**《个人信息保护法》下互金企业的民事法律风险及合规方案**

庄燕君等人

2021年8月20日，第十三届全国人民代表大会常务委员会第三十次会议表决通过了《个人信息保护法》（以下简称“《个保法》”），并将于2021年11月1日起正式实施。《个保法》在第七十条专门设置了公益诉讼条款，明确将个人信息保护的民事责任纳入检察公益诉讼法定领域。次日，最高人民检察院下发《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》（以下简称“《通知》”），明确要求推动公益诉讼条款落地落实，推动形成个人信息保护多元共治新格局。

对于互联网与金融企业而言，其业务模式决定了企业的经营活动频繁关涉个人信息处理活动，其业务规模亦决定了个人信息处理活动的体量，如若互金企业未能合法合规地收集、使用、提供、公开个人信息，极易触发民事、行政与刑事等多元法律风险。特别是以检察机关提请公益诉讼为路径的民事救济，带有极强的政府监管色彩，互金企业应当充分认识到该类公益诉讼对涉案企业的重大影响。如何防范民事法律风险，将成为互金企业建设个人信息保护制度的工作重点之一。

**一、个人信息保护多元共治格局下的民事法律风险与公益诉讼**

《网络安全法》、《数据安全法》与《个保法》共同构建起网络空间治理和数据保护的规范体系。然而，前两者均是以侵害网络安全和数据安全的行政责任和刑事责任为其规范保障，而《个保法》除了设置相关行政责任与刑事责任外，还特别设置了民事责任作为对侵犯公民个人信息权益的救济途径。这一制度设计的法律效果在于，对于高度依赖个人信息处理活动的互金企业而言，其《个保法》项下的民事法律风险显著提高，且涉案企业会因该民事责任面临更为不利的后果。

1. **《个保法》相关规则导致民事法律风险显著提高**

《个保法》项下的民事责任具有以下两个显著特征，其功能均在一定程度上导致个人信息处理者的民事法律风险有所提高。

第一，在举证责任方面，《个保法》实行举证责任倒置规则。《个保法》第六十九条第一款规定，处理个人信息侵害个人信息权益造成损害，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。不同于“谁主张，谁举证”的一般规则，除非个人信息处理者能够证明自身在被控侵犯公民个人信息权益的行为中不存在过错，否则承担民事侵权责任。举证责任的倒置，为个人信息处理者增加了更强的证明责任，这也使得个人信息处理者应诉成本显著增加，承担民事侵权责任的风险显著提高。在司法实践中，相关案例显示互联网企业在处理个人信息过程中因无法证明不存在过错而承担相应的民事责任。[[1]](#footnote-1)

第二，在救济途径方面，《个保法》对侵犯众多个人信息权益的案件设立公益诉讼。在侵害个人信息权益的案件中，原告（被侵权人）往往是个人信息权益的所有人（自然人）。由于受到时间精力、财力物力的限制，加之当今对个人信息的处理往往牵涉互联网专业技术，因此自然人在主张侵权损害赔偿时，往往在调查取证上遇到相当大的障碍而难以获得理想的效果。《个保法》第七十条针对侵犯众多个人信息权益的行为，允许以检察院等机关或组织为原告向人民法院提起公益诉讼。相较于自然人极其有限的调查取证手段，《人民检察院公益诉讼办案规则》（以下简称“《公益诉讼规则》”）第三十五条第一款赋予了检察机关更为有效的调查取证手段。一方面，检察机关可以向有关单位和个人询问情况、收集证据、勘验现场，相较于个人取证，有关单位和个人的配合程度更高，取得有利证据的可能性更大。另一方面，检察机关可以咨询专业人员或专业机构，委托鉴定、评估等，以获取有利证据，而自然人往往缺乏财力和资源采取这些手段的。因此，在检察机关提起公益诉讼的情况下，原告调查取证的能力更为强大，更加有可能取得证明涉案企业民事责任的证据。

