDPA 的规定，数据主体可以反对将其个人数据处理后用于直接营销。法律中没有关于电话营销的一般规则，但是在保险或金融等行业中有某些特定的行业性法规。如果接收者可以用较为简单的方式取消对邮件的订阅，则直接的电邮营销可被允许。

5.6 数据共享与处理

当个人数据被提供给数据控制者之外的自然人和法人时，数据控制者必须采取行动以预防该自然人或法人非法披露个人数据。PDPC 有可能将在 PDPA 下的附属法规中就此提供进一步的指引。

5.7 儿童隐私保护

如果数据主体的年龄在 10 岁至 20 岁之间，除非与《泰国民法与商法典》第 22 至 24 条下所规定的未成年人可独立自行做出行为的情形相关，则均须同时从该数据主体及其合法监护人处取得同意。

如果该数据主体年龄低于 10 岁，则必须从数据主体的合法监护人处取得同意。

5.8 可问责性

a) 通过设计的数据保护和默认的数据保护

PDPA 中没有关于通过设计的数据保护和默认的数据保护的明确规定。

b) 数据保护影响评估（DPIA）

泰国没有进行数据保护影响评估的法律要求。尽管如此，数据控制者仍被要求在必要时或“技术改变”时对安全措施进行评审。PDPC 有可能在 PDPA 的附属法规中就此做出进一步指引。

c) 数据处理活动记录

除非根据 PDPC 的规定，数据控制者被认定为是“小型组织”，否则其需要对以下信息进行记录：

- 收集的个人数据；
- 各个种类的数据的收集目的；
- 数据控制者的详细信息；
- 个人数据的存储期限；
- 访问个人数据的权利与方法，包括用于评估某一名自然人是否有权访问个人数据以及访问个人数据的条件；
- 在没有得到数据主体的同意的情况下，对于个人数据的使用或披露行为；
- 何数据控制者拒绝数据主体请求的情况；以及
- 为保护个人数据所采取的安全措施。

数据处理者必须根据 PDPC 在 PDPA 的附属法规中最终确定的规则和方式记录所有处理活动。

d) 数据保护官（DPO）以及代表

在以下情况中，需要任命数据保护官：

- 如果数据控制者或数据处理者是 PDPC 规定且已经公布的公共机构；
- 数据控制者或处理者有关数据收集、使用或披露的活动需要大范围地对个人数据或系统进行监控；

- 数据控制者或处理者的主要活动在于对 PDPA 规定中的敏感种类个人信息进行收集、使用或披露。

- 数据控制者或处理者必须向数据主体以及 PDPC 提供 DPO 的详细信息、联络地址、联络方式。

位于泰国境外且受 PDPA 域外效力管辖的数据控制者则应书面指定一名代表。该代表应位于泰国境内且为数据控制者授权来代表其行事。该代表对于数据控制者对个人数据的收集、使用或披露不受到任何责任限制。

5.9 安全和数据泄漏通知

数据控制者须向 PDPC 毫无延迟地通知数据泄露事故。当可行时，该通知应当在数据控制者发现泄漏事故后的 72 小时内完成（除非该泄漏事故不太可能对个体的权利和自由造成威胁）。当数据泄露使数据主体个人的权利和自由处于高度风险时，也应当毫无延迟地通知数据主体关于该泄露事故以及相应的补救措施事宜。

当出现数据泄露时，数据处理者须通知相应的数据控制者。

5.10 跨境数据传输

除非数据接受国的数据保护标准与 PDPA 规定的标准持平或高于 PDPA 的标准，或数据传输符合下面的情况，个人数据均不可传输至泰国境外：

- 跨境传输是为了遵守法律规定；

- 数据主体已经知晓该传输并给予了同意；

- 跨境传输对于履行或签订数据主体为一方当事人的合同而言是必要的；

- 跨境传输是为了预防或减轻对于数据主体或其他个人的生命、身体健康的威胁；

- 跨境传输对于进行重大公共利益相关的活动而言是必要的。

如果其数据保护政策已由 PDPC 审核并获得认证，则同一关联企业或企业集团内的数据控制者 / 处理者之间的数据传输不受上述要求的约束。如果没有获得该认证，则必须实施适当的保护措施，以使数据主体的权利能够得到充分的实现，这包括了有效的法律救济措施以及 PDPC 所规定且公布的其他措施。

5.11 执法

违反 PDPA 的规定可能会导致最高达 500 万泰铢的罚款。在刑事层面上违反 PDPA 的规定可能会导致最高 100 万泰铢的罚款和 / 或最高 1 年的监禁。受到损害的数据主体可对数据控制者和处理者提起民事诉讼，且法院有权判决数据主体得到实际损失 2 倍的赔偿。

6. 印度

6.1 概述

6.1.1 法律体系

印度的法律体系有着混合性的特点，它有着民法、普通法、衡平法以及惯例法和宗教法。在过去，印度没有针对数据保护进行专门立法，在数据保护方面的主要法律条文为《2000 年信息技术法》（以下简称“《信息技术法》”）中的第 43A 和 72A 条，以及《2011 年信息技术（合理安全实践和程序以及个人敏感数据或信息）条例》（以下简称“《条例》”）。2019 年 12 月 11 日，印度政府在印度议会上颁布了《2019 年个人数据保护法案》（以下简称“《法案》”），该法案将是印度第一部专门针对数据保护的法律。

6.1.2 监管机构

尽管印度拥有诸多对各类活动进行监管或监督的管理机构，但印度并没有专门负责个人数据保护的国家级监管机构，仅由电子和信息技术部负责实施《信息技术法》，并颁布相关条例及解读。有鉴于此，《法案》建议成立印度数据保护局。

6.1.3 地域范围

《条例》不仅允许国内的数据传输行为，同时也允许国际间数据传输行为的发生，但前提是数据接收者应确保达到与印度所遵循的数据保护等级相同的保护程度、且此类数据传输对于履行数据收集者与数据主体之间的合法合同来说必要的，或者已经得到了数据主体的明确授权同意。针对非个人敏感数据或信息，印度并没有国内或跨境数据流的限制。类似地，除非双方已在合同中达成一致或披露行为是为遵循法定义务所必须的，向第三方披露个人敏感数据需要征得数据主体的预先授权同意。关于非敏感个人数据的披露，《条例》并不做限制。《信息技术法》（除《条例》规定的事项外）亦适用于任何人在印度境外使用位于印度的计算机、计算机系统或计算机网络所实施的任何违法犯罪行为。印度储备银行于 2018 年 4 月 6 日发布通知，规定所有银行，中介机构和其他第三方必须在印度境内存储所有与支付数据相关联的信息。《法案》提出了跨境转移个人数据的新制度，并针对个人敏感数据和个人关键数据提出了不同的规定。

6.1.4 数据处理原则

印度没有针对个人数据处理的特定原则。《条例》要求数据收集者或代表企业主体持有数据主体的信息的其他个人具备相应的隐私政策。但《条例》是根据《信息技术法》制定的，仅适用于电子记录，而《法案》则提出了更广泛的适用范围—不仅适用于电子记录，同时也适用于纸质记录。同时，《法案》规定数据收集者确保其隐私政策为数据主体可得，并在其网站上发布该政策。隐私政策中必须明确说明所收集的信息类型、信息使用的目的、信息披露的接收方和信息披露方式，以及其为了保障信息安全所遵循的合理信息安全实践和程序。隐私政策同时也应包含指定的申诉官的详细信息。《法案》同时提出了个人数据处理必须遵循的七大处理原则。

6.1.5 数据处理的合法依据

数据收集者仅可将个人敏感数据用于其收集时的目的，并且存储期限不得超过为合法使用该信息的目的所必须的时限，或其他法律所要求的期限。

6.2 重要定义

6.2.1 个人信息

个人信息仅对自然人的有关信息产生影响。个人数据被称为“个人信息”，在《条例》中被定义为“任何与自然人关联的信息，该信息可直接或间接地与其他企业主体已有的或有可能获得的信息结合从而能够识别该自然人”。

