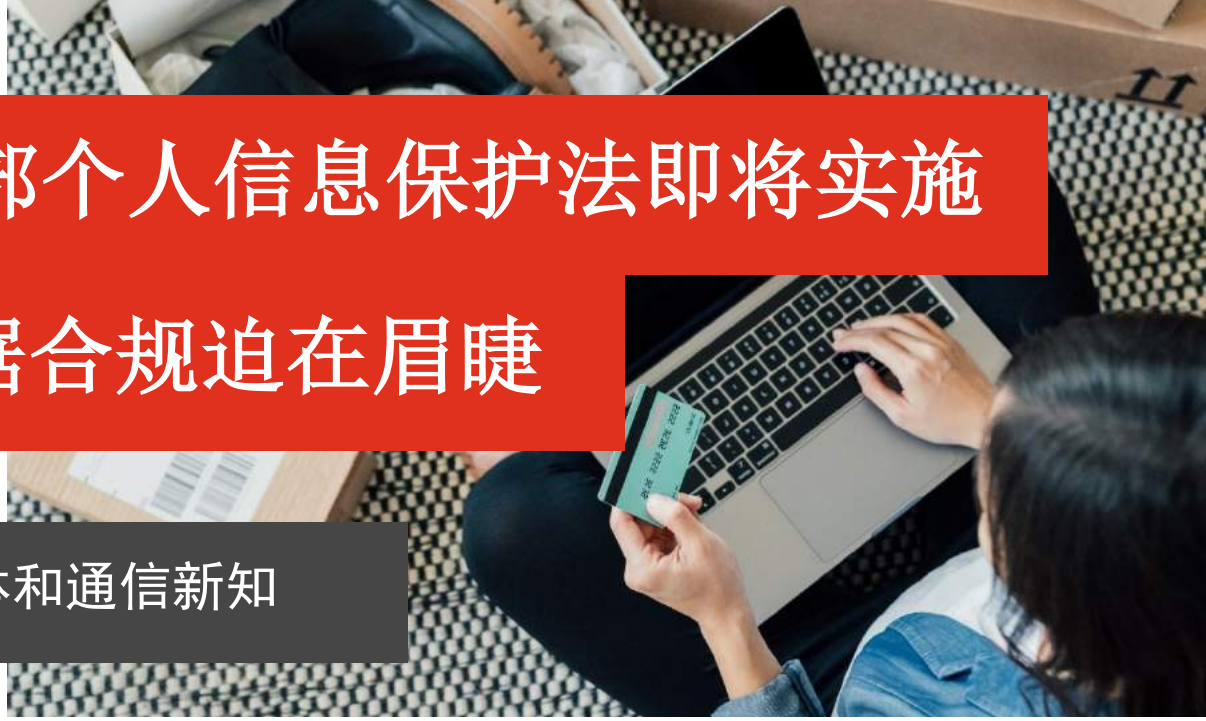


中国首部个人信息保护法即将实施

数据合规迫在眉睫

科技、媒体和通信新知

2021年8月

简介

期待已久的《个人信息保护法》（“个保法”）于2021年8月20日在十三届全国人大常委会第三十次会议20日表决通过，并将于2021年11月1日起施行。

相较于此前的二审稿，最终版本的个保法有诸多方面的变化值得关注，尤其是其将宪法纳入其立法基础，更加彰显中国立法者对于个人信息保护的重视。

需强调的是，个保法为企业的相关合规工作仅留下了两月余的时间，这对于企业而言无疑是十分紧迫的。本文将梳理个保法中相关合规要点，并结合我们在实践中积累的数据合规经验，为企业提供个人信息处理合规建议，以期为企业在这一关键窗口期中创造最大的合规价值。

1. 个保法适用于谁？

对于其适用，个保法坚持了二审稿当中的“属地管辖”原则，即：在中国境内处理自然人个人信息的活动均适用个保法，而无论处理者是否为中国境内实体，也无论其所处理的个人信息是否为中国公民或境内其他自然人的个人信息。

