勤理.
Qinli Legal

法律评论

作者：

贾维恒
weihengjia@qinlilegal.com

曲晓琨
seanqu@qinlilegal.com

如欲垂询更多信息，请联络上海勤理律师事务所专业人士：

叶伟文
资深全球顾问
patyipqinli@qinlilegal.com

陈朕
codychen@qinlilegal.com

费亚力
alexfischer@qinlilegal.com

贾维恒
weihengjia@qinlilegal.com

陆易
cllu@qinlilegal.com

马骋
roma@qinlilegal.com

宋姣琳
jolsong@qinlilegal.com

葛向阳
xyge@qinlilegal.com

韩桢
zhenhan@qinlilegal.com

刘萍
liuping@qinlilegal.com

林泽军
jasonlinzj@qinlilegal.com

马锋
jasonma@qinlilegal.com

蒋利众
lzjiang@qinlilegal.com

棋子落定：《个人信息保护法》解读

中国《个人信息保护法》已于 2021 年 8 月 20 日通过，并将自 2021 年 11 月 1 日起施行。《个人信息保护法》与先前出台的《网络安全法》、《数据安全法》共同构成了网络安全、数据安全和个人信息保护领域的三大基础性法律。

一、 概述

《个人信息保护法》对于（1）个人信息的处理（包括跨境提供）规则，（2）个人在个人信息处理活动中的权利，（3）个人信息处理者的义务，（4）个人信息处理活动所涉各方的法律责任等内容作出了系统规定。其出发点是保护个人对于个人信息处理享有的权利，厘清企业等个人信息处理者应当遵循的规则和履行的义务，同时明确违法和侵权行为的法律责任。

二、《个人信息保护法》的要点

（一）“个人信息”与“敏感个人信息”

《个人信息保护法》对一般的个人信息和敏感个人信息进行了区分。个人信息是一个宽泛的概念，而敏感个人信息是个人信息的一个被特殊保护的部分。个人信息处理者根据其处理的信息不同，需承担不同的义务。

“**个人信息**是以电子或者其他方式记录的与**已识别或者可识别的自然人有关的**各种信息，不包括匿名化处理后的信息”（第 4 条）。

“**敏感个人信息**是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，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**”（第 28 条）。

关于个人信息、敏感个人信息的具体范围及其判定，还可结合、参照《信息安全技术 个人信息安全规范》（GB/T 35273-2020）等文件的规定进行。

另外，《个人信息保护法》规定被匿名化处理的个人信息不作为该法保护和规制的个人信息，“匿名化是指个人信息经过处理无法识别特定自然人且不能复原的过程”（第 73 条第 4 款）。

（二）“域内适用”与“域外适用”

《个人信息保护法》既规制在境内处理个人信息的活动，也规制在境外处理境内个人信息的活动（第 3 条），具体包括以下情形：

- 域内适用：在中国境内处理自然人个人信息的活动，即个人信息处理者、处理活动等在境内。例如，境内公司收集员工信息。
- 域外适用：即使个人信息处理者、处理活动等在境外，当其处理的个人信息为境内自然人的个人信息，且有下列情形的，《个人信息保护法》也将适用。

a. 以向境内自然人提供产品或者服务为目的；

b. 分析、评估境内自然人的行为；

c. 法定的其他情形。

据此，无论个人信息处理者是境内主体还是境外主体，亦无论处理的是境外自然人还是境内自然人的个人信息，只要处理活动发生在境内即受《个人信息保护法》规制；此外，即便处理活动发生在境外，只要个人信息处理者处理境内自然人的个人信息，并落入《个人信息保护法》规定的特定情形，也受《个人信息保护法》规制。一般而言，香港、澳门等属于“境外”范畴，因此，在香港、澳门等进行个人信息处理活动亦属于在“境外处理”。相应的，向香港、澳门等提供个人信息须遵守《个人信息保护法》规定的跨境传输规则（详见下文解读）。

（三）个人对他人处理自身个人信息的权利

个人信息主体就他人对其个人信息处理享有的权利包括：知情权、决定权、限制或拒绝处理权、查阅、复制权、可携权、要求更正和补充权、删除权、要求解释说明权等（第 44-50 条）。该等规定第一次系统明确了个人对其个人信息相关的权利主张，企业等个人信息处理者在制定个人信息保护政策时，应着重设计应对程序和制度。

