DX 时代企业隐私治理指导手册 ver1.1

2021 年 7 月

总务省

经济产业省

变化的历史

版本	变更内容	变更者
1.0	"DX时代的新企业隐私治理指导手册"。	总务省、经济产业省
1.1	增加或修订"3.管理层要解决的三个要求"和"4.隐私治理的关键问题"中的例子。 Ver. 1.0更新后，根据出版后各公司的隐私治理实践状况，加入了更多应作为参考的隐私治理实践实例。 更新的参考资料	总务省、经济产业省

目录

一、本指导手册的定位

为了实现以人为本的社会 5.0，网络空间和物理空间高度融合，企业在促进经济增长和解决社会问题方面发挥着核心作用。通过利用数据创造创新，各方都在推进服务和产品的发展。

在个人数据领域[1]，人们对隐私保护以及创新解决社会问题的需求越来越大。为了应对这种需求，公司需要尽可能地保护消费者的隐私，由此赢得消费者的信任，使他们获得商业优势。本指导手册列出了公司率先采取的步骤，以确保他们积极主动地解决隐私问题，建立信任。这对新业务的顺利运行至关重要。

本指导手册特别针对使用个人数据向消费者提供产品和服务的公司，这些公司可能会受到消费者的直接压力，需要考虑他们的隐私，以及与这些公司做生意的供应商。

我们设想公司中的以下职位将会是主要读者：

- 参与数据使用和数据保护管理的公司经理，或是可以向管理层提出建议的人员；
- 负责全面管理数据使用和保护有关事项的部门负责人等。

此外，我们还设想了以下使用场景。

- 参与数据使用和数据保护管理的公司经理，或是可以向管理层提出建议的人员。
- 负责全面管理数据使用和保护有关事项的部门负责人等。
- 当开始考虑一个可能会对消费者产生重大隐私影响的项目时；
- 当我们被管理层、股东、投资者、母公司或其他相关方要求加强对隐私相关问题的回应时；
- 我们想请管理层加强保护隐私的制度时(要求适当分配管理资源)；
- 如果个人数据的使用在公司、行业等内部引起关注，即个人数据的使用会被批评为隐私问题（即所谓的“丑闻”[2][3]）时，等等。

如上面的例子中包含有你或你正面临的问题，你应当开始阅读本手册。本手册也可以作为广泛参考。[4]

本指导手册的内容部分涉及法律义务，但个别具体的例子应根据个别公司的情况灵活使

[1] 个人数据是指与个人有关的任何信息，而不仅仅是《个人数据保护法》规定的个人数据。

[2] 原文为“炎上“，在日文语境中，当一起事件引发了普罗大众的抨击、批评、或吐槽时，这种一发不可收拾的舆论环境就会被称为炎上。——译者注

[3] 然而，本指导手册并没有提到在发生所谓的 "丑闻"后应如何应对。

[4] 无论公司的规模如何，都会出现隐私问题。对于处理个人数据的中小型企业和风险企业来说，应该参考这本指导手册的思路和考虑，尽管它包含了一些实施上的困难，如建立系统。

用，并允许根据公司的规模和资源来应用。

本指导手册将继续酌情更新，以考虑到社会趋势。如下文所述，隐私的影响和隐私的潜在后果是动态的。

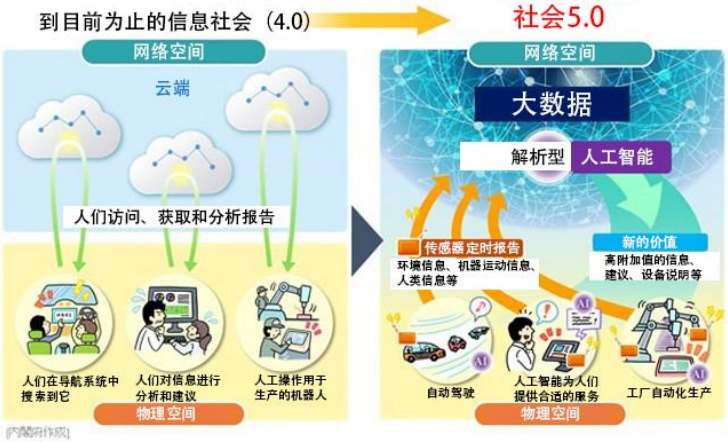
二、指导手册的前提

2.1. 社会 5.0 和企业的作用

由于数字技术的发展和网络空间的扩展，我们今天所处的社会正在经历快速的结构转型。物联网以其高度发达的传感器、摄像头和其他信息采集技术，以及将一切事物连接到网络的能力，正在将现实世界中的人和地面上的各种物体与互联网连接起来。此外，人工智能等技术的最新成果使估算物理空间的各种条件成为可能。因此，物理空间可以被理解和解释为网络空间的数据。结果可以通过各种方式反馈到物理空间。日本政府将"社会 5.0"定义为"以人为本的社会，通过高度整合网络空间和物理空间的系统，实现经济发展和解决社会问题"，并将实现这一社会作为日本要实现的目标[5]。为了实现社会 5.0，业务和管理以及法规制度都需要进行数字化转型。

人们认为，以综合方式促进 DX[6]的发展是重要的。此外，日本正在从创建"实现创新和社会信任的模式"的角度考虑数字治理改革。

图 1 迄今为止的信息社会和社会 5.0



社会 5.0 是网络和物理空间的高级融合，将带来创新的服务和技术，丰富人们的生活。

[5] 内阁办公室协会 5.0 (https://www8.cao.go.jp/cstp/society5_0/index.html)

[6] 数字化转型（DX）是指，例如，根据客户和社会的需求，利用数据和数字技术来应对商业环境的快速变化，对公司的产品、服务和商业模式进行转型，以及对企业本身、组织、流程和企业文化及氛围的转型。它还意味着改造企业本身、组织、流程以及企业文化和氛围，以建立竞争优势。

这些服务包括我们日常使用的各种数字平台提供的服务，正在全球范围内开发和实施的自动驾驶，以及与环境相容并提供舒适和安全生活环境的智能家居。在这样一个社会中，以前由人类和硬件在物理空间中执行的功能将被重新定义、频繁更新、并发展为网络空间中的数据和软件。

网络空间创新的特点是变化迅速，易于跨境发展业务，以及由于数据积累和或直接或间接的网络效应而产生的赢家通吃现象[7]。因此，为了在软件驱动的社会结构转型中保持日本未来的经济增长，无缝连接物理空间和网络空间的创新对于实现社会 5.0 至关重要。

虽然这种创新可能为社会挑战提供解决方案，包括与隐私有关的问题，但创新也会对包括隐私在内的各类问题产生新的风险。

如果不加控制，这些风险可能会导致人们对创新本身的接受度差。为了让创新在社会中扎根并实现可持续的经济发展，社会需要适当地管理它所带来的风险，并让治理实现一系列的社会价值，如生命安全、精神安全、财产安全、隐私、民主和公平竞争。从这个角度来看，作为促进创新的核心，公司必须积极推动创造社会和经济价值的举措，同时减少创新本身带来的风险。换句话说，在开展业务的同时，必须保护个人的权利和利益，赢得社会的信任。然而，积极地处理这些问题本身，就等于在社会（包括消费者）眼中提高公司产品和服务的质量。这可以成为区别于其他公司的一个重要标志。在未来，公司在考虑解决隐私问题时，不应将其作为一种成本，而是将其作为提高产品和服务质量的一种方式，这对公司和个人而言都是一种积极的结论。

考虑到公司的这一重要作用，本指导手册将特别关注与个人数据的使用密切相关的隐私问题。

2.2. 隐私政策

数据的先进使用是实现社会 5.0 的核心，在质量和数量上都将与过去大不相同。特别是，个人数据的使用是公司的业务来源，因为它使公司能够更准确地接近个人的喜好和需求。此外，它对整个社会也非常重要，因为基于对个人的精确分析最终可以导致社会问题的解决。

同时，个人数据的使用越来越多，与它对个人隐私影响的多样化密切相关。

例如，在数据收集方面，数字服务提供商正在收集大量精确的个人数据，这些数据可以提供关于一个人的行为历史、健康、信仰、爱好等详细信息。个人资料如果数据被用于发送

[7] 一个人的网络成员资格不仅增加了这个人的效用，而且也增加了其他用户的效用。直接来说，就是属于同一网络的用户越多，用户的效用就越高的效果。间接来说，在一种商品和其互补商品密切相关的情况下，一种商品的使用量越大，相应品种的互补商品的供应量就越大，因此效用也越大。