6.2.2 个人敏感数据信息

根据《条例》，个人敏感数据作为个人信息的一种类型，包括（a）密码，（b）金融信息（例如银行帐户或信用卡、借记卡及其他付款方式的详细信息），（c）身体、生理和心理健康状况，（d）性取向，（e）医疗记录和以往病史，（f）生物识别信息，（g）任何向提供服务的企业主体提供的与上述信息相关的信息，以及（h）任何企业主体接收的用于处理的与上述信息相关的信息，并且该信息是根据合法合同或其他方式存储或处理的。其中不包括可在公共领域公开可得或访问的信息，或根据《2005 年信息权法》或其他适用法律所提供的信息。《法案》提出了个人敏感数据的广义定义，包括财务数据，与种姓、部落、宗教和政治信仰或隶属关系的相关数据。

6.2.3 数据控制者与处理者

印度法律未包含数据控制者和处理者的概念，《条例》中提到的是企业主体和信息提供者的概念。企业主体是指“任何公司，包括从事商业或专业活动的公司，独资企业或其他个人协会”。信息提供者是指“向企业主体提供个人敏感数据或信息的自然人”。《法案》则提出了“数据受托人”和“数据处理者”的概念，与《通用数据保护条例》(GDPR) 中的概念相同。

6.3 数据主体权利

数据收集者应当采取合理步骤以确保数据主体知悉（a）收集信息的事实，（b）收集信息的目的，（c）信息的计划接收者，以及（d）收集信息的代理商及存储该信息的代理商的名称和地址。为了收集个人敏感数据，数据收集者应当事先征得数据主体的书面授权同意（数据主体可能会拒绝提供）。针对个人信息处理则仅需获得电子授权，无需其他特定的授权同意手续。个人敏感数据仅可出于与信息收集者整体活动相关的目的收集，且该收集是为成功进行该活动所必须的，并应征得信息提供者的书面授权同意。非个人敏感数据的个人信息则无需授权同意。数据主体可以要求审查他们所提供的信息，并要求修正不准确的或不足的信息。数据主体可以随时撤回授权同意。印度不承认“被遗忘权”，但印度法院在针对妇女的性犯罪方面承认了这项权利。《法案》中也提出了被遗忘权这一概念。

6.4 隐私政策和可问责性

数据收集者必须制定并提供隐私政策。该政策需保护（数据主体）所提供的信息，同时数据主体应当能够访问和查看该政策。该政策应当公开发布于企业主体的网站，并提供（a）有关其实践和政策的清晰易懂的声明，（b）收集的个人信息、个人敏感数据或信息的类型，（c）收集和使用此类信息的目的，（d）《条例》规定的允许披露此类信息的情况，以及（e）《条例》中所规定的合理安全实践和程序。即使未处理任何个人敏感数据或信息，也同样需要制定隐私政策。《法案》提出，数据受托人应采取多种措施以确保透明度和责任制，包括采用“隐私设计”以保证其在处理个人数据的通常实践过程中的透明度，采取适当的安全保障措施以及实施程序和机制以解决数据主体的诉求。申诉官应在有限的时间内解决数据主体提出的任何差异或不满。申诉官须在收到申诉之日起一个月内迅速进行纠正。企业主体应当在其官方网站上公布申诉专员的姓名和联系方式。尽管《条例》要求任命申诉专员，但通常不要求设立数据保护官。但《法案》提出，重要的数据受托人必须指定一名数据保护官。关于隐私影响评估方面，《条例》要求那些处理个人敏感数据的相关组织或机构必须具备由独立审计人员进行认证和审计的安全实践措施和程序，审计人员需获得中央政府的批准，每年应当至少进行一次审计或在计算机资源有重大升级时进行审计。同时，《法案》没有设立数据可携权。

6.5 直接营销

《信息技术法》和《条例》对于使用个人敏感数据或信息进行直接营销没有施加任何条件。 但如果信息是由信息提供方处所收集的（包括个人敏感数据或信息），则必须征得数据主体的事先授权同意，包括对该信息收集的目的的同意 。印度电话监管局发布了《2018 年电信商业通信客户偏好管理规定》，该规定要求电信服务提供方设立相关机制以用来记录订阅用户申请不接收未经请求的商业电话，除此以外，印度没有关于使用直销的特定法律法规或政策，也没有关于通过电子邮件进行直销的特定法律或规定。

6.6 儿童隐私保护

《条例》不包含任何针对儿童个人数据处理的规定。《法案》提出，儿童个人数据应当被合规处理，以保障儿童的权利和最大利益，此类处理只有在确认儿童的年龄并征得其父母或监护人的授权同意后才能进行。处理儿童个人数据或提供针对儿童的服务的实体将被归类为“监护”数据受托人，进行画像分析，跟踪或可能会对儿童造成重大伤害的数据处理被予以禁止。

6.7 安全和数据泄露通知

特定类型的网络安全事件需报告给根据《信息技术法》第 70B 条设立的印度计算机紧急响应小组（“CERT-In”）。此类事件包括（a）危及关键系统或信息，（b）有针对性的扫描或探测关键网络和系统，（c）身份信息遭窃取，欺骗或网络钓鱼攻击，（d）未经授权访问 IT 系统或数据，（e）网站损毁或遭到入侵，（f）包括对服务器的攻击在内的恶意代码攻击，以及（g）拒绝服务或分布式拒绝服务攻击。 CERT-In 同时有权收集或分析来自个人和组织的与网络安全事件有关的信息。未经书面授权同意或法院许可，不得披露可能会导致识别受到网络安全事件影响的个人或组织身份的信息。同时，无需另行通知或获取任何监管机构的批准。根据《条例》，应当保持合理

的安全实践措施和程序。企业主体或其代表人“如果已经实施了安全保障实践措施和标准，并具有全面文件化的信息安全计划和信息安全政策，其中包括与业务性质所保护的信息资产相对应的管理、技术、运营和物理安全控制措施的内容，则会被认定已遵守了合理的安全保障实践措施和程序”。有关部门已将国际标准 IS/ISO/IEC 27001 列入“信息技术 - 安全技术 - 信息安全管理系统 - 要求”的标准之一。遵循其他标准的企业主体必须将其安全措施和标准告知有关部门，在获得批准后予以有效实施。企业主体需由中央政府批准的独立审计人员对其安全措施和程序进行认证和审计，审计行为应当至少每年一次或在其计算机资源进行重大升级时进行。数据保护通常受双方之间的合同关系约束，但只要满足《信息技术法》和隐私政策规定的最低要求，双方可以自由的就自身合理的安全措施和程序进行约定。

6.8 执法

《信息技术法》和《条例》中没有关于数据保护的执法规定。

6.9 其他

a) 代理人：印度没有关于规范代表企业主体的第三方代理人的法律法规，针对企业主体的法律规制同样适用于第三方代理人。

b) 罚款：根据《信息技术法》第 72A 条规定，对于违反合法合同的规定或未经授权同意披露个人信息的行为，处以最高 500,000 印度卢比的罚款。《法案》则提出了与全球营业额相关联的罚款条例，即根据违规行为的类型，罚款金额为全球营业额的 2%到 4%不等。

c) 刑事行为：根据《信息技术法》第 72A 条规定，对于违反合法合同的规定或未经授权同意披露个人信息的行为，可判处最高三年的监禁。

d) Cookies：印度没有关于 Cookies 使用的特定法律法规或指南。

7. 阿联酋

7.1 概述

7.1.1 法律体系

阿拉伯联合酋长国（阿联酋）是由阿布扎比、迪拜、阿治曼、富查伊拉、哈伊马角、沙迦、乌姆盖万 7 个酋长国组成的联邦。阿联酋的法律体系基于民法原则和伊斯兰教法建立。联邦法律适用于所有酋长国，规定了民法、刑法、程序法、劳动法等领域的基本法律原则。每个酋长国也有各自的地方法律，由各酋长颁布实施，处理更偏向行政性质的法律问题，如设立地方政府的法令、慈善 / 赈灾、或修订当地不动产法律。