值得注意的是，个保法仍具有域外适用的效力——在中国境外处理中国境内自然人个人信息的活动，如有下列情形，也适用个保法：

1. 以向境内自然人提供产品或者服务为目的；
2. 分析、评估境内自然人的行为；
3. 法律、行政法规规定的其他情形。

在全球经济一体化的大背景下，境外公司通过跨境交付的方式在向中国境内消费者提供商品或服务的情形非常常见，在此过程中，不可避免地会涉及到收集、使用和处理中国消费者的个人信息。在实践中，有些境外公司并未履行中国相关法律法规所规定的义务，如告知同意原则、针对中国用户的隐私政策、个人信息主体权利等，主要原因之一是此前法律规定的不明确。但个保法的出台，为诸多跨国企业敲响了数据合规的警钟。

2. 何为个人信息？何为个人信息处理者？

个保法对于个人信息相关的重要定义进行了明确，为企业的合规工作提供了明确的方向性的指导。

个人信息

个人信息是指以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。这一定义明确了匿名化处理后的信息不适用于个保法，企业可据此对企业处理的信息进行处理、分类，减轻合规负担，但个保法未能明确匿名化处理后的信息如何界定，还有待于进一步澄清。

个人信息处理者

依据个保法，个人信息处理者，是指在个人信息处理活动中自主决定处理目的、处理方式的组织、个人。

这一定义类似于欧盟《通用数据保护条例》（GDPR）中规定的“数据控制者”的概念。依据GDPR，“控制者”指的是那些——不论是单独还是共同——决定个人数据处理目的与方式的自然人或法人、公共机构、规制机构或其他实体。

此外，个保法中提及了个人信息委托者的概念，即：受个人信息处理者的委托而处理个人信息的组织或个人，这与GDPR中规定的“数据处理者”的概念相似。依据GDPR，“处理者”指的是为数据控制者处理个人数据的自然人或法人、公共机构、规制机构或其他实体。

3. 个人信息处理有哪些法律基础？

个保法为处理个人信息的活动提供了7项法律基础，包括：

1. 取得个人同意；
2. 为订立、履行个人作为一方当事人的合同或者按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需；
3. 为履行法定职责或者法定义务所必需；
4. 为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需；
5. 为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息；
6. 依照本法规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；
7. 法律、行政法规规定的其他情形。

上述规定参照了GDPR的相关规定。虽然并未囊括GDPR项下的合法利益（legitimate interest）作为处理个人信息的法律基础，但已经在《网络安全法》的基础上实现了重大发展。《网络安全法》规定，数据收集和使用必须基于数据主体的同意，并没有明确规定无需同意的例外情况，收集个人信息毫无例外都需要数据主体同意，这种要求在实践中是否可行，曾在业界引起争论。

根据个保法的规定，信息主体的同意仍然作为原则性法律基础，但同时提供了第(2) – (7)项例外情形。值得注意的是，最终颁布的个保法新增了“按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需”作为一项新的法律基础，弥补了劳动雇佣活动中个人信息处理活动法律基础的空白。

4. 如何实现个保法要求的“同意”？

“告知+同意”仍是个人信息处理活动法律基础的核心。具体而言，“同意”需要满足哪些条件，是企业在个人信息合规实践中的重点。就“同意”而言，个保法也提出了以下要求：

1. 基于个人同意处理个人信息的，该同意应当由个人在充分知情的前提下自愿、明确作出（即上述告知要求）；
2. 个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，应当重新取得个人同意；
3. 基于个人同意处理个人信息的，个人有权撤回其同意。个人信息处理者应当提供便捷的撤回同意的方式；个人信息处理者不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务；处理个人信息属于提供产品或者服务所必需的除外。

依据上述要求，同意应是明示的、自愿的、明确的、可撤回的，这些要求基本与国际上的普遍实践相一致，有助于企业在处理跨法域的数据合规实践中保持协调、提高效率。

5. 如何处理敏感个人信息？

个保法规定，如下信息应被认定为敏感个人信息，包括：生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

个保法要求，只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息，且处理敏感个人信息应当取得单独的同意。就“告知”要求而言，除上述第4点所述，还应当向个人告知处理敏感个人信息的必要性以及对个人权益的影响。

