国标要不要遵守?个人信息保护法给你答案

作者：潘永建 | 杨迅 | 朱晓阳 | 王雪莹

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，本文为第二篇《国标要不要遵守？个人信息保护法给你答案》。

企业对于《信息安全技术 个人信息安全规范》(“个人信息安全规范”)等个人信息保护国标无疑是纠结的。一方面，这些国家标准规定了个人信息保护的最佳实践，另一方面，这些仅仅是推荐性的国家标准，本身并无强制力，不遵守似乎也不会导致任何形式的处罚(笔者注：当然这一理解并不准确，因为执法机关会以该等国标作为对于法律条文的解释和执法依据)。

《个人信息保护法(草案二次审议稿)》(“二审稿”)或许可以结束这种纠结。在二审稿之前，中国已经有大量的个人信息领域的法律法规和国家标准，与其“另起炉灶”，在此基础上将已有的规定予以整合、改进，成了二审稿的最佳选择。以现行法律法规和国家标准为参考系，二审稿大量整合了此前对于个人信息处理活动的规则，与此同时，二审稿还提出一些富有前瞻性的条款。待国标中的条款“升华”为法律条文后，其强制效力及企业的合规义务将再无疑问。在对二审稿与现行法律、国标的详细对比梳理的基础上，我们挑选出六个最值得关注的立法发展进行分析，兹借本文提出我们的解读意见。

如您需要了解我们的出版物，
请联系:

Publication@llinkslaw.com

一. 最小必要原则

二审稿	其他法律	国家标准
第六条　处理个人信息应当具有明确、合理的目的，并应当限于实现处理目的所必要的最小范围、采取对个人权益影响最小的方式，不得进行与处理目的无关的个人信息处理。 第二十条　个人信息的保存期限应当为实现处理目的所必要的最短时间。法律、行政法规对个人信息的保存期限另有规定的，从其规定。	《民法典》第一千零三十五条 处理个人信息的，应当遵循合法、正当、必要原则，不得过度处理…… 《网络安全法》第四十一条 网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则……网络运营者不得收集与其提供的服务无关的个人信息……	《信息安全技术 个人信息安全规范》第 4.d)条、第 5.2 条、第 6.1 条 例：第 4.d)条 只处理满足个人信息主体授权同意的目的所需的最小个人信息类型和数量。

个人信息安全规范早已提出“最小必要原则”。此外，其他多个部门规章、国家标准也对此予以明确(尽管关注点大多落在 App 合规)，例如不久前四部委联合发布的《常见类型移动互联网应用程序必要个人信息范围规定》以及正在起草的《移动互联网应用程序个人信息保护管理暂行规定》。尽管如此，法律层级还未将最小必要原则落于纸面。此次二审稿的明确规定使得个人信息保护的最小必要原则又向前迈出了一步。

“最小必要”是保护个人信息主体权益的应有之意。对此，二审稿较此前发布的《个人信息保护法(草案)》(“一审稿”)和已有的最小必要原则相关立法，新增了“采取对个人权益影响最小的方式”这一要求，那么如何理解“采取对个人权益影响最小的方式”呢?

已经发布的国家标准《信息安全技术 个人信息安全影响评估指南》似乎可以提供借鉴。个人权益影响是该国标中提出的分析内容之一，亦是个人信息安全影响评估的首要步骤。根据该国标，个人权益影响可分为“限制个人自主决定权”“引发差别性待遇”“个人名誉受损或遭受精神压力”“人身财产受损”四个维度进行考察，后三者较容易理解，发生此等后果时企业也容易洞察，第一个维度“限制个人自主决定权”更值得企业关注。国标中例举“限制个人自主决定权”的情形有：被强迫执行不愿执行的操作、缺乏相关知识或缺少相关渠道更正个人信息、无法选择拒绝个性化广告的推送、被蓄意推送影响个人价值观判断的资讯等，我们可以简单概括为“更少信息茧房，更多开放选项”。

在法律层面没有针对“采取对个人权益影响最小的方式”出台更为详细的细则之前，我们建议，至少在 APP 方面，企业可参考工信部组织制定的团体标准《APP 收集使用个人信息最小必要评估规范》，该规范对个人信息收集、存储、使用、传输、共享、删除等环节如何落实最小必要原则作出了具体指引。除此之外，收集环节的最小必要要求还可参考《常见类型移动互联网应用程序必要个人信息范围规定》划定的三十余种常用服务类型的最小必要信息范围。

