bsi.

...making excellence a habit.™

隐私至关重要

借助 ISO / IEC 27701
有效保护个人信息

面向企业的 BSI 白皮书

引言

从预约挂号到网上银行业务 — 服务的数字化、全球化以及个性化导致个人信息比以往更多地被收集和处理。随着新的服务机会涌现以及新市场参与者的出现，这一趋势在持续不断的增长。

如今，多种多样的平台已成为人们日常生活不可或缺的一部分，个人信息在这些平台中也被广泛的收集。例如，移动应用、会员计划、设备互联位置广告。这意味着我们经常在未经深思熟虑的情况下提供我们的数据，从而导致与以往相比，有更多数据被随意传播。无论是约会网站、电信服务提供商还是公共服务组织，我们几乎每天都看到有关个人信息被泄露的新闻事件。这使得对个人信息滥用问题的关注不断增强，也意味着组织对此决不能掉以轻心。

对这些问题充分的认识，已经引发了个人和政府部门在对个人数据收集、使用和保护方式上越来越多的关注；为此，一些政府部门拟定或者实施了新的法规，旨在提供与个人数据处理相关的指南和要求。

在欧洲，《通用数据保护条例》(GDPR) 的推出协调了各类数据隐私法律，充分反映了我们现在所生活的数字世界的现实状况。

许多其他国家 / 地区（例如，韩国、澳大利亚和中国）也在制定数据保护法规。由于预期监管环境将日益加强以及需要一套通用的概念来处理个人数据保护，国际标准化组织 (ISO) 和国际电工委员会 (IEC) 已经主动创建标准来提供此类指南。这些标准有助于提供框架，以帮助组织在不断变化的监管态势下，证明对个人数据的保护以及对不同法规的遵从。对于组织增强其对隐私和相关义务的承诺的可信度，认证也是非常有用的方式。

管理个人信息

鉴于我们运营所处的环境在不断变化，针对组织应当如何管理和处理数据，以减少个人信息风险的相关指南重大意义。因此，以新国际标准的形式提供的有关组织应当如何管理个人信息，并帮助其证明对全球最新隐私法规的遵从的指南具有非常强大的影响力。这是面向信息管理的 ISO/IEC 27701 应运而生的原因所在。

什么是 ISO/IEC 27701 ？

现已发布的这一新的国际标准正式名称为 ISO/IEC 27701（安全技术 — 对 ISO/IEC 27001 和 ISO/IEC 27002 的扩展以适用于隐私信息管理 — 要求与指南）。通过访问 shop.bsigroup.com/（将在此处发布最新更新），您将继续有机会在开发过程中表达意见和建议。
由于许多组织已经实施了基于 ISO/IEC 27001 的信息安全管理体系 (ISMS)，并且使用来自 ISO/IEC 27002 的指南，在此基础之上，隐私保护指南的提供则非常顺理成章。

ISO/IEC 27701 是在隐私保护方面对 ISO/IEC 27001 和 ISO/IEC 27002 的扩展，针对保护可能受到个人信息收集和处理影响的隐私提供了更多相关指南。设计的目的在于借助更多的要求增强现有 ISMS，以建立、实施、维护和持续改进隐私信息管理体系 (PIMS)。标准草案概述了适用于个人身份信息 (PII) 控制者和 PII 处理者的框架，以有效管理隐私控制，降低个人隐私权面临的风险（参见表一）。这些附加要求和指南的编写，对于任何规模和文化环境的组织都具有实用性和可用性。

表一 — 个人信息管理角色

PII 控制者	PII 处理者
收集个人信息并确定信息处理的目的。 有时多个组织可能共同承担 PII 控制者的角色，在这种情况下，这些组织被称为共同控制者，他们之间需要签订数据共享协议。	仅根据 PII 控制者的指示代表其处理个人信息。
ISO/IEC 27701 能为 PII 控制者提供哪些帮助	**ISO/IEC 27701 能为 PII 处理者提供哪些帮助**
• 提供最佳实践指南 • 在 PII 控制者间提供透明度 • 提供有效方式来管理 PII 流程	• 提供最佳实践指南 • 为客户提供有效管理 PII 的保证

ISO/IEC 27701 的发布计划

ISO/IEC 27701 由负责“身份管理和隐私技术”的 ISO/IEC 工作组起草，并由 BSI 提名的项目编辑 (Project Editor) 领导开发。作为英国政府特许的国家标准机构，BSI 在 ISO 和 IEC 中也作为英国政府的代表。图一显示了以作为国际标准发布为目标的 ISO/IEC 27701 预期发展路线图。