另外，一些酋长国设立了可以在不同程度上拥有立法自治权的自由区。从数据和隐私角度而言，最重要的两个自由区是迪拜国际金融中心（以下简称 DIFC）和阿布扎比全球市场（以下简称 ADGM）。两个自由区均为普通法管辖区且通过了自己的数据保护法律法规。自由区通常被称为近海区，而阿联酋其他地区则被称为陆上区。

7.1.2 监管机构

• 阿联酋陆上区

阿联酋陆上区没有普适的数据保护法也没有统一的数据保护机构。阿联酋宪法 [12]、刑法典 [13]、网络安全法 [14] 均规定个人享有隐私权。DIFC 和 ADGM 自由区有更加全面的数据保护法。某些行业特定的法律对在阿联酋陆上区设立并在受规制行业内运营的实体施加了数据保护相关的义务 [15]。例如，除卫生部下属的联邦或地方政府健康部门批准外，阿联酋健康数据法对健康信息向阿联酋以外地区的传输进行了限制。另外，电信监管机构（TRA）以及其他负责国家数据和网络安全的地方政府部门正在考虑实施一部联邦数据隐私法，但是草案尚未对外公布。

• DIFC

2020 年 6 月 1 日，DIFC 通过了一部新的数据保护法 [16]（DPL，以下简称 DIFC 数据保护法），废除并替代了 2007 年 1 号数据保护法及其相关条例。DIFC 数据保护法于 2020 年 7 月 1 日生效，受规制的实体有三个月的宽限期开展合规工作。DIFC 的监管机构是数据保护专员。

• ADGM

12 宪法第 31 条保护个人在邮政、电报或其他通讯方式中通信的秘密性。

13 阿联酋刑法典（1987 年第 3 号联邦法律）第 378 和 379 条对于侵犯“个人的私人或家庭生活“或被要求保守秘密的人在没有获得同意时泄露秘密规定了从有期徒刑到罚款等不同的处罚。

14 2010 年第 5 号打击网络犯罪联邦法令（网络犯罪法）第 14 条。

15 例如，2019 年第 2 号健康领域使用信息和通信科技联邦法律（健康数据法）和中央银行储值和电子支付监管框架（EPS 条例）。

16 DIFC 2020 年第 5 号法律。其条例亦在 2020 年 7 月 1 日发布。

ADGM 于 2015 年通过了数据保护条例，并于 2018 年和 2020 年对其进行了修订。[17] ADGM 的监管机构是数据保护办公室，负责提升数据保护水平、数据控制者登记管理、监督数据控制者履行义务及维护个人的数据相关权利。

7.1.3 实体和地域范围

考虑到阿联酋没有一部联邦数据保护法，本节将主要讨论 DIFC 数据保护法和 ADGM 数据保护条例的适用范围。

• DIFC

DIFC 数据保护法适用于：（1）在 DIFC 设立的数据控制者或处理者对个人数据的处理活动，不论处理活动是否发生在 DIFC；（2）数据控制者或处理者处理个人数据的行为是其长期稳定业务的一部分而非偶发性活动，不论数据控制者或处理者在何处设立。[18] 为帮助理解 DIFC 数据保护法的适用范围，“发生在 DIFC 的处理行为”指开展数据处理活动的方法或人员的物理位置位于 DIFC 境内。

• ADGM

ADGM 数据保护条例及相关修正案适用于在 ADGM 设立的数据控制者及代表数据控制者处理个人数据的数据处理者。

7.1.4 数据处理原则

由于阿联酋在联邦层面没有一部数据保护法，本节将主要介绍 DIFC 数据保护法和 ADGM 数据保护条例中规定的基本原则。

• DIFC

DIFC 数据保护法规定的数据处理原则包括：（1）合法性、公平性、透明性；（2）目的限制；（3）数据最小化；（4）适配数据主体权利；（5）准确性；（6）存储限制；（7）完整性和保密性。[19]

• ADGM

ADGM 数据保护条例规定的数据处理原则包括：（1）合法性、公平性、安全性；（2）与数据主体权利相对应的目的限制；（3）数据最小化；（4）准确性；（5）存储限制。[20]

7.1.5 数据处理的合法依据

17 2015 年 ADGM 数据保护条例、2018 年条例修正案、2020 年条例第一修正案。

18 DIFC 数据保护法第 6 条。

19 DIFC 数据保护法第 9 条。

20 ADGM 数据保护条例第 1 条。

这部分将简要叙述 DIFC 和 ADGM 规定的数据处理须达到的合法性要求。

• DIFC

DIFC 数据保护法中的数据处理合法性要求与 GDPR 规定十分相似。数据处理可以基于同意、合同必要性、适用法律下履行法律义务所必要、保护数据主体的重要利益、保护掌握个人数据的控制者或第三方的合法权益（数据主体的利益或权利高于控制者或第三方权益的情形除外）等情形。DIFC 政府机构数据处理的特殊情形可以适用其他合法性基础。[21]

• ADGM

ADGM 数据保护条例中的数据处理合法性基础与 GDPR 规定亦类似。数据处理可以基于同意、合同必要性、数据控制者配合监管要求或履行法律义务所必要、保护数据主体重要利益、为 ADGM 或 ADGM 政府机构（如：法院）的利益而履行职责、为保护数据控制者或披露个人数据的接收第三方的合法权益（数据主体的合法利益高于控制者或第三方权益的情形除外）。[22]

7.2 重要定义

7.2.1 个人数据及特殊类别的个人数据

DIFC 数据保护法和 ADGM 数据保护条例均将“个人数据”定义为，指向某一特定的或可识别的自然人的数据。特殊类别的个人数据（ADGM 数据保护条例中称“敏感个人数据”）的定义为，披露或直接 / 间接地与种族或民族血统、政治观点、宗教或哲学信仰、犯罪记录、商会会员、健康信息、性生活相关联的个人数据。DIFC 数据保护法规定的“特殊类别的个人数据”还包括披露政治党派、社会关系的个人数据，及用于识别某个特定自然人的基因数据和生物识别数据。

7.2.2 数据控制者和数据处理者

DIFC 数据保护法和 ADGM 数据保护条例中定义的数据控制者为：可以独自或与他人共同决定个人数据处理的目的和方式的个人。在 ADGM 数据保护条例下，数据控制者是 ADGM 境内的个人，但自然人作为员工履职的情形除外。

DIFC 数据保护法和 ADGM 数据保护条例中定义的数据处理者为：代表数据控制者处理个人数据的人。ADGM 数据保护条例明确将自然人作为员工履职的情形排除在上述定义的范围之外。

7.3 数据主体

DIFC 数据保护法和 ADGM 数据保护条例将数据主体定义为自然人，在 DIFC 数据保护法语境下，数据主体即个人数据关联的特定或可识别的自然人。

7.4 隐私声明

21 DIFC 数据保护法第 10 条。

22 ADGM 数据保护条例第 2 条。

DIFC 数据保护法和 ADGM 数据保护条例都要求数据控制者向数据主体说明其直接或间接从数据主体处获得的个人数据。数据控制者应在收集个人数据时尽早地履行告知义务。数据主体应知晓的相关信息可以通过隐私政策传达，隐私政策应使用明确、直白的语言，以简洁、透明、容易理解且方便访问的形式呈现。

隐私政策应包含以下内容：数据控制者的身份和联系方式、数据保护官（以下简称 DPO）（如有）的联系方式、数据处理目的、收集的个人信息类别、个人信息接收方的身份或类别、数据跨境传输相关信息及传输中采取的安全措施、以及为保证数据处理的公平、透明性所必要的其他与个人数据收集的具体情形相关的信息。[23]

