LINKS Law Offices
通力律师事务所

上海
上海市银城中路 68 号
时代金融中心 16/19 楼
电话: +86 21 3135 8666
传真: +86 21 3135 8600

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

香港
香港中环皇后大道中 5 号
衡怡大厦 27 楼
电话: +852 2592 1978
传真: +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

通力法律评述 | 公司及并购
2020 年 3 月

个人信息合规“再出发”——简评 2020 版个人信息国家标准

作者：潘永建 | 朱晓阳

2017 年 12 月 29 日，国家质量监督检验检疫总局及国家标准化管理委员会公布了《信息安全技术 个人信息安全规范(GB/T 35273-2017)》(简称“**2017 版国标**”)。2017 版国标作为《网络安全法》的重要补充，为企业及政府部门的个人信息合规及监管工作提供了全面、有效的指引。技术日新月异，个人信息合规新问题也层出不穷，2017 版国标和现有网络安全法律体系不断面临新的挑战。在 2017 版国标的基础上，制定机构先后于 2019 年 2 月、2019 年 6 月及 2019 年 10 月发布了三个版本的修订草案，以应对个人信息合规中的新问题、新需求。最终，国家市场监督总局及国家标准化管理委员会于 2020 年 3 月 6 日公布了《信息安全技术 个人信息安全规范(GB/T 35273-2020)》(简称“**2020 版国标**”)以代替 2017 版国标。2020 版国标将于 2020 年 10 月 1 日生效。

1. 2020 版国标的效力

与 2017 版国标相同，“GB/T”的标号表明了 2020 版国标属于推荐性国标。根据《标准化法》，“国家鼓励采用推荐性标准”，从法律效力而言，相较于强制性国标(怠于履行强制性国标规定的义务，可能导致行政处罚或刑事处罚)，推荐性国标不具有强制效力。然而，这并不意味着 2020 版国标对于企业没有拘束力。

For more Llinks publications, please contact:

Publication@llinkslaw.com

如您需要了解我们的出版物，请联系:

Publication@llinkslaw.com

正如 2017 版国标及 2020 版国标中第 1 条“范围”中的描述，“本标准适用于规范各类组织的个人信息处理活动，也适用于主管监督部门、第三方评估机构等组织对个人信息处理活动进行监督、管理和评估”，2017 版国标已经成为我国个人信息立法中的重要参考文件(如《儿童个人信息网络保护规定》《数据安全管理办法(征求意见稿)》等)，也是监管部门开展个人信息相关执法工作的重要评判标准。可以预见，2020 版国标将继续发挥这一作用。

因此，尽管作为“推荐性国标”，2020 版国标具有事实上的“拘束力”，将持续影响企业的个人信息合规决策，并在政府的个人信息立法及执法中作为标尺。

2. 2020 版国标的主要修订内容

1) 将“隐私政策”修改为“个人信息保护政策”

这一修改将为全球隐私政策的翻译带来小小的麻烦，因为根据 2020 版国标“隐私政策”不再是“privacy policy”的恰当中文翻译。

表面上看，2020 版国标将沿用已久的“隐私政策”修改为“个人信息保护政策”，似乎化简为繁。但实际上，更改后的称谓更加准确地指出了“privacy policy”的性质，以及在中国法语境下“隐私”与“个人信息”的区别。

总体而言，“隐私”和“个人信息”的范围是存在重合的，这表现在，具有私密性质的个人信息属于隐私。但更重要的是，它们之间存在明显的不同：隐私不都是个人信息，个人信息亦不都是隐私。因此，2020 版国标将“隐私政策”的表述变更为“个人信息保护政策”是具有积极意义的，因为企业收集和使用的大部分个人的信息(比如姓名、电话号码)都不是“隐私”，而是“个人信息”。

为遵照 2020 国标要求，企业宜使用“个人信息保护政策”的表述来替代原有的“隐私政策”称谓。

2) 个人生物识别信息

2017 版国标中界定了“个人敏感信息”，并将“个人生物识别信息”列为个人敏感信息的一类。2017 版国标在附录中列举的个人生物识别信息包括：个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等。保护个人生物识别信息的根本意义在于，不同于传统安全措施(比如密码)的可变更性，个人生物识别信息在很大程度上在个人信息主体的整个生命过程中都无法改变，在遭遇安全危机时无法像修改密码或重置密码一样，修改、重置个人生物识别信息。这一点使得泄露和滥用个人生物识别信息的危害后果更加严重。