图一 — ISO/IEC 27701 发布计划

标准的正式发布，目的在于使组织能够获得针对 ISO/IEC 27701 的认证，以此作为 ISO/IEC 27001 管理体系的扩展。换而言之，计划寻求通过 ISO/IEC 27701 认证的组织还需要通过 ISO/IEC 27001 认证，以对信息安全和隐私管理的承诺。

ISO/IEC 27701 适用性

针对个人信息保护的要求和指南，因组织的环境以及适用国家法律和法规而异。ISO/IEC 27001 要求充分理解并考虑这种环境因素。ISO/IEC 27701 则更加具体。它包括与下列内容的对应：

- ISO/IEC 29100 中定义的隐私框架和原则；以及
- 侧重于 PII 的 ISO/IEC 27018 和 ISO/IEC 29151。

不过，所有这些对应都需要考虑到本地法律和法规。另外值得注意的是，ISO/IEC 27701 适用于所有作为 PII 处理者、控制者或者二者兼备的组织；ISO/IEC 27018 专门适用于公有云服务提供商。

BS 10012:2017+A1:2018* 是特定于英国发布的标准。它提供了针对个人信息管理体系的最佳实践框架，与欧盟 (EU) GDPR 的原则保持一致。ISO/IEC 27701 和 BS 10012 之间的重要差别之一是 ISO/IEC 27701 是结构化的，因此，PIMS 可被认为是对 ISMS 要求和控制的扩展。

ISO/IEC 27701 可被 PII 控制者（包括那些 PII 联合控制者）和 PII 处理者（包括那些外包 PII 处理服务的处理者）使用。

遵循 ISO/IEC 27701 要求的组织通常会输出一些书面的证据以证明其处理个人信息的方式。这些证据有助于组织证明其与商业伙伴签订的个人数据处理活动相关的协议的符合性。还可能有助于促进与其他利益相关方的关系。如果需要，将 ISO/IEC 27701 与 ISO/IEC 27001 一并使用可提供对此证据的独立性的认证，尽管遵循这些标准不能作为法律法规的合规性证据。

ISO/IEC 27701 的优势

- 在利益相关方之间提供透明度
- 有助于增强信任
- 提供更具协作性的方法
- 更有效的业务协议
- 更清晰的角色和职责
- 通过与 ISO/IEC 27001 相结合减少复杂性

* 发布的 2018 版 (BS 10012+A1:2018) 是对 BS10012:2017 的修订。此修订涵盖了对 BS10012:2017 一些条款的轻微改动；这些改动的目的在于响应英国《数据保护法案 2018》(Data Protection Act 2018)。

如需验证是否一致地实施了标准所规定的适当运营控制，并执行相关隐私法规的合规要求，必须采取措施：

1. 建立相关监管要求与标准控制项之间的对应关系；
2. 列举标准控制项尚未完全涉及的具体监管要求，以及满足这些要求所需要的条件；
3. 在审核周期中，将上述内容融入风险评估流程。

以 ISO/IEC 27701 中的数据泄露管理的控制项和 GDPR 的泄露通知要求（条款 33）为例，标准中的安全事件管理的控制项与 GDPR 的数据泄露要求直接对应。

不过，标准不包含 GDPR 中所规定的 72 小时通知要求。如组织需证明其已经实施并履行 GDPR 的要求，他们必须向审核员证明，组织有在数据泄露确认后 72 小时内通知数据主体和隐私监管机构的统一流程， 也有流程确定泄露事件是否涉及欧洲公民或者泄露数据处理是否在欧洲发生，且在上述情况下将在要求的时限内触发通知。

映射标准与法规的对应关系并识别特殊的监管要求及其适用条件，是控制者和处理者能够通过 ISO/IEC 27701 证明其符合众多隐私法规的必要机制。

数据隐私法律

随着组织数据安全和降低数据泄露风险所面临的挑战日益增多，隐私法律也要不断更新迭代以跟上持续变化的业务态势。值得注意的是， 欧盟 GDPR 已经引起了广泛的关注。

GDPR 旨在维护个人有权保护与其相关的个人信息基本权利和自由。

在数据处理活动以及个人信息在欧盟成员国间自由流动方面，这些权利同样必须被维护。数据处理应当维护个人数据归属的自然人的利益。世界各地都有类似的法律来保护个人信息和公民权利，这也包括一些行业特定法规，例如，医疗健康、零售和银行业。

