环球律师事务所 GLOBAL LAW OFFICE SINCE 1979

Microsoft

国内外标准兼容下的个人信息合规体系构建

2021年5月

版权声明

编撰团队

北京市环球律师事务所

孟洁、张淑怡、王程、许国盛、董杰睿

微软公司

李思宏、王劲松

联系人：

孟洁

电话：010-65846768

邮箱：mengjie@glo.com.cn

导 读

什么是 ISO/IEC 27701 标准？以及该标准有哪些内容？

国际标准化组织（International Organization for Standardization，ISO），于 2019 年 8 月 5 日发布了 ISO/IEC 27701:2019（简称《ISO/IEC 27701》），作为用于隐私信息管理的《ISO/IEC 27001》和《ISO/IEC 27002》的扩展，在组织范围内增强保护隐私信息的力度。其保护对象为个人可识别信息（Personally Identifiable Information，PII），规制对象为 PII 控制者与 PII 处理者。

《ISO/IEC 27701》由正文和附件共同组成，其中正文分为八个部分，附件分为七个部分。

一、正文部分

第一部分为标准范围介绍。《ISO/IEC 27701》对《ISO/IEC 27001》和《ISO/IEC 27002》进行了扩展，建立、实施、维护和持续改进隐私信息管理系统（PIMS），并在组织范围内进行隐私管理，为 PII 控制者和 PII 处理者在处理 PII 过程中应承

担的责任和义务提供了指引。《ISO/IEC 27701》适用于作为在信息安全管理系统（ISMS）中处理 PII 的 PII 控制者和 PII 处理者的所有类型和规模的组织，包括国有和私营公司、政府实体和非营利组织。

第二、三、四部分，分别介绍了《ISO/IEC 27701》参考的国际标准文件、使用的术语、定义和缩略词，以及该标准的行文结构。

第五部分介绍了《ISO/IEC 27001》中关于 PIMS 的规定以及该标准对 PIMS 的附加规定。从以下七个方面对 PII 控制者和 PII 处理者进行规范和指导，包括：组织的背景、领导、风险处置的预先计划、支持手段、操作方法、绩效评估、改进措施。

第六部分介绍了《ISO/IEC 27002》中关于 PIMS 的规定以及该标准对 PIMS 的附加规定。从以下十四个方面对 PII 控制者和 PII 处理者进行规范和指导，包括：信息安全政策、信息安全负责组织、人力资源安全、资产管理、访问控制、加密措

施、物理与环境安全、操作安全、通信安全、系统获取、开发与维护、供应商关系、信息安全事故管理、信息安全方面业务的连续性管理和合规要求。

第七部分介绍了《ISO/IEC 27002》中对于 PII 控制者的相关规定以及该标准对于 PII 控制者的附加规定。从以下四个方面对 PII 控制者的权利义务进行进一步规范和指导，包括：PII 收集和处理条件、对 PII 信息主体的义务、设计隐私和默认隐私、PII 的共享、传输和公开披露。

第八部分介绍了《ISO/IEC 27002》中对于 PII 处理者的相关规定以及该标准对 PII 处理者的附加规定。从以下四个方面对 PII 处理者的权利义务进行进一步规范和指导，包括：PII 收集和处理的条件、对 PII 信息主体的义务、隐私设计和默认隐私、PII 的共享、传输和披露。

二、附表部分

附件 A 列出了 PII 控制者在实现 PIMS 时所需采取的控制目标和控制措施，包括 PII 控制者委托 PII 处理者，或与另一

个 PII 控制者共同控制 PII 的情形。

附件 B 列出了 PII 处理者在实现 PIMS 时所需采取的控制目标和控制措施，包括聘请分包商处理 PII 的情形。

附件 C 将《ISO/IEC 27701》与 GDPR（第 5 至 49 条）进行比较和映射，以体现遵守《ISO/IEC 27701》标准的要求和控制措施与履行 GDPR 要求义务的相关性。

附件 D 将《ISO/IEC 27701》与《ISO/IEC 29100》进行比较和映射，以指示遵守《ISO/IEC 27701》标准的要求和控制措施与《ISO/IEC 29100》中规定的隐私保护基本原则的相关性。

附件 E 将《ISO/IEC 27701》与《ISO/IEC 27018》和《ISO/IEC 29151》进行比较和映射，以体现《ISO/IEC 27701》标准规定的要求和控制措施与《ISO/IEC 27018》和《ISO/IEC 29151》的规定保持一致。

附件 F 列出了《ISO/IEC 27701》使用的术语，并指出其他司法管辖区所使用的具有相同或相似含义的替代术语。

附件 G 介绍了《ISO/IEC 27701》对《ISO/IEC 27001》和

《ISO/IEC 27002》规制范围的扩展，以及扩展条款的对应方法和应用样例。

从上述解读和与以往发布的国际标准的比较可以看出，《ISO/IEC 27701》在《ISO/IEC 27001》和《ISO/IEC 27002》的基础上对 PII 控制者和 PII 处理者进行了更高标准的安全管理，使得隐私信息管理系统的规范更加全面，能够实际应用于不同规模、不同文化环境组织的 PII 保护。

本报告通过对比《GB/T 35273》（2020 版本）与《ISO/IEC 27701》，梳理出两项标准的关系及在个人信息全生命周期角度控制措施以及企业内部架构角度的建议要求，旨在协助企业了解组织安全管理的底线与需求，指导企业对个人信息安全落地软着陆。本报告将不仅有利于企业完成在中国大陆的数据合规工作，也将为未来项目出海、适用其他法域规定打下良好的基础，更有助于进一步切实落地各国的具体要求，构建更加完备的一体化隐私与信息安全保护体系。

目　　录

一、概述

2019 年 8 月 6 日，国际标准化组织（International Organization for Standardization，ISO）与国际电工委员会（International Electrotechnical Commission, IEC）正式发布了《ISO/IEC 27701 安全技术—对用于隐私管理的 ISO/IEC 27001 和 ISO/IEC 27002 的扩展—要求和指南》（以下简称“《ISO/IEC 27701》”）。作为对 ISO/IEC 27001 和 ISO/IEC 27002 的扩展，《ISO/IEC 27701》旨在明确建立、实施、维护和持续改进**隐私信息管理体系（PIMS）**，并提供相关指南，为处理者和控制者提供了与 PIMS 相关的落地性合规指引。

在《ISO/IEC 27701》发布前，《ISO/IEC 27001》作为国际上公认的信息安全管理体系标准，仅提出了信息安全管理体系的基本要求；《ISO/IEC 27002》则为在组织内启动、实施、保持和改进信息安全管理措施提供了实施指南。此外，无论《ISO/IEC 27001》还是《ISO/IEC 27002》都未能区分 PII 控制者和 PII 处理者二类不同受规制的对象在实现和满足不同国家和地区的隐私保护管理的全面要求。因此，新的国际标准《ISO/IEC 27701》隐私信息管理体系应势而生。一方面，《ISO/IEC 27701》在《ISO/IEC 27001》和《ISO/IEC 27002》的基础上，将保护目

标由单独的信息安全扩大为信息安全+隐私安全；另一方面，《ISO/IEC 27701》明确区分了 PII 控制者和 PII 处理者，以助力组织更好地保护用户隐私和个人信息的内部合规管理。

此外，欧盟 GDPR 数据保护机构（European Data Protection Board）积极参与了《ISO/IEC 27701》的落地，具体体现在《ISO/IEC 27701》附录 D 提供的《ISO/IEC 27701》与 GDPR 的条文比对，展示了《ISO/IEC 27701》与 GDPR 在合规措施方面的异同：两者在总体维度与要求上相差不多，国际上认为《ISO/IEC 27701》是目前与 GDPR 合规思路最为接近，在满足 GDPR 合规基础上落地《ISO/IEC 27701》实践难度非常小。

2017 年 12 月 29 日，在中国大陆地区，全国信息安全标准化技术委员会（以下简称“信安标委”）首次发布《信息安全技术 个人信息安全规范》（2017 版本）（以下简称“《GB/T 35273》（2017 版本）”）；后经过几轮对《GB/T 35273》（2017 版本）的征求意见与修改，2020 年 3 月 6 日，信安标委在初版实践的基础上，发布了《信息安全技术 个人信息安全规范》（2020 版本）（以下简称“《GB/T 35273》（2020 版本）”）。尽管《GB/T 35273》（2020 版本）仍然是国家推荐性标准，但在我国《个

人信息保护法（草案）》尚未正式发布之前，《GB/T 35273》（2020 版本）将仍然成为企业个人信息保护合规工作实际依赖的重要标尺与操作指南。

总体而言，《ISO/IEC 27701》和《GB/T 35273》（2020 版本）在个人信息处理的控制措施方面整体要求比较相似，虽然针对细节要求各自又有独特规定与侧重点；但《ISO/IEC 27701》对组织如何构建隐私安全管理体系进行了系统化的论述，而《GB/T 35273》（2020 版本）在第 10 和 11 章对组织的个人信息管理要求进行规定。故本报告将从两个维度进行分析，一方面，从控制措施的角度并按照《GB/T 35273》（2020 版本）的逻辑思路，梳理并对比两份标准的相关规定，归纳出各自的重点，以兹能够提供读者相互借鉴的思路；另一方面，从组织内部管理体系的构建角度，分析两份标准的异同，并指出《ISO/IEC 27701》对企业构建内部合规架构的帮助，以为企业进行数据合规工作提供更加全面、完备、具有可实践的操作指引。

二、组织控制措施对比分析

1. 适用范围

1.1 适用的情形与主体

从适用的情形（即被规制的对象）来看，《GB/T 35273》（2020 版本）和《ISO/IEC 27701》均是针对个人信息的处理活动进行了规范。但从适用的主体（被规制对象）来看，两份文件在撰写思路上存在差异，进而导致适用范围可能存在细微差异。具体而言：

《GB/T 35273》（2020 版本）聚焦于规范个人信息整个生命周期内的数据处理活动，除 9.1 c）涉及受委托者（处理者）的若干义务外，主要规范了数据控制者在开展收集、保存、使用、共享、转让、公开披露等个人信息处理活动各个环节中应遵循的保护原则和安全要求。根据不同的使用目的和方式，《GB/T 35273》（2020 版本）既适用于进行个人信息处理活动的数据控制者，也适用于对个人信息处理活动进行监督、管理和评估的主管监管部门、第三方评估机构等组织。

而《ISO/IEC 27701》则以处理个人信息时组织所担任的角色为切入

点，将标准的适用范围定义为信息安全管理体系（ISMS）中处理 PII（个人可识别信息）的 PII 控制者和/或 PII 处理者的所有类型和规模的组织，包括公共和私营公司、政府实体和非营利组织。

1.2 适用的地域范围

从适用的地域范围来看，由于《GB/T 35273》（2020 版本）是国内的标准，通常不具有域外效力。

相较而言，《ISO/IEC 27701》的适用范围更加广泛，该标准属于 ISO 管理体系标准（包括特定行业的标准，旨在能够单独或作为一个组合管理体系来实施），是一个国际标准。同时，需要注意的是，根据《ISO/IEC 27701》的规定，针对不同国家和地区保护 PII 的要求和指引，还需要确保符合当地相关法律法规的要求，结合当地的法律法规进行本地化解读。

2. 信息类别

《GB/T 35273》（2020 版本）和《ISO/IEC 27701》均将拟处理的信息分为两类，分别为个人信息和特殊类别信息（含个人敏感信息）。

2.1 个人信息

《GB/T 35273》（2020 版本）和《ISO/IEC 27701》对于个人信息采用了不同的表述方式，前者使用的是“personal information”，后者则使用“personal identifiable information”，但两个定义在本质上是相同的，均采用了“识别”加“关联”的认定方法。

具体而言，《GB/T 35273》（2020 版本）项下的个人信息定义为“**以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。**”因此，在判定何为个人信息时，通常考虑两条路径：

一是“识别”，即从信息到个人，由信息本身的特殊性识别出特定自然人，个人信息应有助于识别出特定个人；

二是“关联”，即从个人到信息，如已知特定自然人，则由该特定自然人在其活动中产生的信息 （如个人位置信息、个人通话记录、个人浏览记录等）推导出某个特定人，也属于个人信息。

《ISO/IEC 27701》项下的个人可识别信息（以下简称“PII”）[1]的定义为：“**与信息主体相关且可用于识别特定主体的任何信息；或直接或间接与 PII 主体关联的任何信息**”。

由此可以看出，《GB/T 35273》（2020 版本）和《ISO/IEC 27701》在个人信息的定义上均有可“识别”或者可“关联”的要素，在本质上并无差异。

2.2 个人敏感信息/特殊类别的个人信息

《GB/T 35273》（2020 版本）和《ISO/IEC 27701》均适用于特殊类别的个人信息主体。然而，两者有所区别的是，《GB/T 35273》（2020 版本）采用的术语为“个人敏感信息”；《ISO/IEC 27701》采用的术语为“特殊类别的 PII”。尽管两者在健康信息和与儿童有关的信息方面存在一定的交集，但与《ISO/IEC 27701》的概括式定义不同，《GB/T 35273》（2020 版本）采用的是概括式定义+具体举例的方式，企业在实操中，往往更加容易通过所举的例子理解并判断自己所控制或者处理的数据是否属于个人敏感信息。具体而言：

[1] 《ISO/IEC 27701》没有直接定义个人可识别信息，而是引述《ISO/IEC 27000》和 《ISO/IEC 29100》的定义。

《GB/T 35273》（2020 版本）对“个人敏感信息”的概括式定义为，“个人敏感信息，是指一旦被泄露、非法提供或滥用，可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等后果的个人信息”，并且，附表 B 中举出的实际样例为一般企业较容易出现的情况，如下表所示：

个人财产信息	银行账户、鉴别信息(口令)、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息
个人健康生理信息	个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等
个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等
个人身份信息	身份证、军官证、护照、驾驶证、工作证、社保卡、居住证等
其他信息	性取向、婚史、宗教信仰、未公开的违法犯罪记录、通信记录和内容、通讯录、好友列表、群组列表、行踪轨迹、网页浏览记录、住宿信息、精准定位信息等

《ISO/IEC 27701》采用的术语是“特殊类别的 PII”，但因考虑到各国因不同的文化环境对于何为特殊类别的 PII 在理解上有可能存在差异，而《ISO/IEC 27701》并未对“特殊类别的 PII”下明确的定义，而是通过提示某些类别的 PII 如儿童信息、健康信息属于特殊类别的 PII，要求组织对于该类信息应当给予更多重视与更高级别的保护。并且，《ISO/IEC 27701》明确要求组织在标准落地时，即构建 PIMS 时应当结合所适用国家的本国数据保护法要求以及本国法域中对该概念所做的相关规定，切合于本地适用情况进行理解与操作。由此，给各国的企业实操留下了充足的自治空间。

3. 规制对象

3.1 个人信息控制者

《GB/T 35273》（2020 版本）和《ISO/IEC 27701》[2]对个人信息控制者的定义具有相似性，即规定个人信息控制者是指“有能力决定个人信息处理目的、方式等的组织或个人”。

[2] 《ISO/IEC 27701》并没有直接定义个人信息控制者，而是引述了《ISO/IEC 29100》和《ISO/IEC 27000》中的定义。

不同之处在于，《ISO/IEC 27701》规定，如果自然人出于个人目的使用数据，该自然人不构成 PII 控制者；《GB/T 35273》（2020 版本）则没有正面回应此问题。

3.2 共同控制者

（1）共同控制者的定义

《GB/T 35273》（2020 版本）没有给出“共同控制者”的明确定义，而是直接针对该场景下个人信息控制者提出要求，并举例第三方插件未单独征得个人信息主体同意收集个人信息这一特定情形明确第三方插件提供方[3]与网站运营者在个人信息收集阶段为共同个人信息控制者。《ISO/IEC 27701》对“共同控制者”作出了明确、单独的定义，即“共同控制者是指可以共同确定处理目的和处理方法的两个或多个个人信息控制者”，因此只要符合“共同控制者”定义所描述情形的企业，都应当履行“共同控制者”的相关义务与责任。在此情境下，根据《ISO/IEC 27701》对“共同控制者”的明确定义可从侧面帮助理解《GB/T 35273》（2020 版本）中“共同控制者”这一概念。

[3] 例如网站经营者在其网页或 App 中部署的统计分析工具、软件开发工具包 SDK、调用地图 API 接口等。

（2）对共同控制者的具体规制要求

《GB/T 35273》（2020 版本）和《ISO/IEC 27701》对共同控制者的规制要求基本是相似的，即均要求共同控制者之间：

（a）应当签订合同等形式明确各控制者的责任和义务。

（b）向数据主体明确（透明）告知双方应分别承担的责任和义务。

在具体描述上，《GB/T 35273》（2020 版本）要求“当个人信息控制者与第三方为共同控制者时（例如服务平台上的签约商家），个人信息控制者应当通过合同等形式与第三方共同确定应满足的个人信息安全要求，以及在个人信息安全方面自身和第三方应分别承担的责任和义务，并向个人信息主体明确告知。如未向个人信息主体明确告知第三方身份、以及在个人信息安全方面自身和第三方应分别承担的责任和义务，个人信息控制者应承担因第三方引起的个人信息安全责任”。

《ISO/IEC 27701》则要求“组织应与任何共同个人信息控制者确定处理个人信息（包括个人信息保护和安全要求）方面各自的角色和责任；应以透明的方式确定处理个人信息的角色和责任；应满足适用的法律和/或法规的要求。同时，这些角色和责任应记录在合同或任何类似的

涉及处理个人信息条款和条件的约束性文件中[4]”（例如，在某些司法管辖区内，这种协议被称为“数据共享协议”）。

3.3 个人信息处理者

《GB/T 35273》（2020 版本）并没有定义或使用个人信息处理者这一术语，需要结合“委托处理”条款相关的具体要求进行理解，从本推断出从本质上可以推断出《GB/T 35273》（2020 版本）已经涵盖了对“个人信息处理者”的规定；而《ISO/IEC 27701》则明确定义了 PII 处理者[5]，其定义为：听从 PII 控制者的指令，代表 PII 控制者处理 PII 的相关者。两部标准对于委托处理者的具体要求，请参见本报告第 7.1 节的分析。

4. 个人信息的收集

[4] 共同控制者之间签订的协议内容包括以下内容：（1）PII 共享的目的/PII 共同控制者关系；（2）作为 PII 共同控制者关系一部分的组织（PII 控制者）的身份；（3）根据协议共享和/或转让和处理的 PII 的类别；处理操作概述（如转让、使用）；（4）各自角色与职责的描述；（5）实施 PII 保护的技术和组织安全措施的责任；（6）PII 泄露时的责任确定（例如，谁将在何时互相通知信息）；（7）PII 的保留和/或清除条款；（8）未能遵守本协议的责任；（9）如何履行对 PII 信息主体的义务；（10）如何向 PII 信息主体提供有关共同控制者之间安排的本质内容的信息；（11）共同控制者之间协议的核心内容；（12）PII 信息主体如何获取其有权接收的其他信息；（13）PII 信息主体的联系点。

[5] 《ISO/IEC 27701》没有直接定义 PII 处理者，而是援引了《ISO/IEC 29100》的规定。

《GB/T 35273》（2020 版本）	《ISO/IEC 27701》
合法性 **（第 5.1 条、第 5.4 条）**	有相似内容规定 （第 7.2.2 条）
最小必要性 **（第 5.2 条）**	有相似内容规定 （第 7.4.1 条）
多项业务功能的自主选择 **（第 5.3 条）**	颗粒度较粗，提示注意某些法域类似规定 （第 7.2.3 条）
充分、透明告知要求 **（第 5.4 条）**	有相似内容规定 （第 7.3.2 条）
收集个人信息时的授权同意与例外 **（第 3.6 条、第 3.7 条、第 5.4 条、第 5.6 条）**	有相似内容规定 （第 7.2.3 条）
个人信息保护政策 **（第 5.5 条）**	分散于多个条款 （第 6.2.1.1、6.15.1.3、7.3.9、7.4.2 条）

4.1 合法性要求

《GB/T 35273》（2020 版本）和《ISO/IEC 27701》均规定了收集、处理个人信息须获得合法依据。虽然两部标准规定的个人信息收集合法性依据在种类上基本相似，但合法依据的适用逻辑却有所不同。《GB/T 35273》（2020 版本）将征得个人信息主体同意作为个人信息合法收集的唯一依据，而将为公共利益、保护信息主体的重大权益等情形[6]作为征得同意的例外情形予以规定。不同的是，《ISO/IEC 27701》将征得同意与为公共利益、保护信息主体的重大权益等情形[7]并列，并没有做例外与否的区分，更近似于 GDPR 列举合法性事由的体例。

[6] 《个人信息安全规范（2020 版本）》规定的征得同意的例外情形包括：（1）与个人信息控制者履行法律法规规定的义务相关的；（2）与国家安全、国防安全直接相关的；（3）与公共安全、公共卫生、重大公共利益直接相关的；（4）与刑事侦查、起诉、审判和判决执行等直接相关的；（5）出于维护个人信息主体或其他个人的生命、财产等重大合法权益但又很难得到本人授权同意的；（6）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；（7）根据个人信息主体要求签订和履行合同所必需的；（8）从合法公开披露的信息中收集个人信息的，如合法的新闻报道、政府信息公开等渠道；（9）维护所提供产品或服务的安全稳定运行所必需的，例如发现、处置产品或服务的故障；（10）个人信息控制者为新闻单位，且其开展合法的新闻报道所必需的；（11）个人信息控制者为学术研究机构，出于公共利益开展统计或学术研究所必要，且其对外提供学术研究或描述的结果时，对结果中所包含的个人信息进行去标识化处理的。

[7] 《ISO/IEC 27701》规定的处理 PII 的合法依据包括：（1）PII 信息主体的同意；（2）合同的履行；（3）法律义务的遵守；（4）保护 PII 信息主体的关键利益；（5）为公共利益而执行的任务；（6）PII 控制者的正当利益。

4.2 最小必要性要求

《GB/T 35273》（2020 版本）与《ISO/IEC 27701》均规定了收集个人信息应符合“最小必要”要求。两部标准尽管表述上有所不同，但本质上均要求收集的个人信息应当与特定目的相关联，目的并且符合数量最小和必要收集的目的。具体而言：

根据《GB/T 35273》（2020 版本），收集的个人信息类型应与实现产品与/或服务的业务功能有直接关联。其中，直接关联是指没有该等信息的参与，产品与/或服务的功能便无法实现。在自动采集个人信息的场景中，采集频率应是实现产品与/或服务的业务功能所必需的最低频率。在间接获取个人信息的场景中，所获取的个人信息数量也应当是实现产品与/或服务的业务功能所必需的最少数量。

根据《ISO/IEC 27701》，组织应将 PII 的收集限定在与实现特定目的相关联、合比例以及必要收集的最小范围内，包括限定组织间收集 PII 的数量（例如，通过 Web 日志、系统日志收集 PII）。

4.3 多项业务功能的自主选择

《GB/T 35273》（2020 版本）和《ISO/IEC 27701》均提及了不强迫个人信息主体接受多项业务功能，但《GB/T 35273》（2020 版本）作为中国的本土化标准，对不强迫个人信息主体接受多项业务功能的要求更为详尽；《ISO/IEC 27701》则没有详细规定，而是提醒组织注意所涉的法域是否存在该等规定。具体而言：

根据《GB/T 35273》（2020 版本）规定，当产品或服务提供多项需收集个人信息的功能时，个人信息控制者不应违背个人信息主体的自主意愿，强迫个人信息主体接受产品或服务所提供的业务功能及相应的个人信息收集请求，对个人信息控制者的要求包括：

1) 不应通过捆绑产品或服务各项业务功能的方式，要求个人信息主体一次性接受并授权同意其未申请或使用的业务功能收集个人信息。

2) 应把个人信息主体自主作出的肯定性动作，如主动点击、勾选、填写等，作为产品或服务之特定业务功能的开启条件。个人信息控制者应仅在个人信息主体开启该业务功能后，开始收集个人信息；

3) 关闭或退出业务功能的途径或方式应与个人信息主体选择使用业务功能的途径或方式同样方便。个人信息主体选择关闭或退出特定业务功能后，个人信息控制者应停止该业务功能的个人信息收集活动;

4) 个人信息主体不授权同意使用、关闭或退出特定业务功能的，不应频繁征求个人信息主体的授权同意;

5) 个人信息主体不授权同意使用、关闭或退出特定业务功能的，不应暂停个人信息主体自主选择使用的其他业务功能，或降低其他业务功能的服务质量;

6) 不得以改善服务质量、提升个人信息主体体验、研发新产品、增强安全性等为由，强迫要求个人信息主体同意收集其个人信息。

《ISO/IEC 27701》以举例的方式提及某些法域可能对征得同意的方式存在特殊要求，例如与其他协议捆绑同意，但没有对此作出详细指导。因此，从实践的角度来看，公司或者组织可以结合利用《ISO/IEC 27701》和《GB/T 35273》（2020 版本）：以《ISO/IEC 27701》为基础搭建隐私保护合规框架的同时，利用《GB/T 35273》（2020 版本）确定在中国大陆法域内有关个人信息保护的具体要求，并落实到实处。

4.4 充分、透明告知要求

《GB/T 35273》（2020 版本）和《ISO/IEC 27701》均对告知时间和告知内容作出了规定，但在细节要求上却并不一致。就告知的时间而言，《GB/T 35273》（2020 版本）规定相对更为明确；就告知内容而言，在直接收集个人信息的情况下，《ISO/IEC 27701》对于告知具体内容的要求更高，而在间接收集个人信息的情况下，《GB/T 35273》（2020 版本）对于告知具体内容的要求上则更高。具体如下：

（1）告知的时间

根据《GB/T 35273》（2020 版本），收集个人信息的，在基本业务开启前或者扩展业务首次使用前，个人信息控制者应向个人信息主体明确告知相关信息；而《ISO/IEC 27701》未对告知的时间作严格的规定，仅要求组织应参照法律法规和商业惯例时，确定告知的时间。

（2）告知的内容

A. 直接收集时的告知

根据《GB/T 35273》（2020 版本），收集个人信息时，个人信息控制

者应当向个人信息主体明确告知收集、使用个人信息的规则，例如收集和使用个人信息的目的、方式和范围等。具体而言，当产品或服务提供多项收集、使用个人信息业务功能的，除个人信息保护政策外，个人信息控制者宜在实际开始收集特定个人信息时，向个人信息主体告知收集、使用该个人信息的目的、方式和范围，以便个人信息主体在作出具体的授权同意前，能充分考虑对其的具体影响。

此外，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。

《ISO/IEC 27701》对告知的内容作出了更高的要求，即除了告知收集个人信息的类型，以及收集、使用个人信息的规则外，还建议额外告知以下信息：

1) 信息处理的法律基础；

2) 如果未直接从 PII 主体处收集信息，应告知该信息的来源；

3) PII 主体提供 PII 是基于法定要求还是合同要求，以及未能提供 PII 的后果；

4) 处理 PII 用于自动化决策；

5) 如果处理 PII 的目的发生变更或扩展，组织应当向 PII 主体告知更新后的信息。

B. 间接收集时的告知

在间接获取个人信息的场景中，《GB/T 35273》（2020 版本）并未规定个人信息控制者对信息主体的告知义务，而是规定个人信息控制者应当要求个人信息提供方说明信息来源，并对个人信息来源的合法性进行审查与确认。同时，个人信息控制者应当了解个人信息提供方已获得个人信息主体对处理其信息的授权同意范围，包括使用目的，以及个人信息主体是否授权同意转让、共享、公开披露等。组织开展业务所需进行的个人信息处理活动超出授权同意范围的，应在获取个人信息授权后的合理期限内或处理个人信息前，再次征得个人信息主体的明示同意。

此外，《GB/T 35273》（2020 版本）规定，当涉及个人信息共享、转让的时候，数据共享方或转让方应当告知个人信息主体共享、转让个人信息的目的、数据接收方的类型以及可能产生的后果。而共享、转让个人敏感信息前，还应额外向个人信息主体告知所涉及的个人敏感信息类型、数据接收方的身份和数据安全能力。

而《ISO/IEC 27701》对间接收集的规定则相对简略，仅要求如果未直接从 PII 主体处收集信息，则组织应向 PII 主体告知信息的来源。

4.5 收集个人信息时的授权同意与例外

（1）须征得同意的情形

如第 4.1（1）节“收集合法性要求”部分所述，《GB/T 35273》（2020 版本）和《ISO/IEC 27701》均将征得同意作为收集个人信息的合法依据，但不同的是《GB/T 35273》（2020 版本）强调，在一些特殊场景下获得个人信息的，应当征得个人信息主体的“明示同意”。根据《GB/T 35273》中的定义，该“明示同意”涵盖范围较广，包含任何明确无歧义的同意；而《ISO/IEC 27701》要求同意基于自由提供、特定目的且明确无歧义要求同意基于自由意愿提供、目的特定且明确无歧义。具体而言：

根据《GB/T 35273》（2020 版本），在收集个人信息时，应当向个人信息主体告知收集、使用个人信息的目的、方式和范围，并获得个人信息主体的“授权同意”。**在特定情况下，需要征得个人信息主体的明示同**

