个人信息保护标准实施对组织合规的影响

在当前的数据治理框架下，个人信息保护无疑是最受关注的内容之一，2018 年以来，随着我国国家标准 GB/T 35273-2017《信息安全技术个人信息安全规范》标准的实施，以及欧盟通用数据保护条例（GDPR）的生效，个人信息保护的热度进一步攀升。本文就当前形势下，数据安全与个人信息保护的核心内容，以及组织如何使用国家标准开展个人信息保护合规工作进行简要论述，以供参考。

数据安全和个人信息保护的关系

众所周知，当前网络安全的内涵和外延已经和从前有很大不同，尤其是数据安全已成为近年来的高频词，同时其包含的内容也有所扩展，比如，原来看到的数据安全事件，大部分总结起来就是两个字“泄漏”。但从 2017 年开始，很多数据安全事件不只是泄漏问题，菜鸟与顺丰、华为与微信关于数据的争端，支付宝的帐单事件，大数据杀熟，嘀嘀顺风车个人标签不可修改等等。这些新事件与原来网络安全中所强调的保密性、完整性、可用性几乎没有关联，所以亟待一些新的要求和规定，来完善数据安全方面的治理方法。

其次，数据安全因相关方不同呈现不同的保护需求。比如，从企业角度出发，其主要关注的是“商业秘密保护”；从个人角度出发，个人处于相对弱势的位置，需要国家通过公权力的方式对组织提出相关要求，让组织能够保护好个人信息；此外，从国家安全、社会公共利益角度来看，与其相关的重要数据则需要额外的保护措施。如何理解重要数据的概念，打个比方，现在很多场景都可以对个人进行精确画像，以致于对个人生活习惯、行踪轨迹等非常了解，一旦数据滥用、泄露对个人造成的伤害也会更加精准和严重。换个角度，如果对关键信息基础设施或者对一种社会现象、一类社会群体，同理也可以进行精确画像，这类重要数据一旦被恶意使用很可能会对公共利益产生危害，甚至影响国家安全。

个人信息保护，简单来说，是从个人权益角度出发看数据安全问题，而正是因为个人观点、立场等的差异性，个人信息用途的多样化，导致个人信息保护变得格外复杂，也促使对个人信息保护的治理手段趋向于多元化。目前，纵观全球，通过监管处罚、法律诉讼、企业自律、推广实践、宣传引导等一系列方式进行综合治理成为了主流做法。自《网络安全法》实施以来，我国进一步加快个人信息保护治理工作的步调，其综合治理的框架已逐步完善，国家标准《个人信息安全规范》的发布正是其中重要的一个环节，标准对于各类组织个人信息保护方面的合规和自律工作有着重要的指导意义。

《个人信息安全规范》标准的适用价值

《个人信息安全规范》标准于 2016 年立项，于 2017 年底正式发布，从当前全国信息安全标准化技术委员会立项的个人信息保护相关标准来看，正在制定过程中的标准有《个人信息去标识化指南》、《个人信息安全影响评估指南》、《数据出境安全评估指南》等，2018 年新立项标准《个人信息安全工程指南》制定项目，以及《个人信息告知同意指南》研究项目，可见以《个人信息安全规范》为基础的个人信息保护标准体系已现雏形。因此，以《个人信息安全规范》为组织个人信息保护合规的基础，是构建完善、可持续的个人信息保护体系。

从《个人信息安全规范》标准的适用范围来看，标准的推荐使用对象比较广泛，包括各类作为数据控制者的组织，还有主管监管部门、第三方机构等。事实上，《个人信息安全规范》已经得到了非常广泛的关注与应用，以主管监管部门为例，2017 年 7 月 -9 月，中央网信办等四部门指导，信安标委秘书处组织十款产品隐私条款评审过程中，大量参考了标准的相关要求，2018 年 1 月，国家网信部门在通报“支付宝年度账单事件”时，提及了标准。2018 年 5 月，银保监会发布《银行业金融机构数据治理指引》提到应符合相关标准，2018 年 4 月，我国政府在“联合国打击网络犯罪政府专家组”会议的有关评论意见中论述了标准的重要作用。除此之外，各行各业开展了很多关于《个人信息安全规范》标准有关的宣贯、研讨、实务等活动，进一步扩大了标准的影响力。

