

个人信息处理合规要点

作者：潘永建 | 杨迅 | 邓梓珊 | 沙莎

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，本文为第三篇《个人信息处理合规要点》。

实践中，个人信息处理情形多样，既可能由单一主体进行，也有可能由多个主体共同决定个人信息的处理目的和方式，还有可能是某一主体委托第三方按一定要求处理个人信息。不同于此前《信息安全技术 个人信息安全规范(GB T35273-2020)》(以下简称“《个人信息安全规范》”)沿用 GDPR 的规定，采用“个人信息控制者”，《个人信息保护法(草案二次审议稿)》(以下简称“二审稿”)采用“个人信息处理者”的概念。在具体规定层面，《个人信息安全规范》主要围绕个人信息控制者处理个人信息的要求与规范展开，而二审稿主要围绕“个人信息处理者的义务”与“处理个人信息的要求与规范”展开，似乎意在区分“个人信息处理者”与“其他参与处理个人信息的主体”的不同义务。本文根据二审稿的规定，厘清处理个人信息的过程中，不同主体应当遵守的义务，为承担不同个人信息处理角色的企业提供合规思路。

.....
如您需要了解我们的出版物，
请联系：

Publication@llinkslaw.com

一. 处理个人信息的主体

《民法典》： 信息处理者	有权收集、存储、处理、提供个人信息的主体
《个人信息保护法(草案)》： 个人信息处理者	自主决定处理目的、处理方式等个人信息处理事项的主体
《个人信息安全规范》： 个人信息控制者	有能力决定个人信息处理目的、方式等的组织或个人
GDPR： 控制者	决定个人数据处理目的、方式的组织或个人

一般而言，区分“控制者”和“处理者”的目的主要是确定权责。通过上述不同条文对比，我们可以发现“有权”/“自主”/“有能力”决定如何处理个人信息的主体需要对个人信息主体承担主要责任。至于如何解释“自主决定”“有能力决定”，中国法尚未作出明确解释。值得注意的是，二审稿区分了“个人信息处理者”与“其他参与处理个人信息的主体”，具体情形可以分为：

- (1) 个人信息处理者处理个人信息；
- (2) 个人信息处理者全权委托他人处理个人信息，由受委托方处理个人信息；
- (3) 个人信息处理者向第三方提供其处理的个人信息，由接收方在指定范围内处理个人信息。

即使二审稿未作场景上的明确区分，实务操作中企业仍应区分“共同处理”还是“委托处理”，即首先应明确框定“我方”的数据处理需求，探明“对方”实际的数据处理能力，了解“对方”对合同项下的数据是否也有处理的需求。在构成共同处理的场景下，主要明确各自的权利义务，划分数据和隐私安全责任，发生侵权事件后的追偿权利等；在委托处理的场景下，主要明确受托方处理数据的范围和目的，是否允许转委托等。

二. 个人信息处理义务

根据个人信息的全生命周期，我们暂将二审稿中参与个人信息处理的各方区分为个人信息处理者、受委托处理个人信息的主体，以及个人信息的接收方。这三类主体处理个人信息时应当遵守一般义务的同时，还应当遵守各自的不同义务。

1. 处理个人信息的一般义务	
(1) 合法正当	处理个人信息应当合法、诚信、正当，不得误导、欺诈。
(2) 处理个人信息的目的	- 处理个人信息目的明确、合理，并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。 - 处理目的、方式、个人信息种类发生变更时应当重新取得个人同意。
(3) 公开透明	处理个人信息公开、透明，明示处理的目的、方式和范围。
(4) 个人信息质量	避免因个人信息不准确、不完整对个人权益造成不利影响。

