

网安法、个保法、数安法下的法律责任

作者：潘永建 | 杨迅 | 杨坚琪 | 胡鑫超

数字经济方兴未艾，正在日益与互联网、人工智能、云计算等行业深度融合发展。数据是数字经济的重要支撑，已成为除土地、劳动力、资本和技术外的第五类“生产要素”。数据保护与规范亟需法律从个人信息与隐私保护、企业数据权益、国家安全与监管等维度作出系统性的制度安排。作为数据保护制度的基础法律，《个人信息保护法》和《数据安全法》的重要性毋庸置疑。2021年4月29日，《个人信息保护法(草案二次审议稿)》《数据安全法(草案二次审议稿)》公布。从企业使用数据和合规遵从的视角，通力网安数据业务小组对审议稿作出系列解读，本文为第六篇《网安法、个保法、数安法下的法律责任》。

在本系列的前几篇文章中，我们已对《个人信息保护法(草案二次审议稿)》(以下简称“《个保法》”)和《数据安全法(草案二次审议稿)》(以下简称“《数安法》”)中的重点和亮点从多个维度进行了梳理和解读。尽管在《个保法》和《数安法》的框架下，数据安全保护制度已经初步建成，但该制度是否能够被有效执行，仍然取决于违法行为是否承担法律责任，以及权利主体能否得到充分救济。

相较于《网络安全法》(以下简称“《网安法》”),《个保法》和《数安法》对违反规定处理数据的法律后果作出更具针对性的规定，将对企业的业务运营产生直接的影响,有一些法律后果甚至直接决定企业的生死存亡。本文拟比较归纳《网安法》《个保法》《数安法》下的法律责任，就《个保法》和《数安法》的新变化和新要求作出提示，希望为相关企业预判和把握法律风险提供有益参考。

.....
如您需要了解我们的出版物,
请联系:

Publication@llinkslaw.com

1. 未履行安全保护义务

1) 数据安全保护

《网安法》	《数安法》
第五十九条 网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。 关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。	第四十四条 开展数据处理活动的组织、个人不履行本法第二十六条、第二十八条、第二十九条、第三十条规定的数据安全保护义务的，由有关主管部门责令改正，给予警告，可以并处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；拒不改正或者造成大量数据泄露等严重后果的，处五十万元以上五百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上五十万元以下罚款。

【条文解读】

相较于《网安法》，《数安法》大幅加重了企业及相关责任人员未履行数据安全保护义务的法律责任：

- 对企业而言：当其未按照网络等级保护制度要求履行数据保护义务，或在发生数据安全事件时未及时补救并履行报告义务时，其罚款标准从原先的“1 万元以上 10 万元以下”提高至“5 万元以上 50 万元以下”，拒不改正或造成严重后果时，甚至可能受到暂停相关业务、停业整顿、吊销相关业务许可证或营业执照、以及高达 500 万元的罚款处罚。
- 对责任人员而言：除直接负责的主管人员外，《数安法》将“其他直接责任人员”纳入到责任主体的范围内，且对其罚款的额度最高将达 50 万元。

2) 个人信息保护

《网安法》	《个保法》
第六十四条 网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改	第六十五条 违反本法规定处理个人信息，或者处理个人信息未按照规定采取必要的保护措施，由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得；拒不

正, 可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款, 没有违法所得的, 处一百万元以下罚款, 对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款; 情节严重的, 并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。 违反本法第四十四条规定, 窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息, 尚不构成犯罪的, 由公安机关没收违法所得, 并处违法所得一倍以上十倍以下罚款, 没有违法所得的, 处一百万元以下罚款。	改正的, 并处一百万元以下罚款; 对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。 有前款规定的违法行为, 情节严重的, 由履行个人信息保护职责的部门责令改正, 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、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; 对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款。
--	---

【条文解读】

同样地,《个保法》承继了严厉惩罚个人信息违法行为的国际通行做法, 设置了更为严格的法律责任。对于“情节严重”的违规处理个人信息行为, 违法企业可能被处以 5000 万元以下或者 上一年度营业额5%以下罚款。而相关责任人的罚款数额也大幅提高, 将可能受到高达百万的惩处。

尽管本条提出了如此高额的罚款规定, 但具体何种违法行为将落入“情节严重”的范围,《个保法》尚未作出明确界定, 有待监管部门出台更为细致的规则指导行政裁量。但无论如何,《个保法》看齐 GDPR 的罚款上限将大大增加企业的违法成本, 遏制企业违法违规处理个人信息的行为。

2. 重要数据出境

《网安法》	《数安法》
第六十六条 关键信息基础设施的运营者违反本法第三十七条规定, 在境外存储网络数据, 或者向境外提供网络数据的, 由有关主管部门责令改正, 给予警告, 没收违法所得, 处五万元以上五十万元以下罚款, 并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照; 对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。	第三十条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理, 适用《中华人民共和国网络安全法》的规定; 其他数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理办法, 由国家网信部门会同国务院有关部门制定。 第四十四条 开展数据处理活动的组织、个人不履行本法第二十六条、第二十八条、第二十九条、第三十条规定的数据安全保护义务的, 由有关主管部门责令改正, 给予警告, 可以并处五万元以上五十万