7.5 直接营销

DIFC 对于直接营销发布了一份专门的指引，明确了开展直接营销必须满足的要求[24]，同时根据接收方的身份和营销渠道的不同而设置了不同的要求。ADGM 尚未颁布类似的指南。但 DIFC 数据保护法和 ADGM 数据保护条例均规定，如个人数据会被用于直接营销的目的，数据控制者有义务告知数据主体并为数据主体提供拒绝的权利。

7.6 数据共享与处理

ADGM 数据保护条例没有关于数据共享的专门条款。在政府公共机关（下称要求机关）要求该组织 / 个人或其子 / 母公司披露或传输个人数据时，DIFC 数据保护法为数据控制者和数据处理者提供了一些指引。当接收到这类要求时，数据控制者或处理者应：（1）尽合理的注意和勤勉义务来核实要求的有效性和恰当性，确保该情形下个人数据的披露仅为满足政府机关所提出的要求；（2）评估数据传输的影响，及对任何可能涉及的数据主体的权利造成的风险，并在适当条件下采取措施以最大程度降低风险；（3）在合理可行的范围内，从要求机关处获得书面且有约束力的承诺，保证该要求机关将尊重数据主体的权利并遵守 DIFC 数据保护法中规定的一般数据保护原则。[25]

7.7 儿童隐私保护

DIFC 数据保护法和 ADGM 数据保护条例中均没有儿童隐私保护相关的条款。为了应对针对儿童的网上犯罪增长的态势，阿联酋在国家层面开展了一些儿童保护的项目。阿联酋设立了一个名为 E-Safe 的非营利性组织，旨在创造更安全的网络体验并保护儿童免受各种形式的剥削[26]。2016 年，阿联酋政府颁布了一部儿童权益法[27]。这部法律要求电信公司将在网络上流通的任何儿童色情内容报告相关政府部门或实体[28]。儿童权益法第 5 条明确，考虑到儿童监护人的权利和义务，儿童基于公共道德享有隐私权。

23 见 ADGM 数据保护条例第 6、7 条和 DIFC 数据保护法第 29、30 条。

24 数据保护专员，DIFC 数据保护政策指引：直接营销和电子通信，更新于 2020 年 7 月 1 日。

25 DIFC 数据保护法第 28 条。

26 http://www.esafesociety.org/en/why-e-safe/

27 2016 年关于儿童权利的联邦第 3 号文件（wadeema's law）。

28 同上，儿童权益法第 29 条。

7.8 可问责性

7.8.1 通过设计的数据保护和默认的数据保护

ADGM 数据保护条例中没有关于通过设计的数据保护和默认的数据保护的规定。DIFC 数据保护法第 14（3）条中提出了这一概念，数据控制者和处理者有义务采取必要的措施将通过设计的数据保护和默认的数据保护融入数据处理过程中，以达到法律要求并有效保护数据主体的权利。这些措施至少应包括：（1）通过隐私设计使得数据处理体现数据保护原则，如在决定处理方式和处理时做到数据最小化；（2）默认情况下，仅处理为实现某一特定目的所必要的个人数据，且在未经数据主体参与的情况下，不将个人数据披露给不特定群体。

7.8.2 数据保护影响评估（DPIA）

ADGM 数据保护条例中没有具体涉及 DPIA 的条款。DIFC 数据保护法规定，当开展高风险处理行为时，数据控制者有义务评估处理行为可能对个人数据保护造成的影响以及可能对相关数据主体权利造成的威胁。当个人数据的处理不属于高风险行为时，数据控制者也可以选择开展 DPIA。DPIA 过程应至少包括：（1）系统描述即将发生的处理行为及其目的，包括数据控制者追求的合法利益（如有）；（2）评估数据处理行为是否为实现其目的所必要、是否与其目的成比例；（3）识别并考量数据处理的合法性基础；（4）评估可能对数据主体权利造成的风险；（5）为降低风险预计可以采取的措施。[29]

7.8.3 数据处理活动记录

ADGM 数据保护条例和 DIFC 数据保护法均规定，数据控制者有义务建立并维系个人数据处理行为的书面记录。[30] DIFC 数据保护法规定，书面记录应包括如下内容：（1）数据控制者名称及联系方式、其任命的 DPO（如有）、共同控制者（如有）；（2）数据处理的目的；（3）数据主体类别的描述；（4）个人数据类别的描述；（5）个人数据已经 / 即将披露的接收方类别，包括位于第三国的或国际组织接收方；（6）个人数据已经 / 即将被传输到第三国或国际组织时的接收方身份（如有），如接收方未达到数据保护专员认定的充分保护水平，应记录传输过程中采取的恰当安全措施；（7）销毁不同类别个人数据的时限（如有）；（8）对数据控制者采取的技术或组织安全措施的系统介绍（如有）。

7.8.4 数据保护官（DPO）和 GDPR 代表

ADGM 数据保护条例未对数据控制者提出任命 DPO 的要求，然而 DIFC 数据保护法第 16 条要求数据控制者设立 DPO。数据控制者和处理者都可以选择是否任命 DPO。但是当数据控制者或处理者开展高风险数据处理活动时，除了履行司法职责的法院以外，DPO 应由 DIFC 政府机构任命。DIFC 数据保护法规定了 DPO 的职权、地位、角色和任务。[31]

29 DIFC 数据保护法第 20 条。

30 ADGM 数据保护条例第 12（1）条和 DIFC 数据保护法第 15 条。

31 DIFC 数据保护法第 17、18 条。

7.9 安全与数据泄露通知

ADGM 数据保护条例第 9（4）条规定，当数据处理者持有的个人数据遭到未经授权的侵入（包括含有个人数据的设备损毁或遭到非法披露），不论侵入是物理的、电子的或其他方式的，数据处理者均有义务在第一时间通知数据控制者。数据控制者也有义务在个人数据发生未经授权的侵入（包括含有个人数据的设备损毁或遭到非法披露）及其处理者发生安全事件时通知监管机构，不论侵入是物理的、电子的或其他方式的。数据控制者不得无故拖延通知义务的履行，在可以实现的前提下，应在数据控制者得知安全事件后的 72 小时内完成通知。

DIFC 数据保护法亦规定，数据控制者和数据处理者在发生安全事件时应承担通知义务。[32] 当个人数据泄露且对数据主体的秘密、安全和隐私造成减损时，数据控制者应通知数据保护专员且应在情况允许的范围内第一时间履行通知义务。数据处理者应在得知个人数据泄露后及时通知相关控制者，不得无故拖延。DIFC 数据保护法规定，当个人数据泄露可能对数据主体的安全或权利造成较大风险时，数据控制者应在可能的情况下第一时间通知数据主体。如果安全事件对数据主体可能造成紧迫的危害，数据控制者应及时与数据主体沟通。当与数据主体逐一沟通存在显著困难或成本过高时，数据控制者可以发布一份公告或采取其他措施以与逐一通知同等有效的方式通知数据主体。

7.10 跨境数据传输

将个人数据传输至 DIFC 和 ADGM 以外的区域是受到限制的 [33]。DIFC 和 ADGM 均对个别国家 / 地区的保护充分性进行了认定。个人数据传输至上述提供充分保护水平的国家 / 地区时不需要获得额外的许可或采取额外的措施。个人数据传输至未被认定为充分保护水平的国家 / 地区时需要满足额外的要求，比如 ADGM 要求跨境传输获得监管机构的许可，获得数据主体的书面同意，或数据传输方和接收方之间存在有法律约束力的合同。当个人数据在集团公司内部传输时，DIFC 数据保护法认可有约束力的公司规则可以作为一种恰当的安全措施。数据保护专员也发布了标准数据保护条款，基本仿照欧盟的标准合同条款为模板。[34]

7.11 执法

如数据控制者和数据处理者违反相关数据保护立法的规定，ADGM 和 DIFC 的监管机构均有权对其处以罚款。在 ADGM 语境下，罚款上限为 25000 美元 [35]。根据 DIFC，数据保护专员最高可以判处 100,000 美元的行政罚款 [36]。数据控制者或处理者违反 DIFC 数据保护法规定时，结合违法行为的严重性以及对数据主体造成实际损害的风险，数据保护专员还可以自由裁量一个他认为合适且与违法行为相称的罚款金额 [37]。