(5) 禁止性规定	不得从事危害国家安全、公共利益的个人信息处理活动。
(6) 个人同意	处理个人信息应当取得个人同意，同意应当自愿、明确。
(7) 自动化决策	- 保证决策的透明度和结果公平合理。 - 通过自动化决策进行商业营销、信息推送：应当同时提供不针对其个人特征的选项，或者向个人提供拒绝的方式。
(8) 公共场所安装进行图像采集、个人身份识别的设备	- 安装的条件：应当为维护公共安全所必需；遵守国家有关规定；设置显著的提示标识。 - 用途：只能用于维护公共安全的目的；不得公开或者向他人提供，取得个人单独同意的除外。
(9) 个人信息跨境提供需要遵守的规则	境外机构要求提供中国境内存储的个人信息：非经中华人民共和国主管机关批准，不得提供；国际条约、协定有规定的，可以按照其规定执行。
2. 委托处理个人信息情形下的委托方与受托方	
(1) 处理个人信息的范围	- 委托方与受托方约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务。 - 受托方应当按照约定处理个人信息，不得超出约定的处理目的、处理方式等处理个人信息。
(2) 接受监督	委托方对受托方的个人信息处理活动进行监督。
(3) 个人信息返还、删除	委托合同不生效、无效、被撤销或者终止的，受托方应当将个人信息返还个人信息处理者或者予以删除，不得保留。
(4) 非经同意不得转委托	未经个人信息处理者同意，受托方不得转委托他人处理个人信息。
(5) 受托方个人信息保护义务	履行个人信息保护义务，采取必要措施保障所处理的个人信息的安全。
3. 接收个人信息的第三方	
处理个人信息的范围	个人信息主体同意的处理目的、处理方式和个人信息的种类。
个人同意	原先的处理目的、方式改变的，应重新取得个人同意。

1. 处理个人信息需采取对个人权益影响最小的方式

处理个人信息方面，除了个人信息处理应在“最小必要范围”这一要求外，二审稿还在一审稿的基础上新增“对个人权益影响最小的方式”。这一修订对处理个人信息的主体提出了更高的要求，保障个人信息主体的权益。

该表述与个人信息安全影响评估制度(“DPIA”)的评估事项较为类似。DPIA 旨在特定情形下对个人信息处理活动进行评估，并根据评估结果采取适当的安全保护措施，降低对个人信息主体权益的影响。即使是《信息安全技术 个人信息安全影响评估指南(GB/T39335-2020)》(以下简称“《个人信息安全影响评估指南》”)也未要求必须将对个人信息主体权益的影响降至最低，但二审稿却

提出此要求，对个人信息处理提出了更为严苛的要求。在实操层面，如何理解“影响最小”，是否需要衡量成本与效率，尚需立法进一步明确。

2. 利用个人信息进行自动化决策的相关要求

在自动化决策方面，二审稿增加商业化营销与信息推送需要“向个人提供拒绝的方式”，这一规定直指实践中个性化广告无法关闭或关闭流程繁琐的弊端，与二审稿第十六条规定的“个人信息处理者应当提供便捷的撤回同意的方式”相呼应，新增的这一规定要求企业在进行精准化营销的同时，赋予用户“拒绝权”，使得用户可以自主、便捷地退出或关闭该等自动化营销和推送。

3. 受委托处理个人信息的要求

在委托处理个人信息方面，除了一审稿规定的合同履行完毕或合同解除，二审稿还增加了委托合同不生效、无效、撤销等情形下删除个人信息的要求，且“不得保留”。按照这一要求，一旦委托合同无效、终止等，受委托处理个人信息的企业从可访问数据中“删除”相关个人信息是不够的，必须在其数据库中彻底删除个人信息。

三. 个人信息处理者的义务

个人信息处理者处理个人信息时应特别注意的义务，我们首先总结在下表中，表后我们选取几项重点内容进行解读：

•	对个人信息处理活动负责，保证个人信息安全。
•	处理个人信息的原则性规定(见上表)。
•	提供便捷的撤回同意的方式。
•	处理敏感个人信息应遵循更高要求，取得单独同意。
•	两个以上的个人信息处理者共同决定个人信息的处理目的和处理方式的，应当约定各自的权利和义务。个人信息处理者共同处理个人信息，侵害个人信息权益的，应当承担连带责任。
•	委托处理个人信息应遵守的义务(见上表)。
•	个人信息处理者因合并、分立等原因需要转移个人信息的，应当向个人告知接收方的身份、联系方式。接收方应当继续履行个人信息处理者的义务。接收方变更原先的处理目的、处理方式，应当依照本法规定重新取得个人同意。
•	自动化决策的相关规定(见上表)。
•	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。
•	个人信息跨境提供的规则