从标准主体内容来看，首先，标准明确了个人信息、个人敏感信息、个人信息控制者、个人信息主体、收集、去标识化、匿名化、共享、转让等重要的定义，这对规范个人信息处理相关用词的规范性，以及界定相应措施和责任有着很好的支撑作用；其次，标准所提出的个人信息安全七大原则，一方面和国际通行的原则保持一致，另外强调了权责一致原则的重要性，即一旦出现侵害个人信息主体的情形，个人信息控制者应承担相应责任。标准的主体内容中，分别从收集、保存、使用、委托处理、共享、转让、公开披露各环节提出相应要求，同时提出了组织的相关管理要求。在标准制定过程中，以解决问题的实效性为根本出发点，兼顾与国际接轨增加全面性，同时兼顾考虑要求自身的可操作性以及平衡发展的需求，设置了主体的条款内容，形成了适应当前国情需要，可有效指导组织提升个人信息保护水平的最佳实践。

《个人信息安全规范》标准合规实践思路

从组织实践角度出发，要落实标准要求，实现全面、可持续的合规管理，可以参考以下思路。

总体来看，组织应从两个角度全面考虑个人信息安全工作，一是对内建立体系，二是对外接受监督；其次，从落实责任、关键工作、能力提升三方面逐步提升个人信息保护水平；此外，如果组织有多款产品或服务涉及个人信息处理，应主动向不同产品线拓展个人信息保护工作，如果组织属于平台运营方，其生态内涉及用户从平台入口访问众多合作伙伴的产品或服务，或生态内有密切的业务合作，同样应基于平台管理者角色，主动向平台生态内合作伙伴提出相应的个人信息安全要求，以带动整体保护水平的提升。

在落实责任层面，其一，个人信息保护合规工作开展的顺利与否直接取决于组织的负责人是否重视，是否提供了足够的资源保障，标准强调了“组织应明确其法定代表人或主要负责人对个人信息安全负全面领导责任”；其二，组织的多个部门应进行明确分工，形成以责任部门和责任人为核心的组织架构；其三，责任部门和责任人应根据组织所运营的产品或服务的具体特点，制定个人信息保护的目标、方针等策略性文件，以及相应的工作计划，比如可以选取一款典型产品就当前情况与《个人信息安全规范》标准要求进行差距分析，全方位识别弱点环节，为制定工作计划提供参考。

在关键工作层面，其一，建立和维护个人信息清单尤为重要，拥有完善的个人信息清单是组织全面、有效、持续实施的个人信息安全保障措施的重要前提，对组织所持有的个人信息可知、可查，对组织个人信息处理活动可视、可溯，也是组织个人信息安全保障能力的重要体现；其二，实施个人信息安全影响评估（PIA）有助于组织提前发现和预防风险事件。比如，在产品设计、上线前进行个人信息安全影响评估，分析对个人权益可能造成的影响，如个人的自主权利、引发差别待遇、精神压力、财产损失等，进一步采取相应措施降低风险，为产品和业务稳定上线运营提供保障。就个人信息安全影响评估，

国家标准《个人信息安全影响评估指南》正在制定中，进一步提供了细致实用的参考；其三，发布隐私政策接受社会监督。隐私政策是体现组织个人信息保护策略公开透明的重要举措，是个人以及社会了解组织的窗口，组织应基于上述步骤的工作成果，归纳总结相关策略、规则，形成完善的隐私政策，体现重视个人信息保护工作，主动接受监督的态度。《个人信息安全规范》标准附录中给出的隐私政策的模板可以作为参考。

在能力提升方面，组织应建立个人信息保护的技术体系，采用技术手段和工具系统强化个人信息安全能力。其一，应加强数据安全能力，避免防止个人信息的泄漏、损毁、丢失。加强数据安全能力已有很多现有途径可选，比如采取参考国家有关数据安全能力成熟度标准强化安全能力，参照等级保护、云计算服务相关标准加强系统和平台安全等；其二，积极采取去标识化措施降低个人信息处理的风险，个人信息去标识化是普遍被认为最有效、简便的降低风险的措施，组织应该充分结合业务场景考虑使用此种方法，正在制定的国家标准《个人信息去标识化指南》对去标识化过程和管理措施给出了详尽的参考；其三，应逐步在产品中实现隐私设计（Privacy-by-design）和默认隐私（Privacy-by-default）理念，将个人信息保护与产品功能体验相结合，实现个人信息主体权利实施的便捷化。此外，合规能力的展现也是组织应该重视的工作，一方面有助于以合规推动业务发展，另一方面可适当减少对接监督管理工作的成本。

总之，以数据为驱动力的时代已然来临，数据安全的合规能力将成为组织赖以生存和发展的必备技能，同时也是构建开放、包容、安全、有序的数字社会的重要前提。