针对不满十四周岁未成年人个人信息的处理，个人信息处理者应当取得未成年人的父母或者其他监护人的同意，且应当制定专门的个人信息处理规则。

6. 个人信息跨境传输需满足哪些要求？

依据个保法的规定，个人信息处理者因业务需要，可在满足下列条件之一的情况下，向境外提供个人信息：

1. 通过国家网信部门组织的安全评估；
2. 经专业机构进行个人信息保护认证；
3. 按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务；
4. 法律、行政法规或者国家网信部门规定的其他条件。

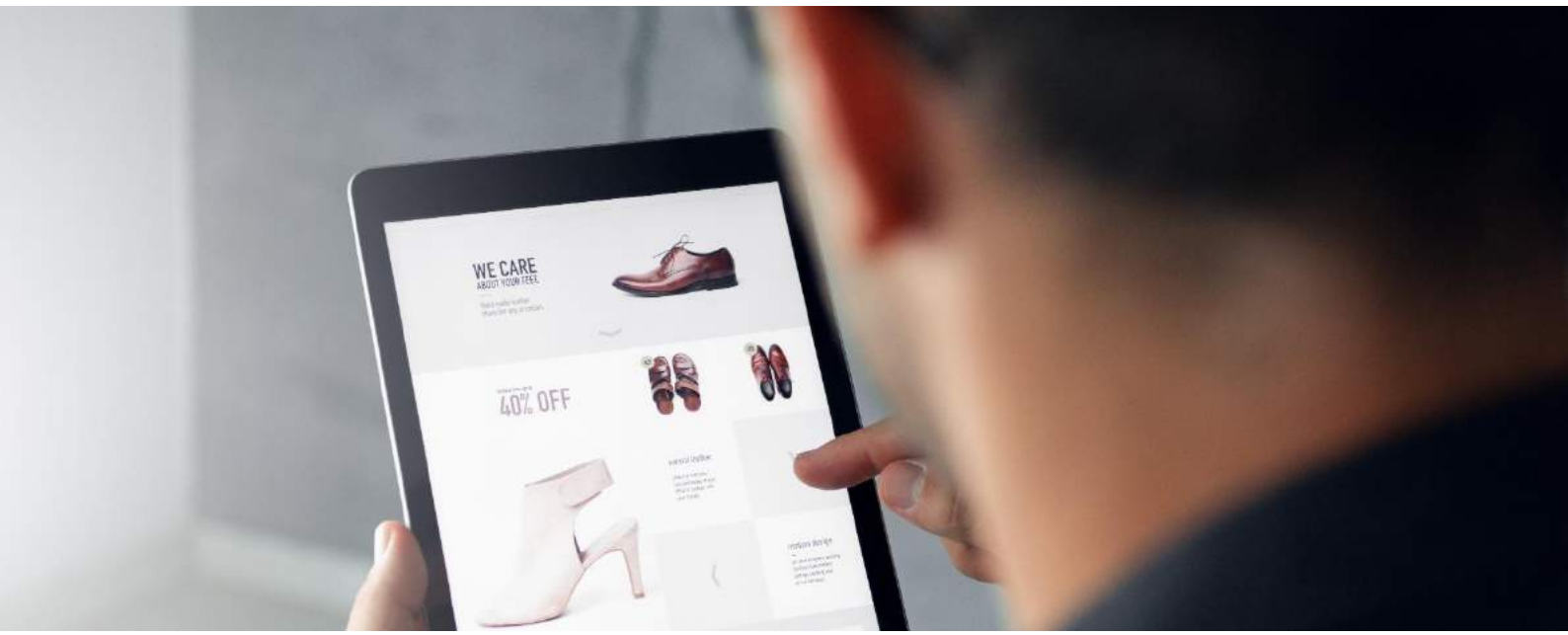
除上述要求外，个人信息处理者向中国境外提供个人信息的，应当向个人告知境外接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使本法规定权利的方式和程序等事项，并取得个人的单独同意。

对于数据本地化，个保法沿用了二审稿的作法——关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者，应当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，应当通过国家网信部门组织的安全评估。对此企业应当预先结合自身情况审查评估其是否适用数据本地化的要求。近期颁布的并将于2021年9月1日开始实施的《关键信息基础设施安全保护条例》，对于如何认定关键信息基础设施给出了更明确的指引，企业应及时评估其是否为关键信息基础设施运营者，以作出相应的合规安排。

