汉坤法律评述
漢坤律師事務所
融贯中西 · 务实创新
2018 年 2 月 4 日

汉坤网络安全和数据合规系列之八：个人信息安全的“GSP”来了！

唐志华 | 朱敏 | 黄颖

在食品、药品和医疗器械等许多注重质量管理的行业，都有自己的 GMP（Good Manufacturing Practices）和 GSP（Good Sales Practices）等管理规范，而新出台的《信息安全技术 个人信息安全规范》（GB/T 35273-2017）（以下简称“**《规范》**”），从其体系架构和文本内容上来讲，无疑就是个人信息保护领域的“GSP”（Good Security Practices）。

2017 年 12 月 29 日，国家质量监督检验检疫总局和国家标准化管理委员会以国家标准形式联合发布了《规范》。2018 年 1 月 24 日，国家标准全文公开系统正式对外公布《规范》全文，并将于 2018 年 5 月 1 日正式施行。《规范》在遵循《网络安全法》要求的基础上确立的个人信息保护框架，全面而详尽规定了个人信息处理各个环节的合规要求。

一、 功能区分+定性定量+过程管理

对《规范》的整体内容进行分析研究后，我们认为，《规范》的内在整体逻辑架构可以概括为：功能区分+定性定量+过程管理。申言之，《规范》首先对相关主体的业务功能作了核心业务功能和附加业务功能的区分，这是为不同业务功能下提出不同合规要求的一项基础区分；其次，就相关主体在业务中可能涉及的个人信息，《规范》从定性和定量上也提出了不同的要求，例如提出了目的明确原则（合法、正当、必要）和最少够用原则（数量最少和频率最低）等，此外还涉及收集方式、存放地域和存储期限等；再者，《规范》从过程管理的角度对个人信息或数据的各个流转环节提出了针对性的规范化要求，主要涉及收集、保存、使用、委托处理、共享/转让、公开披露和兼并收购等。

为了更加直观和清晰的展现上述框架，我们整理了如下的表格，相信这份表格不仅有助于理解《规范》的整体架构和内容，对于指导各个企业的个人信息合规实践也会有一定的帮助。

表 1

个人信息 业务功能	定性定量			过程管理						
	类型	数量	频率	收集	保存	使用	委托处理	共享/转让	并购重组	公开披露
适用原则	目的明确、最少够用			选择同意、公开透明、确保安全、主体参与						
核心业务功能 1（示例：支付）	身份信息、银行账户等	1	1	明示同意	时间最小、去标识、加密	-	-	明示同意、安全影响评估、告知共享情况	-	-
核心业务功能 2										
…										
附加业务功能 1（示例：定位）										
附加业务功能 2（示例：理财）										
…..										

二、 《规范》明确回答了实务中的若干待定问题

1. 个人信息权属问题

《规范》创设性地提出了“个人信息控制者”概念，并将其定义为“有权决定个人信息处理目的、方式等的组织或个人”。通过这个概念，如同之前很多涉及个人信息保护问题的文件一样，《规范》继续淡化或回避个人信息权属的问题。我们认为，在个人信息保护和大数据经济发展的对立平衡中，个人信息的权属问题实际上是一个伪命题，或者至少在现阶段无法给予一个明确而清晰的界定。《规范》采用“个人信息控制者”的表述，强调了该主体为个人信息的实施控制者，而非权利所有者。其实，《规范》巧妙地处理该问题，并不会影响个人信息保护整套规则的创设，相反，如此操作在现阶段不失为一个明智之举，有利于推进个人信息保护工作的整体进程，而不至于形成一个前提性障碍。

2. 收集环节中的同意规则

实践中，同意规则的异化是个行业普遍现象，对于很多网络运营者来说，让用户注册时认可其隐私政策文本是一种常见的高效率低成本的获取用户同意方式。而该类隐私政策文中往往使用笼统和模糊的措辞并以此获得用户的概括授权，从而达成减轻甚至免除己方责任的目的。而《规范》则较为详细地规定了用户知情同意规则的具体合规要求。

《规范》第 5.3 条提出个人信息收集的总要求：收集个人信息前，应当明确告知收集有关的情况，并获得个人信息主体的授权同意。我们认为此处的“授权同意”包括“明示同意”和“默示同意”。《规范》第 5.5 条则将网络产品或服务的业务功能分为核心业务功能和附加业务功能，对收集个人敏感信息的同意要求作了进一步的特别规定。