1. **公益诉讼对涉案企业的不利影响**

相较于民事责任的一般救济途径，公益诉讼具有更强的政府监管色彩，其独特的运行机制在一定程度上导致涉案企业面临更为不利的后果。

第一，涉案企业所面临的赔偿数额量级更高，达到“1+1＞2”的效果。《个保法》第七十条明确规定，提起公益诉讼的前提是“侵害众多个人的权益的”，这导致涉案企业面临的赔偿数额在量级上有明显提高。如果由受到侵害的自然人单独提起民事诉讼，不少受侵害的自然人可能没有意识到自己的个人信息受到了侵害，或者考虑到司法程序较为复杂而放弃提起诉讼。但是，在民事公益诉讼中，一方面，检察院通过公告的形式，可以让更多未能意识到个人信息受到侵害的自然人主张权利，另一方面，自然人的调查取证、主张赔偿的成本显著降低，促使更多受害者主张权利。因此，一旦涉案企业败诉，其承担的赔偿金额将远高于由自然人提起诉讼时其所承担的赔偿。此外，公益诉讼中检察机关更加强大的调查取证能力，可能获取更多不利于涉案企业的证据，导致涉案企业在败诉的同时承担更高的赔偿金额。同时，检察机关在调查取证时所采用的专业手段，价格相对较为高昂，一旦涉案企业败诉，将承担更高的诉讼费用。

第二，公益诉讼促使民事调查与行政、刑事调查的衔接更高效。《通知》明确要求，各级检察机关要积极稳妥办理涉及互联网平台企业的相关案件，加强与行政机关协作配合，健全行政执法与公益诉讼检察衔接机制。一方面，未来检察机关将在个人信息保护领域和有执法权的行政机关加强配合，可能采取包括证据共享在内的各种方式，推动行政执法进程加速。因此，涉案企业可能在面临人民检察院提起的民事公益诉讼的同时，还需要接受包括市场监管部门、公安部门的行政调查。另一方面，如果涉案企业被公安机关列为侵犯个人信息犯罪的刑事调查对象，除了向公安机关共享取得的证据外，由于案件证据材料相对更加完整，检察机关也可能加快审查起诉阶段的进程，使得刑事调查与民事公益诉讼、行政调查的衔接更加紧密、高效。因此，《个保法》中公益诉讼的确立，可能形成未来侵犯个人信息刑事、行政、民事责任“三管齐下”的格局，大大增加涉案企业的应对、处理成本，为企业的日常运营带来沉重负担。

第三，公益诉讼的公告机制致使涉案企业面临对商誉的不利影响。在现代社会的企业经营中，声誉是企业重要的“软资产”之一。在业内和公众中拥有较高声誉的企业，往往能够获得更多的商业机会，以扩张商业版图；一旦企业被曝出违法、违规等负面消息，小则股价下跌，大则因为失去公众和商业伙伴信任而走向没落。与普通的民事诉讼不同，《公益诉讼规则》第九十一条明确规定，民事公益诉讼中，人民检察院认为社会公共利益受到损害，存在违法行为的，应当在具有全国影响的媒体发布公告，公告期间为三十日。相关企业一旦因为侵害公民个人信息而被人民检察院提起公益诉讼，除了可能的侵权损害赔偿外，还可能面临巨大的声誉损失和商业机会损失。

**二、互金企业降低个人信息保护项下民事法律风险的合规方案**

鉴于互金企业在个人信息保护项下具有较高的民事法律风险，且公益诉讼的救济途径在一定程度上对涉案企业造成更大范围的不利后果，互金企业应当将防范民事法律风险作为建设个人信息保护制度的工作重点之一。我们认为，构建完善的个人信息保护合规体系是降低民事法律风险的最佳解决方案。