	元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；拒不改正或者造成大量数据泄露等严重后果的， 处五十万元以上五百万元以下罚款 ，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照， 对直接负责的主管人员和其他直接责任人员处五万元以上五十万元以下罚款 。
--	---

【条文解读】

不同于原先《网安法》仅针对关键信息基础设施运营者(CIIO)的重要数据出境活动作出限制，《数安法》将**普通的数据处理者(即 CIIO 之外的数据处理者)**的重要数据出境也纳入监管范围，并明确其相应的法律责任。根据目前《数安法》的规定，CIIO 应在中国境内存储重要数据，确需对外提供应通过安全评估，否则将按照《网安法》第六十六条进行处理；而其他数据处理者如违反后续相关配套管理办法的规定，则根据《数安法》第四十四条予以处罚。

我们理解，对违规出境重要数据的处罚，《数安法》与《网安法》整体上保持一致，即由有关主管部门责令改正、警告、处 **5 万元以上 50 万元以下** 罚款、直接责任人员 **1 万元以上 10 万元以下** 罚款等。值得注意的是，虽然《数安法》第四十四条明确了“拒不改正”和“造成严重后果”的法律责任(包括对违法处理者处以 **50 万以上 500 万** 以下的罚款等，以及对直接责任人员处以 **5 万元以上 50 万元** 以下的罚款)，但是却未能明确在 CIIO 违规出境重要数据造成严重的情况下，是仅基于《网安法》第六十六条进行处罚，还是同样受到《数安法》第四十四条的约束。从体系解释的角度来看，如果 CIIO 仅受到《网安法》第六十六条的约束而不受到《数安法》第四十四条约束的，那么非 CIIO 的普通数据处理者甚至可能受到更严厉的处罚，这显然不符合立法者的制度设计要求。为确保相关规定的合理性，《数安法》第四十四条未来是否同样能够适用于 CIIO，有待立法者予以澄清。

3. 未经审批对外提供数据

《个保法》	《数安法》
第四十一条 中华人民共和国境外的司法或者执法机构要求提供存储于中华人民共和国境内的个人信息的， 非经中华人民共和国主管机关批准，不得提供 ；中华人民共和国缔结或者参加的国际条约、协定有规定的，可以按照其规定执行。	第四十六条 违反本法第三十四条规定， 拒不配合数据调取的 ，由有关主管部门责令改正，给予警告，可以并处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款。
第六十五条 违反本法规定处理个人信息，或者处理个人信息未按照规定采取必要的安全保护措施的，由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得；拒不改正的，并处一	违反本法第三十五条规定， 未经主管机关批准向境外的司法或者执法机构提供数据的 ，由有关主管部门责令改正，给予警告，可以并处十万元以上一百万元以下罚款，对直接

百万元以下罚款;对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。 有前款规定的违法行为,情节严重的,由履行个人信息保护职责的部门责令改正,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、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;对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款。	负责的主管人员和其他直接责任人员可以处二万元以上二十万元以下罚款。
--	-----------------------------------

【条文解读】

《个保法》和《数安法》均规定了向境外司法或执法机构提供数据的事先审批要求。对于这一要求,《数安法》第四十六条新增了“未履行报批义务”需要承担法律责任,但《个保法》尚未参照《数安法》第四十六条的规定,就“未经审批向境外机构提供个人信息”的行为制定专门对应的法律后果(目前《个保法》仍然通过第六十五条的统一规定对违反《个保法》的要求处理个人信息实施行政处罚)。

实践中,大量跨国企业存在向境外监管机构提交境内数据的情况,例如:

- 在华开展业务的跨国金融机构,出于反洗钱与反恐怖融资监管要求,需向母国提供金融数据;
- 在美上市外国公司需根据《外国公司问责法案》向美国公众公司会计监督委员会(PCAOB)提交会计师事务所出具的审计报告;
- 美资企业依据“澄清境外数据合法使用法案”(CLOUD Act)规定,配合美国政府的执法部门提供其在全球范围内控制的数据。

如我们在[《个人信息保护法和数据安全法二审稿对跨国金融机构的影响》](#)中所述,履行上述义务可能会导致在华的企业面临法律上的“困境”,即一方面需要依据境外监管部门的要求需要及时提供境内的数据,另一方面依据中国法律的要求则根据审批后方可提供。

4. 个保法下的举证责任

《个保法》
第六十八条 个人信息权益因个人信息处理活动受到侵害,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。

【条文解读】

互联网时代,个人信息处理活动具有技术性和隐蔽性,一般的用户无法理解其个人信息如何被处理,更遑论证明处理者的处理行为与自身个人信息被侵害之间的因果关系。司法实践中,考虑到原告举