32 DIFC 数据保护法第 41、41 条。

33 ADGM 数据保护条例第 4、5 条和 DIFC 数据保护法第 26、27 条。

34 DIFC 数据保护法第 27（2）条。

35 ADGM 数据保护条例第 17（3）条。

36 DIFC 数据保护法第 62（2）条及附录 2。

37 DIFC 数据保护法第 62（3）条。

8. 沙特阿拉伯王国

8.1 概述

8.1.1 法律体系

沙特阿拉伯王国（KSA，以下简称“沙特”）法律体系的基石是伊斯兰教法。伊斯兰教法是源自一系列不同渊源的基本原则的组合，包括古兰经、圣行（圣训）和伊斯兰教法学者的著作。除伊斯兰教法外，沙特也颁布了一些成文法，主要包括皇家敕令、皇家法令、内阁委员会决议、内阁决议和通知。上述法律最终都应符合伊斯兰教法，不得与伊斯兰教法相冲突。

8.1.2 监管机构

沙特没有一部法律集中规定数据 / 隐私保护相关事项，也没有设立国家统一的数据保护监管机构。然而，某些法律法规虽并不专门处理数据 / 隐私问题，但是其中包含一些具体的条款，在特定语境下规定了数据和隐私保护的权利。[38]

8.1.3 实体和地域范围

在国家层面，沙特没有一部统一的数据隐私保护法，但某些和数据、隐私相关的法律条款可能有域外效力。例如，保护线上服务提供商所使用的消费者数据的电商法除适用于设立在沙特境内的电商平台外，也适用于向位于沙特的消费者提供商品 / 服务的平台，不论该平台在何处登记设立。换句话说，位于阿联酋的线上服务提供商，如通过网站向位于沙特的消费者提供商品 / 服务，也需要遵守沙特电商法的要求。

8.1.4 数据处理原则

由于沙特没有统一的数据保护法，因此不存在以成文法形式明确的数据处理原则。

8.1.5 数据处理的合法依据

沙特没有一部数据保护法规定数据处理的合法性基础。某些适用于特定行业的法律可能要求在处理个人数据前获得数据主体的同意。另外，某些情形下，未获得同意时处理个人数据可能构成刑事犯罪。为明确具体的法律义务，在沙特运营的公司应该关注与其业务和所处理数据相关的特定部门法 / 行业法。

沙特通信和信息技术委员会（CITC）发布了一份物联网监管框架（简称 IoT 框架），框架要求物联网服务提供者遵守“数据安全、隐私和保护要求”。IoT 框架进一步规定，物联网提供者和实

38 可参见，沙特基本法（A90/1992 号皇家法令），沙特电商法（M126/2019 号皇家法令）、电信法（M12/2001 号皇家法令），及其他相关法律。

施者必须“遵守现行和未来颁布的所有与数据管理（即安全、隐私、保护）相关的法律、法规、要求”。这一规定意味着，当国家颁布实施了数据保护法后，物联网服务提供者须遵守所有通行的数据保护理念及原则。这些原则包括目的限制、数据最小化、存储限制等等。

8.2 重点定义

8.2.1 个人数据与特殊类别个人数据

沙特没有统一的法定“个人数据”定义。虽然伊斯兰传统和教法中将某些与个人或及家庭相关的数据认定为敏感信息，但是沙特法律并没有普遍规定“敏感个人数据”这一概念。

不同的法律保护、规制不同类别的数据。例如，反网络犯罪法保护电子形式的数据，包括但不限于银行和信用信息。电信法适用于可识别到订阅者个人的数据、订阅者之间互相通信的内容及与通信相关的信息。沙特医疗健康实践法保护健康信息，比如可识别到某一病人的数据、个人健康状态及所接受的治疗。

沙特法律也没有一个针对个人数据的通用分类系统。然而，云计算监管框架[39]（简称 CCRF）将云服务提供商掌握或处理的消费者数据分为以下四个级别：

第 1 级别：非敏感消费者数据，不论消费者是个人或私营企业，这类数据外包不受任何行业法规特别的限制；

第 2 级别：敏感消费者数据，不论消费者是个人或私营企业，这类数据外包亦不受任何行业法规特别的限制；

第 3 级别：私营企业掌握的消费者数据，这类数据受到行业特殊规则或监管机构决议的特殊限制，及政府当局持有的敏感消费者数据；

第 4 级别：归属于相关政府机构的高度敏感或秘密的消费者数据。

CCRF 要求在沙特运营的云服务提供商依据数据的不同敏感程度以不同的默认级别的安全水平保护消费者数据。

8.2.2 数据控制者和数据处理者

沙特法律中没有数据控制者和数据处理者的概念。

8.3 数据主体权利

沙特目前的法律法规没有规定具体的数据主体权利。沙特法律能总结出的数据主体权利就是一项普遍的隐私权和在法院中要求行使隐私权的权利。CCRF 要求云服务提供商赋予消费者删除个人

39 云计算监管框架第 3.3.1 条。

数据的权利。

8.4 隐私声明

CCRF 规定云服务提供商应向消费者提供某些特定的先合同信息，比如云服务提供商数据处理活动的细节。除此之外，沙特法律未对隐私政策应向数据主体说明的内容进行更多的规制。

8.5 直接营销

沙特法律没有特殊的条款规制那些为营销目的而使用个人数据的行为。然而，就大原则而言，为任何目的使用、收集、向第三方共享个人数据都应获得数据主体的同意。

8.6 数据共享与处理

沙特国内法未对数据共享做特殊规定。外国要求披露数据时，必须基于双边司法互助条约（MLAT）或联合国公约（沙特与要求披露数据的接收国需均为公约成员国）的基础上提出。在沙特国内负责管辖所有沙特与条约伙伴签署的 MLAT 的中央机关为内政部。

8.7 儿童隐私保护

儿童保护法 1436H 与儿童保护系统条例构成沙特儿童权益保护的主要法律框架。这两部法律总括地规定了儿童享有的权利，但其条款没有特别提出儿童与隐私相关的权利。

8.8 可问责性

a) 通过设计的隐私保护和默认的数据保护

沙特国内法中没有实施设计和默认的数据保护的要求。

b) 数据保护影响评估（DPIA）

沙特国内法中没有开展 DPIA 的要求。

c) 数据处理活动记录

沙特国内法未要求对数据处理行为进行记录。

d) 数据保护官（DPO）和 GDPR 代表

目前，沙特国内法未要求收集、使用、处理个人数据的实体任命 DPO。

8.9 安全和数据泄露通知

鉴于沙特没有国家级的数据监管机构，除影响云服务提供商（以下简称CSP）的数据泄露需报告外，目前法律未规定数据控制者或处理者承担报告数据泄露事件的义务。在 CCRF 规定下，CSP 在得知出现安全漏洞或信息泄露，且该安全漏洞或数据泄露影响或可能影响消费者的云内容、数据、或 CSP 所提供的云服务时，必须通知消费者，不得无故延迟。如安全漏洞或数据泄露影响或可能影响（1）第 3 级别的消费者数据；（2）相当多消费者的消费者数据；（3）由于依赖受到安全漏洞或数据泄露影响的云服务而波及相当多数量的沙特人民时，CSP 必须在得知出现安全漏洞或信息泄露后通知沙特通信与信息技术委员会（以下简称委员会），不得无故延迟。

虽然 CCRF 没有针对数据泄露规定罚则，但沙特反网络犯罪法规定了数据泄露相关的罚款规则。反网络犯罪法处罚犯有下列违法行为的个人 / 实体：（1）为删除、销毁、更改、重新分配信息的目的访问他人电脑，处以不超过 300 万沙特里亚尔（约 80 万美元）的罚款和 / 或不超过 4 年的有期徒刑；（2）访问他人银行、信用或所持有证券的相关信息，处以不超过 200 万沙特里亚尔（约 53 万美元）和 / 或不超过 3 年的有期徒刑；（3）干扰通过电脑或信息网络进行的数据传输，处以不超过 50 万沙特里亚尔（约 13 万美元）的罚款和 / 或不超过 1 年的有期徒刑。