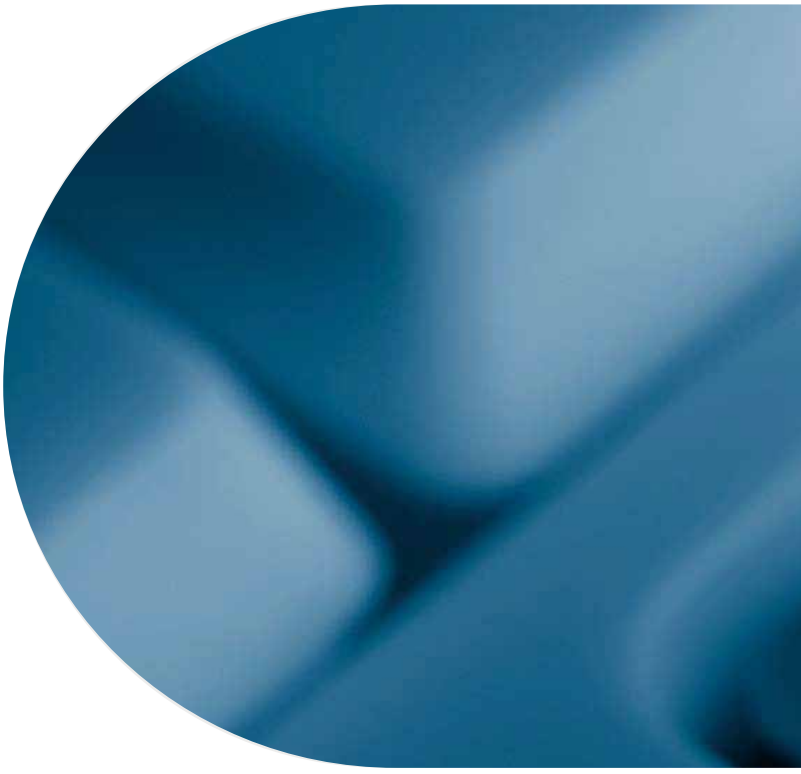
医疗健康行业

作为一个会收集最敏感个人信息的行业，医疗健康行业特定数据保护法律具有重大意义。例如，《法国公共卫生法》（条款 L.1111-8）要求托管某些类型健康 / 医疗数据的服务提供商必须获得针对此类活动的认证。美国《健康保险携带和责任法案》(Health Insurance Portability and Accountability Act) 规定了患者的敏感数据保护的标准， 并且要求美国的健康计划、医疗健康结算机构和医疗健康提供商、或者作为可接触个人健康信息的供应商或分包商的任何组织和个人须遵守此标准。

欧洲数字单一市场政策也同样值得关注。这是 2015 年公布的一项政策，涵盖数字营销、电子商务和电信领域。其目的在于为个人和企业提供更多机会，打破现有壁垒。它有三大核心支柱：

- 访问在线产品和服务
- 为数字网络与服务的持续增长和繁荣提供条件
- 欧洲数字经济的增长

该项政策为跨境数据处理和商务提供了便利。不过，欧盟成员国的数据隐私法律的差异被认为是欧洲数字单一市场成功的一大障碍。因此，GDPR 的推出是非常积极的变化，它有助于协调整个欧盟在数据隐私保护方面的法律法规。



认证机制以帮助证明数据保护法律的合规性

GDPR 鼓励制定数据保护认证机制和数据保护标志与标识，来帮助证明控制者和处理者遵守相关的数据处理操作法规（GDPR (EU) 2016/679，条款 42）。此外，此类认证和标志还可用于证明组织已经采取正确的措施以符合 GDPR 的方式处理个人信息。

一致的认证机制可以将所有重要的“责任”因素纳入考虑范围，促进风险降低并改进个人信息的自由流动。这有助于组织提供有用的服务，同时，如**图二**所示，可增强流程透明度并向客户证明在个人信息保护方面的诚信度。