（四） 处理个人信息应遵循的原则、规则

个人信息的“处理”涵盖全周期、各个环节，包括：“收集”、“存储”、“使用”、“加工”、“传输”、“提供”、“公开”、“删除”等活动（第 4 条）。

《个人信息保护法》规定了处理个人信息时，处理者应当遵循的原则，包括：合法、正当、必要和诚信原则，目的限制、最小必要原则，公开、透明原则，准确性原则，当责原则等（第 5-9 条）。根据这些大原则，《个人信息保护法》进一步对个人信息处理者在处理个人信息时应遵守的规则进行了详细规定，概要梳理和分析如下。

1. 取得同意

除特定情形外，个人信息处理者处理个人信息前应取得个人同意（第 13 条）。

作为例外之一，“为订立、履行个人作为一方当事人的合同所必需，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”的情形下，个人信息处理者可以在没有个人同意的情况下，处理相关个人信息。但是，个人信息处理者仍应当遵循各项处理原则、规制，不能非法、过度处理个人信息。基于本规定，公司处理员工的个人信息可以适用比较宽松的规则，与之相应的，制定合法的规章制度，也是公司当务之急。

此外，该法还规定了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**（第 14 条）；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（第 15 条）；以及特定个人信息处理活动应取得**单独同意**的情形。

2. 明确告知

除法定情形外，个人信息处理者在处理个人信息前，应以显著方式、清晰易懂的语言真实、准确、完整地向个人告知相关事项（包括：a.个人信息处理者的名称或者姓名和联系方式；b.个人信息的处理目的、处理方式，处理的个人信息种类、保存期限；c.个人行使权利的方式和程序；d.其他应当告知的法定事项）；并在相关事项变更时，将变更部分告知个人；通过制定**个人信息处理规则**的方式告知相关事项的，处理规则应当公开，并且便于查阅和保存（第 17、18 条）。

据此，由于任何企业都有可能成为个人信息的处理者，所以企业应当尽快制定、完善和公开个人信息处理规则，并及时更新。

3. 处理敏感个人信息的特殊规则

对于敏感个人信息的处理，《个人信息保护法》在一般个人信息处理规则之外，额外制定了下列特殊规则：

- 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。
- 处理敏感个人信息应当取得个人的**单独同意**（法律、行政法规规定应当取得**书面同意**的除外）。
- 除依法告知一般事项外，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**（依法可以不向个人告知的除外）。
- 处理不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的同意，并制定**专门的个人信息处理规则**。
- 遵循其他法律、行政法规对敏感个人信息处理的规定，如**取得相关行政许可或者其他限制**等。

此外，个人信息处理者处理敏感个人信息还应当事前进行**个人信息保护影响评估**（第 55 条）。

企业在经营活动中，涉及到处理个人敏感信息的情形非常常见。比如收集员工的家庭情况信息，在合规调查时收集员工的资产和金融信息，在开发客户业务过程中收集对方公司相关负责人的

背景信息等。《个人信息保护法》对于敏感个人信息的处理规定了比较严苛的条件和程序，对于企业经营中的个人信息保护合规提出了巨大的挑战。

4. 跨境传输规则

个人信息的跨境传输在《网络安全法》中也有提及，而《个人信息保护法》就跨境传输规则作了进一步规定（第 38-43 条）。

首先，个人信息处理者跨境传输个人信息应具备下列条件之一：

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

其次，个人信息处理者向境外传输个人信息前，应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权利的方式和程序等事项，并取得个人的**单独同意**。

第三，特定个人信息处理者，即关键信息基础设施运营者和处理大量个人信息的处理者，应当将在中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，须通过国家网信部门组织的安全评估。

第四，对于向外国司法或执法机构提供的特殊情形，《个人信息保护法》规定个人信息处理者不得擅自向外国司法或执法机构提供境内的个人信息，除非获得主管机关批准。

《个人信息保护法》关于境内收集和产生的个人信息在境内存储和跨境提供需通过安全评估的规定和《网络安全法》的思路一致，但《个人信息保护法》在《网络安全法》对于关键信息基础设施运营者的要求的基础上进一步要求“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”亦应遵循同等规则。目前，“规定数量”的界定尚不明确，有待国家网信部门后续释明。此外，国家此前曾就《个人信息出境安全评估办法（征求意见稿）》等文件公开征求意见，目前关于个人信息出境安全评估的具体规则亦不明确，《个人信息保护法》出台后，相信关于个人信息出境安全评估的细则亦将逐步落地。