以收集个人敏感信息为例，根据《规范》第 5.5 条，若为核心业务功能所必需而收集，网络运营者应当向个人信息主体告知所收集的具体个人敏感信息，并明确告知拒绝提供或拒绝同意将带来的影响，应允许个人信息主体选择是否提供或同意自动采集；而若为其他附加功能而收集个人信息的，收集前应向个人信息主体逐一说明个人敏感信息为完成何种附加功能所必需，并允许个人信息主体逐项选择是否提供或同意自动采集个人敏感信息。当个人信息主体拒绝时，可不提供相应的附加功能，但不应以此为理由停止提供核心业务功能，并仍应保障相应的服务质量。鉴于附加业务功能的非

必要性，为该等功能而收集个人信息的合规要求显然更为苛刻。

也就是说，在网络产品或服务涉及个人信息收集时，应分三步进行考虑：

- 第一步，判断是否属于收集行为。某些产品或服务进在本地访问的方式获取了客户信息的方式可能不属于收集行为，也就不需要信息主体授权；
- 第二步，在确认属于收集行为的基础上，区分产品或服务的核心业务功能和附加业务功能。对于前者，仍可使用隐私政策文本等方式获得概括授权同意，对于后者则应当采取逐一授权的方式来获取明确的同意；
- 第三步，区分该信息属于一般个人信息还是个人敏感信息。对于前者，企业可以采取概括授权，包括“默示同意”（Opt-Out）和“明示同意”（Opt-In）；但对于后者，企业则只能采取“明示同意”的方式，即需要个人信息主体作出书面声明或者肯定性动作，例如主动勾选、主动点击“同意”等。

表 2：授权同意的方式

信息 / 业务	个人敏感信息	一般个人信息
核心业务功能	应当明示同意	明示或默示同意
附加业务功能	应当逐一明示同意	明示或默示同意

关于隐私政策文本，中央网信办、工信部、公安部、国家标准委等四部门组成的专家工作组于 2017 年 8 月 24 日至 9 月 24 日期间对 10 款网络产品和服务的隐私条款进行评审，评审结果显示 10 款产品和服务在隐私政策方面均有不同程度的提升。随后，上述 10 款产品所属公司也共同签署了《个人信息保护倡议书》，倡议内容包括“尊重用户的知情权”、“遵守用户授权，强化自我约束”等。值得注意的是，《规范》也详细地规定了《隐私政策》的主要内容及合规要求，并在附录中以 9 页的篇幅展示了隐私政策模板，为各个平台和 APP 制定《隐私政策》提供了重要的参考指引。

3. 间接获取个人信息时的有限尽调

个人信息控制者获取个人信息的来源，除了个人信息主体主动提供或者个人信息控制者自动收集之外，还存在从第三方个人信息提供方间接获取的可能性。就该种个人信息来源而言，《规范》做出了明确的规定：

1) 应要求个人信息提供方说明个人信息来源，并对其个人信息来源的合法性进行确认；

2) 应了解个人信息提供方已获得的个人信息处理的授权同意范围，包括使用目的，个人信息主体是否授权同意转让、共享、公开披露等。如本组织开展业务需进行的个人信息处理活动超出该授权同意范围，应在获取个人信息后的合理期限内或处理个人信息前，征得个人信息主体的明示同意。

上述规定，对于个人信息控制者从第三方渠道间接获取信息数据提出了审慎注意的义务和要求。而为满足上述合规要求，从方法论上而言，相关企业必须对个人信息提供方的相关业务行为进行有限

但必要的尽职调查，审阅该提供方的相关政策文件，审查其个人信息保护行为，从而最大化的保护自身的利益。

4. 服务终止后信息数据的保存和处理

对于个人信息的保存环节，《规范》根据个人信息保护的“最少够用原则”以及“确保安全原则”，提出了个人信息保存时间最小化、去标识化处理的具体要求。对个人敏感信息的储存，还要求个人信息控制者采用加密等安全措施，对于其中的个人生物识别信息，还应先行采用技术措施加以处理。

对于实践中用户较为关心的服务终止后控制者如何继续保存和使用用户个人信息的问题，《规范》明确了解决措施：个人信息控制者在停止运营其产品和服务时，应当停止收集活动、逐一送达或公告的形式通知个人信息主体，并对所持有的个人信息进行删除或匿名化处理。

5. 流转环节中的三方关系处理规则

如果说前面的讨论内容都是涉及个人信息控制者和个人信息主体之间的双方关系，那流转环节其实主要就是规范了三方关系的处理。《规范》在该部分重点介绍了涉及第三方的个人信息处理环节中的规范要求，并明确区分了个人信息“委托处理”、“共享”、“转移”、“公开披露”、“共同控制”和“并购重组”等各种情形及其适用规则。