可以看出，在数据跨境传输机制方面，个保法在某些方面与GDPR项下个人数据与非欧盟国家之间的传输规定有相似之处。根据GDPR，如需将个人数据传输至非欧盟国家，则需要欧盟委员会对数据传输目的国的数据保护水平进行充分性认定，建立白名单制度。如果个人信息出境的目标国不在白名单之列，则需要通过有法律强制力的协议或标准数据保护条款提供额外的保证。

另外，针对近期的数据合规执法案例，个保法重申：非经中华人民共和国主管机关批准，个人信息处理者不得向外国司法或者执法机构提供存储于中华人民共和国境内的个人信息。

针对境外组织和个人侵害中国公民的个人信息权益等的行为，国家网信部门可以将其列入限制或者禁止个人信息提供清单，予以公告，并采取限制或者禁止向其提供个人信息等措施。



7. 个人信息主体应有哪些权利？

个保法赋予了个人信息主体一系列的权利。值得关注的是，最终版的个保法借鉴了国外立法的经验，新增了可携带权，即数据主体有权请求将个人信息转移至其指定的个人信息处理者，符合国家网信部门规定条件的，个人信息处理者应当提供转移的途径。个保法中对与可携带权的规定仍有待进一步的细化，如转移的方式。更细化的规则后续有望出台，企业应密切关注。

8. 个人信息处理者应履行哪些义务？

个保法对于个人信息处理者规定了若干义务，其中以下内容尤为值得关注。

个人信息保护负责人及代表

类似于GDPR中的数据保护官的设置，个保法要求处理个人信息达到国家网信部门规定数量的个人信息处理者应当指定个人信息保护负责人，负责对个人信息处理活动以及采取的保护措施等进行监督。

此外，与GDPR相类似，个保法在特定情况下有域外管辖权。这意味着，在中国尚未设立营业场所或分支机构的外国公司，如果他们在中国境外的处理个人信息的行为落入到个保法域外效力的适用范畴，则需要尽快在中国境内设立专门机构或指定代表，负责处理个人信息保护相关事务，以满足个保法的此项法律要求。

个人信息影响评估

对于特定情形的个人信息处理活动，如涉及敏感个人信息的处理、自动化决策、委托处理、跨境传输等，个人信息处理者应进行个人信息保护影响评估并记录。

自动化决策

近年来，“大数据”杀熟的问题愈演愈烈，越来越多的企业利用大数据分析、评估消费者的个人特征用于商业营销。有一些企业通过非法获取面部识别信息、交易信息等个人信息掌握消费者的经济状况、消费习惯、对价格的敏感程度等信息，对消费者在交易价格等方面实行歧视性的差别待遇，误导、欺诈消费者。

对此，个保法明确规定个人信息处理者利用个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇。通过自动化决策方式作出对个人权益有重大影响的决定，个人有权要求个人信息处理者予以说明，并有权拒绝个人信息处理者仅通过自动化决策的方式作出决定。

9. 重大互联网平台的特殊义务

对于提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，个保法规定了更加严格的义务：

- 建立个人信息保护合规制度体系，成立主要由外部成员组成的独立机构对个人信息保护情况进行监督；
- 遵循公开、公平、公正的原则，制定平台规则，明确平台内产品或者服务提供者处理个人信息的规范和保护个人信息的义务；
- 对严重违反法律、行政法规处理个人信息的平台内的产品或者服务提供者，停止提供服务；
- 定期发布个人信息保护社会责任报告，接受社会监督。

实践中，互联网平台成为了侵害个人信息行为的重灾区，最终版本的个保法对二审稿中的相关规定进行了完善，值得互联网公司重点关注，并积极采取合规措施予以应对。

10. 主管机关和法律责任

个保法并没有规定单一的主管机关。具体而言，国家网信部门负责统筹协调个人信息保护工作和相关监督管理工作，国务院有关部门在各自职责范围内负责个人信息保护和监督管理工作。此外，县级以上地方人民政府有关部门也应履行个人信息保护和监督管理职责。

个保法对于个人信息违法行为设置了严格的处罚措施，值得企业关注。违反个保法处理个人信息的规定，或者未履行个人信息保护义务的，最高处罚可至没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照。而针对直接负责人员，除可达100万元的罚款外，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。