在 2017 版国标的基础上，2020 版国标新增了关于个人生物识别信息收集的特殊要求，即“收集个人生物识别信息前，应单独向个人信息主体告知收集、使用个人生物识别信息的目的、方式和范围，以及存储时间等规则，并征得个人信息主体的明示同意。”

2020 版国标对于收集个人生物识别信息的特别要求具体体现在: “单独告知”、告知收集的“目的、方式、范围及存储时间”以及“明示同意”, 其中最为关键的莫过于“单独告知”的要求。基于此规定, 在个人信息保护政策中对个人生物识别信息进行相关的告知可能不是完全合规的做法, 妥善做法是单独起草有关个人生物识别信息的政策, 并在收集个人生物识别信息时, 以弹窗或其他方式对个人生物识别信息相关内容进行告知并通过用户点击等获取同意。

此外, 值得注意的是, 2020 版国标还规定了对个人生物识别信息的存储、传输、共享和披露的要求。

3) 用户画像的限制

用户画像长期以来被企业用于精准营销活动。尽管业界不断地争论如何合法合规地使用用户画像, 但法律法规一直未提供明确指引。

2020 版国标在第 7 条“个人信息的使用”中新增了一个条款(第 7.4 条)以规定对用户画像的使用限制。首先, 用户画像中对用户的特征描述不应包括某些不恰当的内容, 比如色情、暴力信息, 或有关种族、宗教、残疾、疾病歧视的信息; 其次, 除非为实现用户授权同意的收集和使用目的所必需, 使用个人信息时应消除明确身份指向性, 避免精准定位到特定个人。

4) 多项业务功能的自主选择

《网络安全法》要求收集和使用个人信息须符合必要性原则, 但是如何界定“必要性”尚不明确。何等“必要性”才构成《网络安全法》中的“必要”一直困扰着个人信息控制者。例如, APP 通常由多项功能组成, 通常可以分为主要功能和次要功能, 我们理解, 为实现 APP 的主要功能而收集个人信息构成“必要”, 而为次要功能收集个人信息的必要性可能要因案而异。在这种情况下, 允许用户针对各项业务功能进行单独的同意显得尤为重要。

2020 版国标为解决这一问题提供了一些思路: (1)APP 应就 APP 的每一项次要功能告知用户, 并寻求用户对每一项功能的同意; (2)如果用户不授权同意使用某一次要功能时, APP 不得阻挠用户使用 APP 的主要功能, 亦不得降低 APP 整体的服务质量; (3)用户有权关闭或退出某些次要功能, 其关闭或退出的途径或方式应与选择使用该功能的途径或方式同样方便。

如此, 用户有权对每项业务功能进行自主的选择, 用户的同意变得可以拆分, 个人信息控制者对个人信息的收集和使用也可以单独进行, 进而可以实现针对每一功能进行必要性评估。

5) 征得授权同意的例外

2020 版国标修改了收集、使用个人信息的例外情形。具体而言: (1)征得授权同意的例外情形中, 新增了一项“与个人信息控制者履行法律法规规定的义务相关的”; (2)“根据个人信息主体要求签订和履行合同所必需的”的例外中附加了一条注释, 即“个人信息保护政策的主要功能为公开个

人信息控制者收集、使用个人信息范围和规则，不宜将其视为合同”，这意味着个人信息控制者援引该例外的前提是，个人信息控制者已和个人信息主体签订了主合同(比如服务合同或销售合同)。仅以“履行个人信息保护政策”作为抗辩是不够的。

6) 个性化展示的使用

2020 版国标在第 7 条“个人信息的使用”中新增了一个条款(第 7.5 条)以规范个性化展示相关问题。个性化展示一直充满争议，“大数据歧视”是其中一个重要原因。《电子商务法》已经对该问题作出了规定，2020 版国标在《电子商务法》基础上作了进一步的补充。

根据 2020 版国标，个性化展示的内容应与非个性化展示的内容进行显著区分，例如，通过标明“定推”的字样。其次，在向个人信息主体提供个性化展示的内容时，应同时向其提供非个性化展示的内容。此外，在向个人信息主体推送新闻信息服务的过程中使用个性化展示的，应向其提供简单直观的退出或关闭个性化展示模式的选项。最后，2020 版国标强调了在使用个性化展示向用户提供业务功能时，用户对于个性化展示的控制能力，国标建议个人信息控制者建立一种用户自主控制的机制，以保障用户调控个性化展示相关性程度的能力。

7) 注销账户

账户注销无论是对企业还是用户而言都是令人头疼的问题。试图注销 APP 账户的用户往往会发现 APP 根本没有提供注销的渠道，因为企业珍视用户资源，往往通过阻止用户注销的方式来“挽留”用户及其个人信息。