带有政治目的的传单，民主可能会受到威胁。

在数据分析领域，由非人类算法（包括使用机器学习的人工智能）做出的决定在社会中发挥着越来越重要的作用，而这些决定的安全性与合理性越来越存疑。例如，机器学习使用现有情况的统计模型来对对象进行估计和判断，这使得它很难处理新的对象，并且在情况发生变化时准确性较低。物理空间的每一次变化都可能使其在估计和判断时犯错，包括可能对物体及其特征犯错。尤其在网络空间的估计和判断被反馈到物理空间时，它就有发生事故的风险。众所周知，机器对偏移数据做分析，或进行不适当的统计处理，也会导致错误的估计和判断。

图 2 物联网和人工智能应用和隐私问题的例子

使用物联网设备等	当物联网设备从消费者那里获取数据时，消费者很难意识到他们的数据正在被获取，即使他们意识到了，也没有机会反映他们对获取数据的想法。此外，物联网设备获取的数据首先可能涉及到消费者以外的人（由物联网设备的摄像头所捕获）。 要测量的数据（What）：很难知道一个物联网设备将测量什么数据。 测量的时间与地点（When & Where）：很难知道测量的时间和地点 测量数据的解释（How）：我们不知道测量的数据将如何解释。 测量的主体（Who）：我们不知道谁负责数据采集。 测量的目的（Why）：很难向消费者传达测量的目的。
使用人工智能来猜测特定个人的身份	在数据的使用方面，当直接从消费者那里获得的数据有限时，使用人工智能，以类推的方式，通过从一个人的行为等方面推测其属性和其他方面信息，从而进行机械判断（包括所谓的剖析），可能会导致估计和判断的不准确，以及将数据用于其他目的。此外，可能会出现隐私问题[8]。

[8] 《经合组织人工智能原则》（OECD，2019 年）、《以人为本的人工智能社会原则》（促进全面创新战略委

然而，随着信息和通信技术的发展以及信息隐私概念的出现，了解尊重权利的必要性变得越来越重要，这导致了"个人信息控制"的发展。这包括目前不太明显的新隐私问题[9]，如因数据分析而可能产生的不公平待遇，或对个人政治选择的干预[10]。

另一方面，在日本的购物中心和商业设施中安装安全摄像头的案例中，对安装本身的担忧起初引起了大量的社会争论，但现在社会对安装这种摄像头有了一定的考虑，变得更容易接受了。另一方面，安全摄像机的图像使用超出其最初的安全目的，以及具有识别功能的监控摄像机的出现，引起了人们对所捕获图像数据的关注，欧洲和美国开始出台严格的法规[11]。

因此，对隐私的负面影响是多方面的，从对个人隐私的侵犯到对个人的波及所导致的社会负面影响。此外，困难在于隐私的概念不能被视为一个固定的概念，因为个人的看法和社会的可接受性可能因环境和时间的推移而变化。隐私风险在个人和社会中可能变得很高。如果公司不能对隐私风险作出适当的反应，其将为前者带来相关商业风险[12]。

公司必须认识到，隐私风险在对公司构成风险之前就已经对个人构成了风险，而且会影响到整个社会，并在任何时候都将隐私方面的考虑和举措纳入其业务活动中。

在本手册中，我们将隐私问题定义为对隐私的任何负面影响，从对个人隐私的侵犯到对社会价值的负面影响。手册中也包含了公司对这类事件的处理方式。

2.3. 公司隐私治理的重要性

公司往往是通过使用个人数据为社会创新和创造价值。因此，公司未来将在解决隐私问题方面发挥核心作用。如果我们不采取适当的行动来限制隐私问题的发生，个人将感受到隐私风险。这一点，加上人们对隐私风险和变化的恐惧，将导致整个社会对数据使用的普遍不信任，这反过来会扼杀创新。这种情况不利于在社会 5.0——即以人为本的社会——平衡经

员会，2019 年）和《人工智能使用指导手册》（总务省，2019 年）也很有帮助。

[9] 在前外务大臣有田八郎声称自己的隐私被三岛由纪夫的小说《聚会之后》侵犯，并要求刊登道歉广告和赔偿损失的案件（"聚会之后 "案）中，东京地方法院认为，由于隐私权可以被理解为不向公众披露私人生活的法律保障或权利，因此被害人有权要求对侵权行为发出禁令并赔偿精神损失。

[10] 曾有公司利用基于数据分析的预测结果来影响招聘过程，海外也曾有基于社交网站个人信息的心理分析结果被用来影响投票行为的案例。

[11] 2019 年 7 月，欧盟公布了关于通过视频设备处理个人数据的准则草案。其中包括根据 GDPR 处理摄像头图像和面部识别技术的准则草案，也包含有商业角度的严格规定。另一方面，2020 年 2 月发布的欧洲人工智能战略白皮书《论人工智能--欧洲的卓越和信任方法》正在定稿中，对使用面部识别的立场发生了变化。它的地位目前还不稳定。在美国，一项法令于 2019 年 6 月生效，禁止在包括警察在内的 53 个市政机构中使用面部识别技术及通过面部识别技术获得的信息。最近，一些公司宣布他们将不再提供面部识别软件。

[12] 关于隐私问题的更多信息，见第 5.2 节，"识别隐私风险（识别隐私问题）"。

济发展和社会问题。因此，解决隐私问题是实现社会 5.0 的一个重要部分。

在处理隐私问题时，公司需要重申这样一个事实：即使通过网络空间，他们所处理的也不仅仅是数据，而是物理空间中的有血有肉的个人，他们需要认真思考，确保不损害个人的基本权利。从企业社会责任的角度来看，也有必要采取适当的措施来阻止隐私问题的发生，以免损害消费者或个人的基本权利[13]。

目前，日本对隐私问题的回应是基于《个人信息保护法》(2003 年第 57 号法律，以下简称《个人信息保护法》)，该法规范了个人信息的处理。规范个人信息处理的《个人信息保护法》(2003 年第 57 号法律，以下简称《个人信息保护法》) 是主要规范。在过去，这意味着公司不得不在其业务运营中处理隐私问题。为此，企业在经营过程中考虑隐私问题时，往往从合规的角度出发，关注是否符合《个人信息保护法》的规定。

另一方面，随着新的隐私问题的出现和人们对隐私意识的增强，人们对公司的社会可接受性提出了质疑，这些质疑不一定局限于遵守《个人数据保护法》。此外，还有一些案例，公司无法避免在隐私问题上受到批评，导致所谓的"丑闻"。企业很有必要根据个人数据在企业中的使用方式，考虑对个人权益和社会价值的影响，更加积极主动地进行处理和解释，而不是简单地遵守外部法律和规定。

然而，从最近的批评来看，很明显，虽然重点是遵守法律法规，但从某种意义上说，重点是被动地采取了遵守法律法规的个别措施。从某种意义上说，人们被动地把注意力集中在遵守法律的个人反应上，而对个人反应背后的根本目的，即如何阻止隐私问题的发生，却认识不足。在这种情况下，处理隐私问题本身就被视为一种"合规成本"，一些公司在遵守法律和法规的前提下，尽可能地"合理化"其反应。这可能导致一个恶性循环，即公司本身遭受损失，变得保守，对使用个人数据犹豫不决，即使它已经遵守了法律。