意[8]，包括：

1）收集个人敏感信息前，应当征得信息主体的明示同意；

2）收集个人生物识别信息前，应征得个人信息主体的明示同意；

3）收集年满 14 周岁未成年人的个人信息前，应征得未成年人或其监护人的明示同意，收集不满 14 周岁的未成年人的，应征得监护人的明示同意；

4）超出授权范围使用个人信息的，应再次征得个人信息主体的明示同意；

5）共享、转让个人敏感信息或个人生物识别信息的，应征得个人信息主体的明示同意；

6）变更个人信息使用目的时，应重新取得个人信息主体的明示同意；

7）开启基本业务功能前以及重新划分基本业务功能后，征得个人信息主体对基本业务功能收集、使用其个人信息的明示同意；

[8] 明示同意时指信息主体通过书面主动声明或自主作出肯定性动作，对其个人信息进行特定处理作出明确授权的行为。肯定性动作包括个人信息主体主动作出声明（电子或纸质形式）、主动勾选、主动点击“同意”、“注册”、“发送”、“拨打”、主动填写或提供等。

8）首次使用扩展业务前，允许个人信息主体对扩展业务功能逐项选择同意；以及

9）经法律授权或具备合理事由确需公开披露个人信息时，事先征得个人信息主体明示同意。

《ISO/IEC 27701》将征得同意作为收集个人信息的合法依据之一，也提示了在特定情况下应当征得信息主体的同意。这些具体情形包括：

1）未经相关 PII 信息主体事先同意，组织不得为营销和广告目的使用合同处理的 PII。组织不应将提供此类同意作为接收服务的条件；

2）更改或扩展 PII 处理目的可能需要更新和/或修订法律依据。可能还需要另行征得 PII 主体的同意。

（2）对征得同意过程的记录

《GB/T 35273》（2020 版本）并未要求组织应当建立并记录征得同意的程序，而《ISO/IEC 27701》则对此作出了详细规定。具体而言：

《ISO/IEC 27701》要求组织对授权同意的“记录”非常重视，并作出了如下规定：

1）组织应明确记录何时需要征得同意以及征得同意的要求；

2）组织应确定并记录每一个流程，通过该流程，组织可以证明是否、何时以及如何征得 PII 主体对 PII 处理的同意；

3）组织应根据成文的程序征得 PII 主体的同意并记录在案。

（3）收集未成年人个人信息的特别规定

《GB/T 35273》（2020 版本）专门针对未成年人的个人信息收集做出了规定，而《ISO/IEC 27701》仅提及当涉及特殊主体如儿童时可能需要遵守额外的规定，并没有专门针对未成年人规定信息收集的条款。具体而言：

根据《GB/T 35273》（2020 版本），收集年满 14 周岁以上未成年人的个人信息前，应征得未成年人或其监护人的明示同意；收集不满 14 人个人信息周岁未成年人的个人信息，应征得其监护人的明示同意。

而《ISO/IEC 27701》仅提示了某些司法辖区对如何收集和征求同意

有具体要求（例如不得与其他协议捆绑）。此外，收集某些类型的数据（例如用于科学研究）和某些 PII 主体（例如儿童）的数据时，还需要遵守额外的规定。

（4）同意的撤回

《GB/T 35273》（2020 版本）和《ISO/IEC 27701》均规定了应当向信息主体提供撤回同意的方法，但《ISO/IEC 27701》对撤回同意的告知、撤回同意的机制和撤回同意的后果提出了更具体的要求。具体而言：

- 撤回同意权的告知

虽然《GB/T 35273》（2020 版本）和《ISO/IEC 27701》均规定个人信息控制者应当向个人信息主体提供撤回同意的方法，但《ISO/IEC 27701》更加强调组织必须向 PII 主体**告知撤回的权利和权利行使的方法**（如下），使他们有权随时撤回同意。

- 撤回同意权利行使的方式

《GB/T 35273》（2020 版本）对于撤回同意的方式没有详细地描述，仅规定个人信息控制者应当向个人信息主体提供便捷撤回其授权同意

的方法，而《ISO/IEC 27701》则要求，**撤回同意权行使的方式应与征得同意的方式相一致**。例如，如果通过电子邮件或网站征得同意，则撤回同意也应当使用相同的方式，而不能通过电话或传真等其他方式。此外，《ISO/IEC 27701》还要求组织应当**对用户撤回同意的请求进行记录，记录方式应与其记录用户同意的方式亦相同**。

- 撤回同意的后果

对于撤回同意的后果，根据《GB/T 35273》（2020 版本）规定，一旦撤回同意，个人信息控制者后续不得再处理相应的个人信息，撤回授权同意不影响撤回前基于授权同意对个人信息的处理。《ISO/IEC 27701》对此做出了相似的规定，但《ISO/IEC 27701》额外要求：**撤回同意前在 PII 进行处理过程中所得出的结果不应再用于新的处理过程**。例如，如果 PII 主体撤回对其用户画像的同意，则该主体的画像不应再被使用或查看。

对于涉及共享的 PII，《ISO/IEC 27701》规定，组织应实施一定的政策、程序和/或机制，将 PII 主体撤回同意的情况告知已共享 PII 的第三方，具体的措施由组织自行决定，赋予了较大的自主权。

（5）征得授权同意的例外

如 4.1 部分所述，两部标准规定的关于收集个人信息的合法性依据在适用逻辑上不同，但在合法依据的种类上基本相似，具体而言：

《GB/T 35273》（2020 版本）（第 5.6 条）	《ISO/IEC 27701》（第 7.2.2 条）
与个人信息控制者履行法律法规规定的义务相关的	履行法律义务
与国家安全、国防安全直接相关的	履行与公共利益相关的工作
与公共安全、公共卫生、重大公共利益直接相关的	履行与公共利益相关的工作
与刑事侦查、起诉、审判和判决执行等直接相关的	履行与公共利益相关的工作
出于维护主体或其他个人的生命、财产等重大合法权益但又很难得到本人授权同意的	维护 PII 主体的重大利益
所涉及的个人信息是主体自行向社会公众公开的	没有规定

根据主体要求签订和履行合同所必需的	履行合同
没有规定	PII 控制者的合法利益
从合法公开披露的信息中收集个人信息的，如合法的新闻报道、政府信息公开等渠道	没有规定
维护所提供产品或服务的安全稳定运行所必需的，如发现、处置产品或服务的故障	履行合同
个人信息控制者为新闻单位，且其开展合法的新闻报道所必需的	没有规定
个人信息控制者为学术研究机构，出于公共利益开展统计或学术研究所必要，且其对外提供学术研究或描述的结果时，对结果中所包含的个人信息进行去标识化处理的	履行与公共利益相关的工作

两部法规均规定了履行法律义务、公共利益、维护 PII 主体的重大利益、履行合同的合法性依据，但《GB/T 35273》（2020 版本）额外对主体自行公开信息、维护他人生命财产利益、PII 控制者为新闻单位或

学术研究机构的情形进行了额外规定；而《ISO/IEC 27701》则指出 PII 控制者的合法利益也可作为处理个人信息的合法性依据。需要注意的是，在合规实践时，《ISO/IEC 27701》必须结合本国/本地区关于数据保护的要求，对规定存在错位的地方，以本国/本地区的数据保护法为主。例如，中国大陆的《GB/T 35273》（2020 版本）没有规定 PII 控制者的合法利益是处理个人信息的依据，则组织在中国大陆实践个人信息保护时，就不能将 PII 控制者的合法利益作为合法性依据考虑。

4.6 个人信息保护政策的要求

《GB/T 35273》（2020 版本）和《ISO/IEC 27701》均提及了组织应当提供个人信息保护政策，并在个人信息保护政策的制定、内容设定[9]

[9] 《GB/T 35273》（2020 版本）规定，个人信息保护政策应包括但不限于：1）个人信息控制者的基本情况，包括主体身份、联系方式； 2）收集、使用个人信息的业务功能，以及各业务功能分别收集的个人信息类型。涉及个人敏感信息的，需明确标识或突出显示；3）个人信息收集方式、存储期限、涉及数据出境情况等个人信息处理规则；4）对外共享、转让、公开披露个人信息的目的、涉及的个人信息类型、接收个人信息的第三方类型，以及各自的安全和法律责任；5）个人信息主体的权利和实现机制，如查询方法、更正方法、删除方法、注销账户的方法、撤回授权同意的方法、获取个人信息副本的方法、对信息系统自动决策结果进行投诉的方法等；6）提供个人信息后可能存在的安全风险，及不提供个人信息可能产生的影响；7）遵循的个人信息安全基本原则，具备的数据安全能力，以及采取的个人信息安全保护措施，必要时可公开数据安全和个人信息保护相关的合规证明；8）处理个人信息主体询问、投诉的渠道和机制，以及外部纠纷解决机构及联络方式。

和实施细则[10]方面均作出了明确且详细的指引，但两部标准在政策内容和形式上有所不同。具体来说：

从内容上看，《GB/T 35273》（2020 版本）采用的术语为个人信息保护政策，其内容侧重于对组织内个人信息全生命周期的保护；而《ISO/IEC 27701》所采用的术语为信息安全政策（information security policies），**其内容既包括对外告知个人信息的保护政策，也包括组织内部有关信息管理和保护体系的构建**，即内容上更为丰满，为组织提供了内外兼顾的信息安全保护体系。

从形式上看，《GB/T 35273》（2020 版本）要求个人信息保护政策的内容应当清晰易懂、公开发布且易于访问、应逐一送达个人信息主体、更新时重新告知个人信息主体等；《ISO/IEC 27701》则要求**保留声明及相关流程的副本**。在文件更新时，依然要**保留历史版本的副本**。

5. 个人信息的保存

《GB/T 35273》（2020 版本）和《ISO/IEC 27701》均对个人信息的存储时间、去标识化处理作出了规定，但各自的要求程度不同：

[10] 参见《GB/T 35273》（2020 版本）附录 C 表格。

《ISO/IEC 27701》对存储时间要求更高，《GB/T 35273》（2020 版本）对去标识化处理要求则更高。此外，《ISO/IEC 27701》对存储介质进行了额外限制。

《GB/T 35273》（2020 版本）	《ISO/IEC 27701》
个人信息保存时间最小化 （第 6.1 条）	有规定，但颗粒度更细 （第 7.4.7 条）
存储介质要求 没有规定	有规定 （第 6.5.3.1 条）
收集后去标识化处理 （第 6.2 条）	有相似水平规定 （第 7.4.5 条）
个人敏感信息的传输和存储 （第 6.3 条）	要求对特殊类别的 PII 分类，并提示注意某些法域的对特殊类型 PII 使用的特别规定 （第 6.5.2、7.4.9、6.10.2 条）
个人信息控制者停止运营的三点要求 （第 6.4 条）	仅对删除 PII 的技巧选择提供建议 （第 7.4.5、7.4.8 条）

5.1 保存时间最小化

对于个人信息的保存，《GB/T 35273》（2020 版本）要求个人信息的保存期限应为**实现个人信息主体授权使用目的所必需的最短时间**。

《ISO/IEC 27701》在《GB/T 35273》（2020 版本）的基础上，额外规定，组织应**制定并维持其保存信息的时间表**，该时间表应当考虑到法律、监管和商业要求。**当这些要求发生冲突时，则有必要（基于风险评估）做出商业决定并记录在适当的时间表中**。组织应规定和记录数据最小化目标以及如何实现该目标，包括使用哪些机制（例如去识别化）。显然，《ISO/IEC 27701》强调“记录”与“基于风险评估”的思维在不同的条款中都有渗透，并且对一些抽象性比较高的机制设定了较为细致的指引。

5.2 存储介质要求

《GB/T 35273》（2020 版本）没有对存储介质作出规定，而《GB/T 35273》（2020 版本）则详细规定，组织应**对用于存储 PII 的可移动介质和/或设备的任何使用予以备份**。除非不可避免，组织**不应使用没有对 PII 进行加密的可移动物理介质和/或设备**。在使用未进行加密的物

理介质和/或设备的情形下，组织应采取一定的流程和控制措施（例如，防篡改的包装）以降低 PII 泄露的风险。至于具体应采取何种流程和控制措施，《ISO/IEC 27701》没有加以严格限制，赋予了组织一定的自由度，根据实际情况进行合理设计。

5.3 去标识化处理

对于去标识化处理，《GB/T 35273》（2020 版本）要求个人信息控制者在收集个人信息后，宜**立即进行去标识化处理，并采取技术和管理方面的措施，将去标识化后的信息与可用于恢复识别的个人的信息分开存储并加强访问和使用的权限管理。**

虽然《GB/T 35273》（2020 版本）的上述规定（在文字上采用了“宜”）也只是建议性的要求，但《ISO/IEC 27701》没有提出在收集后即进行去标识化处理的建议，仅规定了**在结束处理 PII 后对 PII 进行去标识化或删除处理。**

5.4 个人敏感信息的传输与存储

《GB/T 35273》（2020 版本）和《ISO/IEC 27701》均提及了对个人

敏感信息的特殊要求。不同的是《GB/T 35273》（2020 版本）对于个人敏感信息的传输与存储提出了明确的要求，而《ISO/IEC 27701》则要求对特殊类型的 PII 应单独分类，并提醒注意各国/各地区对于个人敏感信息的使用和分类存在其本地法上的特殊规定。具体而言：

《GB/T 35273》（2020 版本）要求控制者在传输和存储个人敏感信息时，应采用加密等安全措施；将个人生物识别信息与个人身份信息分开存储；存储个人生物识别信息时，应采用技术措施确保信息安全后方进行存储，例如仅存储摘要信息，在采集终端中直接使用个人生物识别信息实现身份识别、认证等功能，以及在使用面部识别特征、指纹、掌纹、虹膜等实现识别身份、认证等功能后删除可提取个人生物识别信息的原始图像。

而《ISO/IEC 27701》则仅提示各国/各地区可能对特殊类型 PII 的定义存在差异，组织应注意对该等类型的 PII 单独分类，并提请注意各国/各地区对此类 PII 可能存在特殊的规制。

5.5 个人信息控制者停止运营

《GB/T 35273》（2020 版本）对个人信息控制者停止运营后信息应

当如何处理作出了规定，而《ISO/IEC 27701》则未提及这一部分内容。

具体而言，《GB/T 35273》（2020 版本）要求，当组织停止运营其产品或服务时，应及时停止继续收集个人信息，将停止运营的通知逐一送达或以公告的形式通知个人信息主体，并对持有的个人信息进行删除或匿名化处理。

6. 个人信息的使用

对于个人信息的使用，《GB/T 35273》（2020 版本）和《ISO/IEC 27701》两部标准在内容差异性上比较显著。虽然《GB/T 35273》（2020 版本）和《ISO/IEC 27701》对个人信息的访问控制、展示限制、使用目的限制、用户画像的使用限制、自动化决策和个人信息主体享有的权利等方面均作出规定，但《GB/T 35273》（2020 版本）还额外对**个性化展示的使用**、不同业务所收集个人信息的**汇聚融合**进行了详细规制。考虑到本报告的篇幅有限，避免赘述，对于《GB/T 35273》（2020 版本）的特有规定部分请参见《GB/T 35273》（2020 版本）第 7.5 和 7.6 条以及**本报告附表 A**。以下将对《GB/T 35273》（2020 版本）和《ISO/IEC 27701》均有规定的部分进行对比分析。

《GB/T 35273》（2020 版本）	《ISO/IEC 27701》
个人信息访问控制措施 **（第 7.1 条）**	有规定，且颗粒度更为详细 （第 6.6 条）
个人信息的展示限制 **（第 7.2 条）**	有相似规定 （第 6.8.2.9 条）
个人信息使用的目的限制 **（第 7.3 条）**	有规定，但颗粒度更细 （第 7.2.1 条、第 7.2.2 条、第 8.2.3 条）
用户画像的使用限制 **（第 7.4 条）**	有规定，但颗粒度较粗 （第 7.2.2 条、第 7.3.10 条）
个性化展示的使用 **（第 7.5 条）**	没有直接对应的规定，但取决于具体情况，个性化展示可能会涉及到自动化决策 （第 7.3.10 条）
基于不同业务目的所收集的个人信息的汇聚融合 **（第 7.6 条）**	虽无直接对应的规定，但根据内容可以参考第 7.2.2 条和第 7.2.5 条
信息系统自动决策机制的使用 **（第 7.7 条）**	有相似规定 （第 7.3.10、7.2.5 条）

6.1 个人信息的访问控制措施

对于个人信息的访问控制措施，《GB/T 35273》（2020 版本）从人员控制这一维度，对访问的最小授权、操作、管理和审计人员分离、重要操作（如批量修改、拷贝、下载）、超权限操作和对个人敏感信息的操作要求制定审批流程等，即要求对人员进行管控，同时要求对人员访问系统进行控制。

《ISO/IEC 27701》则是从访问系统与人员控制两个维度进行了更加细致的规定，从而为企业内部制定访问控制措施提出了进一步、可落地的详细指引。具体而言：

一方面，《ISO/IEC 27701》要求授权人员在访问时应当使用专门的网络或网络服务（如 VPN），同时要求组织对该专门网络进行监控，提示用户注意，链接到未授权和不安全的网络服务可能影响整个组织。对于敏感或关键业务或高风险场所用户网络的连接，应采取特定的控制措施。

另一方面，《ISO/IEC 27701》对访问人员的控制同样作出了规定。但此部分与《GB/T 35273》（2020 版本）规定的内容相似，均对访问人

员的授权分级、审批流程等作出规定。《ISO/IEC 27701》还额外要求对授权进行定期审计或在有任何变更时应进行评审，以确保所有人员未超权限进行访问；以及要求在被授权人员离职后删除其访问的权利。

6.2 个人信息的展示限制

《GB/T 35273》（2020 版本）和《ISO/IEC 27701》均对个人信息的展示限制作出了规定，但限制的策略有所不同。《GB/T 35273》（2020 版本）是从展示个人信息的内容入手，要求通过界面（如显示屏、纸面）展示个人信息的，宜对个人信息采取去标识化的处理等方式，降低在展示环节的泄露风险。而《ISO/IEC 27701》则是从承载个人信息设备的外界物理防护角度进行规定，要求清除桌面上纸张、在空出办公室时应将敏感或关键业务信息锁起来（理想情况下，在保险柜或保险箱或其他形式的安全设备中），从而为组织提高展示限制措施上提出新的思路。

6.3 个人信息使用的目的限制

对于个人信息使用的目的限制，《GB/T 35273》（2020 版本）与《ISO/IEC 27701》均有规定，均要求在使用个人信息时不得超出合理、相关且最小必要的范围，且当确需变更处理目的时，应另行征得个人信

息主体的同意。

6.4 用户画像的使用限制

《GB/T 35273》（2020 版本）和《ISO/IEC 27701》均提及了用户画像的使用限制。但着眼于整体组织管理层面的《ISO/IEC 27701》，更多的也是为组织接受当地法律法规规范留有余地，仅提及如果 PII 主体撤回对用户画像的同意，则该主体的画像不应再被使用或查看。而《GB/T 35273》（2020 版本）不仅对画像本身的内容作出限制，还对画像的使用加以规制。具体而言：

在画像的内容方面，《GB/T 35273》（2020 版本）规定用户画像中对个人信息主体的描述不得包含淫秽、色情、赌博、迷信、恐怖暴力或者表达民族、种族、宗教、残疾、疾病歧视等内容；

在画像的使用方面，《GB/T 35273》（2020 版本）要求不得侵害公民、法人和其他组织的合法权益、危害国家安全等，且除了为达到个人信息主体授权同意的使用目的所必需外，使用个人信息时应消除个人身份的明确指向性，避免精确定位到特定个人。

6.5 信息系统自动决策机制的使用

对于信息系统自动决策，《GB/T 35273》（2020 版本）和《ISO/IEC 27701》均要求组织在使用信息系统自动决策机制时进行个人信息安全影响评估/隐私影响评估。但《GB/T 35273》（2020 版本）将规制的情形限定为**对信息主体权益产生显著影响的自动化决策机制，**而《ISO/IEC 27701》限定的情形为组织**“仅”使用信息系统自动决策的方式处理 PII**。此外，《ISO/IEC 27701》另行提示组织**某些私法管辖区可能存在特殊规定，包括需告知自动化决策的存在、允许 PII 主体拒绝自动化决策或针对某些类别的 PII 不得进行完全自动化处理的规定，**组织应当**遵守当地国家/地区规定的这些特别义务。**

7. 个人信息的委托处理、共享转让、公开披露、跨境传输

《GB/T 35273》（2020 版本）和《ISO/IEC 27701》均对个人信息的委托处理、共享、转让、公开披露和跨境传输进行了规制。《ISO/IEC 27701》对个人信息委托处理和跨境传输规定的要求更高、更为细致，而《GB/T 35273》（2020 版本）对个人信息的共享、转让和公开披露提出了更高的要求。

《GB/T 35273》（2020 版本）[11]	《ISO/IEC 27701》
委托处理 **（第 9.1 条）**	有规定，且颗粒度更细 （第 6.12 条、第 7.2.6 条、第 7.2.8 条、第 8 条）
共享、转让 **（第 9.2 条、9.3 条）**	有相似规定 （第 7.2.1 - 7.2.5 条、第 7.3.2、 7.3.3、7.3.7 条、第 7.4.5、7.4.8 条、以及第 7.5.3、7.5.4 条）
公开披露 **（第 9.4 条）**	有规定，但颗粒度较粗 （第 7.2.2、7.2.3、7.2.4、7.2.5 条，第 7.3.1、7.3.2、7.3.3 条， 以及第 7.5.4 条；此外， 《GB/T 35273》（2020 版本）中的第 9.4（e）条由于涉及责任方面则并没有对应规定）
第三方接入管理 **（第 9.7 条）**	有规定，但颗粒度较粗 （第 6.12 条、第 7.2.6 条）
跨境传输 **（第 9.8 条）**	有规定，且颗粒度更细 （第 7.5.1 条、第 7.5.2 条）

[11] 由于第 9.5 条和第 9.6 条已经分别在上文 4.1 节和 3.2 节进行了讨论，此处不再赘述。.

7.1 委托处理

对于委托处理，《GB/T 35273》（2020 版本）和《ISO/IEC 27701》均对个人信息主体的授权、委托处理的监督方式和权责分配、个人信息控制者和受委托者（PII 处理者）各自义务进行了规定。值得注意的是，因《GB/T 35273》（2020 版本）并未对“个人信息处理者”或“分包商”规定专门的术语和定义，需要结合与委托处理相关的具体要求，理解实质上已经涵盖了对“个人信息处理者”或“分包商”的规定。就委托处理的监督方式和权责分配而言，两部标准的要求是相似的，但《ISO/IEC 27701》对于需要个人信息主体的授权以及个人信息控制者和受委托者（PII 处理者）各自义务的规定颗粒度更为细致、全面，从而为组织提高合规线提供指南。两者对于委托处理的要求具体如下：

（1）信息主体的授权要求

《GB/T 35273》（2020 版本）没有要求个人信息控制者针对委托行为请求个人信息主体的书面授权，仅要求个人信息控制者在作出委托行为时，不得超出已征得的个人信息主体授权同意范围，并且应对委托行为进行个人信息安全影响评估。

根据《ISO/IEC 27701》的规定，**在两种情况下，组织的委托处理需要获得用户的书面授权**：1）如果组织将 PII 的部分或全部处理任务分包给另一个组织，则在分包商处理 PII 之前，需要向用户进行披露并获得用户的书面授权，比如既可以在 PII 处理者和用户签订的合同中约定适当的授权条款，也可以采用特定的“一次性”授权协议；2）当委托处理部分 PII 或全部 PII 的组织发生变更时，需要在新的分包商处理 PII 之前，获得用户对于该变更的书面授权。针对这类情况，既可以在 PII 处理者和用户签订的协议中约定适当的条款，也可以采用特定的“一次性”授权协议的形式。

（2）委托处理关系中个人信息控制者的义务

《GB/T 35273》（2020 版本）和《ISO/IEC 27701》对于控制者的要求基本一致，即均要求控制者与受委托者（PII 处理者）订立合同，合同中须约定受委托者（PII 处理者）的责任和义务[12]；作出委托行为前，应当进行个人信息安全影响评估/隐私影响评估；以及对该委托处理行为进行记录。

[12] 《ISO/IEC 27701》要求组织应与其使用的任何分包商签订书面合同，并应确保其与分包商的合同包括《ISO/IEC 27701》附录 B 中所述的所有适当的控制措施。

然而，《GB/T 35273》（2020 版本）在同一条款内进一步要求对受委托者进行审计，以及个人信息控制者得知或者发现受委托者未按照委托要求处理个人信息、或未能有效履行个人信息安全责任的，控制者负有阻止义务，并采取或要求受委托者采取有效的补救措施（例如更改口令、回收权限、断开网络连接等）控制或消除个人信息面临的风险。必要时，个人信息控制者应终止与受托者的业务关系，并要求受托者及时删除从控制者处获取的个人信息。《ISO/IEC 27701》虽然没有直接点名 PII 处理者或者委托处理者，但在“供应商关系”部分规定了与供应商确定的信息安全策略，包括适当的审计供应商人员和控制措施的协议以及其他信息安全策略，从而给组织更为全面、宏观的指导。即使《ISO/IEC 27701》没有具体说明何种情况下才需要进行认证、审计或者签订一般合同条款，但是在具体落实《GB/T 35273》（2020 版本）时，它可以为第三方认证服务提供指导意见。

（3）委托处理关系中受委托者的义务

《GB/T 35273》（2020 版本）和《ISO/IEC 27701》均对受托者的义务进行了规定，《GB/T 35273》（2020 版本）通过第 9.1 条规定了受委托者的义务；而《ISO/IEC 27701》则是通过附录 B 全面且详尽地规定

了 PII 处理者的义务。具体而言：

《GB/T 35273》（2020 版本）	《ISO/IEC 27701》
通过合同约定受托者的责任和义务 **（第 9.1 d）1）项）**	PII 控制者与处理者之间的合同要求 （第 6.12.1.2 条、第 8.2.1 条）
在委托结束时不再存储相关个人信息 **（第 9.1 条 c）款 5）项）**	临时文件的删除 （第 8.4.1 条）
在委托结束时不再存储相关个人信息 **（第 9.1 条 c）款 5）项）**	处理完毕后 PII 的返还、传输和删除 （第 8.4.2 条）
协助响应个人信息主体请求 **（第 9.1 条 c）款 3）项）**	PII 主体权利保障 （第 8.3 条）
	广告营销下的处理 （第 8.2.3 条） PII 处理者的目的限制

没有要求	（8.2.2 条） PII 控制者的处理指令侵权时的告知 （第 8.2.4 条） 合规措施的告知 （第 8.2.5 条 PII 传输要求 （第 8.4.3 条） 不同法域间的 PII 共享 （第 8.5.1、8.5.2 条） PII 披露记录、告知和禁止披露情形 （第 8.5.3、8.5.4 条、8.5.5 条） 使用分包商处理 PII 的告知和要求 （第 8.5.6、8.5.7、8.5.8 条）
违反要求处理的反馈、再委托时的授权、未提供足够安全保护水平或发生安全事件的反馈 **（第 9.1 条 c）款）**	没有要求

总体来看，《GB/T 35273》（2020 版本）与《ISO/IEC 27701》对于受委托者义务的规定是协调相容的，但可以看出《ISO/IEC 27701》规定更为全面、详尽的，从而为控制者更好地监督、控制受委托者的处理行为提供系统性保障，进而保护被处理信息的安全。由于本报告篇幅所限，《ISO/IEC 27701》的相关附录，可通过本报告附件 B《ISO/IEC 27701》全文翻译进一步查阅。

7.2 共享、转让

《GB/T 35273》（2020 版本）和《ISO/IEC 27701》均对个人信息的共享、转让进行了规定，并均要求在共享转让时进行个人信息安全影响评估/隐私影响评估[13]、对共享、转让行为进行记录。不同的是，《GB/T 35273》（2020 版本）详细区分了因收购、兼并、重组、破产原因而进行的共享转让和非因收购、兼并、重组、破产原因进行的共享转让，而《ISO/IEC 27701》着眼于数据处理的大方向，并没有深究收购、兼并、重组、破产等这些情景。具体而言，我们可以借鉴《ISO/IEC 27701》的指导意义，利用《GB/T 35273》（2020 版本）将合规工作落实到实处：

[13] 由于转让本身属于改变 PII 的处理主体的情形，则需根据相关要求进行隐私影响评估。虽然《ISO/IEC 27701》本身没有明确点明这一点，但根据转让行为性质指导控制者进行相关评估。

在发生收购、兼并、重组、破产等变更时，《GB/T 35273》（2020 版本）要求个人信息控制者向个人信息主体告知有关情况；变更后的个人信息控制者应当继续履行原个人信息控制者的责任和义务，如变更个人信息使用目的，则应重新取得个人信息主体的明示同意；此外，如破产且无承接方的，应对数据做删除处理。

对于非因收购、兼并、重组、破产原因导致的个人信息共享和转让，对个人信息控制者的要求包括：

1）事先开展个人信息安全影响评估，并依据评估结果采取有效的保护个人信息主体的措施；

2）向个人信息主体告知共享、转让个人信息的目的、数据接收方的类型，并事先征得个人信息主体的授权同意（共享、转让经去标识化处理后的个人信息，且确保数据接收方无法重新识别或者关联个人信息主体的除外）；