《个人信息保护法》关于个人信息处理者非经批准不得向外国司法或执法机构提供存储于中国境内的个人信息的规定和《数据安全法》的思路一致。此前的实践中，以美国证监会对中国公司进行调查要求提交文件资料、要求境内会计师事务所提供审计底稿等案件为例，在资料出境前，通常需要由律师、法证技术专家参与进行涉密筛查，根据《保守国家秘密法》以及关于个人信息保护的相关法律法规等对国家秘密、个人信息等敏感信息进行屏蔽处理，进而出具相应工作报告和法律意见，以获取中国证监会的批准并最终出境。《数据安全法》和《个人信息保护法》施行后，对于外国司法、执法机构发起的跨境调查，包括刑事调查、行政调查，甚至民事诉讼过程中的调查等，境内当事人提交相关文件资料都应在遵守现行中国法律法规和中国参加的国际公约/条约的同时，按照上述两部法律的规定履行相关手续。

（五）个人信息处理者的义务

个人信息处理者除了应遵守上述个人信息处理的原则、规则等外，还应当履行《个人信息保护法》规定的下列义务（第 51-59 条）。

首先，所有个人信息处理者均应履行下列义务：

1. **采取合规管控措施**，包括：

- 制定**内部管理制度和操作规程**；
- 对个人信息实行**分类管理**；
- 采取相应的加密、去标识化、操作权限控制等安全技术措施；
- 定期对相关人员进行安全教育和培训；
- 制定并组织实施个人信息安全事件应急预案等。

2. **合规审计**，对其处理个人信息遵守法律、行政法规的情况进行**定期合规审计**。

3. **通报**，发生或者可能发生个人信息泄露、篡改、丢失的，立即采取补救措施，并依法通知主管部门和个人。

4. **个人信息保护影响评估**，下列情形应事前进行个人信息保护影响评估，并记录处理情况：

- 处理敏感个人信息；
- 利用个人信息进行自动化决策；
- 委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息；
- 向境外提供个人信息；
- 其他对个人权益有重大影响的个人信息处理活动。

其次，特定类型的个人信息处理者还应履行以下特别义务：

5. 境外的个人信息处理者，应在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，并将该等机构或代表的相关信息报送主管部门。

6. 处理大量个人信息的个人信息处理者应指定**个人信息保护负责人**，负责对个人信息处理活动等进行监督，同时要公开负责人的联系方式，并将负责人的相关信息报送主管部门。

7. 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，还应当：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；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；对严重违法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等。

关于个人信息分类管理问题，《个人信息保护法》的规定与《数据安全法》关于数据分类分级保护制度、加强重要数据保护的规定一脉相承。目前，关于重要数据目录、数据和个人信息分类、分级的统一标准尚不清晰，有待国家出台细则进行明确。《信息安全技术 个人信息安全规范》（GB/T 35273-2020）、《信息安全技术 健康医疗数据安全指南》（GB/T 39725-2020）等文件在不同程度上对数据和信息的范围判定、分类及定级制定了相应规范，具有一定参考价值。数据和个人信息处理者还需根据所处行业、自身业务等情况进行数据和个人信息分类、分级工作。

此外，由于《个人信息保护法》与《网络安全法》、《数据安全法》涉及的问题，如关键信息基础设施、个人信息和重要数据出境安全评估、数据和个人信息分类分级等问题，相互交织，而且需最终落实到技术措施层面执行，网络运营者/数据处理者/个人信息处理者有必要在网络和数据安全、个人信息保护问题上通盘考量，落实各方面的合规工作。

（六）法律责任

个人信息处理者违法处理个人信息，或者不履行个人信息保护义务，根据《个人信息保护法》第七章的规定，应承担相应法律责任，主要内容梳理如下。

1. 行政责任

- 视违法行为的情节严重程度而定，包括：

a. 对企业责令改正、给予警告、没收违法所得、责令暂停或者终止提供服务、处以**罚款（至高5,000万元或上一年度营业额5%）**、以及**责令暂停相关业务或停业整顿、吊销相关业务许可或者吊销营业执照**。

b. 对企业直接负责的主管人员和其他直接责任人员处以**罚款（至高100万元）**、以及**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**。