二. 处理个人信息的合法基础

二审稿	其他法律	国家标准
第十三条　符合下列情形之一的，个人信息处理者方可处理个人信息： (一)取得个人的同意； (二)为订立或者履行个人作为一方当事人的合同所必需； (三)为履行法定职责或者法定义务所必需； (四)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； (五)依照本法规定在合理的范围内处理已公开的个人信息； (六)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； (七)法律、行政法规规定的其他情形。 依照本法其他有关规定，处理个人信息应当取得个人同意，但有前款第二项至第七项规定情形的，不需取得个人同意。	《民法典》第一千零三十五条 处理个人信息的，应当符合下列条件：(一)征得该自然人或者其监护人同意，但是法律、行政法规另有规定的除外；…… 《网络安全法》第四十一条 网络运营者收集、使用个人信息，应当……经被收集者同意；第四十二条 网络运营者……未经被收集者同意，不得向他人提供个人信息。	《信息安全技术 个人信息安全规范》第 5.6 条、第 9.5 条

《民法典》及《网络安全法》等现有法律建构的处理个人信息的合法性基础均是围绕知情同意展开，但以知情同意作为唯一的合法性基础存在诸多缺陷，亦不是国际社会的通行做法，我们曾在过往文章《<个人信息保护法(草案)>的明惑之思》一文中作过详细阐释。

二审稿破除了这一做法，并修改、整合个人信息安全规范第 5.6 条“征得授权同意的例外”和第 9.5 条“共享、转让、公开披露个人信息时事先征得授权同意的例外”的情形作为与知情同意并列的处理个人信息的合法性基础。新规对于企业合规的直接利好在于，不再以取得知情同意作为原则性做法，而可以尝试依赖于第二项至第七项的规定开展个人信息处理活动，可以一定程度降低企业一一获取用户授权同意的合规成本，也可保护企业避免因合规需求而失去商业发展空间。

上述第二项至第七项的合法基础需要未来立法和司法进行释义。例如，“为订立或者履行个人作为一方当事人的合同所必需”“为履行法定职责或者法定义务所必需”应如何理解？是否一旦存在合同关系或法定义务即可在相关所有个人信息处理活动中免于知情同意？如不是，免于知情同意的范围是什么？对此问题，敬请期待我们个人信息保护法系列解读中的后续文章《知情同意不再是唯一合法基础》。

三. 利用已公开的个人信息

二审稿	其他法律	国家标准
第十三条　符合下列情形之一的，个人信息处理者方可处理个人信息：(五)依照本法规定在合理的范围内处理已公开的个人信息； 第二十八条　个人信息处理者处理已公开的个人信息，应当符合该个人信息被公开时的用途。超出与该用途相关的合理范围的，应当依照本法规定取得个人同意。 个人信息被公开时的用途不明确的，个人信息处理者应当合理、谨慎地处理已公开的个人信息。利用已公开的个人信息从事对个人有重大影响的活动，应当依照本法规定取得个人同意。	《民法典》第一千零三十六条 处理个人信息，有下列情形之一的，行为人不承担民事责任：(二)合理处理该自然人自行公开的或者其他已经合法公开的信息，但是该自然人明确拒绝或者处理该信息侵害其重大利益的除外；	《信息安全技术 个人信息安全规范》第 5.6 条 征得授权同意的例外 以下情形中，个人信息控制者收集、使用个人信息不必征得个人信息主体的授权同意：f) 所涉及的个人信息是个人信息主体自行向社会公众公开的；

个人信息安全规范中，“利用已公开的个人信息”明确属于获取授权同意的例外情形之一，但其推荐性国标的“尴尬”地位使得企业不敢贸然依赖该豁免规定。此外，仅有这样一句原则性的描述并无助于解决现实中的公开个人信息利用问题。最普遍的问题便是，只要是公开的个人信息，就可以不考虑使用目的，随意使用吗?