对于个人信息控制者将用户个人信息委托他人处理时，《规范》明确了个人信息控制者不得超越授权范围，且应当对委托行为进行个人信息安全影响评估。根据《规范》，个人信息原则上不得共享、转让和公开披露。需要进行上述操作时，应当事先征得个人信息主体的同意，涉及个人敏感信息的，应当征得该信息主体的明示同意。同时，也应当对信息受让方进行个人信息安全影响评估，并且告知个人信息主体共享、转让和公开披露的具体情况。

在《规范》第 8.2 条“个人信息共享、转让”部分，尤其需要提请注意的是其中的 e）项，即“承担因共享、转让个人信息对个人信息主体合法权益造成损害的相应责任”。我们理解，这里的责任，既包括个人信息控制者在共享和转让过程中因为自身的原因造成信息泄漏或损毁等不良事件，也包括个人信息控制者未能对接收方尽到审慎调查义务，将个人信息共享或转让给了不具备相应信息安全能力的接收方。而后一种情形应当引起提供方更多的重视，因为这种情形下相应的个人信息已经超出自身的掌控范围，风险系数已经放大。

此外，在附件 D“隐私政策模板”中，《规范》其实在一定程度上明确给予了“附属公司/关联公司”和“授权合作伙伴”（如供应商、服务提供商等）的有限信息使用权。对于收购、兼并、重组等情形中的个人信息转让，个人信息控制者负有告知义务，如变更个人信息使用目的时，还应重新取得个人信息主体的明示同意。

6. 《规范》的其他亮点

此前，《网络安全法》等法律法规虽曾给出个人信息的定义，但并未明确与个人信息处理相关的一些关键术语。对此，《规范》就很多与个人信息保护实务密切相关的概念做出了回应，例如个人敏感信息、个人信息主体、个人信息控制者、收集、明示同意、用户画像、删除、公开披露、转让、共享、匿名化、去标识化等，为实务操作提供了明确的指引。

还值得一提的是，《规范》最后以资料性附录的形式提供了个人信息示例、个人敏感信息判定、

保障个人信息主体选择同意权的方法和隐私政策模板，不仅颇具特色，而且使得《规范》结构更加完整。前两项附录列明了个人信息、个人敏感信息的范围和类型，将实践中存在争议的网络身份标识信息、个人上网记录等信息均明确列入个人信息范畴中。后两项附录则以模板的方式直观展现了相应的功能界面和政策文本，具有极高实践参考价值。尤其是隐私政策模板，相信会被很多互联网公司或平台型公司所广泛参考和采用。

三、 对企业的建议

《规范》对《网络安全法》中提及的个人信息保护相关条款进行了详细的规定，虽然部分规定略显严苛，对于企业的合规要求也明显提高，从而会导致企业运营成本的相应增加。但相比于此前的制度空白，该标准的出台无疑为企业合规政策的拟定和对个人信息的保护提供了较为全面的指引。

因此，我们建议企业尽早完善内部合规制度。规模达到一定条件的企业应明确责任部门和负责人员，对于从事大数据业务的企业来说，首席信息官（Chief Information Officer，“CIO”）的职位设置或将成为常态。此外。企业还需建立个人信息岗位人员管理及培训制度、个人信息安全影响评估制度及审计制度、个人信息安全事件处置与报告制度等，并且在个人信息处理全生命周期的各个环节严格遵守《网络安全法》、《规范》及其它配套规则的要求。

值得注意的是，虽然《规范》仅是推荐性国家标准，原则上并不强制要求各类组织执行，但并不意味该标准无足轻重。《规范》开篇就提及“适用于主管监管部门、第三方评估机构等组织对个人信息处理活动进行监管、管理和评估”。而在近期刚发生的某热点事件中，网信办相关负责人也强调了《规范》所提倡的精神。由此可见，该标准虽然为推荐性标准，但在实践中，将可能被作为政府部门的监管与执法的重要参考依据，因而应当引起网络运营者的足够重视。

汉坤网络安全和数据合规系列：

之一：健康医疗大数据领域的政策和法律问题

之二：《网络安全法》简评

之三：数据出境不再任性

之四：网安审查，大幕开启！

之五：个人信息保护，刑法的归刑法

之六：数据出境安全评估，操作指南来了！

之七：CII，网安法核心制度重磅落地

特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国法律及实务的最新动态和发展，上述有关信息不应被看作是特定事务的法律意见或法律依据，上述内容仅供参考。

如您对上述内容有任何问题或建议，请与汉坤**唐志华律师（+8621-6080 0905; david.tang@hankunlaw.com**）、或**朱敏律师（+8621-6080 0955; min.zhu@hankunlaw.com**）联系。