1. **合规体系对互金企业的重大意义**

合规体系对互金企业的意义首先在于帮助企业切割个保法项下的民事责任。从国内外的行政和刑事执法的经验上看，拥有一套完善的合规体系能够在很大程度上降低甚至免除企业的行政和刑事责任。这一解决方案同样适用于《个保法》项下的民事责任。这是因为，《个保法》民事责任以过错责任为基础，只要涉案企业能够证明其业已搭建一套完善的合规体系并充分贯彻落实，即可主张其不存在过错，进而切割民事责任。一套完善的事前合规制度，有效而严格的事中合规检查和实施，及时的事后内部调查和合规制度更新，可以在很大程度上证明企业已经尽最大可能完成了对个人信息的保护义务，进而切割企业所面临的民事责任，由违反公司制度的员工个人承担侵权责任。

合规体系更为积极的意义在于帮助互金企业建立违法犯罪的预防体系，进而营造企业良好的合规文化。一套完善的合规体系，在很大程度上可以预防违法犯罪的发生。第一，企业对经营业务的各个环节建立严格的制度，既可以避免系统性的较大的合规风险，也可以降低企业员工利用企业管理漏洞从事违法违规行为的风险，达到使员工“不能违法犯罪”的目的。第二，企业加强对合规制度的教育培训，也可以使员工意识到违法行为的后果严重性，并且向员工传达企业对不合规行为的零包庇、零姑息态度，达到使员工“不敢违法犯罪”的目的。第三，企业通过对员工有关合规制度的宣传培训，营造出企业良好的合规文化与氛围，达到使员工“不想违法犯罪”的目的。

1. **如何为互金企业搭建合规体系**

健全的合规体系应当包括制度建设、合规体检、内部调查等事前、事中、事后三个维度。具体就互金企业所涉个人信息保护保护合规工作而言，则应当包括如下三方面内容：

第一，针对行业一般风险和互金企业的特别情况建立个人信息保护合规制度。企业合规体系构建的本质目的是“防患于未然”。在合规风险尚未转化为实际的法律责任之前，企业应当充分评估所在行业的一般风险和企业自身面临的特别风险，并通过建立合规制度最大程度消除法律责任风险。就个人信息保护而言，互金企业所面临的行业一般风险包括企业未经授权或超越权限采集公民个人信息数据、企业或其员工传播或倒卖个人信息问题、个人信息处理不当导致的个人信息泄露问题等。针对这些问题，互金企业应当制定关于个人信息收集、存储、使用、加工、传输、提供、公开、删除等活动的设备技术要求与程序要求。同时，互金企业还应当根据其主营业务、经营范围、营业规模、所在地的监管形势等因素，为该互金企业所面临的特别化合规风险制定特别的合规制度。

第二，针对企业合规制度及其实施情况进行合规体检。合规制度的建立只是合规体系构建的第一步，互金企业还应当确保合规制度严格落实到其日常经营中。日常经营中对合规制度的落实，主要通过进行定期全方面合规体检和不定期的专项合规体检得以保证。全方面合规体检的内容包括但不限于：（1）合规制度是否因为法律法规的更新、执法标准的变化而落后，是否需要针对企业的业务拓展和变化而补充、修订；（2）合规制度是否在企业的日常运营中得到充分遵守；（3）企业对合规制度的执行是否存在强有力的监督。不定期的专项合规体检将针对企业合规制度中的某项或者某几项合规制度，进行专门的检查。

第三，针对已发生的合规风险展开内部调查，完善合规制度。即便合规制度再完善、执行监督再严格，企业也难免会面临紧急的合规风险。出现合规风险后，企业首先应当对违反国家法律法规和企业相关制度的员工展开内部调查，并对员工违法违规的证据予以固定，以确保在未来可能面临的刑事和行政执法中配合政府部门的调查，减轻企业责任。在处理完合规风险后，企业也应当总结本次合规风险发生的原因，并将获得的经验教训体现在企业的合规制度中，以避免重蹈覆辙，遭受更为严厉的处罚。

1. 详见北京市第一中级人民法院（2017）京01民终509号民事判决庞理鹏诉过北京趣拿信息技术有限公司案，《最高人民法院发布第一批涉互联网典型案例》，载《人民法院报》2018年8月17日。 [↑](#footnote-ref-1)