事实上，此前的司法实践中对此问题已有涉及，二审稿对此作出进一步明确对于公开的个人信息的利用必须符合个人信息被公开时的用途，而对于公开时用途不明的，处理应当合理、谨慎。我们理解，此处的“合理、谨慎”可以结合上述“最小必要”及“对个人权益影响最小的方式”进行解读。

当然，二审稿仍然遗留了部分未解答的问题。例如，一个最基本的问题是，“公开”的范围如何界定?是仅限于完全公开的网站、微博等，还是包括半公开的场合(例如需要注册进入的论坛、贴吧)? 甚至是否包括微信朋友圈和微信群聊? 这些问题也有待于其他法律或行政法规对二审稿进行细化。

四. 个人信息跨境传输

二审稿	其他法律	国家标准
第三十八条 个人信息处理者因业务等需要，确需向中华人民共和国境外提供个人信息的，应当至少具备下列一项条件： (一)依照本法第四十条的规定通过国家网信部门组织的安全评估； (二)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； (三)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，并监督其个人信息处理活动达到本法规定的个人信息保护标准； (四)法律、行政法规或者国家网信部门规定的其他条件。 第三十九条 个人信息处理者向中华人民共和国境外提供个人信息的，应当向个人告知境外接收方的身份、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本法规定权利的方式等事项，并取得个人的单独同意。 第四十条 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；法律、行政法规和国家网信部门规定可以不进行安全评估的，从其规定。	《网络安全法》第三十七条 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个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。	未有现行的相关国家标准

自从《网络安全法》生效以来，个人信息跨境传输便成为企业，尤其是外资企业头顶的一柄“达摩克里斯之剑”，而这种情况在《个人信息和重要数据出境安全评估办法(征求意见稿)》《个人信息出境安全评估办法(征求意见稿)》这两部草案公布后显得尤甚。对于大量不构成关键信息基础设施运营者的企业而言，个人信息跨境传输的相关义务是否需要履行，如何合规地履行，成为一个无法回避却无从下手的问题。

通过过往法规草案及二审稿可见，个人信息跨境传输规则行至今日历经若干阶段，整体趋势是由“松”至“严”，又由“严”转向“松而有序，严而有度”：现行的法律法规和国家标准只针对关键信息基础设施运营者在中国境内收集和产生的个人信息跨境传输作出约束性规定；而上述两部法律草案尝试扩大义务范围至所有网络运营者，要求所有网络运营者在个人信息跨境传输之前均须完成主管部门安全评估；而在一审稿和二审稿中，立法者区分关键信息基础设施运营者和一般网络运营者，并为后者提供了多种可以合规出境个人信息的路径。我们有理由相信，中国并不寻求个人信息的“出口禁令”，而是会通过立法、司法手段，引导企业有序、合规地进行个人信息的跨境传输和利用。

有关二审稿下个人信息跨境传输规则的详细解读，请见个人信息保护法系列解读系列文章《个人信息出境规则新动向》。

五. 个人信息安全影响评估

二审稿	其他法律	国家标准
第五十五条　个人信息处理者应当对下列个人信息处理活动在事前进行风险评估，并对处理情况进行记录： (一)处理敏感个人信息； (二)利用个人信息进行自动化决策； (三)委托处理个人信息、向他人提供个人信息、公开个人信息； (四)向境外提供个人信息； (五)其他对个人有重大影响的个人信息处理活动。 风险评估的内容应当包括： (一)个人信息的处理目的、处理方式等是否合法、正当、必要； (二)对个人的影响及风险程度； (三)所采取的安全保护措施是否合法、有效并与风险程度相适应。 风险评估报告和处理情况记录应当至少保存三年。	《网络安全法》第三十七条 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个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。	《信息安全技术 个人信息安全影响评估指南》
	《儿童个人信息网络保护规定》第十六条 网络运营者委托第三方处理儿童个人信息的，应当对受委托方及委托行为等进行安全评估……第十七条 网络运营者向第三方转移儿童个人信息的，应当自行或者委托第三方机构进行安全评估。	《信息安全技术 个人信息安全规范》第 11.4 条

个人信息安全规范中明确提出了“个人信息共享、转让”“个人信息委托处理”等多个场景下的个人信息安全影响评估要求，但作为一份推荐性国标，该等要求略显“底气不足”。二审稿第一次在法律层面对个人信息安全影响评估的情形进行归纳总结，并对评估的内容进行简单列举，这预示着个人信息安全影响评估将作为一项法定义务由个人信息处理者予以落实，建议企业加以重视。

围绕二审稿第五十五条，我们对其中“其他对个人有重大影响的个人信息处理活动”和不同个人信息处理活动场景下的特殊评估内容进行重点解读：

(一) “其他对个人有重大影响的个人信息处理活动”