2020 版国标力图解决这一问题：要求企业应为用户提供简便易操作的注销账户的方法。如果用户在注销的过程中需要进行身份核验，那么其需要再次提供的个人信息不得多于其注册时提供的个人信息；在 APP 提供多个产品或功能的情况下，2020 版国标禁止企业设置不合理的条件或提出额外要求以阻止用户注销。例如，不得提出“注销账户的任一功能将导致用户无法使用其他功能”的强制要求，除非这些功能之间相互依存，注销任一功能将导致其他功能无法实现或失去意义。最后，用户注销账户后，企业应及时删除其个人信息或进行匿名化处理。

3. 国标与主要域外个人信息保护法律的差异

在服务涉外客户的过程中，我们发现一个现象在跨国公司中较为普遍：许多跨国公司(尤其是欧美跨国公司)认为，其公司根据欧盟或者美国法制定了隐私政策，而欧盟 GDPR 或者美国的 CCPA 无疑是全球范围内最为“完备”的个人信息保护法律，因此这些隐私政策只需经过简单的翻译便可适用于中国市场。然而这种理解忽视了域外法律与中国法律的差异，不仅可能导致在中国法律下的合规问题，更有可能造成其隐私政策在中国境内“水土不服”，无法达到预期的效果。为何不能直接将全球隐私政策翻译后在中国进行使用?主要原因如下。

1） **GDPR 或 CCPA 中的术语和机制与中国法下的术语和机制不同**：一些 GDPR 或 CCPA 中出现的术语和机制在中国法律下没有对应的概念。例如，GDPR 下有一重要的概念“个人信息控制者”，意思是确定个人信息处理目的和方式的一方。尽管 2020 版国标定义了中国法下的“个人信息控制者”，但这一概念尚未获得中国其他法律法规的认可。GDPR 与中国个人信息保护法律下“个人信息控制者”的区别不仅仅在概念方面，GDPR 中还规定了一些中国法未规定的“个人信息控制者”的权利和义务。因此，在中国的个人信息保护政策或其他法律文件中谈论“个人信息控制者”无异于空中楼阁。

2） **中国个人信息保护法律中有一些来源于中国数据实践和法律环境的独特要求**：GDPR 和 CCPA 或许是世界上最“先进”的个人信息立法，但在某些方面，2020 版国标和中国个人信息保护法律可能比 GDPR 或 CCPA 更加严苛。例如，正如上文提到的，2020 版国标中规定了“多项业务功能的自主选择”的要求，而 GDPR 和 CCPA 就该方面未有强制性规定。除此之外，2020 版国标中有关于个人生物识别信息的要求(尤其是个人信息控制者收集个人生物识别信息前，须单独告知个人信息主体并获得其单独同意)，而在 GDPR 和 CCPA 中却没有。因此，如果企业仅遵循 GDPR 或 CCPA，那么他们可能在不经意间已违反中国法的这些规定。

3） **中文和英文或其他西方语言存在本质的不同**：根据我们的经验，谷歌翻译在英语与西方语言(例如：法语、德语和意大利语)之间的互译水平远比在英语与中文之间的互译水平要优秀，这仅仅是中文与英语(或其他西方语言)本质差别的一个体现。而英文和中文法律用语方面的差异更进一步加剧了这一问题。实践中，很难通过直译的方式将全球隐私政策的英文翻译成中文后直接在中国使用，即使是经过细心校准后的翻译也有可能在中外法律存在差异的方面产生歧义。我们审阅过很多企业的全球隐私政策翻译件，其中相当一部分的翻译在中文环境和中国法语境下显得不那么恰如其分。

鉴于上述情况，如果跨国公司希望在中国个人信息合规方面拥有出众表现，那么懂得“入乡随俗”便是第一课。具体而言，跨国公司应当将其全球隐私政策翻译得尽可能“地道”，与此同时，还应结合中国相关法律和实践，定制中国版“个人信息保护政策”。相信 2020 版国标在这方面可以为跨国公司提供指引。

4. 结语

2020 版国标总结了个人信息合规方面的过往经验，同时展望了我国立法和执法的最新趋势。2020 版国标的重要性和影响力绝不会因为其推荐性国标的性质而有所削弱。在《个人信息法》尚待颁布的情况下，我们期望客户和其他读者能够沿着 2020 版国标指引的方向，在个人信息合规之旅上顺利地“再出发”。

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

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	香港	伦敦
T: +86 21 3135 8666 F: +86 21 3135 8600	T: +86 10 8519 2266 F: +86 10 8519 2929	T: +852 2592 1978 F: +852 2868 0883	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 2020