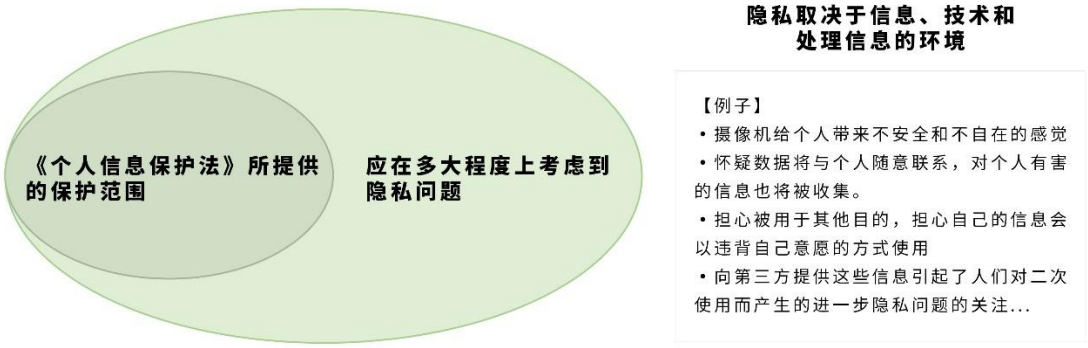
相比之下，有许多公司，包括国内和国际公司，通过使用个人数据来获得客户和消费者的信任，从而扩大其业务。在这些公司中，隐私保护不应被视为一个单纯的合规问题，而是一个重要的管理战略，管理层应积极推动建立一个系统和结构，以适当地评估和应对与其业务有关的隐私风险。同时，他们应该与社会或利益相关者沟通，并寻求获得隐私风险管理之外的公众信任。减少与企业产品和服务相关的隐私风险，使其更有利于隐私保护，将有助于公司赢得包括消费者在内的社会的信任。隐私措施不应被视为一种成本，而应被视为提高产品和服务质量的一种方式。

[13] "社会责任指导手册"（ISO 26000:2010）和 "企业与人权指导原则"（联合国人权理事会，2011）已经制定。在日本，根据《商业与人权指导原则》制定的 "商业与人权行动计划 "也在加速发展，公司将被要求采用这些计划。

在一个快速变化的时代，仅靠合规不足以管理风险和获得社会的信任。因此，公司有必要在解决隐私问题方面发挥积极作用，主动与消费者和其他利益相关者进行沟通，同时保持对法律法规的遵守。此外，公司需要主动向社会披露和解释其隐私做法，并通过与利益相关者对话，确保他们能够信任公司。这是一种在组织上向"遵守和超越"的方法的转变[14][15]。

换句话说，企业隐私治理的基本理念是，管理层应积极致力于解决隐私问题，以便通过适当的风险管理和对隐私问题的信任来提高企业价值。它应当建立一个在整个组织内解决隐私问题的系统，并使之发挥作用[16]。

图 3 应考虑到隐私问题的程度



[14] 为了促进个人数据的使用，政府一直在努力制定举措，支持公司处理隐私问题。尤其是在物联网促进联盟下成立的、与经济产业省（METI）和总务省（MIC）联合运作的数据分配促进工作组，三年来一直在为如何解决个别企业的隐私问题提供专家建议。同时，工作组将积累的信息以 "新数据分配交易案例研究 " 的形式发布，为企业提供有用的信息（1.0 版于 2017 年发布，2.0 版于 2018 年修订）。此外，自 2017 年以来，为了促进有望得到高度利用的相机图像的使用，同时考虑到其特点，出版并修订了《相机图像利用指导手册》，其中概述了企业在保护消费者隐私和与消费者进行适当沟通时应考虑的事项。(1.0 版于 2017 年出版，2.0 版于 2018 年修订）。)此外，我们还出版了《摄像机图像利用指导手册：预先通知和通报的参考案例集》（2019 年）和《私营部门经营者利用摄像机图像的公共目的举措的考虑：考虑传染病控制的使用案例》（2021 年）。这些举措的共同点是，虽然遵守《个人信息保护法》是自然而然的前提条件，但它们从帮助公司在更高层次上处理隐私问题的角度提供建议和信息，而不仅仅是遵守法律所需的建议。另一方面，过去的努力仅限于为个别企业提供具体行动。为此，我们决定在数据分配促进工作小组下设立 "企业隐私治理模式研究小组"，以讨论更多的普遍举措，支持企业向遵守和解释模式的组织转型。

[15] "治理创新：重新设计法律和架构以实现社会 5.0"（经济产业省，2020 年出版）也描述了公司遵守和执行的必要性。

[16] 日本商业联合会（Nippon Keidanren）也在 2019 年 10 月发布了《关于适当使用个人数据的宣言》。管理层应认识到，保护个人数据和网络安全措施不仅有助于创造中长期的企业价值，降低商业风险，还能实现个人安全和保障。

专栏 个人数据在抗击新的冠状病毒感染中的应用

在许多国家，使用个人数据对抗新的冠状病毒感染的需求迅速增加。

不同国家采取的方法包括，例如，通过允许卫生当局跟踪受感染者的位置来确保隔离的有效性，以及使用蓝牙功能通知人们可能与受感染者接触的接触意识应用程序。拥堵的数据也被用来直观地显示感染控制措施的实施程度，并鼓励行为改变。

在这些举措中，有公共机构自己建立机制收集数据的例子，但在需要快速反应的情况下，已经掌握大量个人数据的私营部门经营者可以从履行社会责任的角度出发，自行决定公布其对个人数据的分析结果。此外，政府已要求企业与其合作，提供相关数据。

在日本，政府也向平台运营商和移动运营商提出了提供数据的要求。

被要求提供数据的公司必须迅速做出适当的决定，在保护用户隐私的同时，他们可以提供多少数据，面对提供数据用于公共利益与通过保护用户的数据隐私获得用户信任之间的挑战，我们必须做出一个适当的决定。

答复要求的公司在其管理层和业务部门中对处理个人数据的重要性有着强烈的认识，因为他们在业务中处理和使用大量的个人数据。这使我们能够考虑并迅速决定如何回应这一要求。

在某些情况下，公司只有在事先与政府达成协议，即政府承诺数据的预期用途，在适当的时候公布使用结果，并允许公司在无法确保适当使用的情况下停止提供数据后，才对数据请求作出回应[17]。这是公司承担隐私治理责任和减少用户隐私风险的一个例子。

另一方面，为了保护利益相关者的安全和社会对公司的信任，公司一直在自主采取各种措施，如鼓励员工和商业伙伴做 lifelog[18]。这种形式的个人数据使用有可能很快就会显现。在这种情况下，必须充分考虑雇员和商业伙伴的隐私以及与用户和消费者的关系，这一点是无可争议的。

今后，在开展经济活动的同时，有必要采取适当的措施，防止疫情的传播，同时要求企业继续在有效使用个人数据和基于隐私的适当处理个人数据之间取得平衡。

这些例子表明，在未来社会中，持有和使用个人数据的公司可能会在公共利益方面发挥重要作用，提前建立有效的内部隐私治理机制以应对这一问题。

三、管理层需要解决的三个要求

随着我们朝着实现社会 5.0 的方向发展，企业有望通过使用数据在创新中发挥主导作用。隐私保护和数据利用不应视为二元对立，而应视为在尊重隐私的同时使数据利用的利益

[17] 例如，应要求提供数据的雅虎日本与卫生、劳动和福利部（MHLW）达成协议，根据该公司隐私专家小组的建议，提供有助于集群控制新冠肺炎的信息。

[18] Lifelog 是用户使用电脑、移动设备等在互联网内外的活动记录（行为历史）。
(摘自总务省的 "生命记录服务工作组报告：基于听证会的未来考虑"。)

最大化。在一个以使用数据为前提的社会中，企业对消费者隐私的一贯保护将使个人服务和产品的质量得到改善，这将使企业获得商业优势，赢得消费者和利益相关者的信任，从而提高企业价值。如何提高管理质量对管理层而言是至关重要的。因此，在数字社会中，管理者必须将与隐私有关的举措视为一种商业战略，并将隐私视为竞争力的一个要素。

当然，如果公司没有考虑到隐私风险，或者没有防止个人或社会出现隐私问题，社会对他们的信任被动摇，这可能会对他们的销售和利润产生负面影响，在某些情况下甚至可能导致对其业务开展与业务持续性的担忧。因此，这一点也很有必要纳入到考虑范围中。

首先，股份公司的管理层作为一个优秀的管理者，负有谨慎的责任。这种义务包括建立一个与公司规模相适应的风险管理系统。因此，如果由于这种系统的故障而造成损失，不仅负责相关部门的董事需要承担责任，其他董事也可能受到牵连[19]。对于追求数字化转型的公司来说，管理和正确使用个人数据是一项重要的业务工作。值得注意的是，如果没有建立适当的内部控制，可能会导致个别管理人员对泄漏或“丑闻”给公司造成的任何损失承担责任[20][21]。