3）共享、转让个人敏感信息前，除 2）中告知内容以外，还应告知个人信息主体涉及的个人敏感信息类型、数据接收方的身份和数据安全能力，并事先征得个人信息主体的明示同意；

4）通过合同等方式规定数据接收方的责任和义务；

5）准确记录和保存个人信息的共享、转让情况，包括共享、转让的日期、规模、目的，以及数据接收方的基本情况等；

6）个人信息控制者发现数据接收方违反法律法规要求或双方约定处理个人信息的，应立即要求数据接收方停止相关行为，且采取或要求数据接收方采取有效补救措施（如更改口令、回收权限、断开网络连接等）控制或消除个人信息面临的安全风险；必要时个人信息控制者应解除与数据接收方的业务关系，并要求数据接收方及时删除从个人信息控制者获得的个人信息；

7）因共享、转让个人信息发生安全事件而对个人信息主体合法权益造成损害的，个人信息控制者应承担相应的责任；

8）帮助个人信息主体了解数据接收方对个人信息的保存、使用等情况，以及个人信息主体的权利，例如，访问、更正、删除、注销账户等；

9）个人生物识别信息原则上不应共享、转让。因业务需要，确需

共享、转让的，应单独向个人信息主体告知目的、涉及的个人生物识别信息类型、数据接收方的具体身份和数据安全能力等，并征得个人信息主体的明示同意。

《ISO/IEC 27701》则对记录的内容提出了更细致的指导，规定组织在向第三方传输 PII 或者接收来自第三方传输的 PII 时，应当进行记录，**确保与第三方的合作能够支持 PII 主体在将来提出的请求**，记录的具体要求包括：

PII 控制者应当对下列两类转让进行记录：（1）会对自第三方传输来的 PII 进行更改，且将其作为个人信息控制者的一项管理义务时，应当对从第三方转移来的这类 PII 进行记录；或（2）为执行 PII 主体的正当要求而向第三方传输 PII（比如个人信息主体撤回同意之后，个人信息控制者要求第三方删除信息，第三方将信息转移给控制者）时需要记录。

组织应该制定记录保存时间的政策。组织应当在仅对遵守最小化原则收集而来的信息进行传输时，进行记录。此外，组织应制定并实施相关政策、流程和/或机制，当对所共享的 PII 发生更改、撤回同意或拒绝处理的情况时，向与之共享 PII 的第三方进行告知。

7.3 公开披露

《GB/T 35273》（2020 版本）和《ISO/IEC 27701》均对个人信息的公开披露进行了规定。《GB/T 35273》（2020 版本）明确了个人信息原则上不应公开披露，在对于公开披露做出相应的程序性限制条件的同时，禁止了特定信息的公开披露。而《ISO/IEC 27701》仅强调了个人信息控制者具有记录义务。同上述共享、转让一节，两部标准在指引的逻辑上存在较大不同，具体而言：

《GB/T 35273》（2020 版本）**严格禁止个人生物识别信息和我国公民的种族、民族、政治观点、宗教信仰等个人敏感数据的分析结果对外公开批露**。对于其他信息的公开披露，《GB/T 35273》（2020 版本）原则上是禁止的，**如法律授权或具备合理事由确需公开披露，信息控制者应当充分重视风险，并满足以下要求：**

1） 事先开展个人信息安全影响评估，并依据评估结果采取有效的保护个人信息主体的措施；

2） 向个人信息主体告知公开披露个人信息的目的、类型，并事先征得个人信息主体的明示同意；

3） 公开披露个人敏感信息前，除 2）中告知的内容外，还应当告知个人信息主体涉及的个人敏感信息的内容；

4） 准确记录和保存个人信息公开披露的情况，包括公开披露的日期、规模、目的、公开范围等；

5） 承担因公开披露个人信息对个人信息主体合法权益造成损害的相应责任。

对于 PII 的公开披露，《ISO/IEC 27701》**依然仅强调组织的记录义务**，即组织需要记录向第三方披露 PII 的情况，包括披露的 PII 及其类型、披露的对象以及披露的时间。根据《ISO/IEC 27701》，组织在正常运营过程中可以披露 PII，但要对披露行为进行记录。对第三方任何额外的披露，例如因合法调查或外部审计进行的披露，也应当记录在册，记录的内容应当包括披露的来源和做出披露的权利来源。

7.4 第三方接入管理

《GB/T 35273》（2020 版本）在第三方接入管理方面，明确要求当个人信息控制者在其产品或服务中接入具备收集个人信息功能的第三

方产品或服务，且二者之间不为委托处理关系或共同个人信息控制者的情形时，个人信息控制者应当做到：

1）建立第三方产品或服务接入管理机制和工作流程，必要时应建立安全评估等机制设置接入条件；

2）应与第三方产品或服务提供者通过合同等形式明确双方的安全责任及应实施的个人信息安全措施；

3）应向个人信息主体明确标识产品或服务由第三方提供；

4）应妥善留存平台第三方接入有关合同和管理记录，确保可供相关方查阅；

5）应要求第三方根据本标准相关要求向个人信息主体征得收集个人信息的授权同意，必要时核验其实现的方式；

6）应要求第三方产品或服务建立响应个人信息主体请求和投诉等的机制，以供个人信息主体查询、使用；

7）应监督第三方产品或服务提供者加强个人信息安全管理，发

现第三方产品或服务没有落实安全管理要求和责任的，应及时督促整改，必要时停止接入；

8）产品或服务嵌入或接入第三方自动化工具（如代码、脚本、接口、算法模型、软件开发工具包、小程序等）的，宜采取以下措施：

9）开展技术检测确保其个人信息收集、使用行为符合约定要求；

10）对第三方嵌入或接入的自动化工具收集个人信息的行为进行审计，发现超出约定的行为，及时切断接入。

《ISO/IEC 27701》并不像《GB/T 35273》（2020 版本）将涉及委托处理和共同个人信息控制者的情形排除在第三方接入管理的规范情形以外再进行讨论和规制；《ISO/IEC 27701》更多地是从大方向上统一进行概括性的讨论。

《ISO/IEC 27701》首先从供应商关系的角度出发，提出在确保供应商关系中的信息安全同时，做到对供应商服务交付的管理。具体而言，在信息安全方面，组织应当制定供应商关系的信息安全策略、在供应商

协议中强调安全、确保信息与通信技术供应链的安全；在供应商服务交付管理方面，组织应当监督和评审供应商的服务，当涉及供应商服务的变更时，也要做到跟进管理。

其次，当组织与个人信息处理者签订合同时，《ISO/IEC 27701》也提供了相应的建议：组织应当与其合作的所有个人信息处理者签订书面合同，同时确保其与个人信息处理者签订的合同中涵盖了适当的控制性及安全性措施，包括考虑了信息安全风险评估以及个人信息处理者处理个人信息的范围等等。

7.5 跨境传输

就个人信息的跨境传输，《GB/T 35273》（2020 版本）并未明确说明跨境传输的要求，而采用了引述其他相关法律法规的方式，而《ISO/IEC 27701》对个人信息跨境传输则进行了详细规定，从而为组织如何实践跨境传输的要求提出了更为具体的建议。具体而言：

《GB/T 35273》（2020 版本）规定，在中华人民共和国境内运营中收集和产生的个人信息向境外提供的，个人信息控制者应符合国家网

信部门会同国务院有关部门制定的办法和相关标准的要求[14]。

如果存在因业务需求、政府和司法监管要求进行跨境信息传输时，组织需详细说明需要进行跨境传输的数据类型，以及跨境传输遵守的标准、协议和法律机制（合同等）。

《ISO/IEC 27701》详细要求组织应当识别并用文件证明跨境传输 PII 的依据。PII 传输需要满足相关法律、法规的要求，具体取决于数据接收方所在司法管辖区或国际组织（以及数据输出地）的要求。组织应当记录证明其满足传输的基础和要求。

《ISO/IEC 27701》还提出，在某些司法管辖区，需要由指定监管机关审核信息传输协议/合同。在这些司法辖区中的组织应当确保他们了解这些监管要求。此外，组织应指定并记录 PII 有可能被转让的目的地国家和/或国际组织。应向用户提供在正常业务中可能接收 PII 的国家和/或国际组织名称。如因使用分包商处理 PII 而引起的传输，相应国别/地区的名称也应包括在内。

[14] 2019 年 6 月 13 日，国家互联网信息办公室发布了《个人信息出境安全评估办法（征求意见稿）》对个人信息出境申报评估要求、申报材料、重点评估内容、个人信息出境记录、出境合同内容及权利义务要求、安全风险及安全保障措施分析报告内容要求等内容做出了具体规定。

8. 信息主体的权利

《GB/T 35273》（2020 版本）和《ISO/IEC 27701》均规定了信息主体的查询权、更正权、删除权、注销权、获取信息副本权、及时响应信息主体的请求，但《ISO/IEC 27701》对查询权、更正权、注销权、获取信息副本权、及时响应信息主体请求的规制要求更高、更为细致；而《GB/T 35273》（2020 版本）对删除权提出更高的要求。

《GB/T 35273》（2020 版本）[15]	《ISO/IEC 27701》
查询权 **（第 8.1 条）**	有规定，但颗粒度较粗 （第 7.3.3 条、7.3.6 条）
更正权 **（第 8.2 条）**	有规定，但颗粒度更细 （第 7.3.6 条）
删除权 **（第 8.3 条）**	有规定，但颗粒度较粗 （第 7.3.6 条）
账户注销权 **（第 8.5 条）**	有相似水平规定 （第 6.6.2.1 条）
获取个人信息副本权 **（第 8.6 条）**	有规定，但颗粒度更细 （第 7.3.8 条）
响应个人信息主体的请求 **（第 8.7 条）**	有规定，但颗粒度更细 （第 7.3.4 条、第 7.3.5 条、第 7.3.9 条）
投诉管理 **（第 8.8 条）**	有相似规定，但颗粒度更粗 第 7.3.9 条

[15] 第 8.4 条个人信息主体撤回授权同意权已经在上文 4.5（4）中进行了讨论，未免赘述，此处不再进行讨论。

8.1 查询权

对于查询权，《GB/T 35273》（2020 版本）和《ISO/IEC 27701》均有规定，但《ISO/IEC 27701》的规定更为细腻。具体而言：

《GB/T 35273》（2020 版本）规定个人信息控制者不仅需要在个人信息保护政策中约定个人信息查询权和实现机制，还应当向个人信息主体提供访问特定个人信息的方法，这些信息包括：

1）其所持有的关于该主体的个人信息或类型；

2）上述个人信息的来源、所用于的目的；

3）已经获得上述个人信息的第三方身份或类型。

在个人信息主体提出查询非其主动提供的个人信息时，个人信息控制者可在综合考虑不响应请求可能对个人信息主体合法权益带来风险和损害，以及技术可行性、实现请求的成本等因素后，做出是否响应的决定，并给出解释说明。

而《ISO/IEC 27701》作为国际标准，仅要求组织应向 PII 主体提供

查询其个人信息的方式，PII 主体具体可以访问到哪些信息则应遵循各个国家的数据保护法规。

8.2 更正权

对于更正权，《GB/T 35273》（2020 版本）和《ISO/IEC 27701》均有规定，但《ISO/IEC 27701》的规定更为细腻。具体而言：

《GB/T 35273》（2020 版本）规定，个人信息主体发现个人信息控制者所持有的该主体的个人信息有错误或不完整的，个人信息控制者应为其提供请求更正或补充信息的方法。

《ISO/IEC 27701》不仅要求组织执行政策、程序和/或机制，履行对 PII 主体的义务，以使 PII 主体在提出要求后，能在无不正当理由延迟的情况下访问、更正和删除 PII，还对组织响应个人信息主体的相应要求做出规定（参见下述第 8.6 节）。此外，当 PII 主体对数据的准确性或更正要求存在争议时，组织应当执行政策、程序和/或机制以应该解决该问题。这些政策、程序和/或机制应当包括 PII 主体已做的更改、以及无法进行更正的原因（在无法更正的情况下）。

此外，《ISO/IEC 27701》考虑到某些司法管辖区对 PII 主体有权更正或删除 PII 的情形和程度做出了特殊限制，组织应确定、及时更新并遵守可能适用的限制性规定。因此，《ISO/IEC 27701》作为国际标准在引导适用时，相比国内标准仅需符合国内适用情形，需要考虑的更多更全面。

8.3 删除权

对于删除权，《GB/T 35273》（2020 版本）和《ISO/IEC 27701》均有规定，但《GB/T 35273》（2020 版本）的要求更高，具体而言：

《GB/T 35273》（2020 版本）规定了信息主体行使删除权的条件，包括：

1）个人信息控制者违反法律法规或与信息主体的约定，收集使用个人信息的；

2）个人信息控制者违反法律法规或与信息主体的约定，向第三方共享、转让个人信息，且信息主体要求删除的（在这种情况下，个人信息控制者应立即停止共享、转让的行为，并通知第三方

及时删除）；

3）个人信息控制者违反法律法规或与信息主体的约定，公开披露个人信息，且信息主体要求删除的（在这种情况下，个人信息控制者应立即停止公开披露的行为，并发布通知要求相关接收方删除相应的信息）。

《ISO/IEC 27701》对于删除权的规定与更正权的规定基本一致，并没有像《GB/T 35273》（2020 版本）一样对删除权有详细的规定，这可能是因为删除个人数据可能被视为销毁证据的行为，因其与各个国家的国内法直接关联，《ISO/IEC 27701》作为国际标准难以对此部分进行详细的规定。

8.4 注销权

对于注销权，《GB/T 35273》（2020 版本）和《ISO/IEC 27701》均有规定，《GB/T 35273》（2020 版本）纵向更为细致，《ISO/IEC 27701》横向更为广泛。具体而言，《GB/T 35273》（2020 版本）规定：

1) 通过注册账户提供服务的个人信息控制者，应向个人信息主体

提供注销账户的方法，且该方法应简便易操作；

2) 受理注销账户请求后，需要人工处理的，应在承诺时限内（不超过 15 个工作日）完成核查和处理；

3) 注销过程需要进行身份核验，个人信息主体重新提供的个人信息不应多于注册、使用等服务环节收集的个人信息；

4) 注销过程不应设置不合理的条件或提出额外要求增加个人信息主体义务，如注销单个账户视同注销多个产品或服务，要求个人信息主体填写精确的历史操作记录作为必要注销条件等；

5) 注销账户的过程需收集个人敏感信息核验身份时，应明确对收集个人敏感信息后的处理措施，如达成目的后立即删除或匿名化处理等；

6) 个人信息主体注销账户后，应及时删除其个人信息或做匿名化处理。因法律规规定需要留存个人信息的，不能再次将其用于日常业务活动中。

《ISO/IEC 27701》则横向进一步规定，**组织不应将已经注销或过**

期的用户 ID 再给到其他用户。如果管理或操作用户注册和/或注销的程序以及在提供处理 PII 服务时，发生密码或其他用户注册数据的损坏或泄露（例如，无意的泄露）等访问控制受到损害的情形，组织应当对这些用户的访问控制受到损害的情况予以解决。

8.5 获取个人信息副本权

对于获取个人信息副本权，《GB/T 35273》（2020 版本）和《ISO/IEC 27701》均有规定，但《ISO/IEC 27701》的要求更高，具体而言：

《GB/T 35273》（2020 版本）规定，根据个人信息主体的请求，个人信息控制者应为个人信息主体提供获取以下类型的个人信息副本的方法，或在技术可行的情况下，将以下个人信息副本传输给第三方：1）个人基本资料、身份信息；2）个人健康生理信息、教育工作信息。**因此，对于个人信息副本的获取以及传输，在《GB/T 35273》（2020 版本）的语境下，是有明确且详细的类型限制的。**

根据《ISO/IEC 27701》的要求，PII 主体也享有获取个人信息副本的权利。获取的 PII 副本应当**是以结构化的、常用的、形式易获得的形式呈现。**《ISO/IEC 27701》还提及，根据某些司法管辖区要求，在特定

情况下，组织应当允许以可携带的形式，向 PII 主体或接收 PII 的控制者提供正在处理的 PII 副本（通常是结构化的、常用的和机器可读的形式）将正在处理的 PII 副本提供给 PII 主体或者接收 PII 的控制者。换言之，当在技术可行的情况下，根据 PII 主体提出的请求，组织应当将持有的 PII 副本直接转移到另一个接收方组织。此项规定，也与 GDPR 的“可携权”规定异曲同工。

《ISO/IEC 27701》还规定，如果所请求的 PII 已基于存储和处置政策[16]被删除，则 PII 控制者应向 PII 主体告知，其所请求的 PII 已被删除。

8.6 及时响应信息主体的请求

在及时响应信息主体请求的方面，《GB/T 35273》（2020 版本）和《ISO/IEC 27701》均提及响应时间、响应请求和响应费用，但《GB/T 35273》（2020 版本）的要求更为细腻、可实践，具体而言：

（1）响应时间

[16] 详见《ISO/IEC 27701》第 7.4.7 条。具体法条译文，请参考本报告附件 B。

对于响应时间，《GB/T 35273》（2020 版本）要求在验证个人信息主体身份后，个人信息控制者应当及时响应个人信息主体提出的请求，做出答复及合理解释，并向个人信息主体告知向外部机构提出纠纷解决的途径。《GB/T 35273》（2020 版本）要求的相应时间限制在 30 天内或在法律法规规定的期限内[17]。

《ISO/IEC 27701》则未要求响应的具体时间，仅要求响应时间应当在隐私政策中予以体现，并遵守所适用的法律和/或法规[18]。又一次体现了作为国际标准需要考虑各适用国家/地区当地不同法律法规规定。

（2）响应请求

对于响应请求，根据《GB/T 35273》（2020 版本），个人信息主体提出的请求包括访问、更正、删除、撤回同意、注销账户、获取副本等。

《ISO/IEC 27701》规定的合法请求包括获取 PII 副本或投诉请求，这一点与《GB/T 35273》（2020 版本）并无差距，但《ISO/IEC 27701》则进一步要求组织对处理和响应 PII 主体合法请求的**政策和流程进行**

[17] 《App 违法违规收集使用个人信息自评估指南》规定，App 运营者原则上应在 15 天内回复用户申诉的处理意见或结果。

[18] 某些司法管辖区会根据请求的复杂程度和数量以及是否需要将延迟的信息通知 PII 主体来确定响应时间。

规定和记录，又一次体现了该标准对“记录”的贯穿性倡导。

（3）响应费用

对于响应请求所产生的费用，《GB/T 35273》（2020 版本）规定对于合理的请求原则上不收取费用。但是对于一定时期内多次重复的请求，可视情况收取一定的成本费用。而《ISO/IEC 27701》并未对响应请求的费用做出规定，仅提及某些司法辖区允许组织在某些情况下收取费用（例如，过度或重复请求）。在此点上《ISO/IEC 27701》标准给予了不同适用国家/地区一定的灵活度进行自由规定。

8.7 投诉管理

《GB/T 35273》（2020 版本）针对投诉这一情景单独做出了规定：要求个人信息控制者建立投诉管理机制和投诉跟踪流程，并在合理的时间内对投诉进行相应。

而《ISO/IEC 27701》中与之对应的只有建立处理请求的策略和程序这一更为宽泛的规定，将处理提出的申诉请求作为其中的一个方面进行了说明。与处理其他请求相同，《ISO/IEC 27701》表示组织应定义

并记录策略和程序，在司法管辖区允许的范围内的某些情况下（如过度或重复的请求）收取费用，并且请求应在适当的隐私政策中的定义响应时间内处理[19]。

9. 个人信息安全事件的处置

在发生信息安全事件时，《GB/T 35273》（2020 版本）和《ISO/IEC 27701》均规定了两方面的义务，一是报告监管机构；二是通知个人信息主体。相较而言，《ISO/IEC 27701》的规定更为细腻，不仅区分了 PII 控制者和 PII 处理者在此情况下的不同义务，还额外要求做出记录留存等，具体而言：

《GB/T 35273》（2020 版本）	《ISO/IEC 27701》
个人信息安全事件应急处置和报告 （第 10.1 条）	有规定，但颗粒度更细 （第 6.13 条）
安全事件告知 （第 10.2 条）	有规定，但颗粒度更细 （第 6.13.1.5 条）

[19] 如果一些管辖区根据请求的复杂性和数量以及任何将延迟通报 PII 主体的要求来定义相应时间。

9.1 报告监管机构

在发生信息安全事件时，《GB/T 35273》（2020 版本）要求**按照《国家网络安全事件应急预案》等有关规定及时上报**，报告的内容包括但不限于：涉及个人信息主体的类型、数量、内容、性质等总体情况、事件可能造成的影响、已采取或将要采取的处置措施、事件处置相关人员的联系方式。

《ISO/IEC 27701》规定，对于 PII 控制者和 PII 处理者，一旦发生 PII 泄露，**该组织应当留存记录，包括充足的信息，以便为监管和/或取证目的提供报告**，包括：事件描述、时间周期、事件的后果、报告者姓名、事件报告对象、解决事件所采取的措施（包括负责人和恢复的数据）、事件导致 PII 不可用、丢失、公开披露或变更的事实。如发生涉及 PII 的泄露行为，还应当记录的内容包括对受损的 PII 的描述（如果知道）；如果进行了通知，则应记录通知客户或监管机构所采取的措施。

在发生泄露时，某些司法管辖区要求 PII 处理者不加迟延地（即越快越好）通知 PII 控制者，最好是在泄露行为被发现后尽快通知，以便 PII 控制者采取适当的措施。而某些司法管辖区则要求该组织将涉及 PII 的泄露事件通知相关监管部门（例如 PII 保护机关）。

9.2 通知个人信息主体

在发生信息安全事件时，可能会给个人信息主体的合法权益造成严重危害，如个人敏感信息的泄露，《GB/T 35273》（2020 版本）要求及时将事件的相关情况以邮件、信函、电话、推送通知等方式告知受影响的个人信息主体。难以逐一告知个人信息主体时，应采取合理、有效的方式发布与公众有关的警示信息。告知内容应包括但不限于：

1）安全事件的内容和影响；

2）已采取或将要采取的处置措施；

3）个人信息主体自主防范和降低风险的建议；

4）针对个人信息主体提供的补救措施；

5）个人信息保护负责人和个人信息保护工作机构的联系方式。

《ISO/IEC 27701》区分了 **PII 控制者和 PII 处理者的不同义务**。对于 PII 控制者，在发生泄露事件时，相应程序应包括相关通知和记录。一些司法管辖区规定了何时应将安全事件通知监管部门，以及何时应将安全事件通知信息主体。在通知信息主体时，通知的内容包括：

1）可获得更多信息的联系方式；

2）对泄露行为及其可能后果的描述；

3）对泄露行为的描述，包括受影响人员的数量以及相关记录的数量；

4）已采取或计划采取的措施。

而对于 PII 处理者，**泄露通知的条款应当构成 PII 处理者与 PII 控制者之间合同的一部分**，包括 PII 处理者如何向 PII 控制者提供履行其通知监管部门所必要的信息的义务。在此情况下，通知义务不适用于因 PII 处理者的客户、或 PII 主体、或由他们所负责的系统组件所引起的泄露事件。合同还应规定涉及 PII 泄露事件通知的最大迟延履行期限。

10. 总结

与《GB/T 35273》（2020 版本）相比，《ISO/IEC 27701》在构建数据保护的体系结构方面并无明显差异，均对适用范围、信息类别、规制对象、信息主体权利、个人信息整个生命周期（包括收集、保存、使用、委托处理、共享转让、公开披露等）方面做出规定。但《GB/T 35273》（2020 版本）作为中国大陆地区的一部推荐性国家标准，考虑更多的

是将措施如何实操，指引中国企业逐步重视并践行个人信息保护要求。故，该标准对整体规范的覆盖面与平均细腻度上不亚于《ISO/IEC 27701》，甚至部分针对如何合规地使用个人信息规定得更为全面、细致、更具可落地性；而《ISO/IEC 27701》作为一部国际性标准，更多考虑的是与国际上有影响力的数据保护法律（如 GDPR）的兼容性和联动性，故整体规范侧重于在框架构建的基础上，为各国建构完善的隐私保护合规体系提供思路和空间，对于需要适用本国/本地区法“因地制宜”的部分仅做概括性或较少规定，留给各国/地区进行具体细化。但值得注意的是，《ISO/IEC 27701》对《GB/T 35273》（2020 版本）未规定的内容提供了一些指引，例如在个人信息安全影响评估部分，要求在评估验收标准、安全风险评估以外进一步进行隐私风险评估，可能会为将来《GB/T 35273》（2020 版本）更新、或者《个人信息保护法》的出台提供新的思路与方向。

正如《ISO/IEC 27701》中反复提醒的，在某一国家进行数据合规时，应当参照当地国家的法律法规和商业惯例确定具体的要求，比如对未成年人年龄的限制等。因此，企业在中国进行数据合规实践时，仍应以中国的法律法规和标准为基准，关注中国个人信息保护法律法规以及国家标准的发展动态；同时，对于中国法律法规、国家标准的要求比

较模糊或者欠周详的部分，可以参考《ISO/IEC 27701》国际标准中的操作指引，从而更好地完成所属法域内的数据合规工作，构建更加完备的隐私与信息安全保护体系。

三、组织内部管理体系与 PIMS 体系的对比分析

1. 《ISO/IEC 27701》 与《GB/T 35273》（2020 版本）对比分析

1.1 《ISO/IEC 27701》 与《GB/T 35273》（2020 版本）均有规定部分的点对点对比分析

1.1.1 明确责任部门与人员

《GB/T 35273》（2020 版本）和《ISO/IEC 27701》均对个人信息保护负责人设置做出了规定，且对个人信息保护负责人的职责要求存在重合。《GB/T 35273》（2020 版本）对于个人信息安全组织架构进行了规定，主要包括以下四个方面内容：1）明确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，包括为个人信息安全工作提供人力、财力、物力保障等；2）任命个人信息保护负责人和个人信息保护工作机构；3）在满足一定条件时，设立专职个人信息保护负责人和个人信息保护工作机构；4）个人信息保护负责人和个人信息保护工作机构的职责要求。此外，《GB/T 35273》（2020 版本）还要求为个人信息保护负责人和个人信息保护工作机构提供必要的资源，保障其独立履行职责。

类似地，《ISO/IEC 27701》要求任命一名或多名负责制定、实施、维护和监督组织进行数据治理和开展隐私合规项目的人员，以确保组织能够遵守有关处理 PII 所适用的法律和法规。《ISO/IEC 27701》还要求组织指定一位联系人专门为客户提供 PII 处理服务。当组织是 PII 控制者时，应当为 PII 主体指定一位联系人专门负责处理其 PII 事宜。从职责来看，尽管采用了不同的表述，《ISO/IEC 27701》与《GB/T 35273》（2020 版本）第 11.1 条 d）款规定的第一、二、五、六、十项职责基本一致。《ISO/IEC 27701》还特别要求负责人独立并直接向组织的适当管理层报告，以确保有效管理隐私风险；并要求负责人成为数据保护法律、法规和实践方面的专家。此外，《ISO/IEC 27701》还提及，数据保护官既可由内部工作人员担任，也可选聘外部专家来担任。

1.1.2 个人信息安全工程

《GB/T 35273》（2020 版本）和《ISO/IEC 27701》均对建立个人信息安全工程做出了规定。《GB/T 35273》（2020 版本）要求个人信息控制者在开发具有处理个人信息功能的产品和服务时，应当根据国家有关标准，在需求、设计、开发、测试、发布等系统工程阶段考虑个人信息保护要求，以保证在系统建设时对个人信息保护措施同步规划、同步

建设和同步使用。《ISO/IEC 27701》从实施的具体层面切入，同样提出了对于建立个人信息安全工程的要求，但相比而言要求更高。组织首先应当将 PII 的收集控制在最小必要程度、将 PII 的处理活动控制在充分必要程度；其次，组织应当确保并记录准确、完整及最新的 PII，以及确定数据最小化的目标及规定为达成目标所计划采取的手段和措施；组织还应当在数据处理活动结束时，及时对 PII 及处理活动中产生的临时文件进行去标识化和删除处理；组织应当将处理的政策、程序及机制文档化并遵循相关的制度规范；此外，在 PII 传输方面，组织应当合理控制并确保通过数据传输网络输送的 PII 到达指定的目标处。

1.1.3 个人信息处理活动记录

《GB/T 35273》（2020 版本）和《ISO/IEC 27701》均规定要记录个人信息处理活动。《GB/T 35273》（2020 版本）作仅将记录行为作为企业自愿实践，而《ISO/IEC 27701》则作出了硬性要求。具体而言：

《GB/T 35273》（2020 版本）规定，宜建立、维护和更新收集、使用个人信息的处理活动记录。“宜”字表示仅推荐组织对处理活动进行记录，但没有进行强制要求。推荐记录内容包括：

1）所涉及个人信息的类型、数量、来源（例如从个人信息主体直接收集或通过间接获取方式获得）；

2）根据业务功能和授权情况区分个人信息的处理目的、使用场景，以及委托处理、共享、转让、公开披露、是否涉及出境等情况；

3）与个人信息处理各环节相关的信息系统、组织或人员。

《ISO/IEC 27701》规定组织应明确并安全保留必要的记录，记录的内容至少包括处理的类型、处理的目的、对 PII 和 PII 主体类别的描述（如儿童）、已经或者将要披露的 PII 接收方类别，包括第三国接收方或国际组织、技术和组织安全措施的一般性说明、以及隐私影响评估报告。PII 处理记录应当确定一个对其准确性和完整性能够负责的人。