- 依法**记入信用档案**（进而可能受到监管部门各方面的联合惩戒），并予以公示。
- 构成违反治安管理行为的，依法给予治安管理处罚。

2. 民事责任

- **过错推定**：处理个人信息侵害个人信息权益的，如**个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任**。
- **公益诉讼**：个人信息处理者违法处理个人信息，侵害众多个人的权益的，**人民检察院、法律规定的消费者组织和由国家网信部门确定的组织可以依法向人民法院提起诉讼**。

我们注意到，实践中，已有公司因未举证证明其采取了有效措施保护信息安全而被法院判决就用户隐私信息泄露承担侵权责任[1]。该案中法院当时适用的证明标准还是过错责任原则，《个人信息保护法》确立了过错推定原则后，个人信息处理者无疑将承担更重的举证责任。

此外，值得注意的是，各级检察院已陆续在多个领域提起有关个人信息保护的民事公益诉讼（乃至行政公益诉讼和刑事附带民事公益诉讼）。最高人民检察院在《个人信息保护法》出台的次日（即2021年8月21日）即火速下发了《关于贯彻执行个人信息保护法推进个人信息保护公益诉讼检察工作的通知》，指导该类公益诉讼案件的办理。

3. 刑事责任

《个人信息保护法》也同时规定了违反该法构成犯罪的，应依法追究刑事责任。对此，《刑法》规定了侵犯公民个人信息罪等罪名，最高人民法院、最高人民检察院亦曾出台《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》，个人信息处理者对于违反《个人信息保护法》可能承担的刑事责任应足够重视，避免触碰红线。

[1] 庞理鹏与北京趣拿信息技术有限公司、中国东方航空股份有限公司隐私权纠纷二审民事判决书，(2017)京01民终509号。

二、结语

《个人信息保护法》的出台，补齐了中国网络、数据安全和个人信息保护领域立法的重要一环，其与《网络安全法》、《数据安全法》共同构成了该领域的三大支柱。尽管某些具体问题尚待相关配套细则落地澄清，随着《个人信息保护法》生效在即，各行业企业（尤其是关键信息基础设施运营者及其供应商，互联网、金融、医疗健康、汽车及出行等行业处理重要数据和大量个人信息的企业）都应当即刻，实际上很多企业已经开始，梳理、审阅自身业务、网络和信息系统、处理的数据和个人信息、组织架构、合规管理制度等，逐步推进合规工作并适时落地。

实践中，网络安全、数据安全、个人信息保护问题经常相互关联交错，网络、数据安全和个人信息保护领域的法律、法规等文件又繁多而交织，企业应当统筹管理、技术、法律及合规等资源应对该领域的合规工作，包括搭建合规体系、完善合规管理制度、落实相关技术措施等，做好准备以迎接执法和司法的考验。

本文由上海勤理律师事务所为本所中国大陆及香港之客户及员工编制，内容只供信息提示与参考之用，并不代表本所对相关事项的全部理解，也不构成任何法律建议。在您就本文中涉及的事项做出商业决策前，请务必咨询合资格的专业顾问。如欲垂询有关本文的资料或其它意见，请联络：

叶伟文
资深全球顾问
patyipqinli@qinlilegal.com

陈朕
codychen@qinlilegal.com

费亚力
alexfischer@qinlilegal.com

贾维恒
weihengjia@qinlilegal.com

陆易
cllu@qinlilegal.com

马骋
roma@qinlilegal.com

宋姣琳
jolsong@qinlilegal.com

葛向阳
xyge@qinlilegal.com

韩桢
zhenhan@qinlilegal.com

刘萍
liuping@qinlilegal.com

林泽军
jasonlinzj@qinlilegal.com

马锋
jasonma@qinlilegal.com

蒋利众
lzjiang@qinlilegal.com

关于上海勤理律师事务所

上海勤理律师事务所是 Deloitte Legal 全球网络成员。上海勤理律师事务所编制、发布了本《法律评论》系列刊物，对较为常见的法律问题以及最新进展进行介绍与评论。上海勤理律师事务所定期与政府部门及权威机关就新近出现的法律问题及相关发展进行沟通及商议，并针对相关问题撰写深入评析，提供专业意见。如欲垂询，请联络：

上海勤理律师事务所
中国上海市延安东路 222 号
外滩中心 15 楼第 5 单元
邮政编码：200002
电话：+86 21 6141 1718
传真：+86 21 6335 0003
www.qinlilegal.com