鉴于上述情况，公司管理层必须将隐私问题视为竞争力的一个要素，并作为一个重要的管理战略问题，在公司内部建立和运行一个内部控制体系来支持这一工作。

为了实现隐私治理，管理层应首先做好以下三件事：明确声明对隐私治理的立场；指定一名隐私官员；对隐私倡议的资源承诺。

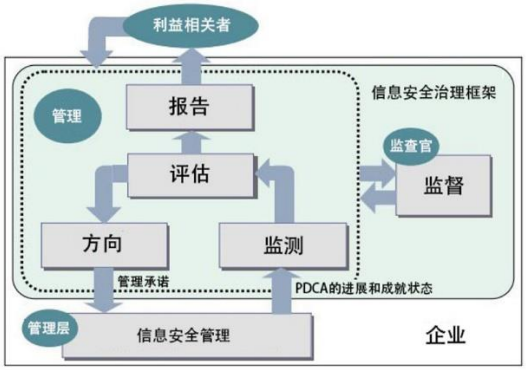
[19] 根据《公司法》第 423 条（对公司的责任）和第 429 条（第三方的责任）以及《民法》第 709 条（一般非法行为）。

[20] 尽管董事们并不对每一次“丑闻”承担个人责任，但如果公司被要求制定 "丑闻政策"作为适合其持有的个人数据及其使用方式的风险管理系统的一部分，他们可能会因其未能建立内部控制的义务而导致的“丑闻”承担个人责任。在这种情况下，个人可能因违反建立内部控制的义务而被追究责任。

[21] 由于这个原因，越来越多的公司外包给其他公司，如云服务提供商，通过获得有关外包业务的安全性、可用性、处理完整性、保密性和隐私的内部控制的保证报告（所谓的 SOC2 报告）来确保信任。

图 4 （参考）信息安全治理的框架

作为参考，信息安全治理的框架如下所示。信息安全治理框架是一个 "方向"，从管理战略和风险管理的角度进行 "监测"，根据指标直观地了解治理活动的状况，它被认为由五项活动组成：监测、评估、监督和报告。类似的框架可能对隐私治理有帮助。



资料来源：《信息安全治理导入指南》（2009 年 6 月，经济产业省）
"图 1-2：信息安全治理框架"
https://www.meti.go.jp/policy/netsecurity/downloadfiles/securty_gov_guidelines.pdf

3.1. 明确说明我们对隐私治理的立场

当企业在自己的企业理念下努力通过创新创造价值时，作为一个组织，以一贯的方式保护消费者的隐私将提高其产品和服务的质量，并赢得消费者和社会的信任。这也将增加公司的价值。

管理层必须认识到这是未来最重要的管理问题之一，并确保组织对隐私保护的一贯做法和应对隐私风险的积极方法在组织内外得到明确的阐述和交流。

此外，自上而下地宣传隐私保护的核心原则和积极应对隐私风险的态度，将有助于在整个组织中灌输隐私问题的意识。不仅在内部，而且在外部向消费者和利益相关者（如股东、商业伙伴）宣传隐私政策，为建立信任提供基础。管理层必须负责[22]确保以符合组织隐私政策的方式来处理隐私问题[23]。根据技术的发展和社会的要求，行为原则和应对政策的内容和操作应不断审查并酌情修订，以确保它们继续满足社会的信任。[24]

[22] Accountability 不仅是指问责制，而且是指能够履行总体责任的状态。

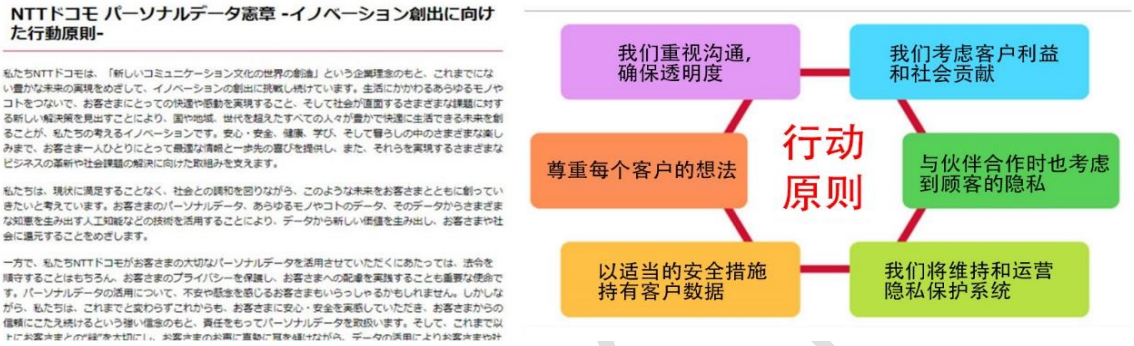
[23] 在阐述总体立场时，有一个全球标准可以作为隐私保护的基础，那就是隐私设计（PbD）的概念。PbD 是一个概念，即在业务发展的一开始就应该考虑隐私保护，而不是在业务或组织中出现隐私问题时才反应。PbD 方法和七个 PbD 原则之一（见本指导手册第 6 节 "隐私设计"），"正和 "而不是 "零和"，与公司的角色和态度一致。因此，它对管理人员是有帮助的。

[24] 应该指出的是，许多公司已经有一份题为 "隐私政策 "的文件。"隐私政策 "是基于《个人信息保护法（总则）》3-6 条和 JISQ15001:2017 中规定的促进个人信息保护的原则和政策。在许多情况下，这适用于 "个人数据保护管理系统-要求 "所要求的内部和外部隐私政策。关键是要确保信息清晰，无论采用何种形式，管理层自己的意图都要体现出来。

案例研究：NTT ドコモ个人数据宪章发布

NTT ドコモ, INC.已经制定并公布了《个人数据宪章--创新行动原则》。本《个人数据宪章》是 NTT ドコモ, INC.的一套原则。

根据其 "创造通信文化的新世界 "的企业理念，公司宣布继续接受挑战，创造创新，以实现空前繁荣的未来，希望与客户一起创造与社会和谐的未来，并在使用个人数据时，肩负保护客户隐私以及遵守法律法规的重要使命。除了遵守法律和法规，它还声明保护客户的隐私是一项重要的使命。



(来源: https://www.nttdocomo.co.jp/info/notice/pages/190827_00.html)

3.2. 任命隐私官

为了实现隐私治理，管理层必须参与其中，并将其对隐私治理的明确立场（如 3.1 所述）具体付诸实践。为此，管理层应指定一名负责的高级行政人员（以下简称"隐私官"），负责处理整个组织的隐私问题。隐私官负责确保该组织的隐私做法与管理层的既定立场一致。管理层应向隐私官索取报告并对其进行评估，以确保组织的内部控制更有效地发挥作用。在这样做的时候，他们应该明确隐私官的责任范围，并确保他们的权力能够支持他们开展必要的行动来遏制隐私问题[25] [26]。

3.3. 将资源用于隐私倡议

管理层需要投入必要和足够的管理资源，以明确的立场来付诸实践。管理层有必要建立

[25] 应该注意的是，隐私官不一定与数据保护官（DPO）相同，根据《通用数据保护条例》的利益冲突条款，数据保护官具有很强的独立性。DPO 可能不担任会导致确定组织内处理个人数据的目的和方法的职位（如董事会成员），但隐私官可以在授权参与确定组织内处理个人数据的目的和方法的职位（如董事会级别）上有效运作。隐私官应该是董事会的成员。根据公司的具体组织结构，最好在适当的位置上任命一个人作为隐私官。

[26] 《个人信息保护法》第三章第三节第 2.(3)条规定："关于设立个人数据处理责任人，作为制度建设的一部分，从跨部门和专业的角度对各部门和员工的个人信息处理进行指导和监督是有效的。在处理个人信息方面，向每个部门和员工提供跨部门的专家指导和监督是有效的。报告中指出了这一点。