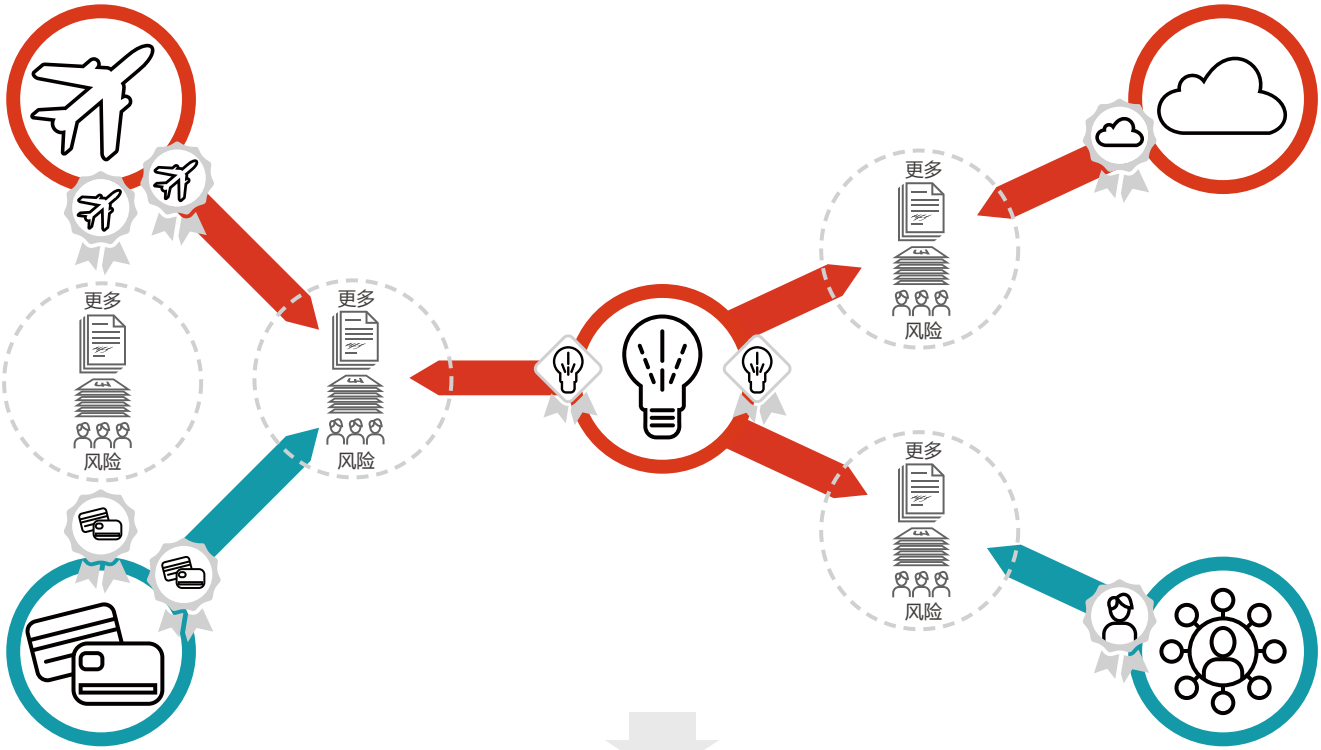
它还凸显了数据处理对于供应链管理的重要性，因为控制者要在数据的整个生命周期对其完全负责。以由航空公司和银行联合推出的信用卡之类的产品为例，来自双方的客户信息需要被交换，以识别哪些客户可能选择此类产品，客户个人信息交换可能引发风险。

各方如何验证另一方将充分保护客户数据？随着更多的商业伙伴的加入，这种风险会不断加剧。例如，与营销公司签约来针对目标客户进行营销，以及在社交媒体平台上购买广告。云服务也可能被营销公司用于存储和处理与这类营销活动相关的数据。认证可作为独立的验证结论，将证明组织用于评估在整个供应链中组织间交换个人信息的风险的流程和控制的有效性。