1.1.4 开展个人信息安全影响评估

《GB/T 35273》（2020 版本）和《ISO/IEC 27701》均对个人信息安全评估做出规定。《GB/T 35273》（2020 版本）要求个人信息安全影响评估，而《ISO/IEC 27701》则区分了信息安全风险评估流程和隐私风险评估流程。

《GB/T 35273》（2020 版本）要求建立个人信息安全影响评估制度，评估并处置个人信息处理活动中存在的安全风险。评估内容主要是围绕处理活动是否遵循个人信息安全基本原则，以及个人信息活动是否对个人信息主体合法权益存在影响，内容包括但不限于[20]：

1) 个人信息收集环节是否遵循目的明确、选择同意、最小必要等原则；

2) 个人信息处理是否可能对个人信息主体合法权益造成不利影响，包括是否会危害人身和财产安全、损害个人名誉和身心健康、导致歧视性待遇等；

3) 个人信息安全措施的有效性；

4) 匿名化或去标识化处理后的数据集能重新识别出个人信息主体或与其他数据集汇聚后重新识别出个人信息主体的风险；

5) 共享、转让、公开披露个人信息对个人信息主体合法权益可能

[20] 关于个人信息安全影响评估的典型评估场景、评估内容、评估流程等的具体规定，请参见《信息安全技术 个人信息安全影响评估指南（征求意见稿）》。

产生的不利影响；

6) 发生安全事件时，对个人信息主体合法权益可能产生的不利影响。

在下述几种情况下，《GB/T 35273》（2020 版本）要求个人信息控制者进行安全评估，包括：

1）在产品或服务发布前，或功能发生重大变化时，应进行个人信息安全影响评估；

2）在法律法规有新的要求时，或在业务模式、信息系统、运行环境发生重大变更时，或发生重大个人信息安全事件时，应进行个人信息安全影响评估。

关于个人信息安全影响评估，《GB/T 35273》（2020 版本）要求形成报告，并以此采取保护个人信息主体的措施，使风险降低到可接受的水平；同时还要求妥善留存报告，确保可供相关方查阅，并以适宜的形式对外公开。这一点与《ISO/IEC 27701》要求对评估过程的文件信息进行保存的规定是一致的。

《ISO/IEC 27701》区分了信息安全风险评估流程和隐私风险评估流程。前者主要用于识别因丧失保密性、完整性和可用性而产生的相关风险；后者则用于识别与 PII 处理相关的风险。同时，《ISO/IEC 27701》还提及，在整个风险评估过程中，组织应当妥善管理信息安全与 PII 保护的关系，既可以将二者合并评估，也可以将二者分开评估，但二者均需限定在隐私信息管理体系（PIMS）的范围内。

《ISO/IEC 27701》**对整个评估过程做出明确规定**，要求整个过程应当包括：

1）建立和维护信息安全风险标准，包括：

a）风险验收标准；和

b）信息安全风险评估的标准。

2）确保重复的信息安全风险评估产生一致的、有效的和可比较的结果；

3）识别信息安全风险：

a）应用信息安全风险评估流程，识别信息安全管理系统范围内与信息保密性、完整性和可用性相关的风险；

b）识别风险主体。

4）分析信息安全风险：

a）评估第 6.1.2 条 c）1）款规定的风险实现后可能产生的后果；

b）评估第 6.1.2 条 c）1）款规定的风险发生的实际可能性；和

c）确定风险等级。

5）评估信息安全风险：

a）将风险分析结果与第 6.1.2 条 a）款中确定的风险标准进行比较；和

b）优先考虑风险处理中的分析风险。

1.1.5 数据安全能力

《GB/T 35273》（2020 版本）要求组织根据有关国家标准的要求，建立适当的数据安全能力，落实必要的管理和技术措施，防止个人信息的被泄漏、损毁、丢失、篡改。《ISO/IEC 27701》则从物理和环境安全方面、操作安全方面、通信安全方面以及信息安全方面的业务连续性管理提出了更详细的规定与实施建议。具体要求详见下文第 2.8，2.9，2.10 以及 2.14 节的介绍。

1.1.6 人员的管理与培训

《GB/T 35273》（2020 版本）与《ISO/IEC 27701》同样要求组织对涉及个人信息的相关人员进行管理与培训。其中《GB/T 35273》（2020 版本）提出了以下六点具体的实施要求：

1) 应与从事个人信息处理岗位上的相关人员签署保密协议，对大量接触个人敏感信息的人员进行背景审查，以了解其犯罪记录、诚信状况等；

2) 应明确内部涉及个人信息处理不同岗位的安全职责，建立发生

安全事件的处罚机制；

3) 应要求个人信息处理岗位上的相关人员在调离岗位或终止劳动合同时，继续履行保密义务；

4) 应明确可能访问个人信息的外部服务人员应遵守的个人信息安全要求，与其签署保密协议，并进行监督；

5) 应建立相应的内部制度和政策，对员工提出个人信息保护的指引和要求；

6) 应定期（至少每年一次）或在个人信息保护政策发生重大变化时，对个人信息处理岗位上的相关人员开展个人信息安全专业化培训和考核，确保相关人员熟练掌握个人信息保护政策和相关规程。

《ISO/IEC 27701》则从人力资源安全管理方面入手，在《ISO/IEC 27002》的基础上，从聘用前、劳务合同履行过程中、劳务关系结束时三个阶段出发，具体介绍了在不同时期，组织应当承当的责任以及相关人员须承担的具体义务。详细介绍请见下文第 2.4 节。

1.1.7 安全审计

作为个人信息安全管理的重要环节，《GB/T 35273》（2020 版本）与《ISO/IEC 27701》均对信息活动中的安全审计做出了详细的介绍与规定。《GB/T 35273》（2020 版本）主要从业务实施角度出发，向组织提出了以下六点具体操作要求：

1) 应对个人信息保护政策、相关规程和安全措施的有效性进行审计；

2) 应建立自动化审计系统，监测记录个人信息处理活动；

3) 审计过程形成的记录应能对安全事件的处置、应急响应和事后调查提供支撑；

4) 应防止非授权访问、篡改或删除审计记录；

5) 应及时处理审计过程中发现的个人信息违规使用、滥用等情况；

6) 审计记录和留存时间应符合法律法规的要求。

《ISO/IEC 27701》与《GB/T 35273》（2020 版本）的操作要求相似，但其除了将审计要求涵盖到具体领域内（如在供应商关系安全管理中同时要求进行安全审计），《ISO/IEC 27701》专门将安全审计的规定列为“合规”领域并详细地进行了介绍和规定（详见下文第 2.15 节）。

1.2 《ISO/IEC 27701》相较《GB/T 35273》（2020 版本）的额外规定

正如上文介绍，《GB/T 35273》（2020 版本）对组织内部管理的要求主要包含在第 11 条“组织的个人信息安全管理要求”，从组织明确责任部门与人员、开展个人信息安全工程、进行个人信息处理活动的记录、开展个人信息安全影响评估、建立适当的数据安全能力、对相关人员进行管理与培训以及开展安全审计这七个大方面入手，在引进相关国家标准及规定的同时，提出了组织作为个人信息控制者的同时必须承担的义务与责任。

而《ISO/IEC 27701》作为一部兼顾不同国家/地区法规要求的标准，其价值在于它不光指出了组织在实施个人信息保护过程中必须要承担的责任，同时针对不同的业务实施层面，向组织提出了建议与措施。相比于《GB/T 35273》（2020 版本），《ISO/IEC 27701》将组织管理划分的

层面更加细致，它在涵盖上述七大方面的同时，建立了一套更加完备的PIMS体系。具体的PIMS体系介绍如下。

2. 《ISO/IEC 27701》下PIMS体系的建立与管理

PIMS体系是在《ISO/IEC 27001》和《ISO/IEC 27002》这两部国际标准基础上的进一步发展。《ISO/IEC 27001》是建立信息安全管理体系(ISMS)的一套规范，其中详细说明了建立、实施和维护信息安全管理体系的要求。《ISO/IEC 27002》则为在组织内启动、实施、保持和改进信息安全管理提供指南和通用的原则。该标准概述的目标是提供有关信息安全管理通常公认目标的通用指南，而其包含的实施规则被认为是制定组织具体指南的起点。而《ISO/IEC 27701》的PIMS则延伸了《ISO/IEC 27001》的ISMS，结合《ISO/IEC 27002》，从不同角度出发为隐私保护体系的建立、实施、维持以及发展提供了详细的落地可行的规定和指引。

2.1 组织的规划、实行与审查

（1）前期规划

首先 PIMS 介绍了建立适用于组织信息安全管理环境的必要要求。这一要求涉及了解组织现状及背景、明确建立信息安全管理体系的目的、理解相关方的需求与期望以及确定信息安全管理体系范围。随后，PIMS 提出了最高管理层在信息安全管理体系中承担角色的具体要求，以及如何通过一份声明的策略来向组织传达领导层的期望。这往往涉及了领导力和承诺、信息安全方针目标，以及角色、职责和承诺在实际情况中的体现与应用。

PIMS 接着又引入了处理风险和机遇的行动对策，以及可实现的信息安全目标与实现计划，并涉及了信息安全风险评估、风险所有者、信息安全风险处置、适用性声明、信息安全目标。与此同时 PIMS 也详细叙述了建立、实施、保持和改进一个有效的信息安全管理体系所需要的支持，包括:资源要求、参与人员的能力、意识、与利益相关方沟通、文档化信息等等。

（2）实行

在确立了组织信息安全体系的规划后，PIMS 提到了实施过程中不可忽略问题：如何运行前期规划及控制、对信息安全进行管理、开展信息安全风险评估、处置信息安全风险等。风险将影响组织目标的实现，

而这些目标可能关系到组织中从战略决策到运营的各种活动， 如具体项目的实施等，这表现在领导、战略、经营、财务、环境、社会、声誉等各个方面。但机遇与风险并存，如果能通过有效的管理控制风险，组织同样可以趋利避害。而对信息安全进行管理，PIMS 却不是让组织将所有的资产置于绝对安全的保护措施，因为“绝对安全”的成本是巨大的。因此，在风险控制措施的选择上，应当考虑组织的内外部环境因素以及相关方的需求和期待。PIMS 对此提供了一般性的战略建议：风险降低、风险转移、风险规避和风险接受。

（3）审查与改进

PIMS 总结了衡量体系的执行、体系与国际标准及管理层期望的符合性、寻求管理层期望反馈的要求，涉及监控、衡量、分析和评价，内部审核，管理评审。同时，也描述了组织应通过纠正行动来识别和改进不符合项，提出了针对不符合项的纠正措施、持续改进的方法。

2.2 信息安全管理方针

PIMS 下的信息安全管理方针可以在提供管理指导与支持的同时，确保组织符合相关法律法规的规定。它强调了对信息安全管理所需的

不同类型管理方针的定义、发布和评审。

首先，信息安全管理方针应由组织定义，并经由管理者批准，旨在阐述组织管理信息安全目标的方法。方针应强调业务战略下对信息安全的要求、法律法规和合同中对信息安全的具体要求、以及针对当前和预期的信息安全威胁环境组织需要达到的要求。同时，信息安全管理方针应包含以下声明：信息安全的定义，指导所有与信息安全活动相关的活动原则及目标，信息安全管理中角色的责任分配，对偏差和异常情况的处理，符合适用的个人信息立法规定要求的声明，以及履行组织和第三方合同规定的责任义务声明。而在实施层面上，则应以具体主题的方针来支持，更进一步确保信息安全控制措施的实施。这种具体主题一般是用来解决目标团体的需要或者包含某个主题，比如访问控制、数据分类、物理和环境安全、数据转移、以及恶意软件的防护等等。这些策略应以一种相关联的、易接受的和易理解的方式通知雇员和相关方。

其次，组织应在发生重大变化时或者按计划定期进行信息安全方针评审，以确保其持续具备适宜性、充分性和有效性。每个方针均应有一个经营管理者批准的特定人，此人负有对该方针进行开发、评审和评价的职责。评审包括评估组织方针改进的机会，以及管理信息安全响应组

织环境、业务状况、法律条件或技术环境变化的方法；同时应将管理评审的结果列为考虑因素之一。修订方针的提出或实施应取得管理层的批准。

2.3 信息安全组织

为建立一个管理框架、发起和控制组织内信息安全的实施和运行，组织应将信息安全融入到项目管理中，对信息安全角色及相应职责进行定义和分配，并且确保划分出可能冲突的职责和权限、减少对资产未经授权或无意的修改及误用；与此同时，组织应与监管机构、特殊权益团体及其他专业安全论坛和行业协会保持适当的联系。

此外，为了确保移动设备使用的安全，组织应针对不同的场景采取配套的安全措施以确保业务信息不被破坏。比如，在公共场所或其他未受保护的区域使用移动设备时，可以使用密码技术和强制使用秘密身份认证信息，来避免未经授权的访问或泄露存储和处理的信息。而在远程工作方面，组织应实施策略及相应的安全措施，来保护远程工作站点访问、处理或存储的信息。

2.4 人力资源安全

组织应该确保员工及承包商理解其职责、符合其应承担的角色要求，并且履行各自的信息安全职责。同时，在变更或终止雇佣关系时，组织应注意保证其本身的利益。

首先，在雇佣前，组织应当依据相关法律法规、道德规范、具体的业务需求，以及涉及的信息类型和相应风险，对候选人进行背景调查。在与员工和承包商签订劳务合同时，合同应列明员工或承包商和组织的信息安全责任。在员工或承包商履行劳务合同过程中，组织应确保其在履行方针下信息安全职责的同时，遵守组织的流程及规范。组织应当对所有员工和承包商进行适当的教育和培训，包括落实安全事件的报告及相应的处置，并且定期通知他们组织方针和流程的变化情况。对于违反信息安全规定的员工，组织应当对其进行正式的违纪处理。组织须明确在变更或终止雇佣关系后，员工或承包商的信息安全职责，确保该职责持续有效。同时，告知该员工或承包商其仍旧须遵守的信息安全要求以及相应的法律责任。

2.5 资产管理

首先，组织须明确组织资产的定义和范围，并且确立适当的保护职责。这些资产应该包括与信息相关的资产及信息处理设施。组织应该制定并维持其资产清单。当建立资产或资产转移到组织时，组织应分配该资产的持有人。被批准管理资产生命周期的个人或其他实体可以被分配作为资产持有人。该资产持有人在整个资产生命周期负有对资产进行合理管理的职责。组织应确立对信息和上述资产的合理使用规则、制定相应的文件并且进行实施。

其次，为确保信息获得与其重要性相匹配的保护，组织应当对包含个人信息在内的数据进行分类、标记，并且根据数据分类体系制定并实施处理资产的程序。为防止介质上存储的信息被泄露、修改、删除或破坏，组织应依据数据分类体系制定和实施对可移动介质的管理程序、使用正式的流程处理不再需要的介质、以及保护运输期间的介质不被未经授权的访问、滥用或损毁。

2.6 访问控制

组织应当限制对信息及信息处理设施的访问，确保授权用户的访问

权限、防止未经授权的对系统和服务的访问。同时，组织需要落实用户保护其身份认证信息的责任。在实施操作中，组织可以建立并实施访问控制策略，同时基于业务和信息安全相关的要求对其进行评审。组织应当向用户提供通过安全登录流程控制其账号访问的能力。

2.7 密码学

密码技术的使用可以保护信息的保密性、真实性和完整性。组织需要制定密码控制使用政策，确保适当有效的密码使用。在实施政策时，组织应考虑世界不同国家/地区应用密码技术的规定和国家限制，以及加密信息跨境传输问题。个别国家或地区可能会要求使用密码技术保护特定类型的个人信息，比如健康数据、居民证件号码、护照号和驾驶证号等。组织应当向消费者提供关于其使用密码技术保护组织处理个人信息的情形，也应通知消费者关于其协助消费者申请自己密码保护的可能性。此外，组织也应针对秘钥的使用、保护和时限问题制定政策，贯穿秘钥生命周期。

2.8 物理和环境安全

为了保护包含敏感信息、关键信息和信息处理设施的区域，组织首

先应当定义安全边界并且制定和实施适当的守则。

在实施层面上，组织应当使用适当的入口控制，确保只有授权人员能访问安全区域；设计和实施办公室、房间和设施的物理安全；设计和采取物理安全来防范自然灾害、恶意攻击或事故等事件；设计和运用安全区域内办公的流程；控制未经授权人员可进入的区域，比如物流交接区等，如果可行的话，该类区域应当与信息处理设施隔离。

在设备方面，为了减少环境方面的威胁和灾害引发的风险以及未经授权访问的可能性，组织应当妥善安放和保护设备；组织应保护设备免于因配套设施的电源中断或其他故障而受到影响；组织应保护电源、传输数据或为信息服务提供支持的通信电缆不被拦截、干扰或破坏；组织应正确维护设备以确保其持续的可用性和完整性；在授权之前，设备、信息或软件不可以被带离场所；组织应考虑在办公场所以外工作的不同风险并保护场外资产和设配；审核认证包含存储介质的设备所有部件，确保敏感数据和许可软件在处置或再利用前已被删除或安全重写；用户在不使用设备时也需要确保设备得到适当的保护；而公司也应采用“清理办公桌政策”和“清理设施屏幕桌面政策”。

在处理个人信息方面，组织应当确保当再分配个人信息存储空间时，

之前存储空间的个人信息为不可见状态。为了能够安全处置和再利用设备，任何可能涵盖个人信息的存储设备也应被视作涵盖个人信息。

2.9 操作安全

针对与信息处理及通信设施相关联的操作活动，组织应当制定操作流程、将其文档化并向需要的用户公开；比如计算机的启动和关机程序、备份、设备维护、介质处理、计算机机房和邮件处理的管理及安全等活动。组织应当控制任何可能影响信息安全的组织变更、业务流程变化、以及信息处理设施和系统的变更情况。为此，组织需要确立正式的管理职责和流程。每当变更发生时，组织应保留涵盖所有相关信息的审计日志。在资源的使用方面，组织需要对其进行监测和调整，同时预测将来的容量以确保系统具备所需的技能。此外，类似于前述第 2.8 节中提到的物理环境隔离，组织也需要分离开发、测试和运行环境，以减少未经授权的访问或更改操作环境。

从具体实践的角度来看，组织除了需要防止恶意软件的侵害以外，对信息、软件和系统图片也应进行备份并定期测试。组织尤其需要针对个人信息的备份、修复及恢复的要求制定政策，并且涵盖对备份信息中个人信息消除问题的进一步规定。为了记录事件和生成证据，组织需要

制造、保存和定期审查记录用户活动、特例、失误及信息安全事件的日志。同样地，系统管理员和系统操作员的活动也应被记录，而该日志也需要被保护和定期审阅。如果可行的话，建议组织同时记录对个人信息的访问情况，包括何时访问、何人访问、被访问的个人信息主体是谁，以及是否发生了任何变更情况。

组织需要保护日志设施和日志信息，防止任何可能对日志的篡改和未授权的访问、落实操作系统的完整性并且建立、实施、规范用户安装软件的守则。组织须及时获得信息系统的技术脆弱性信息，评估组织的暴露程度，并采取适当措施应对相关风险。

2.10 通信安全

为了保护网络中的信息和其信息处理设施，组织应当管理和控制网络，将所有网络服务的安全机制、服务等级及管理需求列明在网络服务协议中。此外，组织也需要在网络中对信息服务、用户和信息系统进行隔离。

在信息传输安全方面，组织需要制定正式的传输政策、流程和控制手段，和与外部主体签署信息传输协议，确保商业信息传输的安全性，

并且保护电子消息中涵盖的信息。同时，组织应当注意信息的保密性，定期审阅和存档反映组织对信息保护需求的保密性要求或者保密协议。

2.11 信息系统的获取、开发和维护

保障信息安全是信息系统生命周期中的必要构成，这一要求同时包括了那些通过公共网络提供服务的信息系统。首先，不论是新信息系统，还是对现有信息系统的加强，组织都应将信息安全相关的要求包含其中。其次，组织应当保护那些通过公共网络提供的应用服务信息不受到欺诈、卷入合同纠纷、未经授权地被修改或披露。组织应当保护应用服务交易中涉及的信息安全，以免发生不完整的传输、路由错误、未经授权的消息更改、未经授权的披露、未经授权的消息复制或重放。

在开发和辅助过程中，组织应当设计和实施信息系统开发周期内的信息安全策略，制定及应用软件和系统的开发规则，通过使用正式变更控制流程，控制开发生命周期内的系统变更。当操作平台更改时，组织需要审查和测试业务关键应用，以确保该更改不会对组织操作或者安全产生不利影响。对于软件包变更的情形，组织应该谨慎考虑，将变更限制在必要范围内并且严格加以控制。与此同时，组织应当建立安全系统工程原则，将其文档化，并且应用到任何信息系统实施、维护工作中。

组织须建立并适当保护系统开发环境的安全，在开发的过程中开展安全功能测试，仔细筛选、保护和控制测试数据。对于外包系统的开发活动，组织也应当予以监督监测。

2.12 供应商关系

组织应当保护供应商可访问的组织资产，和供应商协商探讨其活动中的信息安全要求，在达成一致后须落实到文件中。此外，与供应商达成的协议也应包括关于处理信息、通信技术服务和产品供应链中信息安全风险的相关规定。

协议达成后，组织应当定期监测、审阅和审计供应商服务交付情况。当供应商服务发生变更时，组织在考虑商业信息的关键性、系统的使用以及风险评估中涉及的过程这些因素的同时，应对供应商服务的变更进行管理，这包括维护、改进现有的信息安全策略、流程等控制措施。

2.13 信息安全事件管理

组织应当建立管理职责和流程以快速、有效及有序地对信息安全事态进行响应和处理。当信息安全事态发生时，相关人员应当尽快通过适

当的管理渠道向组织进行报告。组织应当要求使用其信息系统和服务的员工或承包商留意并报告在系统或服务中发现或怀疑的信息安全弱点。

如果安全事态被划分为安全事件，组织应对其进行评估与决策，并按流程文件响应。当安全事件涉及个人信息时，组织应当对其进行审查并且确定是否需要对其进行包括通知和记录在内的特定类响应和处理。

组织应当从对信息安全事件的分析与解决中学习，以减少未来事件发生的可能性或者影响。此外，企业应制定和实施关于鉴定、收集、取得和保存可能成为证据信息的程序。

2.14 信息安全方面的业务连续性管理

组织应当将信息安全连续性嵌入业务连续性管理体系中。组织应首先确立其在不利情况下（如危机或自然灾难中）对信息安全和信息安全管理的连续性要求。其次，组织应当建立、记录、实施和维护相应流程及控制措施，以确保在不利情况下信息安全连续性要求能达到规定的等级。最后，组织须对确立和实施的信息安全连续性控制手段进行定期验证，确保它们在不利的情况下仍有效。组织在使用信息处理设施时，

也应当确保其有足够的冗余来满足可用性需求。

2.15 合规

组织及其信息系统须在文档中明确所有相关的法律法规和合同要求，以及其达到这些要求所须采取的手段和措施。该文档须定期更新。当涉及知识产权及使用具有所有权的软件产品时，组织须采取适当的程序确保其符合法律法规及合同要求。组织应当依据法律法规及合同要求保护记录，以免记录遭到损失、破坏、篡改、未经授权的访问和未经授权的发布。组织应当依照相关的法律法规（如适用），确保隐私以及个人可识别信息的保护。而组织使用密码控制措施也应遵循相关的法律法规及合同的规定。

为了确保信息安全的实施符合组织政策及程序，组织应当开展信息安全审查。当按照计划间隔时间或当重大变更发生时，组织应当审查其管理信息安全的手段及实施情况，即信息安全的控制目标、控制手段，、策略、过程及程序。同时，组织也应当定期审查信息系统是否符合其信息安全策略和标准。而管理者应当定期审查其职责范围内的信息处理和相关程序相应的策略、标准以及其他安全要求的遵循情况。

3. 27701 的优势与借鉴意义

3.1 各国独立的数据隐私保护法规带来的挑战

如今在全球范围内，立法者和执法者都越发意识到对数据使用和数据处理进行管理的重要性，尤其是当涉及到个人验证信息时，提供能规范数据处理和保护个人隐私的法律手段就显得尤为迫切。目前除了欧盟的通用数据保护条例（“GDPR”）以外，美国、瑞士、澳大利亚和新西兰在内的各个国家都先后出台了各自的数据保护新规，层出不穷的法律法规逐渐给各商业实体，尤其是跨国企业带来了挑战。而国际标准《ISO/IEC 27701》PIMS（privacy information management system）的出现将帮助这些企业能够决定、计划、实施和保持一个不光满足于全球不同法域要求、同时符合 GDPR 规定的数据隐私保护的渠道。

GDPR 鼓励数据保护认证机制以及确立数据保护认证标志，以帮助确保控制者和处理者在处理数据的操作中符合法律规范（GDPR 第 42 条）。此外，使用这些认证或者盖印手段可以表明组织在处理个人信息时是采取了符合 GDPR 规定的正确方式。

持续的认证机制可以将“问责制”这个元素带进对数据保护的实施

中、加速降低风险和促进个人信息的流动。这一点可以帮助组织在提供服务的同时，使程序更加透明而且获得客户对其数据保护的信任。

3.2 《ISO/IEC 27701》的借鉴意义

《ISO/IEC 27701》并不打算让组织面面俱到地控制所有情况。相反，《ISO/IEC 27701》要求组织意识到处理个人验证信息和处理其他信息是不同的，企业需要根据情形合理地调整特定的控制手段和实施控制措施。

虽然对于企业或者组织来说，其是否应该实行《ISO/IEC 27701》视具体情况而定，但是，如果企业担心信息保护问题（比如勒索软件、拒绝服务攻击等网络风险），而且想要一个符合 GDPR 的合规指引，《ISO/IEC 27701》无疑是一项非常有用的工具，它不仅涵盖了多方角度，同时提供了安全控制措施来帮助保护个人数据和信息。通过实行《ISO/IEC 27701》这个标准，组织可以：

- 同时符合《ISO/IEC 27701》的规定并且达到 GDPR 的基本合规要求；

- 从信息安全的角度和隐私保护的角度分别进行风险管理，并且实行特定的管控手段；

- 同时有了保护商业信息和个人数据的特定管控手段指引；

- 通过认证《ISO/IEC 27701》，可以向第三方证明你的企业或组织符合 GDPR 的规定以及其他信息安全相关的国际标准；[21]

- 如果你是 GDPR 下的处理者，你可以向你的客户提供符合 GDPR 规定的证明；[22]

- 如果你是 GDPR 下的控制者，你可以向数据主体提供符合 GDPR 规定的证明。[23]

4. 总结

《ISO/IEC 27701》建立了一个以证据为基础的隐私保护项目。同

[21] 需要注意的是，目前正式的 GDPR 认证尚未获得欧盟批准。然而考虑到 PIMS 和 GDPR 之间显然是相互呼应的，那么在欧盟监管机构做出决策之前，PIMS 认证尽管不能作为正式的 GDPR 认证，但也可以视为 GDPR 合规的证明。

[22] 如上。

[23] 如上。

时，《ISO/IEC 27701》向组织提出了一套必须其在个人信息处理活动中承担责任与提出建议的措施。《ISO/IEC 27701》意识到了不同国家隐私法律间相互有重合之处，以此降低了法律适用的复杂性。但当《ISO/IEC 27701》具体落实到特定国家和/或地区时，仍然不可避免地需要参见当地的法律。尤其考虑到中国大陆现有的具有中国特色的法律制度与环境，组织具体在中国大陆落地个人信息保护方案时，则需要参见《GB/T 35273》（2020 版本）。从总体环境来看，《GB/T 35273》（2020 版本）的中心思想与《ISO/IEC 27701》一致，均重视参与个人信息活动的组织在其内部管理时应遵守相应的法律规范并要求落实实施责任；从具体措施来看，组织可使用《ISO/IEC 27701》搭建整体的合规框架，了解组织安全管理的底线与需求。在把握大的方向后，再从《GB/T 35273》（2020 版本）七大方面入手，切实落地各国个人信息保护的具体规定。

附表 A:《信息安全技术 个人信息安全规范（2020 版本）》和《ISO/IEC 27701》比对表

附表 B:《ISO/IEC 27701》中译文（双语）

环球律师事务所 GLOBAL LAW OFFICE SINCE 1979

Microsoft

Guidance Report on the Construction of Personal Information Compliance System under Compatible Domestic and Foreign Standards

May 2021

Copyright Statement

Compilation Team

Global Law Office

Meng Jie, Zhang Shuyi, Wang Cheng, Xu Guosheng, Dong Jierui

Microsoft Corporation

Li Sihong, Wang Jingsong

Contact Person:

Meng Jie

Telephone: 010- 65846768

E-mail: mengjie@glo.com.cn

Introduction

What is ISO/IEC 27701and what is included in the standard?

The International Standardization Organization, on August 5, 2019, issued ISO/IEC 27701: 2019 (hereinafter referred to as "ISO/IEC 27701") as an extension of ISO/IEC 27001 and ISO/IEC 27002 for privacy information management, to improve privacy information protection within the organization. The objects to be protected are Personally Identifiable Information (hereinafter referred to as "PII"), while those to be regulated are PII controllers and PII processors.