一个处理隐私问题的系统，并为其分配足够的人员，以及实施人员培养和招聘。

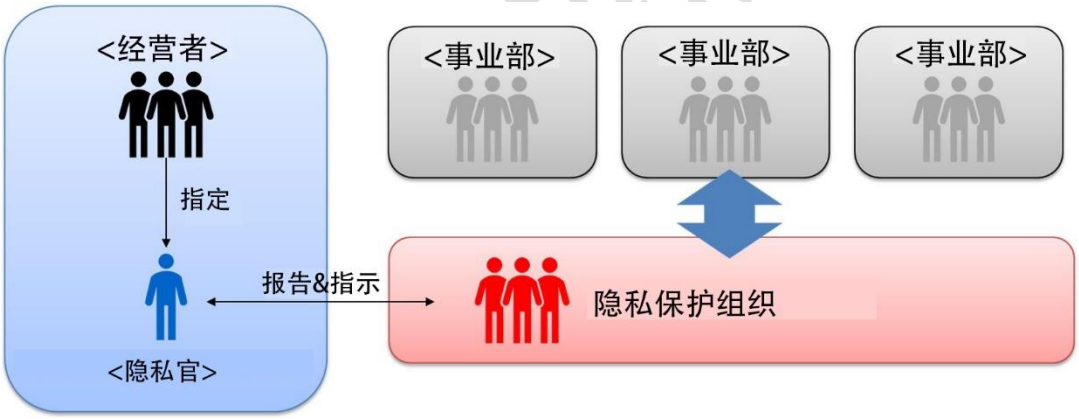
此外，隐私问题不一定取决于商业条件或外部环境，它可能在任何时候出现[27]。因此，预计将持续投入隐私倡议的资源，以确保倡议本身的连续性。

四、隐私治理的主要方面

4.1. 建立一个系统

要使隐私治理发挥作用，就必须整合各部门的信息，找到业务中的隐私问题，并从多个角度考虑解决这些问题的措施，以尽可能地实现目标业务和隐私风险管理的目标[28]。为实现上述目标，最好在企业内部设立一个核心组织，由指定的隐私官（在本指导手册中称为"隐私组织"）领导。

图 5 建立一个隐私保护系统

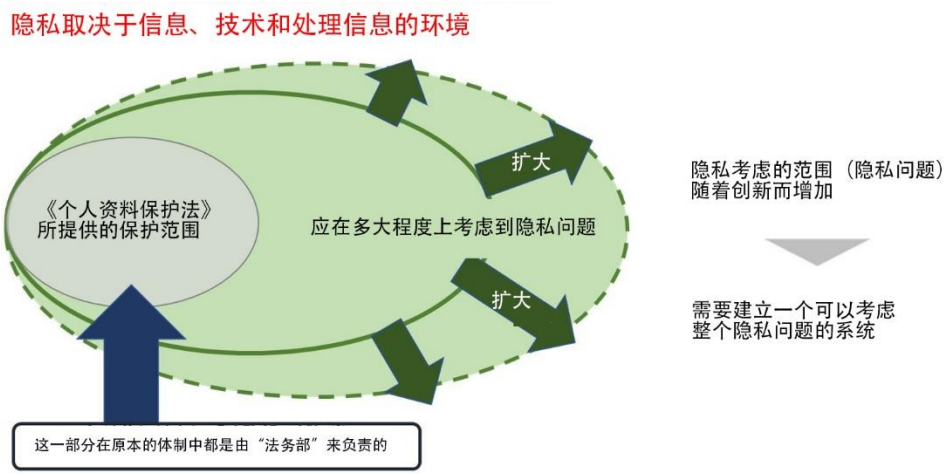


目前，只有少数公司有隐私组织，但它们可以帮助促进与公司内部新业务部门的密切沟通，从外部专家处收集相关信息，并考虑如何从多个角度作出回应。

图 6 需要建立系统来处理日益增长的隐私问题

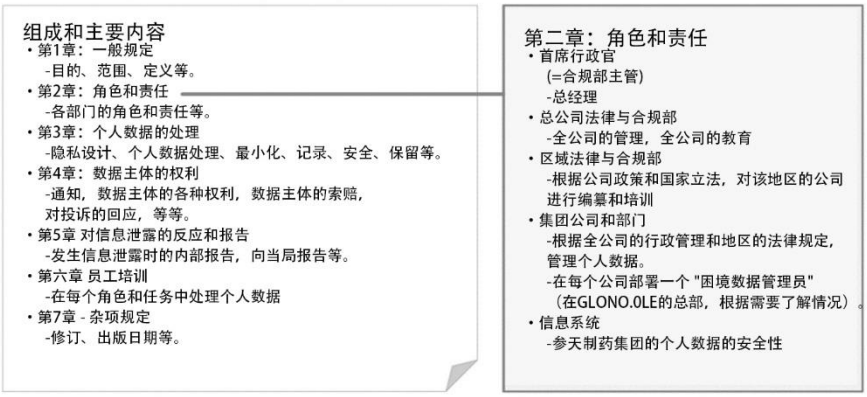
[27] PbD 的概念和 PbD7 原则（见本指导手册，"6.（参考）隐私设计"），如 "主动/预防 "和 "隐私作为默认设置 "是有帮助的。

[28] 在组织中创造和保护价值的活动，通过制定体现管理层制定的隐私治理立场的目标，以最佳方式解决组织所面临的隐私风险，并通过决策和改善绩效来实现这些目标。

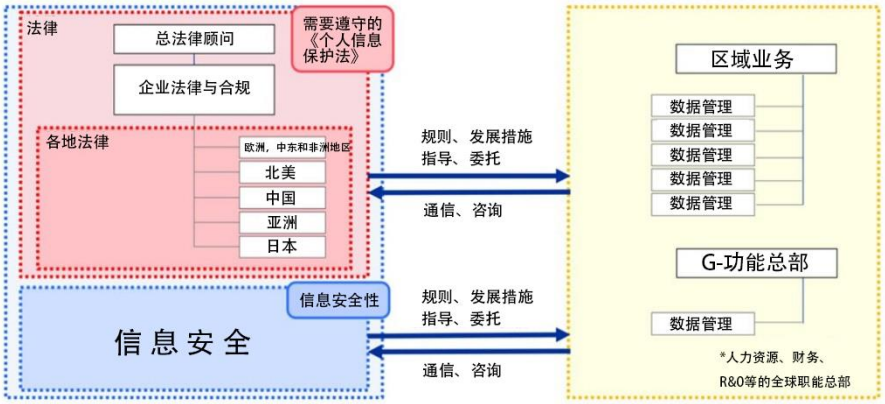


案例研究 参天制药全球隐私治理

2020 年 4 月，参天制药制定了一项全球政策，规定了参天的隐私原则，并通过数据管理员向全球总部下属的地区和职能部门提供指导和鼓励。



全球数据隐私政策（来源）（内部文件）。



建立个人数据保护系统（来源）（内部文件）

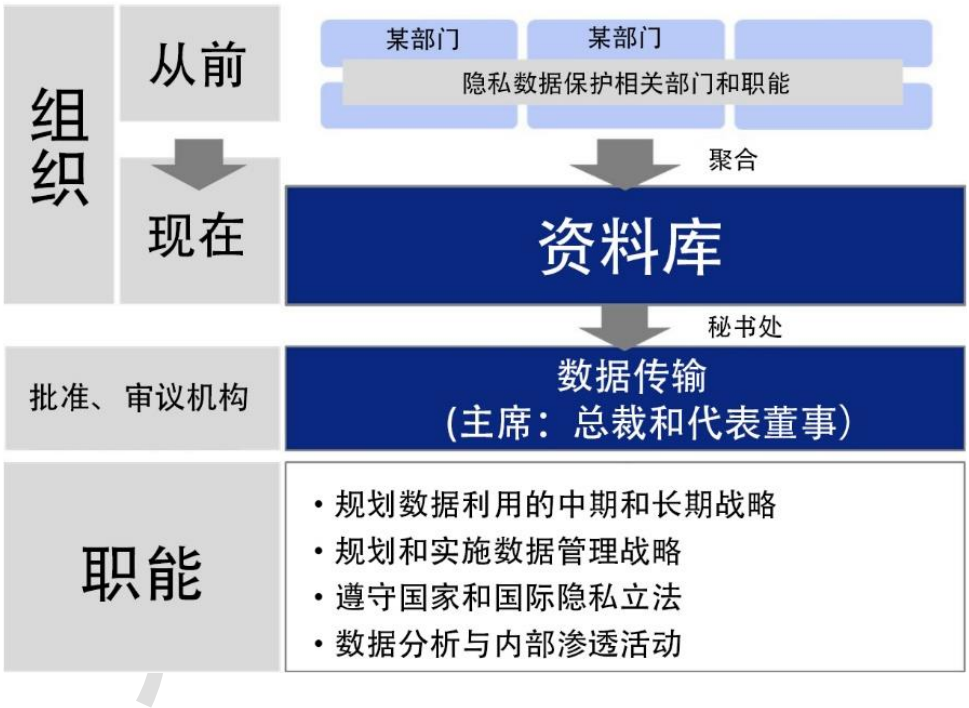
4.1.1. 隐私官的作用

隐私官应依据管理层赋予的权力，管理层澄清立场的内容等，制定实践的政策，并建立一个能够识别和评估隐私风险的系统，考虑相关对策，并确保政策的实施。该政策还应该包括在实际发生隐私问题时的应急反应、消费者救济、原因分析和补救的角度。