“对个人有重大影响的个人信息处理活动”可能与影响个人信息主体权益的高风险个人信息处理活动存在较大重合，参考《信息安全技术 个人信息安全影响评估指南》，该等场景包括但不限于：

- 涉及对个人信息主体评价、打分等直接画像行为，如进行负面标识、预测健康状态等；
- 使用个人信息进行自动分析给出司法裁定或其他对个人有重大影响的决定；
- 系统性的监控分析个人或个人信息，如在公共区域监控、采集个人信息等；
- 收集的个人敏感信息数量、比重较多，收集频率要求高，与个人经历、思想观点、健康、财务状况等密切相关；

- 数据处理的规模较大，如涉及 50 万人以上、持续时间久、在某个特定群体的占比高、涵盖的地理区域广泛或较集中等;
- 对不同处理活动的数据集进行匹配和合并，并应用于业务;
- 数据处理涉及弱势群体的，如未成年人、病人、老年人、低收入人群、文化水平偏低人群、寻求庇护人群等;
- 创新型技术或解决方案的应用，如生物特征识别、IoT、人工智能等;
- 处理个人信息可能导致个人信息主体无法行使权利、使用服务或得到合同保障等。

在《个人信息保护法》的实施细则出台之前，建议企业在出现上述情形前开展个人信息安全影响评估，并对个人信息处理情况进行记录。

(二) 不同个人信息处理活动场景下的特殊评估内容

二审稿第五十五条中列出的三项评估内容较为概括，结合不同的个人信息处理活动场景，企业应对该等评估内容进行特别解释。

以“利用个人信息进行自动化决策”为例，评估“对个人的影响及风险程度”时需要关注自动化决策的效果，为保证自动化决策符合个人信息主体的实际情况，不致产生偏颇从而影响个人信息主体权益，企业至少应关注下述内容:

- 是否定期对自动化决策的效果进行评价;
- 是否对自动化决策使用的数据源、算法等持续优化;
- 是否向用户提供针对自动化决策结果的投诉渠道。

再以“委托处理个人信息、向他人提供个人信息、公开个人信息”为例，建议企业在评估第三项内容“所采取的安全保护措施是否合法、有效并与风险程度相适应”时同时考虑:

- 数据发送方的安全管理保障和安全技术保障能力;
- 数据接收方的安全管理保障和安全技术保障能力(不适用于公开个人信息的场景);
- 个人信息是否进行去标识化处理。

六. 个人信息安全事件的报告义务

<table>
<tr><th>二审稿</th><th>其他法律</th><th>国家标准</th></tr>
<tr><td rowspan="8">第五十六条 个人信息处理者发现个人信息泄露的，应当立即采取补救措施，并通知履行个人信息保护职责的部门和个人。通知应当包括下列事项:
(一)个人信息泄露的原因;
(二)泄露的个人信息种类和可能造成的危害;
(三)已采取的补救措施;
(四)个人可以采取的减轻危害的措施;
(五)个人信息处理者的联系方式。
个人信息处理者采取措施能够有效避免信息泄露造成损害的，个人信息处理者可以不通知个人;但是，履行个人信息保护职责的部门认为个人信息泄露可能对个人造成损害的，有权要求个人信息处理者通知个人。</td><td>《突发事件应对法》第五十六条 受到自然灾害危害或者发生事故灾难、公共卫生事件的单位，应当……向所在地县级人民政府报告;对因本单位的问题引发的或者主体是本单位人员的社会安全事件，有关单位应当按照规定上报情况……</td><td rowspan="8">《信息技术安全技术 信息安全事件管理 第2部分:事件响应规划和准备指南》B.4.2 信息安全事件报告表单示例</td></tr>
<tr><td>《国家网络安全事件应急预案》第4.1条 网络安全事件发生后，事发单位应立即启动应急预案，实施处置并及时报送信息。

注:可能涉及地方法规，如《上海市网络安全事件应急预案》第4.1.1条 发生网络安全事件的单位必须在半小时内口头、1小时内书面报告市委网信办值班室、市应急联动中心和事发地区网络安全主管部门。较大以上网络安全事件或特殊情况，必须立即报告。