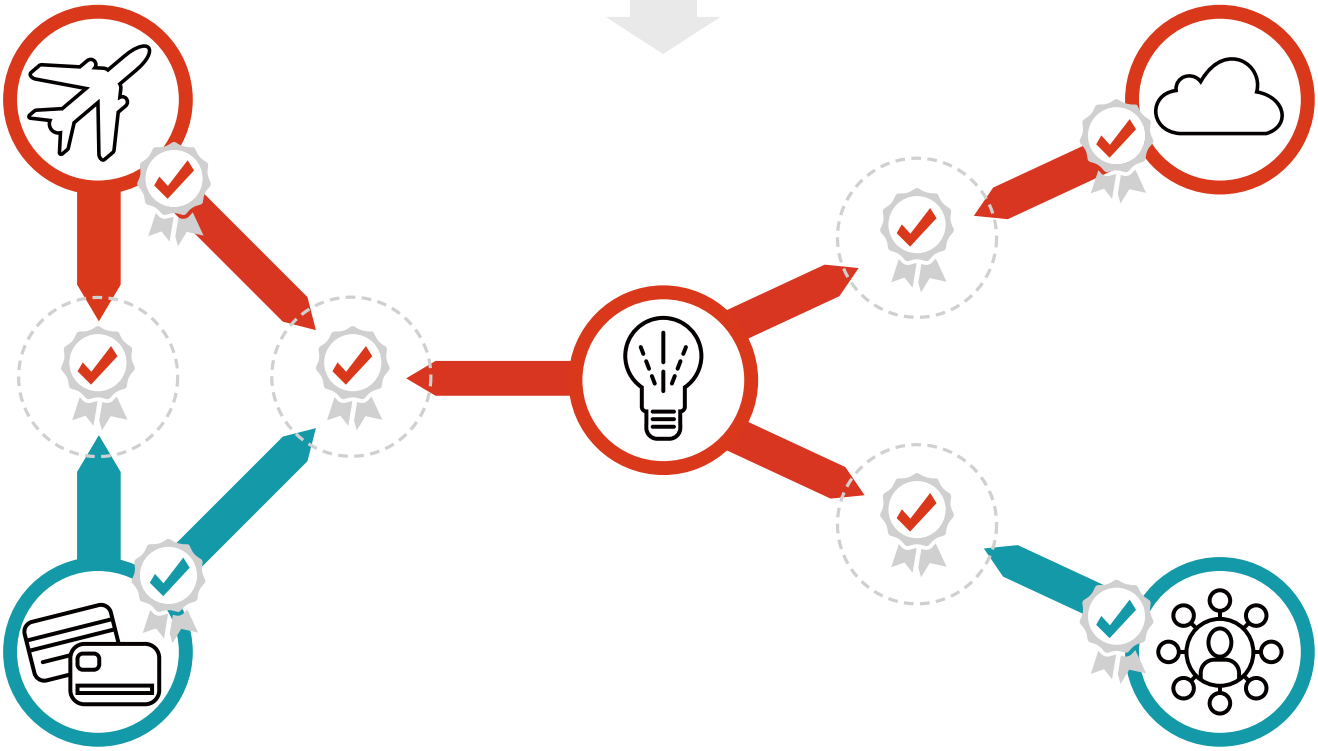
不过，如图二 (a) 所示，如果一个组织使用了一套认证机制，而另一个组织使用了另一套认证机制，这可能无法为业务合作伙伴提供必要的保障或者信任，以证明其客户的个人信息被适当处理。鉴于业务全球化的性质，需要一致和统一的认证机制来证明组织遵守了相关法规，有效保护个人信息并且为业务增长提供助力（如图二 (b) 所示）。在所有领域和行业之间采用一致的 为 GDPR 所认同的认证机制对缓解风险，及打破商务合作伙伴之间的贸易壁垒十分必要。

图二 — 通过一致的数据隐私认证机制促进业务

(a) 组织间碎片化的认证



(b) 一致的认证



近期，欧盟网络与信息安全局(European Union Agency for Network and Information Security, ENISA) 发布了针对 GDPR 认证的建议[ENISA： 欧洲数据保护认证建议 (V 1.0)，2017 年 11 月 ；https://www.enisa.europa.eu/ publications/ recommendations-on-european-data- protection-certifcation]。ENISA 指出认证、标志和标识对于使数据控制者实现并证明其处理操作符合 GDPR 要求起着重要作用。

ENISA 建议在欧盟委员会 (European Commission) 和欧洲数据保护委员会 (European Data Protection Board) 指引和支持下的国家认证机构和监管机构应采用一致的方法以建立和应用 GDPR 认证机制
。他们还建议这种方法应当可扩展并且使用经实践验证和广泛采用的准则。整个欧洲对认证机制的一致性和兼容性性高度重视，可信度和透明度要作为认证机制的重要特征。