The ISO/IEC 27701 is composed of the main body and Annexes, of which the main body is divided into eight sections and Annexes includeseven parts.

I. Main Body

Section I introduces the scope of ISO/IEC 27701. ISO/IEC 27701 expands ISO/IEC 27001 and ISO/IEC 27002, which establishes, implements, maintains and continuously improves the Privacy Management System (PIMS), and manages privacy across the organization. It provides guidance on the responsibilities and obligations of PII controllers and PII processors during the processing of PII. ISO/IEC 27701 applies to organizations of all types and sizes, including public and private companies, government entities, and non-profit organizations, acting as PII controllers and PII processors that process PIIs in an ISMS.

Sections II, III and IV introduce separately the international standard documents referred to in ISO/IEC 27701, terms definitions and abbreviations used, as well as the drafting structure of the standard.

Section V introduces the PIMS provisions stipulated under ISO/IEC 27001 and the additional provisions on PIMS. The PII controllers and PII processors shall be regulated and instructed from the following seven aspects, including: context of the

organization, leadership, planning, support, operation, performance evaluation, and improvement.

Section VI introduces the PIMS provisions in ISO/IEC 27002 and additional provisions on PIMS. The PII controllers and PII processors shall be regulated and instructed from the following fourteen aspects, including: information security policies, organization of information security, human resource security, asset management, access control, cryptography, physical and environmental security, operations security, communications security, systems acquisition, development and maintenance, supplier relationships, information security incident management, information security aspects of business continuity management, and compliance.

Section VII introduces the relevant provisions and additional provisions on PII controllers under ISO/IEC 27002. The PII controllers' rights and obligations shall be further regulated and instructed from the following four aspects, including: conditions for collection and processing, obligations to PII principals, privacy

by design and privacy by default, PII sharing, transfer and disclosure.

Section VIII introduces the relevant provisions and additional provisions on PII processors under ISO/IEC 27002. The PII processors' rights and obligations shall be further regulated and instructed from the following four aspects, including: conditions for collection and processing, obligations to PII principals, privacy by design and privacy by default, PII sharing, transfer and disclosure.

II. Sections of Annexes

Annex A sets forth the control objectives and controls required to be taken by the PII controllers in achieving the PIMS, including cases where a PII controller entrusts a PII processor or is under joint control over PII with another PII controller.

Annex B sets forth the control objectives and control measures required to be taken by the PII processors in achieving the PIMS, including cases where subcontractors are engaged to handle the PII.

Annex C compares and maps ISO/IEC 27701 to GDPR (articles 5 to 49) to reflect the relevance of compliance with the ISO/IEC 27701 and fulfilling the obligations required by the GDPR.

Annex D compares and maps ISO/IEC 27701 to ISO/IEC 29100 to indicate the relevance of compliance with the requirements and control measures under ISO/IEC 27701 and the basic principle of privacy safeguards as set forth in the ISO/IEC 29100.

Appendix E compares and maps ISO/IEC 27701 with ISO/IEC 27018 and ISO/IEC 29151 to reflect the consistency of the requirements and control measures specified in the standard ISO/IEC 27701 with those specified in the ISO/IEC 27018 and ISO/IEC 29151.

Annex F lists the terms used in ISO/IEC 27701 and indicates alternative terms with the same or similar meaning used in other jurisdictions.

Annex G introduces the extension of the regulatory scope of ISO/IEC 27001 and ISO/IEC 27002 by ISO/IEC 27701 and the

corresponding methods and application examples of the extended clauses.

From the above analysis and the comparison with the published international standards, ISO/IEC 27701 provides higher security management for PII controllers and PII processors on the basis of ISO/IEC 27001 and ISO/IEC 27002, which makes the privacy information management system more comprehensive and can be applied for PII protection inorganizations with different scales and different cultures.

This report compares GB/T 35273 and ISO/IEC 27701, sorts out the relationship between the two standards and the control measures from the perspective of the full life cycle of personal information and the recommended requirements from the perspective of the internal compliance structure of the enterprise.

This report aims at assisting companies to understand the bottom line and requirements of organizational security management, and guiding companies to make a soft landing on personal information security compliance. This report will not only

help companies complete data compliance work in mainland China, but also lay a good foundation for future overseas projects. It will also help to further implement the specific requirements of various countries and build a more complete and integrated privacy and information security protection system.

Table of Contents

I. Overview

On August 6, 2019, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) officially released the *ISO/IEC 27701 Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines* (hereinafter referred to as "ISO/IEC 27701"). As an extension to ISO/IEC 27001 and ISO/IEC 27002, ISO/IEC 27701 aimed at improving the **Privacy Information Management System (PIMS)** by providing further guidelines, to processors and controllers implementing PIMS.

Before the release of ISO/IEC 27701, ISO/IEC 27001, as an internationally recognized information security management system standard, only sets out the basic requirements for information security management system, while ISO/IEC 27002 provides implementation guidance for organizations to start, implement, maintain and improve the information security management measures. Neither ISO/IEC 27001 nor ISO/IEC 27002 distinguish the comprehensive requirements of privacy protection management in different countries and regions that the two different regulated objects, PII controller and PII processor have to implement and meet. Therefore, the personal information management system introduced by ISO/IEC 27701 helps to provide guidance in this area. ISO/IEC 27701 expands on the foundations of ISO/IEC 27001 and ISO/IEC 27002, to increase the target objectives from separate information security to information security + privacy security. Meanwhile, ISO/IEC 27701 also clearly distinguishes the roles of PII controller and PII processor to help organizations to better perform compliance management to protect user privacy and personal information.

The active role played by European Data Protection Board in the implementation of ISO/IEC 27701, is specifically reflected in the comparison between the clauses of ISO/IEC 27701 and GDPR provided in Appendix D of ISO/IEC 27701, which further shows the similarities and differences between the measures taken by ISO/IEC 27701 and GDPR compliance requirements: the two are almost similar in an overall aspects and requirements. It is widely known that ISO/IEC 27701 is currently the closet to the GDPR compliance guidelines, and is viewed as one of the easier practical solutions for those familiar with GDPR compliance to implementation.

On December 29, 2017, the National Information Security Standardization Technical

Committee (SAC/TC 260) issued *Information security technology - Personal information security specification* (GB/T 35273 (2017)) in Mainland China for the first time. After several rounds of seeking comments and revisions to GB/T 35273 (2017), SAC/TC 260 issued the first edition of the *Information security technology - Personal information security specification* (2020) (GB/T 35273 (2020)) on March 6, 2020. GB/T 35273 (2020) serves as the national recommended standard, and is viewed as an important benchmark and operation guide that companies can rely on for their personal information protection compliance work before the formal release of the *Protection of Personal Information Law* of China.

In general, ISO/IEC 27701 and GB/T 35273 (2020) share similar overall requirements for personal information processing control measures, although they have separate unique regulations regarding detailed requirements. ISO/IEC 27701 systematically discusses how an organization builds a privacy security management system, while GB/T 35273 (2020) provides for the personal information management requirements of the organization in Chapters 10 and 11. Therefore, this report will carry out analysis from two dimensions: sort out and compare the provisions of the two standards to extract their key ideas and provide readers guidelines for both standards; analyze the similarities and differences between the two standards from the perspective of the construction of the internal management system of the organization, and point out the contribution of ISO/IEC 27701 to the construction of internal compliance structure of the company, so as to provide more comprehensive, complete, and practical operating guidelines for companies to conduct data compliance work.

With the aim of providing a more comprehensive and practical set of operating guidelines for companies to conduct data compliance work, this report will:

(1) compare the provisions of the two standards to extract their **key ideas/objectives;**

(2) highlight the respective **control measures** required or recommended by both standards that should be considered;

(3) analyze the similarities and differences between the two standards from the perspective of the construction of the **internal management system of the organization**,

(4) and point out how ISO/IEC 27701 informs the construction of **internal compliance structure** of the organization.

II. Comparative analysis of organizational control measures

1. Scope of application

1.1 Applicable circumstances and subjects

From the perspective of applicable circumstances (regulated activity), both GB/T 35273 (2020) and ISO/IEC 27701 regulate the processing of personal information. However, from the perspective of applicable subjects (regulated subject), there are differences in the writing ideas between the two documents, thereby leading to possible slight differences in the scope of application. Specifically:

GB/T 35273 (2020) focuses on regulating data processing activities throughout the life cycle of personal information. Except for 9.1 c) involving certain obligations of the entrusted person (processor), it mainly regulates the protection principles and security requirements that data controllers shall follow in all personal information processing procedures such as collection, storage, use, sharing, transfer, and public disclosure. According to different purposes and methods of use, GB/T 35273 (2020) applies to data controllers conducting personal information processing, and also applies to competent regulatory authorities, third-party evaluation agencies and other organizations that supervise, manage and evaluate personal information processing.

ISO/IEC 27701 focuses on the role played by the organization during personal information processing, and defines the scope of application of the standard as PII controllers and/or PII processors of all types and sizes processing PII (personal identifiable information) in the Information Security Management System (ISMS), including public and private companies, government entities and non-profit organizations.

1.2 Applicable geographic scope

From the perspective of the applicable geographic scope, GB/T 35273 (2020), as a domestic standard, usually has no extraterritorial effect.

In comparison, ISO/IEC 27701 has a broader scope of application. It is an international standard as a part of ISO management system (including industry-specific standards designed to be implemented alone or as a combined management system). It should be noted that, according to ISO/IEC 27701, the requirements and guidelines for protecting PII which targeting different countries and regions also need to ensure compliance with

the local laws and regulations, and to be interpreted locally in combination with local laws and regulations.

2. Information category

GB/T 35273 (2020) and ISO/IEC 27701 divide the information to be processed into two categories, namely personal information and special category of information (personal sensitive information).

2.1 Personal Information

GB/T 35273 (2020) and ISO/IEC 27701 adopt different ways to describe personal information. The former uses “Personal Information” (hereinafter referred to as “PI”) while the latter uses “Personally Identifiable Information” (hereinafter referred to as “PII”). The two definitions are the same in essence, that is, both adopt the methods of "identification" plus “association”.

Specifically, personal information under GB/T 35273 (2020) is defined as **“any information that is recorded, electronically or otherwise, that can be used alone or in combination with other information to identify a natural person or reflect the activity of a natural person”.** Therefore, when to determine what personal information is, two paths are usually considered:

The first is “identification”, that is, from information to individuals, to identify a specific natural person by the particularity of information itself, where personal information shall be helpful to identify a specific individual;

The second is "association", that is, from individuals to information, by deducing a specific person if there is a known specific natural person, the information generated by the specific natural person in his/her activities (such as personal location information, individual call records and browsing records, etc.) is also personal information.

The personally identifiable information[24] under ISO/IEC 27701 is defined as **"any information related to the subject of information and that can be used to identify a specific subject; or any information directly or indirectly related to the subject of**

[24] ISO/IEC 27701 does not directly define personally identifiable information, but instead quotes the definitions given in ISO/IEC 27000 and ISO/IEC 29100.

PII".

It can be seen that both GB/T 35273 (2020) and ISO/IEC 27701 require that the personal information can be "identified" or "associated" in the definition of personal information, with no difference in essence.

2.2 sensitive personal information/special categories of personal information

Both GB/T 35273 (2020) and ISO/IEC 27701 stipulate that the standards apply to special categories of PI subjects/PII principals. However, the difference between the two is that the term used in GB/T 35273 (2020) is "sensitive personal information", while that in ISO/IEC 27701 is "special category of PII". Although the two standards have a certain intersection in terms of health information and child-related information, GB/T 35273 (2020) adopts a general definition + specific examples set out its Appendix B, different from general definition adopted in ISO/IEC 27701. In practice, it is often easier for companies to know and judge whether the data they control or process is sensitive personal information through the examples cited. Specifically:

According to the general definition of "sensitive personal information" given in GB/T 35273 (2020), "sensitive personal information refers to the personal information that once disclosed, provided illegally or abused, may endanger personal and property safety, easily leading to damage to personal reputation and physical and mental health or discriminatory treatment". The actual examples cited in Appendix B are more likely to occur in general companies, as shown in the following table:

Personal property information	Bank account, authentication information (password), deposit information (including amount of money, payment and collection records, etc), real estate information, credit records, credit information, transaction and consumption records, flow records, as well as virtual property information such as virtual currency, virtual transaction, game redeem codes.
Personal health information	Records generated from illness treatment, such as disease, hospitalization records, physician's order sheet, examination reports, operation and anesthesia records, nursing records, medication records, drug and food allergy information, birth information, past medical history, diagnosis and treatment, family medical history, current medical history, infectious disease history.
Personal biometric information	Personal gene, fingerprint, voiceprint, palm print, auricle, iris, and facial recognition features, etc.
Personal identity information	ID card, military officer card, passport, driver's license, work permit, social security card, residence permit, etc.
Other information	Sexual orientation, marriage history, religious beliefs, unpublished criminal records, communication records and contents, address list, friends list, group list, whereabouts, web browsing records, accommodation information, precise positioning information, etc.

ISO/IEC 27701 adopts the term "special category of PII". However, since different countries' may have different understandings of what is a special category of PII due to different cultural environments, the international standard ISO/IEC 27701 does not give a clear definition of "special category of PII", but instead requires the organization to pay more attention to and provide a higher level of protection to such information by reminding some special categories of PII, such as child information and health information. And it clearly requires that when implementing the standard, that is, when constructing the PIMS, the organization shall conform to the localized understanding and operation according to the requirements of the national data protection law of the applicable country and the provisions made under the national jurisdiction for the concept. Therefore, it leaves sufficient autonomy for companies in different countries to practically carry out operations in accordance with applicable local laws and regulations.

3. Regulated objects

3.1 Personal information controllers

GB/T 35273 (2020) and ISO/IEC 27701[25] have similar definitions of personal information controllers, that is, personal information controllers are defined as "organizations or individuals that have the ability to determine the purposes and methods of personal information processing".

The difference is that ISO/IEC 27701 stipulates that if a natural person uses data for individual purposes, the natural person does not constitute a PII controller, while GB/T 35273 (2020) does not have a similar exemption.

3.2 Joint-controller

(1) Definition of joint-controller

GB/T 35273 (2020) does not give a clear definition of "joint-controller", but instead directly puts forward requirements for the personal information controller in the scenario, and makes it clear that the third-party plug-in operator[26] and the website operator are joint-controllers of personal information where the third-party plug-in does not separately

[25] ISO/IEC 27701 does not directly define personal information controllers, but instead quotes the definitions given in ISO/IEC 29100 and ISO/IEC 27000.

[26] For example, statistical analysis tools, software development kits (SDKs), and map API interfaces deployed by website operators on their web pages or Apps.

obtain the consent of the personal information subject to collect personal information. ISO/IEC 27701 gives a clear and separate definition of "joint-controller", that is, "joint-controllers refer to two or more personal information controllers who can jointly determine the processing purposes and method". Therefore, companies meeting the conditions described in the definition of "joint-controller" shall perform the obligations and responsibilities of a "joint-controller". In this context, the clear definition of "joint-controller" in ISO/IEC 27701 can indirectly help understand the concept of "joint-controller" in GB/T 35273 (2020).

(2) Specific regulatory requirements for joint-controllers

GB/T 35273 (2020) and ISO/IEC 27701 have basically similar requirements for joint-controllers, that is, both require joint-controllers to:

（c） define the responsibilities and obligations between them by signing a contract or other forms;

（d） clearly (transparently) inform the data subject of the responsibilities and obligations that both parties shall bear respectively.

In terms of specific description, GB/T 35273 (2020) requires that "when the personal information controller and a third party are the personal information joint-controllers (for example, a contracted merchant on the service platform), it shall jointly determine with the third party the personal information security requirements to be met, the respective responsibilities and obligations of the parties for personal information security, and clearly inform the personal information subject of the same; If it fails to clearly inform the personal information subject of the identity of the third party, or the respective responsibilities and obligations of of the parties for personal information security, the personal information controller shall be liable for the personal information security incident caused by the third party."

ISO/IEC 27701 requires that "the organization shall determine the respective roles and responsibilities for processing personal information (including personal information protection and security requirements) with any personal information joint-controller, determine the roles and responsibilities for processing personal information in a transparent manner, and meet the requirements of applicable laws and/or regulations; These roles and responsibilities shall be recorded in a contract or any similar binding

documents[27] containing terms and conditions for processing personal information" (e.g., known as data sharing agreements in some jurisdictions).

3.3 Personal information processor

GB/T 35273 (2020) does not define or use the term "personal information processor". To understand the provisions that essentially cover the term "personal information processor" one needs to refer to and combine the specific requirements relating to the "entrusted processing" in the Article 9.1. ISO/IEC 27701 clearly defines the concept of PII processor[28] as anyone following the instructions of the PII controller to process PII on behalf of PII controller. Please refer to the analysis in section 7.1 hereof for the specific requirements of the two standards for entrusted processors.

4. Collection of personal information

GB/T 35273 (2020)	ISO/IEC 27701
Legality (Articles 5.1 and 5.4)	There are similar requirements (Article 7.2.2)
Minimum necessity (Article 5.2)	There are similar requirements (Article 7.4.1)
Independent selection of multiple business functions (Article 5.3)	The coarse granularity suggests it shall pay attention to similar requirements in some jurisdictions (Article 7.2.3)
Full and transparent disclosure of requirements (Article 5.4)	There are similar requirements (Article 7.3.2)
Authorized consent and exceptions for the collection of personal information (Articles 3.6, 3.7, 5.4 and 5.6)	There are similar requirements (Article 7.2.3)
Personal information protection policy (Article 5.5)	Spread over multiple articles (Articles 6.2.1.1, 6.15.1.3, 7.3.9 and 7.4.2)

[27] Agreements reached between joint-controllers include: (1) the purpose of PII sharing / relationship between PII joint-controllers; (2) identity of the organization (PII controller) serving as a part of the PII joint-controller relationship; (3) type of PII shared and/or transferred and processed according to the agreement; overview of processing operations (e.g., transfer and use); (4) description of their respective roles and responsibilities; (5) responsibilities for implementing PII protection technologies and organizational security measures; (6) responsibility determination when PII is disclosed (for example, who and when to notify each other); (7) PII retention and/or removal clauses; (8) failure to comply with the responsibility of this agreement; (9) how to fulfill the obligations for the PII principal; (10) how to provide the PII principal with the information covering core content of arrangement between joint-controllers; (11) core content of the agreement between joint-controllers; (12) how the PII information subject asks for other information that it has the right to receive; (13) the contact point of the PII principal.

[28] ISO/IEC 27701 does not directly define the PII processor, but instead quotes the provisions of ISO/IEC 29100.

4.1 Legality requirements

Both GB/T 35273 (2020) and ISO/IEC 27701 stipulate that the collection and processing of personal information must have a legal basis. Although the legal basis required by the two Standards for the collection of personal information is basically similar in type, the applicable logic of the legal basis varies. GB/T 35273 (2020) takes obtaining personal information subject's consent as the only basis for legal collection of personal information, while it provides for the public interest and protection of the major rights and interests of information subjects as exceptions[29] for obtaining consent. While ISO/IEC 27701 takes obtaining consent, and the protection of public interest and the major rights and interests of information subjects[30], as equal interest, rather than distinguishing the later interest as an exception. It is more similar to enumerating the legality requirements under the GDPR.

4.2 Minimum necessity requirements

Both GB/T 35273 (2020) and ISO/IEC 27701 stipulate that the collection of personal information shall meet the requirements of "minimum necessity". The two Standards give different expressions, but in essence they require that the personal information collected shall be associated with a specific purpose, and must be collected in accordance with the purpose of minimum quantity and necessary collection. Specifically:

According to GB/T 35273 (2020), the type of personal information collected shall be directly related to the realization of business functions relating to the provisions of products and / or services. The term "directly related" means that without involvement of such information, the business functions of providing products and/or services cannot be

29 Exceptions to obtaining consents specified in Personal Information Security Specification include: (1) In connection with the fulfilment of obligations under laws and regulations by the PI Controller; (2)Directly related to national security or national defense; (3)Directly related to public security, public health or major public interests; (4)Directly related to criminal investigations, prosecutions, trials or execution of court 8 decisions; (5) For the purpose of safeguarding the life, property or other significant legitimate rights and interests of the PI Subjects or other individuals, and it is hard to obtain consent from the PI Subjects; (6) The PI involved is disclosed to the public by the PI Subject; (7) essential to the signing and performing of a contract requested by the PI Subject; (8)The PI is collected from legally and publicly disclosed information, such as legal news reports and government information disclosure; (9)essential to maintaining safe and stable operation of the product or service provided, such as the discovery and handling of product or service failures; (10) The PI Controller is a news agency and the collecting and using of PI are essential for it to carry out legitimate news reporting; (11) The PI Controller is an academic research institution and the collecting and using of PI are essential for it to carry out statistics or academic research for public interests, provided that the PI contained in the results is de-identified when it makes the academic research or the descriptive results available.

30 The legal basis for processing PII as stipulated in ISO/IEC 27701 includes: (1) consent of the PII information subject; (2) performance of the contract; (3) compliance with legal obligations; (4) protection of the key interests of the PII information subject; (5) tasks performed for the public interest; (6) protection of legitimate interests of the PII controller

realized. The automatic collection of personal information shall be of the minimum frequency necessary to realize the business functions of providing products and/or services. The personal information indirectly acquired shall be of the minimum amount necessary to achieve the business functions of providing products and/or services.

According to ISO/IEC 27701, the organization shall limit the collection of PII to the minimum extent that it is associated, be proportionate and necessary to achieve a specific purpose, including limiting the amount of PII to be collected indirectly by the organization (e.g., via web logs and system logs).

4.3 Independent choice among multiple business functions

Both GB/T 35273 (2020) and ISO/IEC 27701 state that PI subjects should not be forced to accept multiple business functions. However GB/T 35273 (2020), as a localized standard in China, has more detailed provisions on this requirement. ISO/IEC 27701 does not provide detailed regulations, but instead issues a reminder that there may be such regulations in the jurisdiction involved.

GB/T 35273 (2020) stipulates that, when a product or service is provided by a number of business functions that require the collection of PI, the PI controller shall not force PI subjects to accept the business functions provided by the product or service and the corresponding requests for PI collection. Requirements on the PI controller include:

1) The PI controller shall not, by bundling the business functions of a product or service, require PI subjects to accept and give consent to bundled requests for PI collection for the business functions that the PI subjects have not used or applied for;

2) The PI Controller shall obtain the affirmative action by PI subjects, such as proactive clicking, ticking, and filling-in, as the condition for activating a specific business function of a product or service. The PI controller shall only initiate the collection of PI after the PI subjects have activated the business function;

3) The PI controller shall provide the way or method for PI subjects to close or exit from a business function as convenient as the one for the PI subjects to opt in for such business function. After the PI subjects choose to close or exited from a particular business function, the PI controller shall stop the PI collection for such business function;

4) Where a PI subject has refused to authorize the use of, closed or exited from a particular business function, the PI controller shall not frequently request consents from the PI subject;

5) Where a PI subject has refused to authorize the use of, closed or exited from a particular business function, the PI controller shall neither suspend any other business function for which the PI subject has opted in voluntarily nor reduce the service quality of any other business function;

6) The PI controller shall not demand a PI subject to authorize the collection of its PI only for the purposes of improving service quality, improving user experience, developing new products or enhancing security.

However, ISO/IEC 27701 states by way of examples that some jurisdictions may have special requirements on the way of obtaining consent, such as binding consent with other protocols without detailed guidance. Therefore, from a practical perspective, a Chinese company or organization may adopt a combination of ISO/IEC 27701 and GB/T 35273 (2020) by: determining the specific requirements regarding protecting personal information of Mainland China and implement them based on GB/T 35273 (2020) while building a compliance framework for privacy protection on the basis of ISO/IEC 27701.

4.4 Full and transparent disclosure of requirements

Both GB/T 35273 (2020) and ISO/IEC 27701 stipulate the time and content of notification, but the details are not consistent. In terms of the notification time, GB/T 35273 (2020) has relatively more definitive provisions. In terms of the content, ISO/IEC 27701 has a higher requirement on the specific content of the notification where personal information has been directly collected, but GB/T 35273 (2020) has a higher requirement where personal information is indirectly collected. The specifics are as follows:

(1) Time of notification

According to GB/T 35273 (2020), the personal information controller shall clearly notify the personal information subject when **collecting the personal information**, for example, before the start of basic business or before extending the use of business for the first time. ISO/IEC 27701 makes no strict requirements on the notification time, but instead only requires the organization to determine the notification time **with reference to laws,**

regulations and business practices.

(2) Content of notification

A. Notification of direct collection

According to GB/T 35273 (2020), the personal information controller shall clearly inform the personal information subject of the rules for the collection and use of personal information when collecting the personal information, such as the purposes, methods and scope of the collection and use of personal information. Specifically, when the product or service provides multiple business functions for the collection and use of personal information, the personal information controller should notify the purpose, methods and scope of collection and use of the personal information to the subject besides the personal information protection policy at the time of actually collecting specific personal information, so that the personal information subject can give full consideration to its specific impact before granting specific authorization and consent.

The personal information subject shall be informed of the purpose, methods, scope, storage duration and other rules of collection and use of personal biometric information before collecting personal biometric information.

ISO/IEC 27701 has a higher requirement for the content of the notification. that is, in addition to notifying the type of collected personal information, and the rules for collecting and using personal information, it also recommends that the following information be included in the notification:

6) Legal basis for information processing;

7) Source of the information, if the information is not collected directly from the PII principal;

8) Whether the PII principal provides PII based on statutory requirements or contractual requirements, and the consequences of failure to provide PII;

9) Whether there is automatic processing of PII for automatic decision-making;

10) Updated information that shall be notified to the PII principal by the organization if the purpose of processing PII is changed or expanded.

B. Notification of indirect collection

GB/T 35273 (2020) does not stipulate the obligation of the personal information controller to inform the information subject of indirect collection for personal information, but instead stipulates that the personal information controller shall require the personal information provider to explain the information source, and review and confirm the legitimacy of the personal information source. The personal information provider is also required to know the scope of authorization and consent that the personal information provider has obtained from the personal information subject for the information processing, including the purpose of use and whether the personal information subject authorizes and agrees to transfer, share and disclose the personal information publicly. Where the personal information processing required by the organization to conduct the business goes beyond the scope of authorization and consent, the explicit consent of the personal information subject shall be obtained again within a reasonable time after obtaining the authorization of personal information or before processing personal information.

In addition, GB/T 35273 (2020) stipulates that when personal information sharing or transfer is involved, the data sharing party or transferor shall inform the personal information subject of the purpose of sharing and transferring personal information, the type of data recipient and the possible consequences. Prior to sharing and transferring sensitive personal information, it is required to inform the personal information subject of the type of sensitive personal information involved, the identity of the data recipient and the data security capability.

ISO/IEC 27701 has relatively simple regulation on indirect collection, only requiring that the organization inform the PII principal of the source of the information when the information is not collected directly from the PII principal.

4.5 Authorized consent and exceptions for the collection of personal information

(1) Cases where consent is required

As stated in section 4.1 (1) “Requirements for legality of collection”, both GB/T 35273 (2020) and ISO/IEC 27701 take the consent as the legal basis for personal information collection. The difference is that GB/T 35273 (2020) states that “explicit consent” of the

personal information subject shall be obtained for personal information collection in some specific situations, while GB/T 35273, uses the term "explicit consent" covers a wide range, including any explicit consent without ambiguity. ISO/IEC 27701 requires consent to be freely given, specificly regarding the purpose for processing and unambiguous and explicit. Specifically:

According to GB/T 35273 (2020), the personal information subject shall be informed of the purpose, methods and scope of collection and use of personal information, and the "authorization and consent" of the personal information subject shall be obtained at the time of collecting personal information. **Under certain circumstances, the explicit consent of the personal information subject is required**[31]**,** including:

1) The explicit consent of the personal information subject shall be obtained prior to the collection of sensitive personal information;

2) The explicit consent of the personal information subject shall be obtained prior to the collection of personal biometric information;

3) The explicit consent of a minor or his/her guardian shall be obtained before the collection of personal information of a minor over the age 14; for the minor under the age of 14, the explicit consent of his/her guardian shall be obtained;

4) The explicit consent of the personal information subject shall be obtained again when using the personal information beyond the above scope of authorization;

5) The explicit consent of the personal information subject shall be obtained when sharing and transferring sensitive personal information or personal biometric information;

6) The explicit consent of the personal information subject shall be obtained again if the purpose of personal information use is changed;

7) The explicit consent of the personal information subject with regard to the collection and use of its personal information through basic business functions shall be obtained before enabling the basic business functions and after re-dividing

[31] Explicit consent refers to the behavior that the subject of personal information makes specific authorization for the specific processing of personal information through active written statement or affirmative action. Affirmative actions include the active statement (electronic or paper form), active check, active click of "agree", "register", "send", "call", active filling or provision by the personal information subject.

the basic business functions;

8) Enable the personal information subject to give consent to extended business functions option by option before its first use of extended business; and

9) The explicit consent of the personal information subject shall be obtained in advance when it is necessary to disclose personal information publicly with legal authorization or reasonable reasons.

ISO/IEC 27701 takes consent as one of the legal basis for PII collection, and also suggests that the consent of the PII principal shall be obtained under certain circumstances. These specific cases include:

1) The organization may not use any contracted PII for marketing or advertising purposes without the prior consent of the subject of the PII information. The organization shall not take granting such consent as a condition for receiving services.