8.10 跨境数据传输

CCRF 根据数据的分类对其传输和存储位置进行了不同程度的限制。例如，除沙特 CCRF 以外的法律法规明确允许出境外，第 3 级别的消费者数据，不论为任何目的、不论以何种形式、不论永久或暂时（例如：数据冗余或缓存），均不得传输至沙特境外。

除 CCRF 或某些法律规定特定类别的数据应本地化存储在沙特境内以外，沙特国内对于数据传输没有一个统一的机制。沙特政府目前尚未发布数据传输协议的标准模板或参考样例，如 GDPR 规定的标准合同条款（SCC）。当沙特通过数据保护法后，这个情况应该会有所改善。同时，为避免违反伊斯兰教法的一般原则，企业较为明智的做法是在个人数据出境前获取数据主体的同意。

8.11 执法

沙特国内没有一个明确的监管机构负责数据和隐私保护的执法问题。然而，某些政府机构承担着执行沙特其他现行法律的任务。违反数据和隐私保护的处罚可能规定在一些关联法规中，或者由法官自由裁量。上述第 9 部分列举了反网络犯罪法下的一些处罚规则。隐私权遭到侵犯的个人也可选择诉诸伊斯兰教法，个人因信息泄露给第三方而受到的损失享有补偿的权利。以非法或不道德方式获取他人个人数据的第三方需要就信息泄露承担法律责任。

四、大洋洲

1. 澳大利亚

1.1 概述

1.1.1 法律体系

澳大利亚在隐私领域的主要立法为 1988 年《联邦》（以下简称“《隐私法》”）。联邦制定了单独的法律监管垃圾邮件和电话营销，且特别制定了电信领域的隐私立法。此外，澳大利亚在特定领域还设有一系列具有强制力的法律、法规及准则，例如在医学研究领域、税务档案号码领域、信用报告领域及联邦机构治理领域。澳大利亚各州和管辖区设有法律用来规范监控所获信息的收集和使用，且有单独隐私立法用以规制各管辖区政府机构行为。部分州和管辖区针对健康信息制定了单独的法律。

1.1.2 监管机构

澳大利亚信息专员办公室（OAIC）负责监督、实施《隐私法》。

1.1.3 实体和地域范围

《隐私法》适用于澳大利亚所有的联邦部门或机构，以及所有年营业额超过 300 万澳元的私人组织。各个机构和组织统称为实体。《隐私法》还适用于年营业额未达到 300 万澳元，但满足特定条件的小型企业。例如，处理个人数据的医疗服务供应商、英联邦合同下的合同服务供应商、信用报告机构、较大型企业集团（集团的一个或多个成员年营业额超过 300 万澳元）的组成部分、应当遵守反洗钱义务的企业，或受到电信强制性数据存储计划约束的企业。

《隐私法》具有域外适用效力，可适用于在澳大利亚境内实施商业行为并收集或保存数据的任何外国实体。

《隐私法》不适用于员工记录，即与员工雇佣相关的个人信息记录（例如聘用、培训、纪律、绩效、个人联系方式、工资、休假额度、纳税情况及银行事务信息），上述信息与雇主和个人之间现在或过去的雇佣关系直接相关。

1.1.4 数据处理原则

《隐私法》确立了 13 项澳大利亚隐私原则（以下简称“APP”），这些原则规范了如何进行个人信息的收集、使用、披露和存储，所涉内容包括：公开、透明的信息管理，匿名和假名，信息的收集、使用、披露规则，直接营销（在有限范围内），境外信息披露，政府识别码，质量和安全，访问以及更正。

1.1.5 数据处理的合法依据 — APP 第 3 条

实体不得进行数据收集，除非数据收集对于实体开展一项或多项功能或活动是合理必要的，且只通过合法、公平的方式进行收集。实体不得收集敏感信息，除非数据主体明示或默示同意数据收集，且相关数据对于实体开展一项或多项功能或活动是合理必要的。

1.2 重要定义

a) 个人信息是指与已识别的个人或可合理识别的个人相关的信息或观点，无论该信息或观点是否真实以及是否以实体形态记录。

b) 敏感信息是指与个体种族或民族，政治立场或党派，宗教、哲学信仰或隶属关系，工会、行业或贸易组织成员身份，性取向或行为，犯罪记录，健康或遗传信息，用于自动生物特征验证或识别的生物识别信息或生物特征模板。

c) 数据控制者和数据处理者：《隐私法》没有对数据控制者或数据处理者的概念做出规定，而是规定个人信息的收集、使用和披露规则，约束前述过程中所涉的所有主体。

1.3 数据主体的权利

a) 访问权 — APP 第 12 条

数据主体有权访问查阅任一实体存储的该主体的个人信息。除非有特殊的例外情形，否则该实体必须在合理期限内（通常为 30 天）向数据主体提供信息。组织可以收取访问费用（政府机构或部门不可收取）。

b) 更正权 — APP 第 13 条

如果与信息相关的个人提出要求，或信息不准确、过时、不完整、不相关或具有误导性，实体必须对个人信息做出更正。在某些情况下，实体必须将信息的更正事宜通知持有相同信息的其他实体。在例外情况下，APP 实体可以拒绝更正信息。

1.4 隐私声明

实体必须有表述明确且版本最新的隐私政策，隐私政策中应包括 APP 第 1.4 条规定的详细内容，以及 APP 第 5 条规定的单独的收集通知。许多实体只有一个包含 APP 第 1.4 条和第 5.2 条要求的隐私政策，即包括详细的标识和联系方式、收集信息的类型、收集信息的方法和目的（包括受澳大利亚法律或命令的任何要求的信息收集行为）、不收集的后果、信息将被如何使用和披露（包括在境外的情况）、信息主体如何访问和更正其个人信息，以及信息主体如何投诉相关隐私实践。

1.5 直接营销

APP 第 7 条 仅适用于纸质营销或有针对性的电子广告。在这些广告中，个人信息是从个人处收集的，个人在合理范围内能够预期到自己提供的信息会被用于直接营销。如果个人信息并非从个人处收集，则不存在合理预期；如果个人信息为敏感信息，则只有在获得个人的明示或默示同意后才能用于直接营销。此外，实体必须提供退出营销的方式相关的信息

《2003 年垃圾邮件法》禁止在未经个人明示或推定同意的情况下，向个人发送其未请求的商业电子通知（包括电子邮件、SMS 和 MMS）。 此外，上述消息中必须清楚地标明发件人并包含有效的退订渠道。

《 2006 年禁止呼叫登记法》和《 2017 年电信（电话营销和研究电话）行业标准》对于电话营销的使用做出了规定。

1.6 数据共享与处理 – APP 第 6 条

为实现特定目的（主要目的，primary purpose）收集的个人信息不得为实现其他目的（次要目的）而使用或披露，除非：

a）个人已明示或模式同意该次要目的（secondary purpose）；

b）个人能够合理地预期到其个人信息将被用于该次要目的，该次要目的必须与主要目的相关（对于敏感信息来说，则必须直接相关）； 或

c）存在澳大利亚法律或法院命令许可的一般情形、与健康相关的情形，或为协助执法机构确有必要使用或披露相关个人信息。

1.7 儿童隐私保护

OAIC 建议认定未满 15 岁的个人不具有同意的能力。

1.8 可问责性

a) 通过设计的数据保护和默认的数据保护

APP 第 1 条 规定了与 GDPR 设计隐私和默认隐私原则类似的要求，鼓励通过实践和程序帮助实体保护个人信息并实现 APP 合规。APP 第 1.1 条鼓励实体以公开透明的方式管理个人数据。APP 第 1.2 条要求实体采取合理的步骤实践、执行程序和系统，以确保实体能够实现 APP 合规。

b) 数据保护影响评估

组织不是必须进行数据保护影响评估的，但政府机构在 OAIC 指导下或澳大利亚 2017 年政府机构隐私规则有所要求时，应当开展数据保护影响评估。

c) 数据处理活动记录

无特殊规定。

d) 数据保护官（DPO）和代表

无特殊规定。

1.9 安全和数据泄露通知

根据 APP 第 11 条，实体必须采取所处情形下合理的措施防止个人信息被滥用、干扰、丢失，以及受到未经授权的访问、篡改或披露。此外，对于实现某一被许可的目的不再必要的个人信息，实体必须采取合理的步骤对该等个人信息进行删除或去标识化。