案例研究 KDDI 数据治理办公室的建立

KDDI 公司在 2020 财年成立了数据治理办公室。作为一个新的组织，巩固和整合各组织在个人数据利用方面的发展和运作职能。

由社长担任主任的数据治理办公室负责数据的使用和治理。此外，由社长主持的数据治理委员会是数据治理的决策机构。



(来源：内部文件)

隐私官将向管理层报告，管理层将检查并确保报告的内容与公司声明的隐私治理方法一致。

4.1.2. 隐私组织的作用

最好能建立一个隐私保护组织，作为隐私保护官之下的核心组织，负责实质性的隐私保

护职能[29]。根据公司的资源建立一个有效的隐私保护组织是很重要的，例如，如果很难保证有一个具有专业知识的全职人员，隐私保护组织应该只由同时为公司工作的员工组成。

隐私官应确保整个公司都知道隐私组织的存在。

隐私组织的主要作用是收集整个企业的新业务和服务产品的信息，以确定对消费者和社会的潜在风险[30]。这其中重要的是要创造一种制度和环境，让新企业和新技术开发部门能够自由讨论他们所关切的问题。

同时，由于个人观念的差异，以及社会接受度随环境和时间的推移而产生的变化，有必要不断收集有关隐私问题的相关信息（市场趋势、技术、系统等）。也有必要与隐私问题的专家（学者、顾问、律师、消费者组织等）建立关系，并在必要时咨询他们。

此外，应进行隐私风险管理，以解决所发现的任何隐私问题，同时确保尽可能实现目标业务。在某些情况下，应考虑采取多方面的方法，包括建议采取更积极的补救措施，而不仅仅是风险管理[31]。在这样做时，有必要不仅从业务计划的角度，而且从法律和合规的角度，以及从系统和信息安全的角度来检查，同时还要考虑社会对服务的用户和消费者的接受程度。

在考虑这个问题时，在必要时要与开发新业务或技术的部门以及相关的法律、系统、信息安全、合规、公共关系、客户服务和政策规划部门协调。最好建立一个制度，灵活及时地召集必要的成员，例如决定负责各部门的成员[32]。

此外，如果企业发生隐私问题，隐私官应与企业单位合作，收集和审查信息，并向隐私官报告，以获得关于初始响应、损害救济、事后响应、原因分析和补救措施的指示。

企业也有必要积累关于讨论的隐私问题的历史信息，以便在必要时使用。定期汇编内部隐私咨询和案例的信息也很重要，并将这些信息报告给隐私官，也要在整个公司分享。

为了使这样一个隐私保护组织发挥作用，必须能够同时联合多个部门，且拥有能够协调这些成员和从不同角度进行研究的人力资源。因此，除了适当分配这些人员外，有必要从中长期的角度系统地开发人力资源，同时牢记隐私保护是一个高度专业化的领域。

图 7 隐私组织的作用

[29] 关于隐私问题的更多信息，见第 5.2 节，"识别隐私风险（识别隐私问题）"。

[30] 例如，一些公司已将对新业务和业务发展项目进行风险评估作为一项规则，并将具有隐私组织职能的部门纳入评估程序。

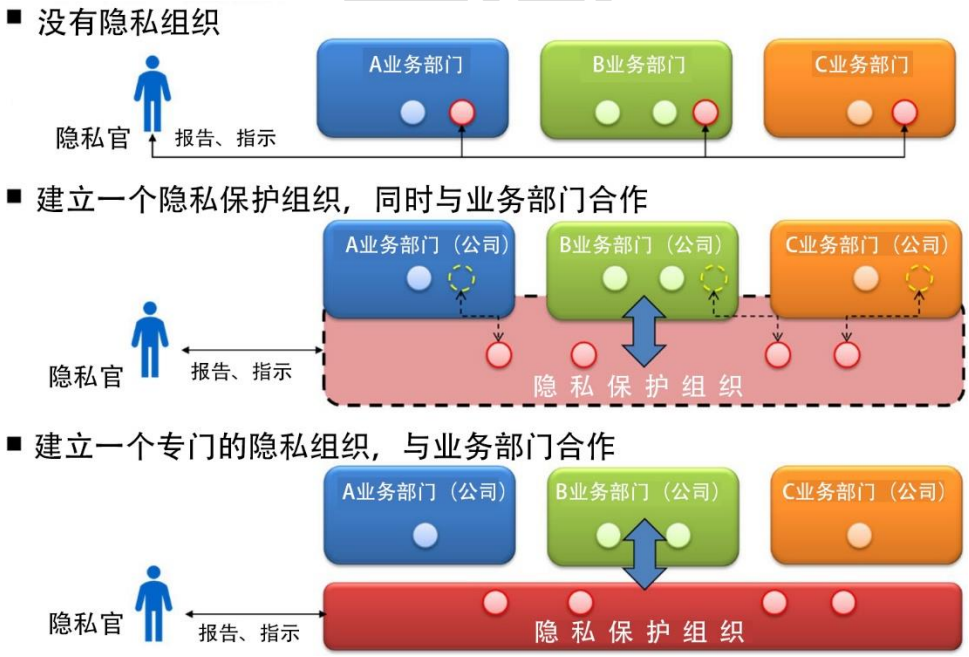
[31] PbD 的概念和 PbD7 原则中的 "正和而不是零和"（见本指导手册 "6.（参考）隐私设计"）是有帮助的。

[32] 传统上，当公司在商业运作中考虑隐私问题时，他们会从合规的角度关注是否符合《个人信息保护法》。因此，在许多情况下，法律部门是负责处理《个人信息保护法》所规定的保护范围种的主要部门。另一方面，由于技术革新和消费者隐私意识的增强，隐私保护方面的考虑范围每天都在变化和扩大，有必要建立一个能够保证隐私问题得到多边考虑的隐私保护组织。隐私组织的结构将取决于公司业务的性质和它所处理的数据，但它可能有大量的技术专家资源，或者它可能由信息安全界的成员领导。

一个隐私组织所联系的实际部门将取决于许多因素，包括公司的规模、其治理结构、它所处理的信息的性质和该组织的位置（如下图所示）。重要的是，无论何种结构，它都应该能够快速识别公司可能造成的任何消费者隐私风险或实际问题，并向隐私官报告，以寻求指导。

由于技术革新和消费者隐私意识的增强，隐私保护方面的考虑范围每天都在变化和扩大，有必要建立一个能够保证隐私问题得到多边考虑的隐私保护组织。隐私组织的结构将取决于公司业务的性质和它所处理的数据，但它可能有大量的技术专家资源，或者它可能由信息安全界的成员领导。

图 8 隐私组织在公司内的地位实例



4.1.3. 业务单位的作用

业务部门需要确保他们处理的产品、服务和数据不会引起隐私问题。业务部门意识到这

一点并积极主动地采取行动是非常重要的。他们应定期咨询并与隐私组织合作，以识别和解决隐私风险。如果你与消费者有接触，你需要充分意识到，你处于与他们建立信任的重要位置，要考虑他们的接受能力。

负责提供服务和业务的部门也必须与客服部门和其他部门合作，建立一个能够在正常情况下接受消费者广泛意见的系统。例如，有必要密切关注产品和服务的评论（如应用商店的评论）以及消费者在社交网站上传播的信息，以便迅速了解消费者的反应。定期与隐私组织分享信息也很重要，这样他们就能迅速合作，处理出现的任何问题。

4.1.4 第三方组织，如内部审计部门和咨询委员会的作用

对隐私问题的风险管理是否充分进行独立监测和评估，将为彻底的内部举措提供基础，并进一步增强外部对公司的信心。例如，可以建立一个独立部门来进行行政职能和风险管理等内部审计制度。此外，应建立一个由第三方视角的外部专家组成的隐私保护咨询委员会或顾问委员会，以接受来自专家的评估和监督。这些专家可以包括学者、顾问、律师和对隐私问题有专长的消费者组织。通过设立咨询委员会，可以在服务发布前获得客观、坦诚的意见，并提前获得对可能出现的问题的适当回应的意见。专家的专业和客观的意见应反馈给管理层和员工，以便整个组织能够确保隐私问题被妥善解决。