2) Where the change or extension of the PII processing purpose may require updating and/or revising the legal basis, it may require additional consent from the PII principal.

(2) Recording of the process of obtaining consent

GB/T 35273 (2020) does not require the organization to establish and implement procedures for recording the process of obtaining consent, but ISO/IEC 27701 gives detailed regulations. Specifically:

ISO/IEC 27701 attaches great importance to the "recording" of the granting of consent, and makes the following provisions:

1) The organization shall clearly record when consent is required and the requirements for obtaining the consent.

2) The organization shall identify and record each procedure, based on which the organization may demonstrate whether, when and how to obtain the consent from the PII principal to the PII processing.

3) The organization shall obtain and record the consent of the PII principal in

accordance with documented procedures.

(3) Special regulations for collecting personal information of minors

GB/T 35273 (2020) has special regulations for the personal information collection of minors, while ISO/IEC 27701 only states that additional regulations may be required when special subjects such as children are involved, with no special clauses on information collection of minors. Specifically:

GB/T 35273 (2020) requires that the explicit consent of a minor or his/her guardian shall be obtained before the collection of personal information of a minor over the age of 14; for the minor under the age of 14, the explicit consent of his/her guardian shall be obtained.

ISO/IEC 27701 issues a general reminder that some jurisdictions have specific requirements on how to collect and solicit consent (for example, no binding with other agreements is allowed). In addition, additional regulations need to be observed when collecting certain types of data (such as those for scientific research) or data of certain PII principals (such as children).

(4) Withdrawal of consent

Both GB/T 35273 (2020) and ISO/IEC 27701 stipulate that information subjects shall be informed on how to withdraw the consent. ISO/IEC 27701 gives more specific requirements on consent withdrawal notification, consent withdrawal mechanism and the consequences of consent withdrawal. Specifically:

- Notification of consent withdrawal

Both GB/T 35273 (2020) and ISO/IEC 27701 stipulate that PI/PII controllers shall provide PI subjects/PII principals with methods to withdraw the consent, but ISO/IEC 27701 emphasizes that the organization must notify PII principals of **the right to withdraw consent and the methods to exercise their right** (see below), so that they have the right to withdraw consent at any time.

- Ways to withdraw consent

GB/T 35273 (2020) does not describe in detail how to withdraw the consent, but instead only stipulates that personal information controllers shall provide personal information subjects with a convenient way to withdraw their authorization and consent, while

ISO/IEC 27701 requires that **the way to exercise the right of consent withdrawal shall be consistent with that of obtaining consent.** For example, the consent that has been obtained through e-mail or a website may be withdrawn in the same way, but not by telephone or fax. ISO/IEC 27701 also requires the organization **to record the user's request for withdrawal of consent in the same way as the user's consent is recorded.**

- Consequences of consent withdrawal

According to GB/T 35273 (2020), the personal information controller shall not process the related personal information after consent is withdrawn. Withdrawal of the authorization and consent will not affect the previous processing of personal information based on the authorization and consent. ISO/IEC 27701 has similar provisions in this regard, but it additionally requires that **the results obtained from the processing of PII before the withdrawal of consent shall not be further used in the processing**. For example, if a PII principal withdraws consent to a user's profiling, the profiling shall no longer be used or viewed.

For PII shared with third parties, ISO/IEC 27701 stipulates that the organization shall implement certain policies, procedures and/or mechanisms to inform the third party of the withdrawal of consent by the PII principal. The specific measures shall be decided by the organizations themselves, giving them greater autonomy.

(5) Exceptions to authorization and consent

As stated in section 4.1, the two standards are different in applicable logic of the legal basis for personal information collection, but the types of legal basis are basically similar, specifically:

GB/T 35273 (2020) (Article 5.6)	ISO/IEC 27701 (Article 7.2.2)
In connection with the fulfilment of obligations under laws and regulations by the PI Controller;	Fulfill the legal obligations
Directly related to national security or national defense;	Perform the work related to the benefits

Directly related to public security, public health or major public interests;	Perform the work related to the benefits
Directly related to criminal investigations, prosecutions, trials or execution of court 8 decisions;	Perform the work related to the benefits
For the purpose of safeguarding the life, property or other significant legitimate rights and interests of the PI Subjects or other individuals, and it is hard to obtain consent from the PI Subjects;	Safeguard the major interests of PII principals
The PI involved is disclosed to the public by the PI Subject;	No requirement
essential to the signing and performing of a contract requested by the PI Subject;	Perform the contract
No requirement given	Legitimate interests of the PII controller
The PI is collected from legally and publicly disclosed information, such as legal news reports and government information disclosure;	No requirement
essential to maintaining safe and stable operation of the product or service provided, such as the discovery and handling of product or service failures;	Perform the contract
The PI Controller is a news agency and the collecting and using of PI are essential for it to carry out legitimate news reporting;	No requirement
The PI Controller is an academic research institution and the collecting and using of PI are essential for it to carry out statistics or academic research for public interests, provided that the PI contained in the results is de-identified when it makes the academic research or the descriptive results available.	Perform the work related to the benefits

Both Standards stipulate the legal basis for fulfilling legal obligations, protecting the

public interests, safeguarding the major interests of PI subjects/PII principals, and the nature of performing the contract. However, GB/T 35273 (2020) provides for exceptions where the PI subject discloses information on its own; protect the lives and property interests of others; or the PI controller is a news agency or an academic research institution. While ISO/IEC 27701 states that the legitimate interests of the PII controller can also be taken as the legal basis for data processing. It shall be noted that ISO/IEC 27701 must be adopted in combination with local data protection requirements in practice, and where there is any mismatch between them, the local data protection laws shall prevail. For example, GB/T 35273 (2020) of China does not stipulate that the legitimate interests of PI controllers serve as the basis for processing, so the company shall not take the legitimate interests of PI controllers as the legal basis when it provides personal information protection in China.

4.6 Requirements of personal information protection policies

Both GB/T 35273 (2020) and ISO/IEC 27701 state that the organization shall provide personal information protection policies, and make clear and detailed guidelines on the formulation, content requirements[32] and implementation rules[33] of personal information protection policies, but the two documents are different in policy content and policy implementation.

From the perspective of content, GB/T 35273 (2020) adopts the term "personal information protection policies", focusing on the protection of the full life cycle of personal information; while ISO/IEC 27701 adopts the broader term "information security policies", **covering the protection policies for personal information disclosed to the public and construction of the organization's internal information**

[32]According to GB/T 35273 (2020), personal information protection policies shall include but are not limited to: 1) Basic information about the PI Controller, including the identity and contact information; 2)Business functions that collect and use PI, and the types of PI each of the business functions collects. Where sensitive PI is involved, relevant content shall be explicitly marked or highlighted; 3) The collection method and storage time of PI, whether cross-border data transfer is involved, and other PI processing rules; 4) Purposes of the sharing, transfer and public disclosure of PI, the types of PI involved, the types of third parties receiving the PI, and respective security and legal responsibilities; 5) Rights of PI Subjects and implementation mechanisms, such as methods to access, rectify or delete their PI, to de-register, withdraw consent, obtain a copy of their PI, and to lodge a complaint about the automated decisions by information systems; 6) Security risks after consenting to PI collection, and possible impacts of not consenting to ant PI collection; 7) The basic principles of PI security followed, the data security capabilities in place, and the PI security protection measures adopted; compliance certificates related to data security and PI protection may be disclosed when necessary; 8) Channels and mechanisms for handling the inquiries and complaints of PI Subjects, and external dispute settlement agencies and their contact information.

[33] See the table in Appendix C of GB/T 35273 (2020).

management and protection system, that is, it has a more comprehensive content, providing the organization with an information security protection system that balances the internal and external considerations.

In terms of the form, GB/T 35273 (2020) requires that the personal information protection policies shall be clear and easy to understand, and they shall be made public and easily accessible, and shall be delivered to the personal information subjects one by one, and the information subjects shall be informed when updating the policies. ISO/IEC 27701 requires **the retention of a copy of the privacy policies and related procedures**. When a file is updated, **a copy of the previous version shall be kept**.

5. Retention of personal information

Both GB/T 35273 (2020) and ISO/IEC 27701 provide for the storage time and de-identification of personal information, but there are different requirements: ISO/IEC 27701 has a higher requirement for the storage time, while GB/T 35273 (2020) has a higher requirement for de-identification. In addition, ISO/IEC 27701 has additional restrictions on storage media.

GB/T 35273 (2020)	ISO/IEC 27701
Minimization of storage time of personal information **(Article 6.1)**	There are requirements but the granularity is finer (Article 7.4.7)
Requirements for storage media **No requirement given**	There are requirements (Article 6.5.3.1)
De-identification after collection **(Article 6.2)**	There are similar requirements (Article 7.4.5)
Transmission and storage of sensitive personal information **(Article 6.3)**	It requires classification of special types of PII, and it is suggested to pay attention to special provisions on use of special types of PII in certain jurisdictions (Articles 6.5.2, 7.4.9 and 6.10.2)
Three requirements for personal information controllers to stop operations **(Article 6.4)**	It provides suggestions on the selection of techniques to delete PII only (Articles 7.4.5 and 7.4.8)

5.1 Minimization of storage duration

For the storage of personal information, GB/T 35273 (2020) requires that the personal information storage time shall be **the minimum duration required to achieve the purpose of authorized use of the personal information subject**.

Compared to GB/T 35273 (2020), ISO/IEC 27701 additionally stipulates that the organization shall **establish and maintain a timetable for information storage**, which shall take into account legal, regulatory and commercial requirements. **In case of a conflict among those requirements, it is necessary (based on risk assessment) to make a business decision and record it in an appropriate timetable.** The organization shall stipulate and record goals of data minimization and the way to achieve such goals, including mechanisms taken (e.g., de-identification). ISO/IEC 27701 emphasis on "recording" and "risk-based assessment" is set out in different clauses, and it has more detailed guidelines for some highly abstract mechanisms.

5.2 Requirements for storage media

GB/T 35273 (2020) does not set the requirements over storage media, but instead specifies in detail that the organization shall **back up any use of removable media and/or devices used to store PI**. Unless it is unavoidable, the organization **shall not use removable physical media and/or devices with no encryption of PI.** When to use unencrypted physical media and/or devices, the organization shall take certain procedures and control measures (e.g., tamper-proof packaging) to reduce the risk of PI disclosure. ISO/IEC 27701 does not impose strict restrictions on the specific processes and control measures to be taken, granting the organization a certain degree of freedom to make reasonable design.

5.3 De-identification

GB/T 35273 (2020) suggests that the personal information controllers should immediately de-identify the personal information after collecting the information, and **take technical and management measures to store the de-identification information separately from the information that can be used to recover and identify individuals, and strengthen the authority management of access and use.**

The above-mentioned clause of GB/T 35273 (2020) is only a suggestion (the word

"suggest" is used in the text), while ISO/IEC 27701 does not propose a recommendation for de-identification after the collection, but only requires that **PII shall be de-identified or deleted after PII is processed**.

5.4 Transmission and storage of sensitive personal information

Both GB/T 35273 (2020) and ISO/IEC 27701 mention the special requirements for sensitive personal information. The difference is that GB/T 35273 (2020) has definite requirements for the transmission and storage of sensitive personal information, while ISO/IEC 27701 requires that special types of PII shall be classified separately, and calls for attention to special provisions on the use and classification of sensitive personal information in different countries. Specifically:

GB/T 35273 (2020) requires the controller to take security measures such as encryption when transmitting and storing sensitive personal information, to store personal biometric information separately from personal identity information, and to take technical measures to ensure information security when to store personal biometric information, such as storing only summary information, directly using personal biometric information in the acquisition terminal to achieve identity recognition, authentication and other functions, and deleting original images from which personal biometric information is extracted after identity recognition, authentication and other functions are achieved by means of facial recognition features, fingerprints, palm prints, or iris.

ISO/IEC 27701 requires that organizations note the possible differences in the definition of special types of PII in different counties, and requires that the organization also note that these types of PII shall be classified separately. It also calls for attention to the special provisions on such PII in different countries.

5.5 Discontinuance of operation by PI Controllers

GB/T 35273 (2020) specifies how personal information controllers should handle information after they stop operations, while ISO/IEC 27701 does not mention such a point.

Specifically, GB/T 35273 (2020) requires that when the organization discontinues operating its products or services, it shall stop collecting personal information in a timely manner, send a notice of operation discontinuation to the subjects individually or notify

them in the form of an announcement, and delete or anonymize the personal information held.

6. Use of personal information

For the use of personal information, the provisions of GB/T 35273 (2020) and ISO/IEC 27701 are quite different in content. While GB/T 35273 (2020) and ISO/IEC 27701 both have provisions for access control, display restriction and use purpose restriction, user profiling use restriction, automatic decision-making and rights enjoyed by personal information subjects, GB/T 35273 (2020) also makes detailed provisions for **the use of personalized display** and **the aggregation and integration** of personal information collected for different businesses. Due to the limited space of this report, to avoid redundancy, please refer to Articles 7.5 and 7.6 of GB/T 35273 (2020) and **Schedule A of this report** for special provisions of GB/T 35273 (2020). The following is the comparative analysis of the parts specified in both GB/T 35273 (2020) and ISO/IEC 27701.

GB/T 35273 (2020)	ISO/IEC 27701
Access control measures of personal information (Article 7.1)	There are requirements with greater details (Article 6.6)
Restrictions on the display of personal information (Article 7.2)	There are similar requirements (Article 6.8.2.9)
Restrictions on the purpose of use of personal information (Article 7.3)	There are requirements but the granularity is finer (Articles 7.2.1, 7.2.2 and 8.2.3)
Restrictions on the use of user profiling (Article 7.4)	There are requirements, but the granularity is coarser (Articles 7.2.2, 7.3.10)
Use of personalized display (Article 7.5)	There is no direct corresponding provisions, but depending on the specific situation, personalized display may involve automated decision making - Article 7.3.10
Fusion of PI collected for different business purposes (Article 7.6)	There is no direct counterpart, but Articles 7.2.2 and 7.2.5 can be referred to according to the content
Use of automatic decision-making mechanism of information systems (Article 7.7)	There are similar requirements (Articles 7.3.10 and 7.2.5)

6.1 Control measures for access to personal information

For personal information access control measures, from the perspective of personnel control, GB/T 35273 (2020) regulates the minimum authorization of access, separation of operators, administrators and auditors, important operations (such as batch modification, copy, download), over-privileged operation and sensitive personal information operation as requirements when developing approval processes, that is, the control of access to the system by personnel of companies and personnel responsible for such personal information.

However, ISO/IEC 27701 makes more detailed provisions from the two dimensions of access to the system and personnel control, thereby providing further and practical guidelines for the development of internal access control measures for companies and organizations. Specifically:

On the one hand, ISO/IEC 27701 requires authorized personnel to use specialized network or network services, such as VPN, when they access the system, and requires the organization to monitor the specialized network, while reminding that links to unauthorized and insecure network services may affect the entire organization. Specific control measures are adopted for sensitive or business-critical connections or connections to user networks in high-risk locations.

On the other hand, ISO/IEC 27701 also provides for the control of visitors. However, this section is similar to the content regulated in GB/T 35273 (2020), and they all provide for the authorization rating and approval process of visitors. ISO/IEC 27701 additionally requires regular audits of authorizations or reviews of any changes to ensure that all the personnel access according to their respective authorization, and requires authorized personnel to delete their access rights when leaving their posts.

6.2 Restrictions on the display of personal information

Both GB/T 35273 (2020) and ISO/IEC 27701 have provisions for the restrictions on the display of personal information, but they are different in restriction strategies. GB/T 35273 (2020) starts with the content of personal information displayed, and requires that the de-identification measures should be adopted to the personal information displayed via the interfaces (such as display screen, paper) to reduce the disclosure risk in display.

While ISO/IEC 27701 makes provisions from the perspective of external physical protection of the equipment carrying personal information, requiring the removal of paper on the desktop and locking of sensitive or critical business information (in safe box or safes or other forms of security equipment in ideal conditions), so as to come up with new ideas for the organization to improve display restrictions.

6.3 Restrictions on the purpose of personal information use

Both GB/T 35273 (2020) and ISO/IEC 27701 have provisions for the restrictions on the purpose of PI/PII use, requiring that the PI/PII shall not be used beyond the reasonable, relevant and minimum necessary scope, and for any change to the processing purpose, the consent of the PI subject/PII principal shall be obtained separately.

6.4 Restrictions on the use of user profiling

Both GB/T 35273 (2020) and ISO/IEC 27701 mention the restrictions on the use of user profiling, but ISO/IEC 27701, which focuses on the overall organization and management, leaves room for the local laws and regulations that the organization is subject to in a larger sense. It only states that if the PII principal withdraws his/her consent to the user profiling, the profiling of the subject shall not be used or viewed. However, GB/T 35273 (2020) not only restricts the content of the profiling itself, but also regulates the use of the profiling. Specifically:

In terms of profiling content, GB/T 35273 (2020) stipulates that the description of the personal information subject in the user profiling shall not contain obscenity, pornography, gambling, superstition, terrorism, violence, or other points expressing discrimination on ethnicity, race, religion, disability or disease discrimination, etc.;

In terms of the use of user profiling, GB/T 35273 (2020) requires that the legitimate rights and interests of citizens, legal persons and other organizations shall not be infringed upon, nor endangering the national security. When using the personal information, unless it is necessary to achieve the purpose of authorization and consent of the personal information subject, the clear directionality to personal identity shall be eliminated to avoid accurate targeting to the specific individuals.

6.5 Use of automatic decision-making mechanism of information systems

For automatic decision-making of information systems, both GB/T 35273 (2020) and

ISO/IEC 27701 require organizations to conduct personal information security impact assessments / privacy impact assessments when using the automatic decision-making mechanism of information systems. GB/T 35273 (2020) limits the regulation to the **automatic decision-making mechanism that has a significant impact on the rights and interests of information subjects**, while ISO/IEC 27701 limits the requirements only to the **organization that processes PII by the automatic decision-making method**. ISO/IEC 27701 separately suggests that the organization may be subject to **special provisions in some jurisdictions, including the provisions that the existence of automatic decision-making shall be informed, the PII principal shall be allowed to reject the automated decisions or some types of PII shall not be fully automated. Such organization should comply with these local special obligations established by the relevant jurisdiction.**

7. Entrusted processing, sharing, transfer, public disclosure and cross-border transfer of personal information

Both GB/T 35273 (2020) and ISO/IEC 27701 have regulations on entrusted processing, sharing, transfer, public disclosure and cross-border transmission of personal information. ISO/IEC 27701 has higher and more detailed requirements on entrusted processing and cross-border transfer of personal information, while GB/T 35273 (2020) has higher requirements on sharing, transfer and public disclosure.

GB/T 35273 (2020)[34]	ISO/IEC 27701
Entrusted processing **(Article 9.1)**	There are requirements (Articles 6.12, 7.2.6, 7.2.8 and 8)
Sharing and transfer **(Articles 9.2 and 9.3)**	There are similar requirements (Articles 7.2.1 - 7.2.5, 7.3.2, 7.3.3, 7.3.7, 7.4.5, 7.4.8, 7.5.3, 7.5.4)
Public disclosure **(Article 9.4)**	There are requirements (Articles 7.2.2, 7.2.3, 7.2.4, 7.2.5, 7.3.1, 7.3.2, 7.3.3 and 7.5.4; in addition, article 9.4(e) in GB/T 35273(2020) has no corresponding provision as it involves responsibility)
Third party access management **(Article 9.7)**	There are requirements, but the granularity is coarser (Articles 6.12 and 7.2.6)
Cross-border transfer **(Article 9.8)**	There are requirements, and the granularity is finer (Articles 7.5.1, 7.5.2)

[34] Since Articles 9.5 and 9.6 have been discussed in sections 4.1 and 3.2 above respectively, no repeated description is made here.

7.1 Entrusted processing

For entrusted processing, both GB/T 35273 (2020) and ISO/IEC 27701 have provisions on authorization of PI subject/PII principals, supervision modes of entrusted processing and assignment of powers and responsibilities, respective obligations of the personal information controller and the entrusted party (PII processor). It shall be noted that as GB/T 35273 (2020) does not provide special terms and definitions for "personal information processor" or "subcontractor", it is required to understand the provisions covering "personal information processor" or "subcontractor" by reference to the specific requirements related to entrusted processing. The two standards have similar requirements for supervision mode of entrusted processing and distribution of rights and responsibilities, but the provisions of ISO/IEC 27701 on the authorization of personal information subject and the respective obligations of the personal information controller and the entrusted party (PII processor) are more detailed and comprehensive, which provides guidance for the organization to improve compliance. The specific provisions for each document on the entrusted process is as follows:

(1) Requirements for authorization of the PI subject/PII principal

GB/T 35273 (2020) does not require the personal information controller to request the written authorization of the personal information subject for entrustment, but only requires the personal information controller to entrust within the scope of authorization, obtain consent of the personal information subject, and evaluate personal information security impact of the entrustment.

According to ISO/IEC 27701, **in two cases, the entrusted processing made by the organization requires the written authorization of the user**: 1) if the organization subcontracts the processing task of PII, in part or in whole, to another organization, disclosure to the user and written authorization from the user are required prior to PII processing by the subcontractor, by making an agreement with appropriate authorization clauses or signing a specific “one-off” authorization agreement between the PII processor and the user. 2) In case of any change to the organization that is entrusted to process PII, in part or in whole, the written authorization of the user for the change shall be obtained before the new subcontractor starts PII processing. Such a case can be handled by making an agreement with appropriate authorization clauses or signing a specific “one-off”

authorization agreement between the PII processor and the user.

(2) Obligations of personal information controller in an entrusted processing relationship

GB/T 35273 (2020) and ISO/IEC 27701 have basically the same requirements for the controller, that is, the controller shall enter into a contract with the entrusted party (PII processor), where the responsibilities and obligations of the entrusted party (PII processor) shall be defined[35]; before the entrustment, a personal information security impact assessment/privacy impact assessment shall be conducted, with a record of the entrusted processing.

However, where GB/T 35273 (2020) further requires auditing the entrusted party according to the same clause and the personal information controller is informed of or discovers that the entrusted party fails to process personal information in accordance with the requirements of the entrustment, or fails to effectively fulfill the responsibility for the personal information protection, the controller has the obligation to ask the entrusted party to stop relevant processing activities, and take or require the entrusted party to take effective remedial measures (such as changing passwords, revoking privileges, disconnecting network) to control or eliminate the security risks to personal information. If necessary, the personal information controller shall terminate the business relationship with the entrusted party and require the entrusted party to delete the personal information obtained from the controller in time. ISO/IEC 27701 specifies the information security policies with suppliers (although not directly name PII processors or entrusted processors) in the section "supplier relationship", including the agreement on appropriate audit of suppliers and control measures, resolution of defects and conflicts, and other information security strategies, which provides more comprehensive and macro guidance to the organization. While ISO/IEC 27701 does not specify the circumstances where certification, audit or conclusion of general contract terms is needed, it can provide guidance for third-party certification when implementing GB/T 35273 (2020).

(3) Obligations of entrusted party in entrusted processing relationship

Both GB/T 35273 (2020) and ISO/IEC 27701 have provisions on the obligations of the

[35]ISO/IEC 27701 requires the organization to enter into a written contract with any of its subcontractors and ensure that its contract with the subcontractor covers all appropriate control measures described in Appendix B of ISO/IEC 27701.

trusted party. GB/T 35273 (2020) stipulates the obligations of the entrusted party in Article 9.1, while ISO/IEC 27701 specifies the obligations of the PII processor in Appendix B comprehensively. Specifically:

GB/T 35273 (2020)	ISO/IEC 27701
Specify the responsibilities and obligations of the trustee through contracts or otherwise **(Article 9.1 d)1))**	Contract requirements between PII controller and processor (Articles 6.12.1.2, 8.2.1)
Not store relevant PI anymore upon termination of the entrustment **(Article 9.1 c)5))**	Elimination of temporary files (Article 8.4.1)
Not store relevant PI anymore upon termination of the entrustment **(Article 9.1 c)5))**	Return, transmission and elimination of PII after processing (Article 8.4.2)
Assist the PI controller to respond to requests made by PI subjects **(Article 9.1 c)3))**	Protection of PII principal rights (Article 8.3)
No performance capability claimed	Processing under advertising and marketing (Article 8.2.3) Purpose restriction of PII processor (Article 8.2.2) Notification of infringement of PII controller's handling instructions (Article 8.2.4) Notification of compliance measures (Article 8.2.5) Requirements for PII transmission (Article 8.4.3) PII sharing among different jurisdictions (Articles 8.5.1 and 8.5.2) Record, notification and prohibition of PII disclosure (Articles 8.5.3, 8.5.4 and 8.5.5) Notifications and requirements for handling PII with subcontractors (Articles 8.5.6, 8.5.7 and 8.5.8)
Feedback on handling violations of requirements, authorization on re-entrustment, failure to provide adequate security protection or feedback on security incidents **(Article 9.1 c))**	No similar requirement

On the whole, GB/T 35273 (2020) and ISO/IEC 27701 are compatible with the provisions on the obligations of the entrusted party, but it can be seen that ISO/IEC 27701 has more comprehensive and detailed provisions and provides a systemic guarantee for the controller to better supervise and control the processing by the entrusted party, thus protecting the security of the processed information. Due to the limited space of this report, appendices of ISO/IEC 27701 can be further consulted through the full translation of ISO/IEC 27701 in Appendix B hereof.

7.2 Sharing and transfer

Both GB/T 35273 (2020) and ISO/IEC 27701 have provisions on the sharing and transfer of personal information, and require personal information security impact assessment/privacy impact assessments[36] during sharing and transfer, with a record thereof. The difference is that GB/T 35273 (2020) distinguishes in detail the sharing and transfer due to acquisition, merger, reorganization, and bankruptcy from those not due to acquisition, merger, reorganization, or bankruptcy. While ISO/IEC 27701, more about providing guidance, focuses on the general direction of data processing, instead of carrying out in-depth study of acquisition, merger, reorganization, and bankruptcy. Specifically, we can learn from the guiding significance of ISO/IEC 27701, and implement the compliance work in accordance with GB/T 35273 (2020).

In case of acquisition, merger, reorganization, bankruptcy or other changes, GB/T 35273 (2020) requires the personal information controller to inform the information subject of the case; the changed personal information controller shall continue to perform the responsibilities and obligations of the original personal information controller, and the explicit consent of the information subject shall be obtained again if the purpose of personal information use is changed; and where there is no subcontractor after bankruptcy, the data shall be deleted.

For the information sharing and transfer not caused by acquisition, merger, reorganization, bankruptcy or other changes, the personal information controller is required to:

1) Conduct personal information security impact assessment in advance, and take effective measures to protect the personal information subject according to the assessment results;

[36]As the transfer itself is a case of changing the processing subject of PII, the privacy impact assessment shall be conducted according to the requirements. Although ISO/IEC 27701 does not explicitly state that, it guides the controller to evaluate according to the transfer nature.

2) Inform the personal information subject of the purpose of sharing and transferring personal information, the type of data recipient, and obtain the authorization and consent of the personal information subject in advance (except for sharing and transferring the personal information de-identified, and ensuring that the data recipient cannot re-identify or associate the personal information subject);

3) Prior to sharing and transferring sensitive personal information, inform the personal information subject of the type of sensitive personal information involved, the identity and the data security capability of the data recipient besides the contents disclosed in 2), and obtain the explicit consent of the personal information subject in advance;

4) Defining the responsibilities and obligations of the data recipient by contracts or other means;

5) Accurately record and store the sharing and transfer of personal information, including the date, size, purpose of sharing and transfer, as well as the basic information of the data recipient;

6) Upon finding that the data recipient violates the laws and regulations or agreement reached by both parties in processing personal information, the personal information controller shall immediately require the data recipient to cease the relevant activity and take or require the data recipient to take effective remedial measures (such as changing passwords, revoking privileges, disconnecting network) to control or eliminate the security risks to personal information; if necessary, the personal information controller shall terminate the business relationship with the data recipient and require the data recipient to delete the personal information obtained from the personal information controller in time;

7) In case of damage to the legitimate rights and interests of the personal information subject due to the security incident as a result of sharing and transferring personal information, the personal information controller shall bear the corresponding responsibility;

8) Help the personal information subject learn about the storage and use of personal information by the data recipient, as well as the rights of the personal information

subject, such as the rights to access, rectification, deletion and de-registration of the account, etc.;

9) Personal biometric information shall not be shared or transferred in principle. If sharing or transferring is really required for business needs, the personal information subject shall be separately informed of the purpose, the type of personal biometric information involved, the specific identity and data security capability of the data recipient, and obtain the explicit consent of the personal information subject.

ISO/IEC 27701 provides more detailed guidance on what to record, and requires the organization to make a record when transmitting PII to or receiving PII from third parties, **to ensure that cooperation with third parties can support the requests raised by the PII principal in the future.** The specific requirements of records include:

The PII controller shall record the following two types of transfers: (1) PII transferred from third parties shall be recorded when PII has been modified as a result of PII controllers' managing their obligations; or (2) the transfers to third parties to implement legitimate requests from PII principles, including the requests to erase PII (for example, after the withdrawal of consent by the personal information subject, the controller requests the third party to delete the personal information and the third party transfers the information to the controller).