ISO/IEC 27701 是一个有潜力的认证机制

ISO/IEC 27701 能够满足上述所有建议，并且预期可被用作认证机制的基础（如条款 42 规定）。如果采用了这种认证机制，组织能够提供其合法处理其客户的个人信息的必要证据，这也包括了跨境数据转移的情况。ISO/IEC 27701 适用于所有规模和不同企业文化的组织。它适用于对于员工和客户 PII 的收集与处理。这套基于信息安全技术控制措施并拓展了隐私要求相关的技术措施，有助于证明组织对于数据隐私法律（例如，GDPR）的合规性。

因此，证明符合 ISO/IEC 27701 所规定的控制措施，并生成其所要求的能够作为组织证明其处理 PII 方式的文档，能够：

- 通过减少重复认证以降低认证工作量
- 通过证明对数据隐私法律的合规性，增强组织和客户间的信任
- 提供证据以使数据保护官能够为最高管理层和董事会成员展现其在隐私法规符合性方面的成绩
- 通过欧盟数字单一市场和跨境数据转移，创造业务机会

而且， ISO/IEC 27701 的应用也将进一步强化组织现有 ISMS ，创建 PIMS 以在整个组织内实现有效隐私管理。通过现有的健全的 ISO/IEC 27001（被公认为成功的信息安全标准）认证审核员网络，ISO/IEC 27701 能够被很好整合到现有审核过程中。

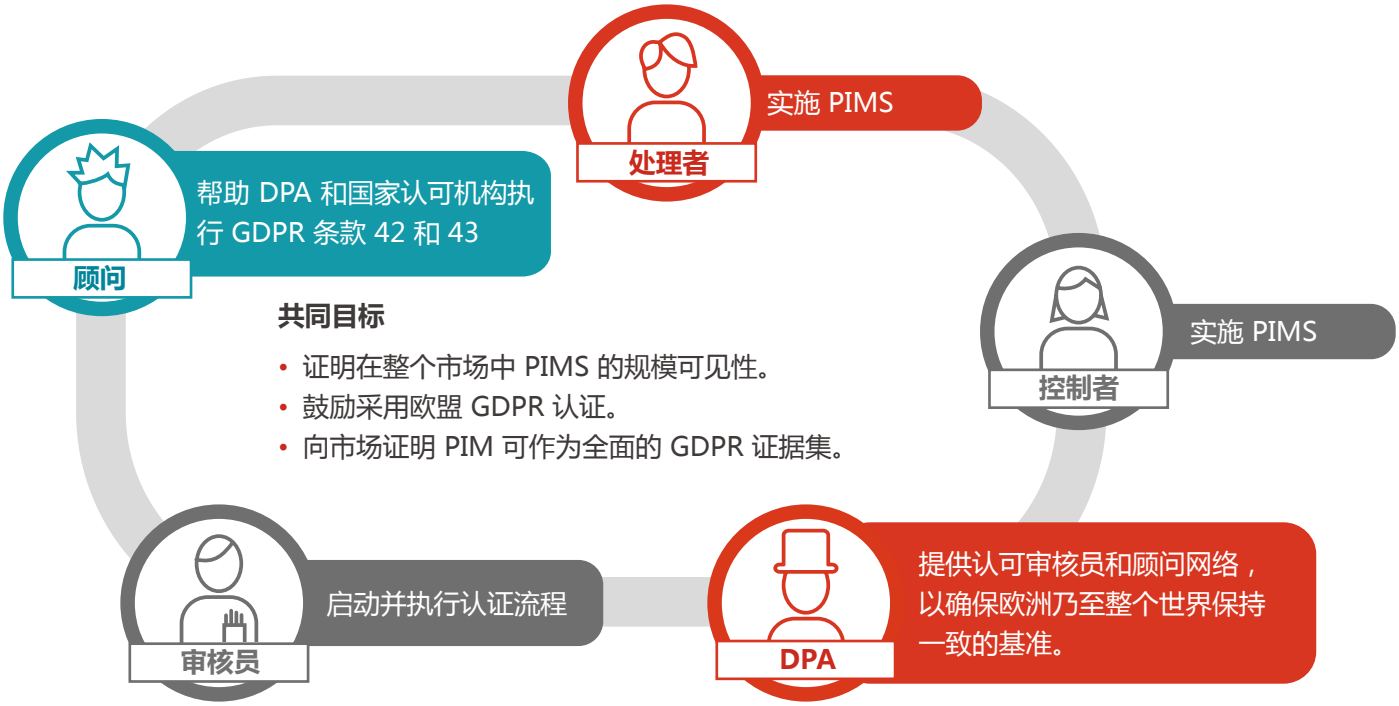
ISO/IEC 27701 通过公认的共识驱动型流程进行开发；这是开发标准的关键任务之一。目前，标准已经引入了各个行业以及监管机构的意见和建议；这也包括由来自所有欧盟国家的数据保护机构 (DPA) 组成的欧洲数据保护委员（原条款 29 工作组）的参与和审查。DPA 以认可机构将需要确保基于 ISO/ IEC 27701 的认证机制，能够充分帮助所有行业以及所有规模的组织证明对隐私法规的符合性。此外，认证机制也需要关注控制者和处理者的需求，ISO/IEC 27701 中也包含了大量与其相关的控制措施。