实体必须对数据泄露事件进行调查，以在数据泄露事件发生之日起 30 天内确定是否应当报告该事件。如果社会一般人认为该数据丢失、未经授权的访问或披露事件有可能对受影响的数据主体造成严重危害，则应当报告该数据泄露事件。实体必须将数据泄露事件通知 OAIC 和受影响的个人，且通知中必须包含某些必须披露的内容。

1.10 跨境数据传输 — APP 第八条

在向境外披露个人信息之前，实体必须与海外接收方签署书面协议，要求他们遵守 APP 的规定。披露数据的实体对海外接收方的 APP 合规情况承担最终责任。上述要求不适用于以下情形：

a）海外接收者受到与 APP 类似的法律或约束机制的规范；

b）相关个人已被告知的相关实体将不会采取措施确保海外接收方遵守 APP 规则的情况后，仍提供信息； 或

c）澳大利亚法律或法院命令要求或授权实体对个人信息进行披露，或存在允许披露的一般情形。

1.11 执法

OAIC 可以签发决定书（迄今最高罚款金额为 20,000 澳元）、有执行力的承诺函，或者发布最高 42 万澳元的民事处罚令或最高 210 万澳元的罚款令。

1.12 立法趋势前瞻

2019 年 7 月，澳大利亚竞争与消费者委员会发布了一项针对数字平台的调查报告。报告对现有立法提出了一些建议，旨在加大《隐私法》对个人信息的保护力度。针对报告中的数项建议，澳大利亚政府已承诺可能在 2021 年采纳落实，包括：

a) 加重处罚，处以下罚款金额中的较高项：（i) 1000 万澳元 (ii) 因滥用信息所获利益价值的三倍，以及（iii）实体年营业额的 10%；

b）扩大个人信息的定义和《隐私法》的适用范围；

c）加强通知和同意要求；

d）引入个人可直接行使的诉讼权，包括考虑引入隐私侵权行为；以及

e）针对社交媒体和在线平台制定具有约束力的隐私法律。

2. 新西兰

2.1 概述

2.1.1 法律体系

新西兰现行隐私立法为《1993 年隐私法》（以下简称《隐私法》）。除此之外，这一领域其他的行业规则包括《1994 年健康信息隐私法》、《2004 年信用报告隐私法》和《2003 年电信信息隐私法》也针对隐私方面提供了保护。

2.1.2 监管机构

隐私保护专员办公室（以下简称 OPC）负责监管《隐私法》的实施；人权审查法庭负责做出具有约束力的《隐私法》相关决定。

2.1.3 实体和地域范围

《隐私法》适用于任何主体，无论其是否具有法人地位，为私营主体还是公共部门机构（统称为机构）。OPC 曾表示，即使数据处理在国外进行，如果国际机构在新西兰境内运作并向新西兰人提供服务，其依然会受到《隐私法》的约束。

2.1.4 数据处理原则

《隐私法》确立了 12 项信息隐私原则（IPPs），内容涵盖数据收集、存储、安全、个人信息访问和更正请求、准确性、保留、使用、披露以及唯一识别码的使用。此外，《隐私法》还规定了一系列额外要求。IPPs 第 5 条至第 8 条以及第 11 条对存储于新西兰境外的数据做出了特别规定。

2.1.5 数据处理的合法依据 — IPP 第 1 条

机构不得收集个人信息，除非信息收集是出于合法目的进行，与机构的职能或活动相关，且为实现该目的是确有必要的。

2.2 重要定义

a) 个人信息

个人信息是指有关可识别的个人的信息，包括与死亡相关的、由登记总处根据《1995 年出生、死亡、婚姻和关系注册法》或此前的其他法律规范记录持有的信息。

b) 数据控制者和数据处理者

《隐私法》没有对数据控制者或数据处理者的概念做出规定，但定义了一个与数据处理者类似的

概念：如果一个机构仅出于为另一机构进行数据处理的目的持有数据，那么认定后者为持有数据的一方。

2.3 数据主体的权利

a) 访问权—IPP 第 6 条以及《隐私法》第 4、5 部分

如果机构持有可以检索的个人信息，那么在数据主体要求时，机构必须确认其是否持有相关信息，并在收到要求通知之日起 20 个工作日内提供对上述信息的访问权限。

b) 更正权—IPP 第 7 条以及《隐私法》第 4、5 部分

除非出现法律允许的例外情况，机构必须主动或在数据主体要求下采取合理措施（在 20 个工作日内）更正信息，以确保相关信息准确、最新、完整且不具有误导性。考虑到信息可能的使用目的，在某些情况下，机构有义务将信息的更正事宜通知持有相同信息的其他实体。

2.4 隐私声明

新西兰没有特定规则要求机构必须制定隐私政策，但是 IPP 第三条确立了一系列机构应当告知消费者的详细内容，包括：机构正在收集的个人信息、收集信息的目的、信息接收方、收集及存储信息的机构名称和地址；如果信息收集是法律要求或法律授权的，则应当告知消费者不提供相关信息的后果，以及 IPPs 为信息主体确立的访问权和更正权。

2.5 直接营销

《隐私法》不包含任何与直接营销相关的特别规定，但 IPPs 中确立的一般规则也适用于直接营销，例如对信息使用透明和获得个人授权的要求。

《2007 年非应邀电子信息法》禁止在未经接收方明示或暗示同意的情况下发送商业电子信息（CEMs）。 此外，商业电子信息中必须清楚地注明发件人并包含有效的退订渠道。

新西兰营销协会负责“请勿来电”和“请勿发邮件”清单的登记工作，上述清单规范电话营销和实体邮件营销的使用。此外，协会还负责一系列适用于直接营销的业务守则和指引。尽管企业可以自愿选择是否加入，新西兰政府已经认可并期望企业遵守这些规则。

2.6 数据共享和数据处理 — IPP 第 10 条

机构为实现某一目的收集的个人信息不得用于实现其他目的，除非该信息是公开可得的；使用该信息是公平、合理的；其他目的或使用得到了数据主体授权；为避免对任何公共部门机关维护法律、依法执行罚款、保护公共收入或执行法定程序造成损害，有必要通过使用个人信息预防或减少对公共健康、公共安全，或个人生命、健康造成严重威胁；该其他目的与初始目的直接相关；使用信息的形式是不识别个人身份的，或 OPC 特别许可了对 IPP 第 10 条的豁免。

2.7 儿童隐私保护

《隐私法》未对儿童个人信息做出不同的规定，而是规定儿童与成人对其个人信息享有相同的权利。虽然如此，OPC 仍建议机构制定实际可行的保护措施，并在涉及到年龄较小的儿童时认定其父母或监护人为其代理人。

《隐私法》在部分情形下允许驳回访问请求，即如果允许访问儿童的个人信息可能会对个人安全造成危害，或披露 16 岁以下个体的个人信息会损害其利益的情形。

2.8 可问责性

a) 通过设计的隐私保护和默认的隐私保护

除一般原则外，IPP 中没有条款明确要求通过设计的隐私保护和默认的隐私保护义务。

b) 数据保护影响评估（DPIA）

数据保护影响评估：根据《隐私法》规定，数据保护影响评估不是强制实施的，但是 OPC 鼓励企业在项目可能影响到个人信息和合理程度的隐私保护时开展数据保护影响评估。

c) 数据处理活动记录

无相关要求。

d) 数据保护官（DPO）

机构有义务设立一个或多个负责人来促进 IPP 合规、处理数据主体根据《隐私法》提出的请求、与委员会合作开展调查、并采取其他方式确保机构合规。但在注册登记方面，无相关要求。