这还可以提高对这些问题的认识。

4.2. 建立和传播业务规则

为了使 4.1 中描述的系统有效运作，在开发或提供服务或技术之前，隐私官和隐私组织需要识别并适当考虑隐私风险。重要的是，隐私官要负责在组织内部制定规则，以确保这种做法被企业所遵守。

例如，在保护隐私的措施上要明确"何时"制定，"由谁"制定评估隐私风险方面的规则[33]。然而，为了避免一刀切的做法，要确保这些原则被理解和确立，并不断审查和修订其内容。隐私官员和隐私组织需要确保这些规则在整个组织中得到传达。

4.3. 培养公司的隐私文化

为了使隐私治理系统和业务有效运作，管理层必须在整个组织内传播其既定立场，并在

[33] 就 "何时 "和 "由谁 "评估隐私风险而言。第 5.3 节"隐私风险评估（PIA）"中给出了一个例子。

整个组织内培养一种可以适当处理隐私风险的企业文化。重要的是，作为个人和消费者，公司的每一位员工都要理所当然地了解隐私问题。

最理想的状态是，这些员工有礼貌，对消费者和社会有反应。这样的文化需要持续的努力，但也需要管理层和隐私官员意识到隐私的重要性，并在任何时候都要传达出来。这些努力为公司内部专业人员队伍的发展提供了基础。

由于隐私每天都在变化，传播的文化需要适应最新的事件和商业活动。以下是与企业文化发展有关的举措的例子：

- 定期的电子学习和培训课程；
- 在诸如员工手册中，提及对隐私问题的立场；
- 分发与隐私政策相关的手册和其他材料；
- 提高认识的活动，如在内部宣传隐私官的活动；
- 对处理个人数据的部门进行强化培训；
- 利用新员工派任和部门调动的时机进行培训支持；
- 将隐私组织作为常规工作轮换过程的一部分。

4.4. 与消费者沟通

隐私治理需要与消费者的持续沟通。此外，还要随时把握消费者和社会对变化的接受程度,企业是如何积极地进行创新和隐私风险管理的?在发生实际问题时该如何应对这点上,对消费者进行积极、易懂的说明也很重要。积极采取这样的措施，从而构建与消费者之间的信赖关系，这是不可或缺的步骤。

4.4.1. 组织活动的公开与宣传

汇总企业对隐私问题的思考方式，以及如何把握、评价和控制风险，并对外公布。例如，像透明性报告(transparency report)[34]那样，积极、易懂地公布消费者特别担心的一些项目，这种方法是有效的。数据的高度利用，会产生新的隐私风险。为了消除消费者的担忧，定期汇总并发送相关信息，消费者也就可以放心地使用服务。

另外，最近关于隐私问题的企业方针以及有关利用个人数据新项目的实施方针等内容实施前向社会公布的情况也增加了。先接受来自消费者的评论，有了讨论、反映之后再实际实

[34] 透明度报告是公司定期发布的报告，以确保其数据处理对消费者的透明度。

行，开展企业的计划，这种与消费者、社会构筑信赖关系的沟通方式正在普遍化。

4.4.2. 与消费者持续沟通

案例研究 NTT ドコモ个人数据仪表板

NTT ドコモ, INC.为客户提供确认或改变他们自己提供的数据的目的地和类型的能力，以及确认他们对处理他们的数据的同意。

(来源: https://datadashboard.front.smt.docomo.ne.jp/)

不仅是定期的报告,在为新消费者添加功能和修改使用规则的同时,如何改善服务和隐私的核风险应对，并迅速地通过简单易懂的网站通知，使消费者能迅速得到信息,从而形成对服务的信赖。另外,当信息更新时向用户发送推送通知，对于不太关心隐私设定的用户通知其进行确认和修改等操作,这种企业面对消费者持续的、积极的接近是很重要的事情。

另外，鉴于隐私是可以变化的，就有必要与各种消费者接触，努力把握消费者的需求。

案例研究：日立公司和博报堂 开展对世俗信息态度的调查

日立公司和博报堂公司一直在进行一项持续的态度调查，目的是对个人态度的变化进行量化。

日立的具体举措
・日立和博报堂 "对大数据处理的消费者信息的认识调查"。
　日立和博报堂一直在进行一项持续的态度调查，目的是随着个人数据使用的不断增长，量化个人态度的变化。继2013年第一次调查和2014年第二次调查之后，2016年进行了第三次调查。
　在2016年的第三次调查中，我们调查了最新的技术趋势，包括对物联网及其使用的期望和担忧，并研究了企业应该如何回应。

(来源)https://www.hitachi.co.jp/products/it/bigdata/bigdata_ai/personaldata_privacy/index.html
(参考）"关于对大数据处理的消费者信息的态度的第五次调查
https://www. hitachi.co.jp/New/cnews/month/2020/12/1222a.html

特别是那些以数据分析为主要业务的公司,当我们和那些日常与消费者面对面接触的公司合作时,也需要提高自己的隐私保护知识，持续进行个人隐私意识调查、把握社会接受度等也是一种方法。到那个时候，不能满足于调查实施本身，将通过意识调查等方法搜集到的结果反映到本公司的措施中更加重要。

4.4.3. 发生问题时与消费者沟通

事实上，当隐私问题发生时，迅速发现问题的发生且在把握问题内容的基础上进行应对是非常重要的。因此，如 4.1 所述，包括相关部门在内，整个组织在发布服务或产品之前，必须研究并构建出发生问题时的应对流程和体制。

对于受到泄漏等实际损害的消费者和实际发生的问题，有必要将所发生的问题的内容、原因和企业为了解决问题而采取的措施在道歉的同时进行简单易懂的传达。特别是对于有可能发生二次损失的消费者，为了避免和减轻二次损失，有必要迅速实施措施(密码变更等)。因此,有必要在可能单独通知的情况下进行个别通知，而在不能单独通知的情况下，就有必要采取新闻发布等手段。另外，根据问题的性质不同，也有提供信息后反而会扩大损失的情况，因此应该与安全专家商量后提供信息。

4.5. 与其他利益相关者的沟通

在隐私治理中，持续与利益相关者沟通，关于企业创新和创造、如何积极地进行隐私风险管理,要积极地向利益相关者解释,因为保护信任关系非常重要。

4.5.1. 对利益相关者作出回应

隐私问题不仅要和消费者建立关系、还有各利益相关者。

图 9 与利益相关者的沟通

（1）商业伙伴(客户、业务委托方)

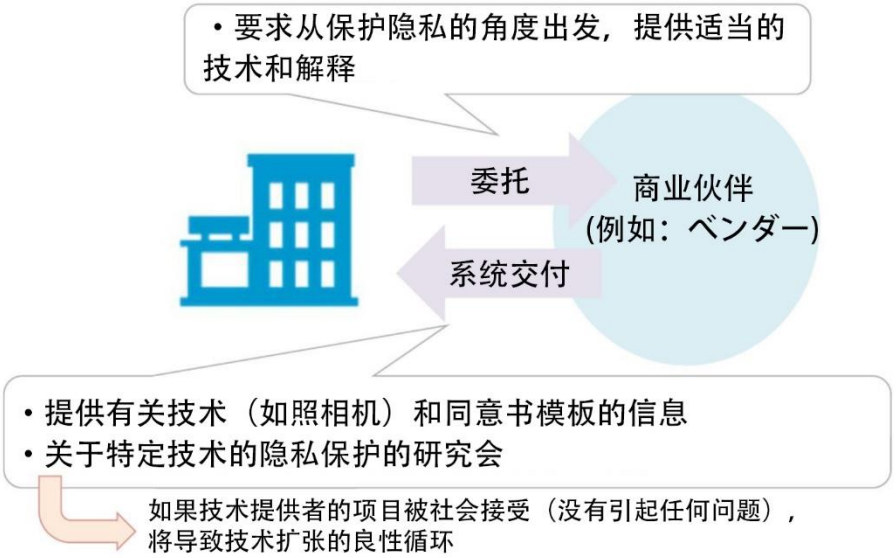
企业在推进事业的时候，有时也会与商业伙伴等多个企业合作实施。如果我们不能妥善应对包括商业伙伴在内的隐私问题，将失去包括本公司在内的相关企业及相关事业整体的信赖。