利益相关方参与的重要性

如前所述，ISO/IEC 27701 是对 ISO/IEC 27001 的扩展，并且是在 ISO 管理体系通用标准框架（通常称为 “AnnexSL” ）中制定的，允许组织更高效地实施多种管理体系。图三显示了各利益相关方的责任及其角色的重要性。

由于已熟悉了现有的 ISO/IEC 27001 ISMS，一旦采用了 ISO/IEC 27701，所有这些利益相关方也更容易掌握新标准。它们拥有共同的个人信息管理的目标，并且需要一种公认的方法来证明个人信息得以认真的对待，这就是 ISO/IEC 27701 的意义所在。

图三 — 针对基于 ISO/IEC 27701 的认证，利益相关方的责任（信息来源：微软）



结论

总之，有效管理个人信息以顺应不断变化的监管态势是复杂的，但是又不容忽视。保护每个人的个人信息是基本人权之一。在与个人生活相关的业务和数据变得日益全球化的情况下，全球各地区都颁布相关法律以保护这些权利。欧盟 GDPR 的颁布旨在确保以合法的方式收集和处理 PII，它支持欧盟数字单一市场所需要的跨境数据转移。

欧盟 GDPR 认为要增强对组织处理个人数据方式的信任，并通过提供组织间的保障创造业务机会。证明合规的认证机制仍然有很长的路要走，如果要在欧盟成员国以及欧洲之外的国家 / 地区间一致地实施认证以支持全球商务和业务，尤为如此。.

ISO/IEC 27701 的引入是对现有标准组合的必要补充。实施 ISO/IEC 27701 规定的控制措施使组织能够保留其处理个人信息的方式的证据。如果个人信息处理具有彼此相关性，此类证据可被用于促进与业务合作伙伴达成协议，而如果具有广泛认可的认证机制，此类证据能够帮助证明其对数据保护法律（例如，GDPR）的符合。

为什么选择 BSI ？

自 1995 年以来，BSI 始终处在信息安全标准领域的前沿，曾经制定了这一领域的世界上首个标准 BS 7799（现在的 ISO/IEC 27001），它是全球最常用的信息安全标准。我们从未止步于此，始终致力于解决新出现的问题，例如，隐私、网络和云安全。这是我们最有能力为您提供帮助的原因所在。

BSI 与遍及 193 个国家 / 地区的 86,000 多家客户合作，是一家在众多行业（包括汽车、航空航天、建筑环境、食品以及医疗保健）具有丰富技能和经验的真正的国际企业。凭借在标准开发和知识解决方案、保障和专业服务等方面的专业所长，BSI 能够通过改进业务绩效帮助客户实现可持续增长、有效管理风险并最终打造更具生存力的组织。

我们的产品与服务

我们为您提供独特的产品和服务互补组合，这些产品和服务通过我们的三大业务流（知识、认证和合规）进行管理。

知识

我们业务的核心在于所创建并传授给我们客户的知识。在标准领域，我们不断强化我们作为专业机构的信誉，汇集来自行业专家的集体智慧打造本地、区域和国际不同层次的标准。全球十大管理体系标准，其中八个是由 BSI 制定颁布的 BS 标准转化而来。

认证

根据特定标准对流程和产品符合性的独立评估可确保我们的客户能够实现高水平的卓越性。我们会就世界级的实施和审核技巧对我们的客户进行培训，以确保他们能够最大限度发挥标准的优势。

合规

要获得实实在在的长期优势，我们的客户需要确保持续合规，满足市场需求或标准，并让合规成为一种植入组织的习惯。我们提供管理咨询服务和具备差别化优势的管理工具来促进这一流程。

bsi.

扫码关注 BSI

www.bsigroup.com/zh-CN/
400 005 0046
infochina@bsigroup.com