证能力有限, 尽管依据法律要求个人信息相关的侵权纠纷仍适用“过错原则”, 但法院会在一定程度上减轻原告的证明责任。例如, 在“庞某与北京趣拿信息技术有限公司等隐私权纠纷案”[(2017)京 01 民终 509 号]中, 北京市第一中级人民法院认为, 原告已举证证明被告具有泄露信息的高度盖然性, 故需由被告提供证据表明已采取措施尽到保护客户信息安全的职责。“申某与上海携程商务有限公司等侵权责任纠纷案”[(2018)京 0105 民初 36658 号]则延续了这一裁判思路: 在本案中, 北京市朝阳区法院认为, 原告证明其将个人信息提供给被告后在较短时间内发生信息泄露, 即已完成合理的举证义务, 则被告应就个人信息泄露无故意或过失的事实负举证责任。

《个保法》吸收司法实践中的经验, 在第六十八条确立了侵害个人信息纠纷中的“过错推定责任”, 即个人信息处理者需自行证明其没有过错。第六十八条体现了通过举证责任的转移实现对个人信息主体的倾向性保护。一般而言, 处理者需就个人信息泄露承担责任, 而责任的多寡将与其安全保护措施完善程度直接相关。根据以往案例, 法院会从企业的技术防护措施、安全管理制度、人员访问权限、监控情况等方面判断企业的安全管理是否存在漏洞。我们理解, 制定并落实完善的内部组织架构和制度流程能够有效证明企业尽到个人信息安全保护的义务, 相应地减少需承担的损害赔偿赔偿责任。

通常, 企业可以自查如下的要点(并非全部), 以检视是否设置合理的内部制度:

- 是否设置专门的个人信息保护负责人;
- 是否制定信息安全管理、数据分级分类制度、访问权限制度等;
- 是否制定个人信息保护政策;
- 是否制定信息安全应急预案并定期进行安全演练;
- 是否制定与客户、经销商、供应商之间关于个人信息处理的制度;
- 是否按照个人信息审计制度定期开展审计;
- 是否按照个人信息安全影响评估制度开展评估。

5. 个人信息保护公益诉讼

《个保法》
第六十九条 个人信息处理者违反本法规定处理个人信息, 侵害众多个人的权益的, 人民检察院、履行个人信息保护职责的部门和国家网信部门确定的组织可以依法向人民法院提起诉讼。

【条文解读】

尽管《民法典》确立了信息处理者违反规定处理个人信息需承担的民事责任, 但由于个人信息保护取证难、维权成本高等问题, 实践中受到侵害的个人信息主体通常会选择放弃诉至公堂。考虑到侵犯公民个人信息的违法行为往往涉及到的信息数量巨大, 受侵害主体多, 立法者通过公益诉讼的方式加大监督和维权力度, 具有合理性和必要性。

实际上, 个人信息保护检察公益诉讼已具有一定实践。最高人民检察院于 4 月 22 日公布的 11 个“检察机关个人信息保护公益诉讼典型案例”中, 既涉及快递、医疗机构、校外培训机构等泄露个人信息

的案件，也包括 App 运营者违法违规收集个人信息和非法获取个人信息并进行消费欺诈的情形，还有涉及通过技术软件、物业服务等不同手段非法获取并交易个人信息的行为。在这些案件中，检察机关不仅向违法者主张公益损害赔偿，还依法追究其刑事责任并处以高额罚金。据了解，全国已有 25 个省级人大常委会作出关于加强检察公益诉讼工作的决定，其中有 19 个省份明确要求检察机关积极开展个人信息保护领域公益诉讼。

虽然“履行个人信息保护职责的部门和国家网信部门确定的组织”有待明确，但《个保法》第六十九条确立的公益诉讼制度必然改变以往个人信息保护领域低概率的维权和极低的违法成本的情况，个人信息相关的违法活动将受到政府和社会更多的监督 and 关注。

如您希望就相关问题进一步交流，请联系：



潘永建
+86 21 3135 8701
david.pan@llinkslaw.com



杨 迅
+86 21 3135 8799
xun.yang@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系: master@llinkslaw.com

上海

上海市银城中路 68 号
时代金融中心 19 楼
T: +86 21 3135 8666
F: +86 21 3135 8600

北京

北京市建国门北大街 8 号
华润大厦 4 楼
T: +86 10 8519 2266
F: +86 10 8519 2929

深圳

深圳市南山区科苑南路 2666 号
中国华润大厦 18 楼
T: +86 755 3391 7666
F: +86 755 3391 7668

香港

香港中环遮打道 18 号
历山大厦 32 楼 3201 室
T: +852 2592 1978
F: +852 2868 0883

伦敦

1/F, 3 More London Riverside
London SE1 2RE
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323



www.llinkslaw.com



Wechat: Llinkslaw

本土化资源 国际化视野

免责声明:

本出版物仅供一般性参考，并无意提供任何法律或其他建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

© 通力律师事务所 2021