GDPR项下的罚款金额上限为2000万欧元或占全球年营业额的4%。由此可见，个保法的处罚力度与国际司法实践高度一致。

11. 合规建议

自2021年7月，多家互联网企业接受网络安全审查，数据安全再次成为关注焦点。据报道，接受审查的互联网企业均掌握行业内的深度用户隐私数据，有些业务与关键信息基础设施相关。为了强化数据安全治理，中国政府最近连出重拳在众多领域加大数据安全治理的执法力度。从修订《网络安全审查办法》征求意见稿到《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》，从《关键信息基础设施安全保护条例》到《汽车数据安全管理若干规定（试行）》，无一不彰显了中国政府对个人信息保护的重视程度和监管力度。

作为数据安全领域的基础法律，《个人信息保护法》与《数据安全法》和《网络安全法》并行成为网络空间治理和数据保护的三驾马车，共同构建起中国隐私保护、网络安全和数据安全的强大法律体系。《个人信息保护法》与《数据安全法》在本年内相继出台并将很快实施，不仅意味着国家已经完成数据安全治理的顶层设计，同时也宣告了数据合规强监管时代的到来，全行业即将面临合规重任。

为了对标国际司法实践，个保法的制定虽然参照了GDPR的相关规定，但个保法依然保留了鲜明的中国特色。因此GDPR项下的合规绝不代表个保法项下的合规。无论是否已经依据GDPR进行合规治理，个保法项下的合规治理和相应的整改措施都不可或缺。

鉴于个保法从最终颁布到正式实施只有2个多月的合规窗口期，中国企业和跨国企业均应尽快采取行动，高度重视并积极组织落实企业的个人信息合规工作。以下建议，供企业开展合规工作进行参考；

1. 针对不同的业务板块、产品，梳理企业个人信息处理活动的现状，个人信息在企业内部及外部流转的生命周期，以及各项处理活动的法律基础、记录、支持文件等；
2. 开展个人信息合规风险评估，识别企业个人信息处理活动风险点，确定各项风险点的风险等级，明确合规事项优先级别及侧重点，并对有关团队和人员进行培训；
3. 审查并评估企业当前的数据处理行为，对照《个人信息保护法》、《数据安全法》及其他有关法律规定的要求和行业实践，制定合规整改方案；
4. 组织实施合规整改方案，进一步审查完善相关文件（如隐私政策、数据主体的同意、数据处理协议等），优化数据处理流程，避免因不合规而给企业造成巨额处罚；
5. 在中国境外的个人信息处理企业，应尽快评估个保法是否对其适用。如果适用，则应依法在中国境内设立专门机构或者指定代表负责处理个人信息保护相关事务，并按照法律规定在政府部门完成信息报送义务；
6. 涉及数据跨境传输的企业，更应尽快完成本企业是否为关键信息基础设施运营者的评估，并积极关注网信部门规定的触发数据本地化要求的个人信息数据数量门槛，以及国家对数据出境安全评估的相关要求，确保数据合规出境。

联系我们

普华永道大中华区和全球的法律、隐私、网络安全和技术团队在数据法律和网络安全合规领域深耕多年，已经协助众多跨国公司和中国企业进行数据合规治理，在业内享有盛名。我们可以为客户合规和风险管理提供全方位多角度的一站式服务，如您希望就个保法或合规建议有更深入的了解，请与我们联系。

瑞栢律师事务所

李晓蓓
公司法主管
科技、媒体和通信及金融科技业务主管
barbara.xb.li@ruibailaw.com
+86 (10) 8540 4686

熊倩
高级经理
sarah.q.xiong@ruibailaw.com
+86 (10) 8540 4608

普华永道中国

周伟然
全球科技、媒体及通信行业主管合伙人
wilson.wy.chow@cn.pwc.com
+86 (755) 8261 8886

高建斌
中国内地科技、媒体及通信行业主管合伙人
gao.jianbin@cn.pwc.com
+86 (21) 2323 3362

贺琪伟
中国内地及香港风险及控制服务主管合伙人
jennifer.cw.ho@hk.pwc.com
+852 2289 2919

李睿
网络安全与隐私保护服务合伙人
lisa.ra.li@cn.pwc.com
+86 (10) 6533 2312