•上述法规均未明确规定通知/报告内容</td></tr>
<tr><td>《证券期货业信息安全事件报告与调查处理办法》第十七条 核心机构和经营机构进行应急报告时应当先进行电话报告，随后书面报送《信息安全事件情况报告书》，内容包括:事件发生时间、地点、简要经过、影响范围初步评估、影响程度初步评估、影响人数初步评估、经济损失初步评估、后果初步判断、原因初步判断、事件性质初步判断、已采取的措施及效果、需要有关部门和单位协助处置的有关事宜、报告单位、签发人和报告时间、联系人与联系方式、与本事件有关的其他内容。</td></tr>
<tr><td>《水利网络安全事件应急预案》通知内容详见《水利网络安全事件报告表》</td></tr>
<tr><td>《工业控制系统信息安全事件应急管理工作指南》第十七条 有关地方工业和信息化主管部门和工业企业应及时向工业和信息化部报告事态发展变化情况和事件处置进展情况。报告信息一般包括以下要素:事件涉及的工业控制系统名称及运营管理单位、时间、地点、原因、来源、类型、性质、危害、影响范围、发展趋势、处置措施等。</td></tr>
<tr><td>《公共互联网网络安全突发事件应急预案》第4.1条 基础电信企业、域名机构、互联网企业应当对本单位网络和系统的运行状况进行密切监测，一旦发生本预案规定的网络安全突发事件，应当立即通过电话等方式向部应急办和相关省(自治区、直辖市)通信管理局报告，不得迟报、谎报、瞒报、漏报。
网络安全专业机构、网络安全企业应当通过多种途径监测、收集已经发生的公共互联网网络安全突发事件信息，并及时向部应急办和相关省(自治区、直辖市)通信管理局报告。
报告突发事件信息时，应当说明事件发生时间、初步判定的影响范围和危害、已采取的应急处置措施和有关建议。</td></tr>
</table>

从上表中可以看出，一审稿和二审稿发布之前，法律层面未专门针对网络安全事件/信息安全事件(“安全事件”)的报告义务和报告内容统一作出规定，而关键行业的主管部门已陆续针对本行业的情况制定相关规则。基于此，我们提示企业，如企业所在行业已发布单行的安全事件报告规则，建议企业对照该等规则进行完整汇报。

下文我们将重点讨论发生安全事件时事发单位应向谁报告，即“履行个人信息保护职责的部门”的指向。二审稿第五十九条指出，国家网信部门、国务院有关部门、县级以上地方人民政府有关部门统称为“履行个人信息保护职责的部门”，但未对“有关部门”进行具体说明。结合上述法律法规，我们对接收报告的部门进行梳理，详见下表:

事件类型	接收报告的部门	行业	通知主体类型
网络安全事件	市委网信办值班室、市应急联动中心和事发地区网络安全主管部门 *以上海为例	不限	不限
工业控制系统信息安全事件	工信部	工业	工业企业
公共互联网网络安全突发事件	工信部应急办和相关省(自治区、直辖市)通信管理局	互联网	基础电信企业、域名机构、互联网企业、网络安全专业机构、网络安全企业
水利网络安全事件	水利相关司局、部直属单位	水利	水利企业
证券期货业信息安全事件	中国证监会	证券	承担证券期货市场公共职能的机构、承担证券期货行业信息技术公共基础设施运营的机构等证券期货市场核心机构及其下属机构(“核心机构”)
	住所地中国证监会派出机构		证券公司、期货公司、基金管理公司、证券期货服务机构等证券期货经营机构(“经营机构”)
	所在地中国证监会派出机构		经营机构分支机构
	相关证券期货交易所 *信息安全事件影响到证券期货交易业务时		经营机构
	中国证券登记结算公司 *信息安全事件影响到证券登记结算业务时		经营机构
	中国证券金融公司 *信息安全事件影响到转融通业务时		经营机构

结语

尽管二审稿尚为法律草案，其具体内容在正式颁布前可能变化，但我们相信已确立的结构体系和相关原则不会发生实质性的改变。《个人信息保护法》可以说是对现有法律法规和国标的“集大成者”，其确定了个人信息保护的主要脉络。当然，《个人信息保护法》作为最高位阶的法律，不可能事无巨细面面俱到，必然有赖于下位法及国标等“毛细血管”对其的补充和支持。相信随着《个人信息保护法》的正式出台，企业严肃对待、严格遵从将成为合规共识。

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	北京	深圳
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	伦敦	
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	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