•	建立机制, 响应个人信息主体的权利(查阅、复制、更正、补充、删除、解释说明个人信息处理规则)。
•	在特定情形下主动删除个人信息。
•	采取必要措施确保个人信息处理活动符合法律、行政法规的规定, 并防止未经授权的访问以及个人信息泄露或者被窃取、篡改、删除。
•	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, 公开负责人的联系方式, 并将个人信息保护负责人的姓名、联系方式等报送履行个人信息保护职责的部门。
•	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, 并将有关机构的名称或者代表的姓名、联系方式等报送履行个人信息保护职责的部门。
•	定期进行个人信息处理活动合规审计、特定处理活动的事前风险评估。
•	发现个人信息泄露的, 立即采取补救措施并履行通知义务。
•	基础性互联网平台服务提供者的特定义务。

1. 主动删除个人信息

二审稿第四十七条规定, 个人信息处理者在以下情形中应当主动删除个人信息:

- (1)处理目的已实现或者为了实现处理目的已经不再必要;
- (2)个人信息处理者停止提供产品或者服务, 或者保存期限已届满;
- (3)个人撤回同意;
- (4)个人信息处理者违反法律、行政法规或者违反约定处理个人信息;
- (5)法律、行政法规规定的其他情形。

二审稿此处修改表明, “主动删除”特定的个人信息成为个人信息处理者必须遵守的义务。以机场、火车站安检中的人脸识别为例, 机场或火车站为了公共安全的目的对旅客进行人脸识别后, 其目的已经达成, 属于二审稿中的“处理目的已经实现”, 机场或火车站不应继续对该等个人生物特征信息进行保留和分享, 而应当主动删除; 再如, 根据工信部近期发布的《关于侵害用户权益行为的 APP 通报(2021 年第 3 批)》¹, 多款天气类、新闻类手机应用软件存在超范围收集个人信息以及违规使用个人信息的情况, 根据二审稿, 此类手机应用软件属于违规收集、使用个人信息, 个人信息处理者应当主动删除该等个人信息。

2. 安全审计义务

二审稿要求个人信息处理者对其个人信息处理活动进行审计。在个人信息处理者的处理活动存在风险或者发生个人安全事件时, 履行个人信息保护职责的部门有权要求个人信息处理者委托第三方进行合规审计, 并对个人信息处理者的负责人进行约谈。

¹ https://www.miit.gov.cn/jgsj/xgj/fwjd/art/2021/art_4723dbffa9c94812b70236b9a1ff951a.html

二审稿对于个人信息处理者的安全审计仅为原则性规定，在安全审计的内容方面，《个人信息安全规范》具体规定了六项内容，可供企业参考，具体包括：(1)审计个人信息保护政策、相关流程和安全措施的有效性；(2)建立自动化审计系统；(3)支撑安全事件处置、应急响应和事后调查；(4)防止非授权访问、篡改、删除审计记录；(5)及时处理审计过程中发现的个人信息违规使用、滥用情况；(6)审计记录和留存时间符合法律法规要求。

3. 基础性互联网平台服务提供者的特殊义务

近期执法部门对互联网巨头展开密集执法。这一形势下，二审稿新增五十七条，对基础性互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者设定特定义务，包括成立由外部成员组成的独立机构、停止对平台内严重违法违规的产品或服务提供者提供服务、定期发布社会责任报告等。

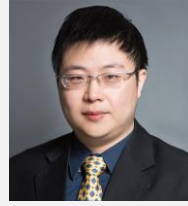
4. 风险评估义务

二审稿在个人信息处理者的事前风险评估方面未对一审稿进行实质性修改。需要提示的是，2021年6月《个人信息安全影响评估指南》即将生效，《个人信息安全影响评估指南》对个人信息出境前评估以及委托处理、向他人提供、公开个人信息前评估的因素和场景等进行了细化，个人信息处理者的事前风险评估宜参照《个人信息安全影响评估指南》行事。

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