2.9 安全和数据泄露通知 — IPP 第 9 条

机构留存信息的时间不得超过合法使用目的所需的时间。

数据泄露报告不是法定强制性义务，但是 OPC 曾发布了一项不具有约束力的有关数据泄露事件的最佳实践指南。

2.10 跨境传输

《隐私法》没有对个人信息跨境传输设立任何具体限制，但规定在新西兰境外传输数据的机构须对海外数据接收者使用和披露信息的情况负责。

如果 OPC 确信从一个海外国家传入新西兰的信息很有可能被传输至另一个数据保护水平低于新

西兰的国家，且认定该传输很可能违反 OECD 准则中规定的数据保护义务，OPC 有权禁止上述跨境传输个人信息。

2.11 执法

OPC 享有有限的执法权力：其可以评估投诉，并要求机构与受影响的个人会面以达成和解。OPC 也有权因机构未配合 OPC 调查对其签发最高 2000 新西兰元的罚款。

如果机构和个人未能达成和解，OPC 可以将投诉移交至人权审查法庭，该法庭可以根据数据泄露的严重程度处以不同的罚款。对于情节较轻的案件，罚款可能在 5,000 新西兰元至 10,000 新西兰元之间；对于情节较严重的案件，罚款可能达到 50,000 新西兰元以上。

2.12 立法趋势前瞻

《2020 年隐私法》将于 2020 年 12 月 1 日生效，并对现有立法进行实质性的变更。重要的变更包括：

- 强制要求报告数据泄露事件；
- 引入合规通知制度；
- 授予 OPC 做出有拘束力决定的权力；
- 加强跨境传输数据保护力度；
- 将以下行为定为刑事犯罪：以某种会对他人个人信息造成影响的方式误导机构，以及在收到访问请求时销毁文件；和
- 加强 OPC 的信息收集权力，将对违反调查规定的机构所做的罚款上限增加到 10,000 新西兰元。

第四部分
我国企业出海的前期规划

一、欧盟

根据 GDPR，除非符合以下条件，否则不允许将欧洲经济区中的个人数据传输到欧洲经济区以外的第三国：

- 欧盟委员会的充分性决定：已获得欧盟委员会批准的国家 / 地区包括安道尔，阿根廷，加拿大（适用《个人信息保护及电子文档法案》(PIPEDA)），瑞士，法罗群岛，根西岛，以色列，曼岛，日本，泽西岛，乌拉圭东部共和国和新西兰 [40]；
- 标准合同条款（“SCCs”）：由欧盟委员会通过或由监管机构通过并由欧盟委员会批准；
- 由主管数据保护机构批准的具有约束力的公司规则（“BCR”）；或者
- 克减（例如明确同意，合同必要性，公共利益，法律主张等）或特定豁免。（GDPR 第 44-50 条）

二、多边协议

1. CPTPP 数据流动框架

全面与进步跨太平洋伙伴关系协定（（以下简称“CPTPP”），旧称为“跨太平洋伙伴关系协定”

40 美国（对于参与到欧盟 - 美国“隐私盾”机制的组织机构而言）原被视为获得充分性决定的国家之一。但是，欧盟法院于 2020 年 7 月 16 日的判决否决了欧盟 - 美国“隐私盾”的效力，因此，组织机构无法再依据该机制进行数据传输。

（TPP），是在以下 11 个参与的经济体间签署的自由贸易协议：澳大利亚、文莱、加拿大、智利、日本、马来西亚、墨西哥、新西兰、秘鲁、新加坡和越南。

CPTPP 第 14.11 条与第 14.13 条包含了一些旨在限制成员国对数据本地化和跨境数据传输的要求的规定。具体而言：

- 第 14.11 条要求“当传输是为了商业活动时，成员国应允许以电子形式进行包括个人信息在内的跨境信息传输”。

- 第 14.13 条禁止成员国将要求公司“使用位于该成员国境内的设施、或将设施设于该成员境内作为允许该公司在该成员国境内开展业务的前提条件”。

（以上两条规定统称为“传输自由规定”）[41]。

自由传输规定反映了各个成员经济体对于促进跨境数据自由传输的承诺，并有望对各个成员国在国家层面上的关于跨境数据传输的规定产生影响。

2. APEC 国家 CBPR 体系

亚太经合组织（APEC）的跨境隐私规则体系（以下简称为“CBPR”）是由政府支持的数据隐私认证体系。公司可以加入该体系以证明其符合国际层面认可的数据保护规定。经过 CBPR 认证的主体在参与 CBPR 的成员国之间转移或接收个人数据时，被视为遵守适用的跨境数据传输要求。目前，有 9 个亚太经合组织成员国 / 地区参与了 CBPR 体系：美国、墨西哥、日本、加拿大、新加坡、韩国、澳大利亚、中国台湾地区以及菲律宾。

为了得到 CBPR 认证，公司需要根据特定的评估框架（即“CBPR 项目要求”）进行评估。该框架是基于亚太经合组织隐私体系而建立的，它包含了 9 条隐私原则：权责一致、预防损失、通知、选择、数据收集的限制、个人信息的使用、个人信息的完整性、安全以及数据的访问与更正。举例而言，CBPR 项目要求下用于评估公司的标准包括：公司隐私政策的可访问性与全面性、有关数据收集和同意的选择权的透明度、以及关于存储和保护个人数据的实施措施和标准。

41 需要注意的是，传输自由规定受到 CPTPP 的一系列分割的影响。例如，该规定不阻止成员国为了实现“合法政策目的”启用或保持数据本地化措施（详见 CPTPP 第 14.11 条的第三段和第 14.13 条的内容）。这一规定亦不能适用于政府采购、政府信息或金融机构（详见第 14.1 条以及第 14.2 条第 3 段的内容）。

环球律师事务所
GLOBAL LAW OFFICE
SINCE 1979

Wolters Kluwer
荷兰威科集团

荷兰威科集团是一家卓越的专业信息服务提供商。来自世界各地法律、商业、税务、会计、金融、审计、风险管理、合规和医疗卫生等领域的专业人士依靠威科集团提供的信息工具及软件解决方案，来高效率地管理其业务，为其客户提供卓有成效的服务，并在纷繁复杂的市场环境中取得成功。

自 1985 年起，威科集团进入中国内地市场，不仅依托卓越的信息服务经验及技术，更植根于本土环境与客户需求，为中国的财税、法律、金融、医疗领域的专业人士提供及时、准确、权威的信息解决方案。

威科集团 2019 年营业收入达 46.12 亿欧元，全球拥有约 19,000 名员工，在欧洲、北美、亚太和拉美地区运营，服务于全球客户。威科集团总部位于荷兰阿尔芬，是泛欧交易所上市公司，同时也是荷兰 AEX 指数和欧洲 100 指数的成分股。威科集团于 1985 年进入中国市场，是改革开放后早期进入中国市场的国外专业信息出版及服务商之一。随着中国业务的快速发展，威科的主要业务：卫生医疗、财税与会计、法律与法规以及金融与合规等四大业务板块全面进入中国，目前在华的员工已经超过 600 人，机构客户超万余家。

自 1836 年成立，威科集团的历史贯穿了两个世纪，承载了革新与重组：从 20 世纪之交的现代工业型经济，到互联网创始之初，再到今天；时光虽然汩汩流过，但是有些事情始终未变。虽然在 184 年的时间里我们历经了许多变化，但是有些事情没有改变：强健的价值和商业原则，对深度专业知识的追求，技术上的创新，以及最重要的一点：坚持致力于帮助客户做出正确决策。

在未来，我们将继续努力为客户提供价值。

环球律师事务所 GLOBAL LAW OFFICE SINCE 1979