The organization shall have a policy on the duration of such records. The organization shall only record the strictly needed information of such transfers in compliance with the minimization principle. The organization shall also develop and implement policies, procedures, and/or mechanisms to inform third parties when the shared PII has any changes, consent is withdrawal or handling rejection to the shared PII.

7.3 Public disclosure

Both GB/T 35273 (2020) and ISO/IEC 27701 have provisions on public disclosure of PI/PII. "GB/T 35273" (2020) states that personal information shall not be publicly disclosed in principle, while making corresponding procedural restrictions on public disclosure, it also prohibits the public disclosure of specific information. However, ISO/IEC 27701 only emphasizes that the PII controller has the obligation of recording.

Similar to the above section on sharing and transfer, there are great differences in the guideline logic between the two standards, specifically:

GB/T 35273 (2020) **strictly prohibits public disclosure of personal biometric information, the analysis results of race, nationality, political opinions and religious beliefs and other personal sensitive data of Chinese citizens.** Public disclosure of other information is prohibited in principle according to GB/T 35273 (2020). **If it is authorized by law or there is a reasonable reason for public disclosure, the information controller shall pay full attention to the risks and meet the following requirements:**

1) Conduct personal information security impact assessment in advance, and take effective measures to protect the personal information subject according to the assessment results;

2) Inform the personal information subject of the purpose and type of public disclosure of personal information, and obtain the explicit consent of the personal information subject in advance;

3) Prior to public disclosure of sensitive personal information, inform the personal information subject of the contents of sensitive personal information involved, besides the contents disclosed in 2);

4) Accurately record and store the public disclosure of personal information, including the date, size, purpose and scope of the public disclosure;

5) Assume the corresponding responsibility for any damage to the legitimate rights and interests of the personal information subject caused by the public disclosure of personal information.

For the public disclosure of PII, ISO/IEC 27701 **still only emphasizes the organization's obligation of recording**, that is, the organization needs to record the disclosure of PII to third parties, including the disclosed PII and the type thereof, as well as object and time of disclosure. According to ISO/IEC 27701, the organization is allowed to disclose PII during normal operations, provided that the disclosure is recorded. Any additional disclosure to third parties, such as disclosure for legitimate investigations or external audits, shall be recorded, including the source of the disclosure and the source of the right to disclose.

7.4 Third party access management

For the third party access management, GB/T 35273 (2020) states that when the personal information controller includes a third-party product or service with the function of collecting personal information in its product or service, and the two are not in an entrusted processing relationship or not joint-controllers of personal information, the personal information controller shall:

1) Establish the third party product or service access management mechanism and work-flow, and if necessary, establish a security evaluation and other mechanisms to set access conditions;

2) Define the security responsibilities for both parties and the personal information security measures that shall be implemented in cooperation with the third party product or service provider by contracts or other means;

3) Mark the product or service that provided by a third party for the personal information subject;

4) Properly keep the contracts and management records regarding the third party access to the platform and ensure that they are available for reference by relevant parties;

5) Require the third party to obtain the authorization and consent to collect personal information from the personal information subject in accordance with the requirements of GB/T 35273 (2020), and if necessary, verify the means of realization thereof;

6) Require the third party product or service to establish a mechanism to respond to personal information subject requests and complaints, so that the personal information subject to query and use;

7) Supervise the third party product or service provider to strengthen personal information security management; if the third party product or service is found not to fulfill the security management requirements or responsibilities, promptly urge to make corrections or discontinue access if necessary;

8) If the product or service is embedded with or connected to the third party

automated tools (such as code, script, interface, algorithm model, SDK, applet), the following measures should be taken:

a) Carry out technical testing to ensure that the collection and use of personal information meet the agreed requirements;

b) Audit the act of automation tools that are embedded or accessed by third party to collect personal information, and cut off the connection in time if it exceeds the agreed act.

Unlike GB/T 35273 (2020) that excludes situations involving entrusted processing and personal information joint-controllers from the normative situation of third-party access management ISO/IEC 27701 is more encompassing in focusing on the organizations supply chain and more general in terms of the organization's duty to manage, supervise and review the relationship with suppliers.

ISO/IEC 27701 first starts from the relationship between suppliers and proposes to manage supplier service delivery while ensuring information security in supplier relationship. Specifically, in terms of information security, the organization shall develop the information security strategy for supplier relationship, emphasize security in supplier agreement, and ensure the security of information and communication technology supply chain; in terms of supplier service delivery management, the organization shall supervise and review the supplier's services, and follow up the management when it comes to the changes of supplier's services.

In addition, ISO/IEC 27701 also gives opinions when the organization signs a contract with the PII processor: the organization shall sign written contracts with all PII processors it cooperates with, and ensure that appropriate control and security measures are covered in the contracts signed with the PII processors, including consideration of information security risk assessment and scope of PII processing by personal information processors.

7.5 Cross-border transfer

GB/T 35273 (2020) does not clearly state the requirements for cross-border transfer of personal information, but instead quotes other laws and regulations, while ISO/IEC 27701 gives corresponding provisions in detail, thus providing more specific recommendations for the organization on how to implement cross-border transfer requirements.

According to GB/T 35273 (2020), where the personal information collected and generated during operations within the China's territory is transferred overseas, the personal information controller shall comply with the requirements of the measures and relevant standards developed by the Cyberspace Administration of China in cooperation with the involved departments of the State Council[37].

If there is cross-border information transfer due to business needs, or governmental and judicial regulatory requirements, it is necessary to describe in detail the types of data to be transferred across borders, as well as the standards, protocols and legal mechanisms (contracts and so on) to be observed for cross-border transmission.

ISO/IEC 27701 requires in detail the organization to identify and document the basis for cross-border transfer of PII. PII transfer needs to meet the requirements of applicable laws and regulations. Specifically, depending on the jurisdiction or international organization in which the data recipient is located (and where the data is exported). The organization shall document and demonstrate that it meets the basis and requirements of transfer.

ISO/IEC 27701 also states that information transfer protocols/contracts need to be reviewed by designated regulatory agencies in some jurisdictions. Organizations in these jurisdictions shall ensure that they are aware of these regulatory requirements. In addition, the organization shall designate and document the destination countries and/or international organizations where the PII may be transferred. Users shall be provided with the names of countries and/or international organizations that might receive PII in the normal operation of business. In the case of transfer resulting from PII processing by subcontractors, the name of the corresponding country/or region shall also be included.

8. Rights of the PI subject/PII principal

Both GB/T 35273 (2020) and ISO/IEC 27701 have provisions on the PI subject/PII Principal's right to access, rectification, deletion, de-registration, obtain a copy of PI/PII and timely response to the PI subject/PII principal's request, but ISO/IEC 27701 has higher and more detailed requirements for the right to access, rectification, de-registration,

[37]On June 13, 2019, the Cyberspace Administration of China issued the Measures for Security Assessment for Cross-border Transfer of Personal Information (Exposure Draft), providing specific provisions on the requirements of application assessment for cross-border transfer of personal information, application materials, key assessment points, cross-border transfer records of personal information, cross-border transfer contract contents and rights and obligations requirements, as well as content requirements of security risk and security measures analysis report.

obtain a copy of the PIIs and timely response to the information subject's request; while GB/T 35273 (2020) has higher requirements for the right of deletion.

GB/T 35273 (2020)[38]	ISO/IEC 27701
Right to Access (Article 8.1)	There are requirements, but the granularity is coarser (Articles 7.3.3, 7.3.6)
Right to Rectification (Article 8.2)	There are requirements, but the granularity is finer (Article 7.3.6)
Right to deletion (Article 8.3)	There are requirements, but the granularity is coarser (Article 7.3.6)
Right to De-registration (Article 8.5)	There are similar requirements (Article 6.6.2.1)
Right to Obtain a copy of PI (Article 8.6)	There are requirements, but the granularity is finer (Article 7.3.8)
Response to requests from PI subjects (Article 8.7)	There are requirements, but the granularity is finer (Articles 7.3.4, 7.3.5 and 7.3.9)
Complaint management (Article 8.8)	There are similar requirements, but the granularity is coarser Sub-Clause 7.3.9

8.1 Right to access

For the right to access, both GB/T 35273 (2020) and ISO/IEC 27701 have provisions, but those set out in the latter are more nuanced. Specifically:

GB/T 35273 (2020) requires that personal information controllers shall stipulate the right to access personal information and implementation mechanism in the personal information protection policy, and shall provide PI subjects with methods to access

[38]The right of the personal information subject to withdraw the authorization and consent in Article 8.4 has been discussed in 4.5(4) above, and no more discussion is given here to avoid redundancy.

specific personal information, including:

1) The personal information or the personal information types held about the subject;

2) Sources and purposes of the above personal information;

3) The identity or type of the third party that has obtained the above personal information.

When the personal information subject makes a request to access the personal information that is not provided voluntarily by him/her, the controller of personal information may decide whether to respond or not after considering the possible risk and damage of not responding to the request to the legitimate rights and interests of the personal information subject, as well as technical feasibility and the cost of realizing the request, before giving an explanation.

But ISO/IEC 27701, as an international standard, only requires the organization to provide PII principals with a way to query their personal information. The specific information that PII principals can access is subject to the data protection laws and regulations of different countries. Therefore, it allows for variation with local laws and regulations.

8.2 Right to rectification

For the right of correction, both GB/T 35273 (2020) and ISO/IEC 27701 have provisions, but those set out in the latter are more nuanced. Specifically:

According to GB/T 35273 (2020), where the personal information subject finds that his/her personal information held by the personal information controller is incorrect or incomplete, the personal information controller shall provide the method for the personal information subject to request correction or supplement of the personal information.

ISO/IEC 27701 not only requires the organization to implement policies, procedures and / or mechanisms to fulfill the obligations to PII principals, so that PII principals can access, correct and delete PII without undue delay after making requests, but also has requirements for the organization to respond to the request of the PII principals (see section 8.6 below). When PII principals have disputes about the data accuracy or correction requirements, the organization shall implement policies, procedures and/or

mechanisms to resolve the issue. These policies, procedures and/or mechanisms shall include the modification made by the PII principal, and reasons for failure to make modifications (in the event of failure to make corrections).

Besides, ISO/IEC 27701 takes into account that some jurisdictions have special restrictions on the circumstances and extent to which PII principals have the right to correct or delete PII, and that the organization shall identify, update and comply with the restrictions that may be applicable. Therefore, when applied as an international standard, ISO/IEC 27701 needs to take into account more points in a more comprehensive manner than domestic standards which only need to comply with application requirements in China.

8.3 Right to deletion

For the right to deletion, both GB/T 35273 (2020) and ISO/IEC 27701 have provisions, but the former has higher requirements, specifically:

GB/T 35273 (2020) stipulates the conditions for the PI subject to exercise the right of deletion, including:

1) The personal information controller collects and uses personal information in violation of laws, regulations and the agreement with the information subject.

2) Where the personal information controller shares or transfers the personal information to a third party in violation of laws and regulations or the agreement with the personal information subject, and the personal information subject requests deletion (in this case, the personal information controller shall immediately stop the sharing and transfer, and notify the third party to delete in time);

3) Where the personal information controller discloses the personal information publicly in violation of laws and regulations or the agreement with the personal information subject, and the personal information subject requests deletion (in this case, the personal information controller shall immediately stop the disclosure and notify the receiving party to delete the information in time).

ISO/IEC 27701 makes basically the same provisions on the right to deletion and the right to rectification. In comparison, GB/T 35273 (2020) makes detailed provisions on the right

to deletion, possibly because the deletion of personal data may be regarded in some jurisdictions as an act of destroying evidence and thus connect directly with different national laws. As an international standard, it is difficult for ISO/IEC 27701 to establish requirements in detail.

8.4 Right to de-registration

For the right of de-registration, both GB/T 35273 (2020) and ISO/IEC 27701 have provisions, but the former is more detailed vertically, and latter is more extensive horizontally, specifically:

According to GB/T 35273 (2020):

a) The personal information controller providing the service through the registered account shall provide the account de-registration method to the personal information subject, which shall be simple and easy to operate;

b) After accepting the request for account de-registration, verification and handling shall be completed within the time limit promised (not more than 15 business days) in case manual intervention is required;

c) If identity check is required for de-registration, the type of personal information required to be provided by the personal information subject shall not be more than that collected for registration, use and other procedures;

d) There shall be no unreasonable conditions or additional requirements to increase the obligations of the personal information subject during the de-registration. For example, when de-registration of a single account means de-registrating more than one product or service, ask the personal information subject to fill in the accurate historical operation records;

e) Where account cancellation requires the collection of sensitive personal information to verify the identity, the handling measures for the sensitive personal information collected shall be defined, such as immediate deletion or anonymization after the purpose is achieved;

f) After the personal information subject cancels his/her account, the personal information shall be deleted or anonymized in a timely manner. Where personal

information is required to be retained by law, it shall not be used again in routine business.

While ISO/IEC 27701 further stipulates horizontally that the organization shall not reissue to users any deactivated or expired user IDs for systems or services that process PII. In the event of corruption or disclosure of passwords or other user registration data (e.g, unintentional disclosure), access control damage in the management or operation of user registration and/or de-registration procedures or when the PII processing services are provided, the organization shall address the damage to the access control of these users.

8.5 Right to obtain a copy of PI/PII

For the right to obtain a copy of PI/PII, both GB/T 35273 (2020) and ISO/IEC 27701 have provisions, but the latter has higher requirements, specifically:

According to GB/T 35273 (2020), at the request of the personal information subject, the personal information controller shall provide the personal information subject with the method to obtain the copy of the following types of personal information, or to directly transmit the copy of the following types of personal information to the third party designated by the personal information subject when technically feasible: 1) basic information and identity information of the subject; 2) health information, education and work information of the subject. Therefore, there are clear and detailed type restrictions on the acquisition and transmission of copies of personal information in the context of GB/T 35273 (2020).

According to ISO/IEC 27701, PII principals also have the right to obtain copies of personal information. The obtained copies of PII shall be used in a structured, common, and easily available manner. "ISO/IEC 27701" also refers to that according to some jurisdictions, the organization shall provide PII principals or controllers receiving PII with a copy of the PII being processed a portable form (usually a structured, commonly used and machine-readable form) under certain circumstances. In other words, the organization shall transfer a copy of the PII held directly to another receiving organization at the request of the PII principal, if technically feasible. This requirement is the same as the provision of “right to data portability” specified by GDPR.

ISO/IEC 27701 also requires that if the requested PII has been deleted according to the

retention and disposal policy[39], the PII controller shall inform the PII principal that the requested PII has been deleted.

8.6 Timely response to the request of PI subjects/PII principals

For timely response to the request of PI subjects/PII principals, both GB/T 35273 (2020) and ISO/IEC 27701 specifies the response time, response to the request and response cost, but the former gives more detailed and practical requirements.

(1) Response time

For the response time, GB/T 35273 (2020) requires that, after verifying the identity of the personal information subject, the personal information controller shall give a timely response to the request of the personal information subject, provide replies and reasonable explanations, and inform the personal information subject of the way to propose dispute resolution to external organizations. GB/T 35273 (2020) requires that the corresponding time limit shall be within 30 days or the period specified by laws and regulations[40].

ISO/IEC 27701 does not require a specific response time, except that the response time shall be reflected in the privacy policy and comply with applicable laws and/or regulations[41]. It once again reflects that as an international standard, it has to take into account different laws and regulations of the applicable countries/regions.

(2) Respond to requests

For responding to requests, requests raised by the personal information subject include access, rectification, deletion, withdrawal of consent, de-registration of account, and obtaining a copy of personal information according to GB/T 35273 (2020).

The lawful requests specified in ISO/IEC 27701 include access to copies of PII or complaint request, which is the same as GB/T 35273 (2020). However, ISO/IEC 27701 further requires the organization to **specify and record the policies and procedures** for handling and responding to the lawful requests of PII principals, once again showing its consistent advocacy for keeping of "records".

---

[39] See Article 7.4.7 of ISO/IEC 27701. For the translation of specific articles, please refer to Annex B hereof.
[40] According to Self-assessment Guide for Illegal Collection and Use of Personal Information by Apps, the app operator in principle, shall reply to the user's complaint handling opinions or results within 15 days.
[41] Some jurisdictions may determine the response time based on the complexity and number of requests and whether the PII principal shall be informed of the delayed information.

(3) Response costs

For the costs incurred in response to the request, GB/T 35273 (2020) requires no charge for reasonable requests in principle. However, for repetitive requests within a certain period of time, a certain cost can be charged as the case may be. ISO/IEC 27701 has no provisions on charges for response to a request, instead, it only refers to that some jurisdictions allow the organization to collect charges under certain circumstances (e.g., excessive or repeated requests). In this regard, the standard ISO/IEC 27701 offers different applicable countries/regions a certain degree of flexibility for excessive behavior.

8.7 Complaint management

GB/T 35273 (2020) has a separate provision on the complaint situation, requiring that the personal information controller shall establish a complaint management mechanism and a complaint tracking process, and respond to complaints within a reasonable time.

However, there is only a broader provision to establish a strategy and procedure for handling the request in ISO/IEC 27701, which describes the handling of complaints as one of its aspects. Same as processing other requests, ISO/IEC 27701 states that the organization shall define and document policies and procedures, and may collect charges in certain circumstances (e.g., excessive or repeated requests) to the extent permitted by the jurisdiction, and that the request shall be handled within the response time limit defined in the appropriate privacy policy.

9. Handling of personal information security incidents

For information security incidents, GB/T 35273 (2020) and ISO/IEC 27701 both stipulate two obligations: one is to report to the regulatory agency; the other is to notify PI subjects/PII principals. In comparison, ISO/IEC 27701 gives more detailed requirements, which distinguishes the different obligations of PII controllers and PII processors under this scenario, and sets additional requirements for record keeping, specifically:

GB/T 35273 (2020)	ISO/IEC 27701
Emergency handling and reporting of PI security incidents (Article 10.1)	There are requirements, but the granularity is finer (Article 6.13)
Notification of PI security incidents (Article 10.2)	There are requirements, but the granularity is finer (Article 6.13.1.5)

9.1 Reporting to the regulatory agency

In case of an information security incident, GB/T 35273 (2020) requires reporting in time according to the National Emergency Response Plan for Cyber Security Incidents and other regulations. The report should cover but not limited to: the category , quantity, content, nature and other general information about the personal information subject, the possible impact of the incident, the measures taken or to be taken, and the contact information of the personnel handling the incident.

ISO/IEC 27701 requires that for PII controllers and PII processors, **the organization shall keep records with sufficient information to provide a report for the regulatory and/or forensic purposes** in case of PII disclosure, including incident description, time period, consequence, name of the reporter, to whom the incident was reported, measures taken (including responsible person and recovered data), and the fact that PII is unavailable, lost, publicly disclosed or altered due to the incident. In case of PII disclosure, the record shall also include a description of the PII compromised(if known); if notification is made, the measures taken to inform the customer or regulatory authorities shall be recorded.

In case of any disclosure, some jurisdictions require the PII processor to notify the PII controller without delay (i.e., as soon as possible), preferably as soon as possible upon the disclosure, so that the PII controller can take appropriate measures. While some other jurisdictions require the organization to notify the regulatory authorities (e.g., PII protection authorities) of disclosure involving PII.

9.2 Notifying PI subjects/PII principals

In the event that an information security incident may lead to serious harm to the legitimate rights and interests of the personal information subject, such as the disclosure of sensitive personal information, GB/T 35273 (2020) requires that the affected personal information subject shall be informed of the incident in a timely manner by e-mail, letter, telephone, or notification. When it is impossible to inform the personal information subjects one by one, a reasonable and effective way shall be adopted to release public warnings. The notice shall include but not be limited to:

1) Contents and the impact of the security incident;

2) Measures taken or to be taken;

3) Suggestions for the personal information subject to prevent and reduce risks independently;

4) Remedial measures provided for the personal information subject;

5) Contact information of the person and the organization in charge of personal information protection.

ISO/IEC 27701 distinguishes different obligations of PII controllers and PII processors. For PII controllers, the procedures shall include notices and records in case of an incident of disclosure. Some jurisdictions have requirements on when to notify the security incident to regulators and when to notify it to the PII subject. While notifying the PII subject, the contents of the notice shall include:

1) Contact information for obtaining more information;

2) Description of the disclosure and its possible consequences;

3) Description of the disclosure, including the number of individuals affected and the quantity of records concerned;

4) Measures taken or planned to be taken.

For PII processors, **the clauses concerning disclosure notification shall constitute a part of the contract between the PII processor and the PII controller**, including how the PII processor provides the PII controller with the information necessary to fulfill its duty of notifying the regulatory authorities. In this case, the notification obligation does not apply to an incident caused by the clients of the PII processors or the PII principal or within the system components for which they are responsible. The contract shall also specify the limits for notification times of PII breaches.

10. Conclusions

ISO/IEC 27701 has no obvious difference in the construction of data protection architecture in comparison with GB/T 35273 (2020). Both have requirements on the application scope, personal information category, regulatory target, rights of PI subjects/PII principals, and the whole life cycle of personal information (including

collection, storage, use, entrusted processing, sharing and transfer, public disclosure). However, GB/T 35273 (2020), as a recommended national standard in China (mainland China), is more about how to implement the measures, so as to arouse Chinese organizations' awareness and persue personal information protection requirements. Therefore, GB/T 35273 (2020) is not second to ISO/IEC 27701 in the coverage of entire specifications and impact, and even more comprehensive, detailed and practical in some provisions on how to use personal information; while ISO/IEC 27701, as an international standard, focuses more on the compatibility and linkage with established influential protection laws at the international scale (such as GDPR). Therefore it focuses on constructing the framework, provide insights and leave room to countries for improving their privacy protection system on the basis of this framework. For the sections that need localization, ISO/IEC 27701 only gives general or soft requirements, leaving it to countries/regions for specification. However, it is worth noting that ISO/IEC 27701 still provides some guidelines for areas where there are no provisions in the current GB/T 35273 (2020), such as the requirements for assessment and acceptance criteria for personal information security impact assessment, further requirement of privacy risk assessment in addition to security risk assessment. It may provide new ideas and directions for future updates to GB/T 35273 (2020) or the promulgation of the Personal Information Protection Law.

As repeatedly reminded in ISO/IEC 27701, for data compliance in specific countries, one should follow local laws and regulations and business practices, such as the age threshold for minors. Therefore, organizations shall, when carrying out data compliance practice in China, follow and watch the development of China's personal information protection laws and regulations and national standards; and for requirements that are ambiguous or incomplete, organizations can refer to the operation guidelines in the international standard ISO/IEC 27701, so as to better carry out data compliance in the jurisdiction and build a more complete privacy and information security protection system.

III. Comparative analysis of internal management system of the organization/PIMS system

1. Comparative analysis of ISO/IEC 27701 and GB/T 35273 (2020)

1.1 Point-to-point comparative analysis of provisions in ISO/IEC 27701 and GB/T 35273 (2020)

1.1.1 Identify responsible departments and personnel

GB/T 35273 (2020) and ISO/IEC 27701 both stipulate the setting of the person in charge of personal information protection, and have overlaps in the responsibility requirements for the person in charge of personal information protection. GB/T 35273 (2020) stipulates the organizational structure of personal information security, which mainly includes the following four aspects: 1) defining that the legal representative or responsible person shall take overall leadership responsibility for personal information security, including providing personnel, financial and material resources for the work of personal information security; 2) appointing the person in charge of personal information protection and personal information protection agency; 3) when meeting certain conditions, setting up the full-time person in charge of personal information protection and personal information protection agencys; 4) identifying the responsibility for the person in charge of personal information protection and personal information protection agency. In addition, GB/T 35273 (2020) also requires that necessary resources be provided for the person in charge of personal information protection and personal information protection agency to ensure their independent performance of their duties.

Similarly, ISO/IEC 27701 requires the appointment of one or more persons responsible for developing, implementing, maintaining and overseeing the organization's data governance and for implementing privacy compliance programs to ensure that the organization is in compliance with all applicable laws and regulations relating to PII processing. ISO/IEC 27701 also requires the organization to designate a contact for use by the PII principals regarding the processing of PII. When the organization is the PII controller, it shall designate a contact for the PII principals specifically regarding the processing of PII. With regard to responsibilities, ISO/IEC 27701 is basically the same as GB/T 35273 (2020) in terms of responsibilities 1, 2, 5, 6 and 10 provided in 11.1 d),

although different expressions are used. ISO/IEC 27701 also specifically requires the responsible person to report independently and directly to the appropriate management of the organization to ensure that privacy risks are effectively managed; it also requires the responsible person to be an expert in data protection laws, regulations and practices. In addition, ISO/IEC 27701 also mentions that the data protection officer can be either an internal or external expert.

1.1.2 Personal information security engineering

GB/T 35273 (2020) and ISO/IEC 27701 both stipulate the establishment of personal information security engineering. GB/T 35273 (2020) requires that the personal information controller, when developing products and services with the function of processing personal information, shall consider the personal information protection requirements in the system engineering phase of demand, design, development, testing and publication in accordance with relevant national standards to ensure that the protection measures for personal information are planned, synchronized and used simultaneously during system construction. ISO/IEC 27701 puts forward higher requirements for establishment of the personal information security engineering in terms of implementation. The organization shall first control the collection of PII to the minimum necessary degree and the processing activities of PII to the sufficient necessary degree; secondly, the organization shall ensure that the PII recorded is accurate, complete and up-to-date, identify the data minimization objectives and specify the means and measures planned to achieve these objectives; the organization shall also de-identify and delete the temporary documents generated in the PII and processing activities at the end of the data processing activities in a timely manner; the organization shall document the processing policies, procedures and mechanisms and follow the relevant internal policies; in addition, in terms of PII transmission, the organization shall properly control and ensure that PII transmitted through the data transmission network reaches the specified destination.

1.1.3 Personal information processing activity record

GB/T 35273 (2020) and ISO/IEC 27701 both stipulate the requirements of recording personal information processing activities. For the recording behavior, GB/T 35273 (2020)

describes it is only the voluntary practice of the organization, whereas ISO/IEC 27701 makes mandatory requirements. Specifically:

GB/T 35273 (2020) stipulates that organizations may establish, maintain and update the records of the processing activity of personal information collected and used. The word "may" indicates that it is only a recommended but not mandatory obligation. The content of the record may include:

1) The type, quantity and source of the personal information involved (e.g. directly collected from the personal information subject or obtained through indirect access);

2) Distinguish the purpose of processing and use scenarios of personal information based on business functions and authorization, as well as the entrusted processing, sharing, transfer, public disclosure, whether or not involve cross-border transfer, etc.;

3) Information systems, organization or personnel related to all aspects of personal information processing activity.

ISO/IEC 27701 stipulates that the organization shall clarify and securely keep necessary records, including at least the processing type, purpose, description of PII and PII principal category (e.g. child), categories of PII receiving parties that have been or will be disclosed, including general notes on the third country receiving parties or international organizations, technical and organizational security measures, as well as privacy impact assessment reports. The PII processing record shall identify a person responsible for its accuracy and integrity.

1.1.4 Personal information security impact assessment

Both GB/T 35273 (2020) and ISO/IEC 27701 stipulate personal information security assessment. GB/T 35273 (2020) requires the personal information security impact assessment, while ISO/IEC 27701 distinguishes between the information security risk assessment process and the privacy risk assessment process.

GB/T 35273 (2020) requires the establishment of a personal information security impact assessment system to assess and deal with security risks in the personal information

processing activities. The assessment mainly focuses on whether the processing activities comply with the basic principles of personal information security, and whether the personal information activities affect the legitimate rights and interests of the personal information subject, including but not limited to:[42]

7) Whether the collection of personal information follows the principles of clear purpose, consent, minimum necessity, etc.;

8) Whether the personal information processing may adversely affect the legitimate rights and interests of the personal information subject, including whether it will endanger personal and property security, damage personal reputation and physical and mental health, and lead to discriminatory treatment;

9) Effectiveness of personal information security measures;

10) The risk of the personal information subject being re-identified by the anonymized or de-identified datasets or being re-identified by the datasets after aggregation with other datasets;

11) Possible adverse effects of sharing, transfer and public disclosure of the personal information on the legitimate rights and interests of the personal information subject;

12) Possible adverse effects of security incidents on the legitimate rights and interests of the personal information subject.

GB/T 35273 (2020) requires the personal information controller to conduct a personal information security impact assessment:

1) prior to the product or service release or after a major change in the functions;

2) in case of new legislative requirements come into effect, or when a major change occurs in the business models, information systems and operating environments, or when a significant personal information security incident occurs.

With regard to the personal information security impact assessment, GB/T 35273 (2020)

[42] For the specific provisions on typical assessment scenarios, assessment content and assessment procedures of personal information security impact assessment, please refer to the *Information security technology - Security Impact Assessment Guide of Personal Information (Exposure Draft)*.

requires the organizations to form personal information security imact assessment reports, take measures to protect the personal information subject and reduce risks to an acceptable level; it also requires that reports be properly kept to ensure that they are accessible to interested parties and made public in an appropriate form. This is consistent with the provision in ISO/IEC 27701 on documentation of the assessment process to be maintained.

ISO/IEC 27701 distinguishes between the information security risk assessment process and the privacy risk assessment process. The former is mainly used to identify risks associated with loss of confidentiality, integrity and availability; while the latter is used to identify risks associated with PII processing. Similarly, ISO/IEC 27701 also mentions that the organization shall properly manage the relationship between information security and PII protection throughout the risk assessment, both of which can be evaluated in combination or separately, but shall be limited to the PIMS.

ISO/IEC 27701 **specifies the entire assessment process**, which shall include:

1) Establish and maintain information security risk standards, including:

   a) Risk acceptance criteria; and

   b) Information security risk assessment standards;

2) Ensure that repeated information security risk assessments produce consistent, effective, and comparable results;

3) Identify information security risks:

   a) Apply the information security risk assessment process to identify risks related to information confidentiality, integrity and availability within the scope of the information security management system;

   b) Identify risk subjects;

4) Analyze information security risks:

   a) Assess the possible consequences of the realization of the risks set out in section 6.1.2 c) 1);

   b) Assess the actual likelihood of the occurrence of the risks set out in section

6.1.2 c) 1); and

c) Determine the risk level;

5) Assess information security risks:

a) Compare the risk analysis results with the risk criteria established in section 6.1.2 a); and

b) Prioritize risk analysis in risk management.

1.1.5 Data security capability

GB/T 35273 (2020) requires the organizations to establish appropriate data security capabilities and implement necessary management and technical measures in accordance with the requirements of relevant national standards to prevent the leakage, damage, loss and tampering of personal information. ISO/IEC 27701 puts forward more detailed regulations and implementation recommendations for business continuity management in terms of physical and environmental security, operational security, communication security and information security. Specific requirements are described in sections 2.8, 2.9, 2.10 and 2.14 below.

1.1.6 Personnel management and training

GB/T 35273 (2020) and ISO/IEC 27701 require the organization to conduct management and training for personnel involved in personal information. GB/T 35273 (2020) puts forward the following six specific implementation requirements:

7) The organization shall sign confidentiality agreements with relevant personnel processing personal information, and conduct background checks for the personnel with extensive access to sensitive personal information to understand their criminal records and integrity status, etc.;

8) The organization shall clarify the internal security responsibilities of different posts involving personal information processing, and establish the punishment mechanism for security incidents;

9) The organization shall require relevant personnel in personal information

processing positions to continue to perform the obligation of confidentiality when they are transferred from the position or terminate the employment contract;

10) The organization shall identify and monitor the personal information security requirements of outsourced-service personnel who may have access to personal information, and sign confidential agreements with them;

11) The organization shall establish corresponding internal systems and policies to provide guidelines and requirements for employees' personal information protection;

12) The organization shall carry out professional training and assessment on personal information security for relevant personnel processing personal information processing positions on a regular basis (at least once a year) or in case of a major change in the personal information protection policies to ensure that relevant personnel are familiar with personal information protection policies and procedures.

In terms of the human resources security management, ISO/IEC 27701, based on ISO/IEC 27002, specifically introduces the responsibilities that the organization shall undertake in different periods and the specific obligations that relevant personnel shall undertake before employment, during the performance of employment contract and at the end of the employment relationship. See section 2.4 below for details.

1.1.7 Security audit

As an important part of personal information security management, the security audit in the information activities is covered by detailed introduction and regulation in both GB/T 35273 (2020) and ISO/IEC 27701. GB/T 35273 (2020) puts forward the following six specific operational requirements to the organization from the perspective of business implementation:

7) The organization shall audit the effectiveness of the personal information protection policies, procedures and security measures;

8) The organization shall establish an automatic audit system to monitor and record the personal information processing activities;

9) The records made in the audit process shall be able to provide support the security incident handling, emergency response and subsequent investigation;

10) The organization shall prevent unauthorized access, tampering, or deletion of audit records;

11) The organization shall timely deal with the illegal use and abuse of personal information discovered during the audit;

12) The audit records and retention time shall comply with the requirements of laws and regulations.

The operating requirements of ISO/IEC 27701 are similar to those of GB/T 35273 (2020), except that the audit requirements are covered in specific areas (e.g. Security audit is required in the supplier relationship security management). ISO/IEC 27701 specifically lists the regulations of security audit as the field of "compliance" and makes detailed introduction and regulation (see section 2.15 below for details).

1.2 Additional provisions of ISO/IEC 27701 as compared to GB/T 35273 (2020 version)

As described above, GB/T 35273 (2020) puts forward the requirements for the internal organization management mainly in Article 11 “Organization's personal information security management requirements” and puts forward the obligations and responsibilities of the organization as the personal information controller in terms of clarifying the responsible departments and personnel, carrying out personal information security engineering, recording personal information processing activities, conducting personal information security impact assessment, establishing appropriate data security capabilities, managing and training relevant personnel and carrying out security audit when new national standards and regulations come into force.

The value of ISO/IEC 27701, as a standard that takes into account the requirements of regulations in different countries and regions, lies in that it not only points out the responsibilities that the organization must bear in implementing the personal information protection, but also puts forward suggestions and measures for different levels of business implementation. Compared with GB/T 35273 (2020), ISO/IEC 27701 divides the organization management into more detailed levels. While covering the above seven

aspects, it establishes a more complete PIMS system. The specific PIMS system is described as follows.

2. Establishment and management of PIMS system under ISO/IEC 27701

The PIMS system is further developed based on two international standards, ISO/IEC 27001 and ISO/IEC 27002. ISO/IEC 27001 is a set of specifications for establishing an information security management system (ISMS), which describes in detail the requirements for establishing, implementing, and maintaining the information security management system. ISO/IEC 27002 provides guidelines and common principles for initiating, implementing, maintaining and improving the information security management within the organization. The objectives outlined in ISO/IEC 27002 provide general guidance on the generally accepted objectives of the information security management, and the implementation rules contained in this standard can be considered a starting point for developing the specific guidelines of the organization. The PIMS of ISO/IEC 27701 extends the ISMS of ISO/IEC 27001 and provides detailed and practical rules and guidelines for the establishment, implementation, maintenance and development of the privacy protection system from different perspectives provided in ISO/IEC 27002.

2.1 Planning, implementation and review of organization

(1) Preliminary planning

First, PIMS introduces the necessary requirement for establishing an information security management environment suitable for the organization. This requirement involves understanding the current situation and background of the organization, clarifying the purpose of establishing the information security management system, understanding the needs and expectations of interested parties, and determining the scope of the information security management system. PIMS then puts forward specific requirements for the role of the top management in the information security management system and how to communicate the leadership expectations to the organization through a strategy statement. This typically involves leadership and commitment, information security policy and objectives, and the embodiment and application of roles, responsibilities and commitments in practical situations.

PIMS then introduces the actions to address risks and opportunities, as well as achievable information security objectives and implementation plans, and involves information security risk assessment, risk owners, information security risk disposal, applicability statement, and information security objectives. At the same time, PIMS also describes in detail the support needed to establish, implement, maintain and improve an effective information security management system, including: resource requirements, ability of participants, awareness, communication with stakeholders and documented information.

(2) Implementation

After establishing the information security system planning of the organization, PIMS mentions the non-negligible problems during implementation: how to carry out preliminary planning and control, manage information security, carry out information security risk assessment and deal with information security risks, etc.. The risk will affect the realization of organizational objectives, which may be related to various activities in the organization from strategic decision-making to operation, such as the implementation of specific projects, etc., manifested in leadership, strategy, operation, finance, environment, society, reputation and other aspects. However, opportunities and risks coexist. If risks can be controlled through effective management, the organization can also draw on advantages and avoid disadvantages. In terms of information security management, PIMS does not force an organization to put all of its assets into absolute security because the cost of "absolute security" is huge. Therefore, in the choice of risk control measures, the internal and external environmental factors of the organization as well as the needs and expectations of interested parties shall be considered. PIMS thus provides general strategic recommendations: risk reduction, risk transfer, risk avoidance, and risk acceptance.

(3) Review and improvement

PIMS summarizes the implementation of the measurement system, the compliance of the system with international standards and management expectations, and the requirements for seeking expected feedback from the management, involving monitoring, measurement, analysis and evaluation, internal audit, and management review. It also describes that the organization shall identify and improve nonconformities through corrective actions, and puts forward corrective measures and continual improvement

methods for nonconformities.

2.2 Information security management policy

The information security management policy under PIMS can ensure that the organization complies with relevant laws and regulations while providing management guidance and support. It emphasizes the definition, publication, and review of the different types of management policies required for information security management.

First of all, the information security management policy shall be defined by the organization and approved by the management, aiming to elaborate the methods for the organization to manage the information security objectives. The policy shall emphasize information security requirements under the business strategies, specific requirements for information security in laws, regulations and contracts, and requirements that the organization needs to meet in the context of current and anticipated information security threats. The information security management policy shall also contain the following declarations: the definition of information security, the guiding principle and objectives of all activities related to information security activities, the responsibility assignment of the roles in the information security management, the handling of deviations and exceptions, the declaration of compliance with the requirements of the applicable personal information legislation, and declaration of obligations under the contract between the organization and third parties. At the implementation level, it shall be supported by the policy of concrete topic to further ensure the implementation of information security control measures. This concrete subject is typically used to address the needs of the target group or to include a topic such as access control, data classification, physical and environmental security, data transfer, and malware protection. These strategies shall be communicated to employees and interested parties in a manner that is relevant, acceptable and understandable.

Second, the information security policy shall be reviewed at the time of significant changes or on a regular basis to ensure its continuing suitability, adequacy and effectiveness. Each policy shall have a certain person approved by the management, who shall be responsible for the development, review and evaluation of the policy. The review shall include assessment of the opportunities for the organizational policy improvement and the ways to manage information security in response to changes in the organizational

environment, business status, legal conditions, or technical environment; the management review results shall also be taken into account. The proposal or implementation of the revised policy shall be subject to the approval of the management.

2.3 Information security organization

In order to establish a management framework, launch and control the implementation and operation of the information security in the organization, the organization shall integrate the information security into project management, define and assign the information security roles and corresponding responsibilities, ensure possible division of conflicting responsibilities and authorities and reduce and prevent unauthorized or unintentional modification and misuse of capital; meanwhile, the organization shall maintain appropriate contacts with regulatory authorities, special interest groups and other professional security forums and industry associations.

In addition, to ensure safe use of mobile devices, the organization shall take appropriate security measures for different scenarios to ensure that the business information is not damaged. For example, when the mobile devices are used in public places or other unprotected areas, cryptographic techniques and the mandatory use of secret authentication information can be used to avoid unauthorized access to or disclosure of stored and processed information. In terms of remote work, the organization shall implement strategies and corresponding security measures to protect the information that is accessed, processed or stored at the remote workstation.

2.4 Human resource security

The organization shall ensure that the employees and contractors understand their responsibilities, meet the requirements of their roles, and perform their respective information security responsibilities. The organization shall take care to ensure its own interests when changing or terminating the employment relationship.

Prior to employment, the organization shall conduct a background investigation on the candidates based on relevant laws and regulations, ethics, specific business requirements, and the type of information involved and the corresponding risks. The labor contract signed with an employee and contractor shall specify the information security responsibilities of the employee or contractor and the organization. When the employee

or contractor performs the employment contract, the organization shall ensure that it complies with the organization's procedures and specifications while performing its information security duties under the policy. The organization shall provide appropriate education and training for all employees and contractors, including the implementation of the reporting of safety incidents and appropriate handling, and shall regularly inform them of changes in the organizational policies and procedures. The organization shall impose a formal disciplinary treatment on the employees who violate information security regulations. The organization shall specify the information security duties of the employee or contractor after the change or termination of employment, ensure the continuity of such duties, and inform the employee or contractor of the information security requirements and corresponding legal responsibilities that remain to be followed by the employee or contractor.

2.5 Asset management

First, the organization shall clarify the definition and scope of the organizational assets and establish appropriate protection responsibilities. These assets shall include information related assets and information processing facilities. The organization shall develop and maintain an inventory of its assets. When an asset is created or transferred to the organization, the organization shall allocate the holder of that asset. An individual or other entity approved to manage the life cycle of an asset may be assigned as the asset holder. The asset holder is responsible for the reasonable management of the asset throughout the asset life cycle. The organization shall establish rules for the fair use of the information and the said assets, prepare and implement appropriate documents.

Second, in order to ensure that the information is protected commensurate with its importance, the organization shall classify and mark the data including personal information, and formulate and implement procedures for disposal of assets according to the data classification system. In order to prevent information stored on the media from being disclosed, modified, deleted or destroyed, the organization shall, in accordance with the data classification system, formulate and implement management procedures for removable media, use formal procedures for handling media that are no longer needed, and protect media during transit from unauthorized access, abuse or damage.

2.6 Access control

The organization shall restrict access to information and information processing facilities, ensure the access rights of authorized users, prevent unauthorized access to systems and services, and implement the responsibility of users to protect their authentication information. During implementation operations, the organization can establish and implement the access control policies and review them based on the business and information security related requirements. The organization shall require the users to follow practices of secret authentication information and control access to the operating systems and applications through secure logins.

2.7 Cryptography

The use of cryptography can protect the confidentiality, authenticity and integrity of information. The organization needs to develop a password control policy to ensure appropriate and effective password use. In implementing policies, the organization shall take into account regulations and national/regional restrictions on the application of cryptography in different parts of the world, as well as cross-border transfer issues of encrypted information. Individual countries or regions may require the use of cryptographic techniques to protect specific types of personal information, such as health data, resident ID number, passport number and driver's license number. The organization shall provide consumers with information about the personal information protected and processed by the organization using cryptographic techniques and shall also inform consumers of the possibility of assisting consumers to apply for their own password protection. In addition, the organization shall also develop policies for the use, protection, and duration of secret keys throughout the key life cycle.

2.8 Physical and environmental security

To protect areas containing sensitive information, key information and information processing facilities, the organization shall first define the security boundary and develop and implement appropriate codes.

In terms of implementation, the organization shall use appropriate entrance control to ensure that only authorized personnel have access to security areas; design and implement physical security of offices, rooms and facilities; design and implement physical security

to protect against natural disasters, malicious attacks or accidents; design and implement procedures for office in security areas; control areas accessible to unauthorized personnel, such as logistics cross connecting area, and if applicable, such areas shall be isolated from information processing facilities.

In terms of equipment, to reduce the risk caused by environmental threats and disasters and the possibility of unauthorized access, the organization shall properly place and protect the equipment; protect the equipment from power outages or other failures in supporting facilities; protect the power supply, transmitted data or communication cables supporting the information services from being intercepted, interfered with or destroyed; properly maintain the equipment to ensure its continuous availability and integrity; the equipment, information or software may not be removed from the premises without authorization; the organization shall consider the different risks of working outside the office space and protect off-site assets and equipment; audit and certify all parts of the equipment including storage media to ensure that the sensitive data and licensed software have been removed or securely rewritten before disposal or reuse; the user also needs to ensure that the equipment is properly protected when not using it, while the organization shall also adopt the clean desk policy and the clear desk and clear screen policy.

In terms of personal information processing, the organization shall ensure that when the personal information storage space is reallocated, the personal information in the previous storage space is not visible. In order to be able to securely dispose of and reuse equipment, any storage equipment which is likely to cover personal information. shall be regarded as covering personal information.

2.9 Operation security

For the operational activities associated with information processing and communication facilities, the organization shall develop and document operating procedures and make them available to the users who need them; such as computer startup and shutdown procedures, backup, equipment maintenance, media processing, computer room and mail processing management and security activities. The organization shall control any organizational changes, business process changes, and changes in information processing facilities and systems that may affect information security. Therefore, the organization needs to establish formal management responsibilities and procedures. In case of any

change, the organization shall maintain an audit record that covers all relevant information. The organization shall monitor and adjust the use of resources and predict future capacity requirements to ensure that the system has the required skills. In addition, similar to the physical environment isolation mentioned in section 2.8 above, the organization also needs to separate the development, test, and operating environments to reduce unauthorized access to or change in the operating environment.

In terms of specific practice, in addition to protecting against malware, the organization shall backup and regularly test the information, software and system images. In particular, the organization needs to develop policies that address the requirements for backup, repair, and recovery of personal information and include further provisions on the elimination of personal information in backup information. To record events and generate evidence, the organization needs to create, keep and periodically review event logs that record the user activities, exceptions, errors, and information security incidents. Similarly, the activities of the system administrator and system operator shall also be recorded, and the log needs to be protected and reviewed regularly. Where feasible, it is recommended that the organization simultaneously record the access to personal information, including the access time, accessor, personal information subject accessed and any change occurred.

The organization needs to protect log facilities and log information from any possible tampering and unauthorized access to the logs, enforce operating system integrity, and establish and implement codes that standardize the installation of software by users. The organization shall timely obtain information on the technical vulnerability of the information system, assess the degree of exposure of the organization and take appropriate measures to address relevant risks. During the audit process, the organization shall carefully plan and approve the audit requirements and activities involving the operating system validation to minimize the interference with business activities.

2.10 Communication security

To protect the information in the network and its information processing facilities, the organization shall manage and control the network and specify the security mechanism, service level and management requirements of all network services in the network service agreement. In addition, the organization also needs to isolate information services, users and information systems within the network.

In terms of information transmission security, the organization needs to establish formal transmission policies, procedures and control means, sign information transmission agreements with external entities, ensure the security of commercial information transmission, and protect the information contained in electronic messages. The organization shall also pay attention to the confidentiality of the information and periodically review and archive the confidentiality requirements or non-disclosure agreement that reflect the organization's information protection requirements.

2.11 Acquisition, development and maintenance of information system

The information security assurance is a necessary part in the life cycle of information systems, including those providing services through public networks. First of all, the new information systems and enhancements to existing information systems shall meet the information security related requirements. Second, the organization shall protect the application service information provided through public networks from fraud, contract disputes, unauthorized modification or disclosure. The organization shall protect the security of the information involved in an application service transaction from incomplete transmission, routing errors, unauthorized message changes, unauthorized disclosure, or unauthorized replication or replay of the messages.

During the development and assistance, the organization shall design and implement the information security policies within the information system development lifecycle, formulate and apply the development rules for software and systems, and control the system changes in the development lifecycle through the use of formal change control procedures. In case of any change in the operating platform, the organization needs to review and test the business-critical applications to ensure that the change will not adversely affect the organization's operation or security. The organization shall consider carefully the software package changes, limit and strictly control the changes to the extent necessary. Meanwhile, the organization shall establish, document, and apply the security system engineering principles to the implementation and maintenance any information system. The organization shall establish and properly protect the security of the system development environment, conduct security function tests during development, and carefully screen, protect and control the test data. The organization shall also supervise and monitor the development activities of the outsourced system.

2.12 Supplier relationship

The organization shall protect the organizational assets that are accessible to the supplier, discuss with the suppliers the information security requirements in its activities, and document such requirements upon agreement. In addition, the agreements with suppliers shall include provisions regarding the information security risks in the information processing, ICT services and product supply chains.

Upon agreement, the organization shall periodically monitor, review and audit the supplier service delivery. In case of any change in the supplier service, the organization shall manage the supplier service changes, if any, including maintenance and improvement of the existing information security policies, procedures and other control measures, while considering such factors as the criticality of business information, the use of the system and the processes involved in risk assessment.

2.13 Information security incident management

The organization shall establish management responsibilities and procedures to respond to and deal with information security events in a rapid, effective and orderly manner. When an information security event occurs, relevant personnel shall report to the organization through appropriate management channels as soon as possible. The organization shall require employees or contractors using its information systems and services to be aware of and report any information security vulnerability identified or suspected in the systems or services.

If a security event is classified as a security incident, the organization shall evaluate and make decisions on it, and respond to it in accordance with the procedure document. When the security incident involves personal information, the organization shall review it and determine whether specific types of response and processing, including notification and recording, are required.

The organization shall learn from the analysis and resolution of the information security incidents to reduce the possibility or impact of future incidents. In addition, the organization shall develop and implement procedures for the identification, collection, acquisition and preservation of information that may become evidence.

2.14 Business continuity management in information security

The organization shall embed the information security continuity in the business continuity management system. The organization shall first establish its continuity requirements for information security and information security management in adverse circumstances (such as crisis or natural disaster). Secondly, the organization shall establish, record, implement and maintain corresponding procedures and control measures to ensure that the information security continuity requirement can reach the stipulated level in adverse circumstances. Finally, the organization shall periodically validate the information security continuity control means established and implemented to ensure that they remain effective in adverse circumstances. When using information processing facilities, the organization shall also ensure that they have sufficient redundancy to satisfy availability requirements.

2.15 Compliance

The organization and its information system shall document all relevant legal, regulatory and contractual requirements, as well as the means and measures taken to meet these requirements. This document shall be updated periodically. When it comes to intellectual property and the use of proprietary software products, the organization shall take appropriate procedures to ensure compliance with laws, regulations and contract requirements. The organization shall protect records from loss, damage, tampering, unauthorized access and unauthorized release as required by laws, regulations and contracts. The organization shall ensure the protection of privacy and personally identifiable information in accordance with relevant laws and regulations, if applicable, and shall also use the password control measures according to relevant laws, regulations and contract requirements.

To ensure that the implementation of information security conforms to the organizational policies and procedures, the organization shall conduct information security reviews. At the planned intervals or in case of major changes, the organization shall review the information security management means and their implementation, that is, the control objectives, control means, policies, processes and procedures of information security. The organization shall also periodically review the compliance of its information systems with its information security policies and standards. The manager shall periodically review the

compliance of the information processing and related procedures within his/her responsibility range with the corresponding policies, standards and other security requirements.

3. Advantages and reference significance of 27701

3.1 Challenges posed by independent national data privacy protection regulations

Today, legislators and law executors around the world are increasingly aware of the importance of managing data use and processing and, especially when it comes to personal verification information, it is particularly urgent to provide legal means to regulate data processing and protect personal privacy. Except for the General Data Protection Regulation ("GDPR") of the EU, various countries, including the United States, Switzerland, Australia and New Zealand, have successively introduced their own new policies on data specifications. The emerging laws and regulations that regulate data in various countries have gradually brought challenges to various business entities, especially multinational organizations. The emergence of the PIMS of the international standard ISO/IEC 27701 will help these organizations decide, plan, implement and maintain a data privacy protection channel that not only meets the requirements of different scopes of law around the world, but also complies with the requirements of GDPR.

GDPR encourages the data protection authentication mechanism and the establishment of data protection certification marks to help ensure that the controllers and processors comply with legal norms during data processing. (Article 42 of GDPR) In addition, the use of these authentications or seals means that the organization processes the personal information in a correct manner meeting the GDPR requirements.

Ongoing authentication mechanisms can bring the element of "accountability" to the implementation of data protection, accelerate risk reduction, and facilitate the flow of personal information, which can make the procedures more transparent and gain customer trust in the data protection while the organization provides services.

3.2 Reference significance of ISO/IEC 27701

ISO/IEC 27701 is not intended to allow the organization to control everything. In contrast, ISO/IEC 27701 requires the organization to be aware that processing the personal verification information is different from processing other information, and that the organization needs to adjust its specific control and implementation control measures

accordingly.

Whether the organization shall implement ISO/IEC 27701 depends on circumstances. However, if the organization is concerned about the information protection issues (such as ransomware, denial of service attack, social engineering and other network risks) and wants a compliance guideline compliance with GDPR, ISO/IEC 27701 is undoubtedly a very useful tool that not only covers multiple perspectives, but also provides security controls to help protect personal data and information. By implementing ISO/IEC 27701, organizations can:

- Meet the requirements of ISO/IEC 27701 and meet the basic compliance requirements of GDPR;
- Make risk management from the perspective of information security and privacy protection, and implement specific control means;
- Have guidelines for specific controls to protect business information and personal data;
- Prove to third parties that your organization or enterprise complies with GDPR and other international standards related to information security by certifying ISO/IEC 27701;[43]
- If you are a handler under GDPR, you may provide your client with the proof of compliance with GDPR;[44]
- If you are a controller under GDPR, you may provide the data subject with the proof of compliance with GDPR.[45]

4. Conclusions

ISO/IEC 27701, while establishing an evidence-based privacy protection program, proposes to the organization a set of measures regarding the responsibilities it must assume in its personal information processing activities and the advices it must propose.

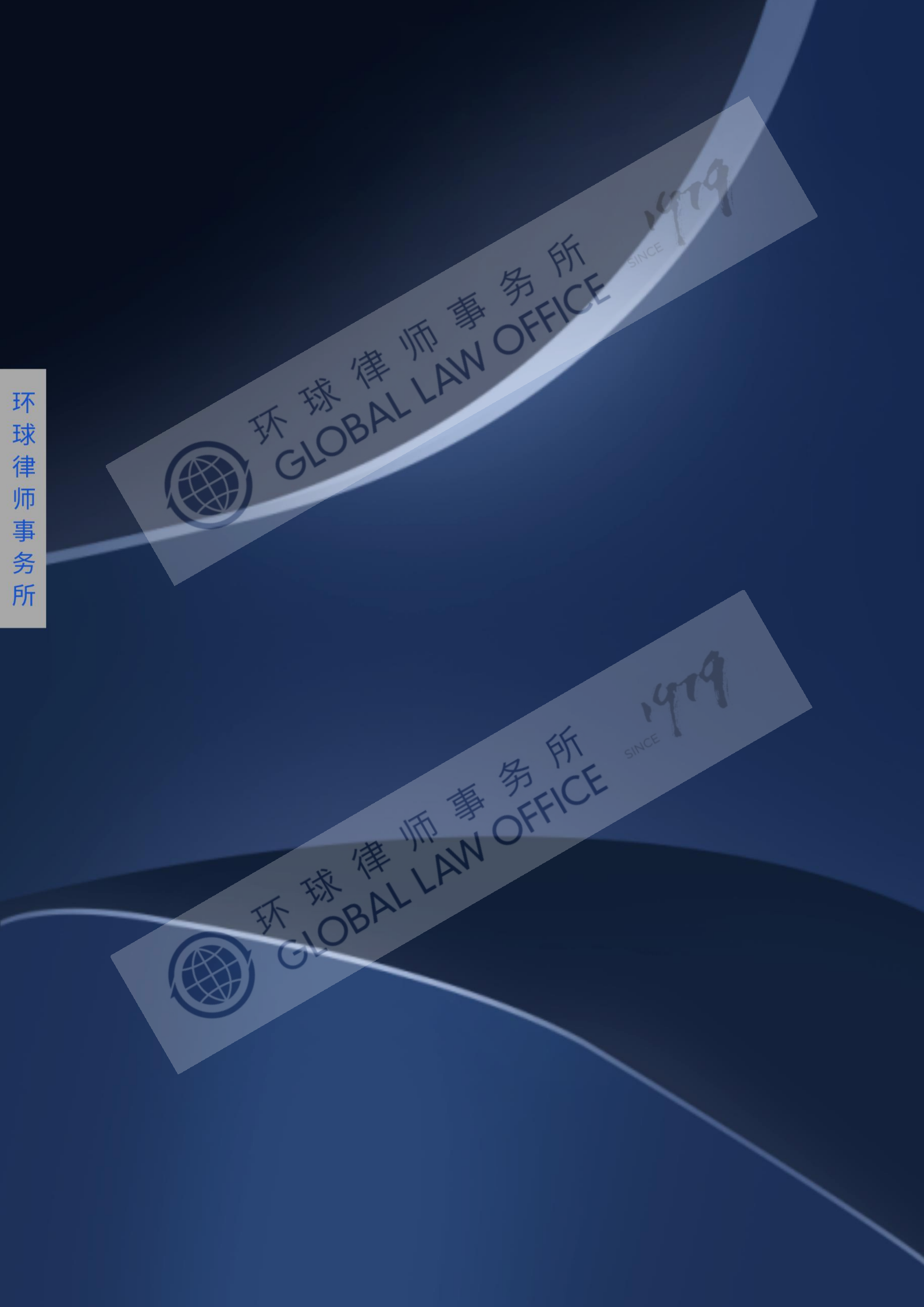
[43] It shall be noted that the official GDPR certification has not been approved by the EU. However, considering that PIMS and GDPR clearly echo each other, PIMS certification, although not a formal GDPR certification, can also be regarded as a proof of GDPR compliance before a decision is made by EU regulators.
[44] As above.
[45] As above.

ISO/IEC 27701 recognizes the duplication of legal norms regarding privacy in different countries and thus reduces the complexity of law application. However, when ISO/IEC 27701 is implemented in specific countries and/or regions, it is still necessary to refer to local laws. In particular, considering the existing legal system and environment with Chinese characteristics in Mainland China, GB/T 35273 (2020) shall be referenced to when organizations implement personal imformation protection schedule in Mainland China. In terms of the overall environment, GB/T 35273 (2020) has consistent main idea with ISO/IEC 27701 that is, the organization that attaches great importance to participation in personal information activities shall comply with relevant laws and regulations in its internal management and shall perform the implementation responsibilities. In terms of specific implementation measures, the organization can use ISO/IEC 27701 to build an overall compliance framework to understand the bottom line and requirements of the organization's security management. After the general direction is considered, the specific personal information protection provisions of various countries can be practically implemented from the seven aspects of GB/T 35273 (2020).

Appendix A：Comparison table of Information Security Technology - Personal Information Security Specification (Version 2020) and ISO/IEC 27701

Appendix B：Bilingual version of ISO/IEC 27701

环球律师事务所


环球律师事务所
GLOBAL LAW OFFICE
SINCE 1979
环球律师事务所
GLOBAL LAW OFFICE
SINCE 1979