特别是随着技术的革新，新的隐私风险也随之产生，因此与供应商等系统相关的客户进行密切的交流尤为重要。以快速的技术革新和不断变化的消费者隐私问题为前提,密切沟通、不断修正消费者对隐私的担忧,在系统方面事前自查是否可以应对问题，可以进行应对是最好的情况。

作为订货方的企业，应该从保护隐私的角度出发，要求客户(供应商等)提供适当的技术

和说明；而客户在尽说明的同时，订货方的企业也要考虑到隐私问题的系统运用,主动提供有关使用技术时的隐私的指导手册、同意书的模板等,为了加深对订货方企业的理解，举办学习会也是有效的应对方法。订货方企业的服务应当以不会引发隐私问题的形式被社会所接受，客户方的技术也能因此进一步扩散，形成良性循环。

图 10 与商业伙伴沟通的例子



另外，将业务委托给其他公司的情况下，因该业务产生问题时，委托方也要承担责任。因此从保护个人隐私的角度来看，我们应该选择一个合适的代理商,并要求委托方说明与应对相关的体制、技术等,与此同时，我们也要协助委托方提高对顾客隐私的处理。发生隐私问题的时候，委托单位应该认真对待顾客和消费者。

（2）集团企业等

即使是以集团内的子公司为主体推进的事业，如果发生隐私问题，整个集团的品牌和信誉也会受损。因此,也有必要意识到其隐私问题对于整个群体的意义。

另外需要注意的是，在海外有据点的情况下，目前对隐私问题的处理在各国都有单独的处理方式，所以每个国家都有对应的必要。

（3）投资者、股东

投资者也要从对企业业绩影响和社会责任的角度出发，对于强化风险管理体制方面，要有以成本作为先行投资来提高评价的倾向[35]。对于股东和投资者，也越来越要求对企业的隐

[35] 达沃斯的 "利益相关者资本主义 "会议和美国商业圆桌会议的 BRT 宣言，为思考所有利益相关者的利益提供了动力。

私问题做出明确的说明，透明报告的制作和公布也有助于高透明度的说明。

（4）有关行政机关

平时要经常确认个人信息保护委员会等处理个人数据利益利用和个人隐私问题的行政机关的咨询窗口，在开展个人隐私风险较高的事业时，事先进行咨询是很重要的[36]。另外，根据行业的不同，需要遵守个别行业法和主管部门制定的方针，在与主管部门进行沟通的同时，要根据行业的特殊性适当运用。

（5）业界团体

根据行业的不同，为了谋求事业的健康发展，也为了加深对消费者的理解，要组成行业团体和认可个人信息保护团体去进行调查研究、宣传推广活动、发表意见、与相关部门联络、提交意见等活动。如果同行业的其他公司在相同的技术领域引起隐私问题，那么本公司同样的服务也有可能失去消费者的信赖。因此，有必要通过业界团体积极参与与隐私问题相关的信息共享活动，积极提供己方信息并获取他方信息。此外，为了有效利用所获得的信息，还需要营造良好的环境。

（6）员工等

企业经常会处理与员工隐私相关的信息，因此有必要对员工的隐私给予照顾。另一方面，有时出于安全等事业运营上的要求，也需要限制员工的隐私。另外，既然要管理有关员工的信息，就存在泄露的风险。因此，也应该将员工视为沟通的主体与其对话，通过员工代表的渠道采取说明、周知等措施很重要[37]。另外，不仅要考虑该企业的员工，还要考虑求职者、退休者、客户的员工等。

4.5.2. 收集有关隐私问题的信息

因为个人隐私每天都在变化，所以不仅要进行上述的消费者意识调查，还要关注国内外法律制度的动向，与业界团体交换信息，持续获取社会和舆论等最新动向，这是非常重要的。

特别是个人信息保护委员会的网站，个人信息保护法、相关指导手册以及问答等相关信息的发布一直在进行。另外，在日本产业部的个人信息保护网站上，过去经济产业省实施的有关个人数据的讨论结果等信息也被发布过。

另外，从顾问委员会聘请的专家和熟悉隐私问题的律师那里收集信息也是有益的做法。

[36] 由个人信息保护委员会设立的 PPC 商业支持服务台，就使用新技术的新商业模式中需要考虑的个人信息保护法问题等提供咨询，作为提高企业对个人信息保护和适当有效使用的认识的一部分。

[37] 2019 年，在招聘求职者（应届毕业生）方面出现了不当获取数据分析和使用的案例，但应该注意到，在监测雇员方面也可能出现类似的结构，不仅提供分析的一方要承担同等或更大的责任，而且使用分析的公司也要承担同样的责任。

4.5.3. 其他举措

对隐私风险的把握和应对策略的探讨,需要业界应对或跨界应对，单个公司难以应对、讨论的情况下,要以业界团体、政府、民官运营的财团为核心,召集专家，讨论适当的应对措施和需要考虑的事项，公布结果等措施也要同步进行[38]。

五、(参考)隐私风险政策

在下文中，我们提出了一些关于管理隐私风险的具体想法供参考。这里描述的想法是基于国际标准以及国际组织和国家的努力，但在公司内部使用这些想法时，最好能考虑到它们的背景、优势和劣势，逐条使用。

5.1. 识别和组织及有关各方处理的个人数据的生命周期

在开展一项新业务时，我们会确定与隐私有关的风险。为了做到这一点，首先要理清目标企业的个人数据的生命周期是什么。

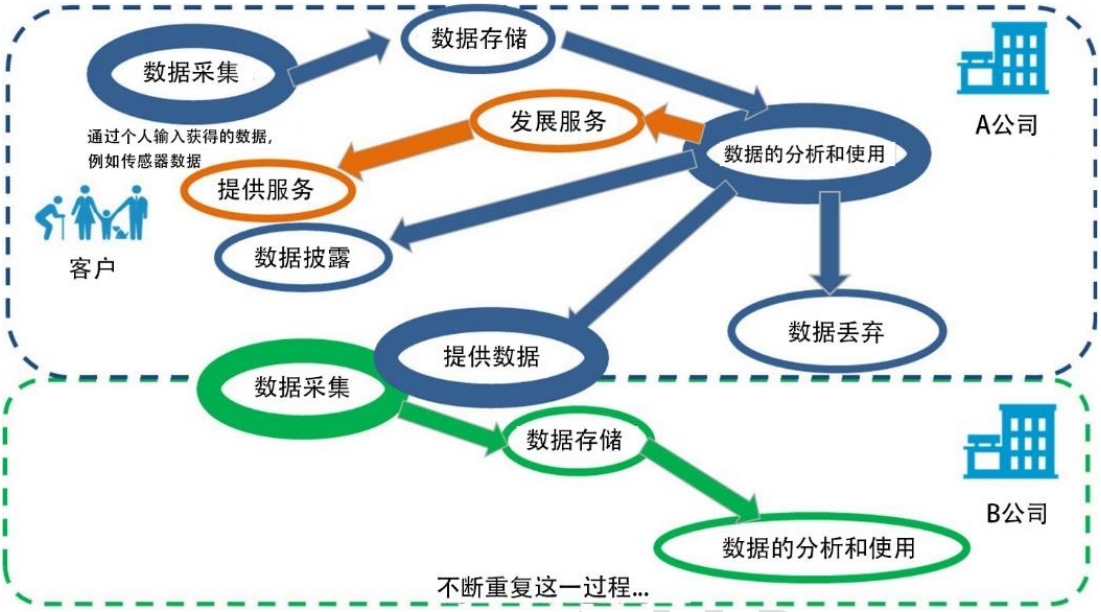
具体来说，需要梳理的要点有以下几点：

- 确定参与项目的各方（消费者、合作伙伴、承包商等)。
- 识别涵盖的企业所处理的个人数据
- 个人数据不仅包括直接获得的数据,还包括从第三方购买的数据或通过分析推断的数据。

下图说明了数据的生命周期，从获取到重新提供或处置。此外，有必要确认数据的生命周期，如哪些部分的数据将被外包，数据是否会被两个或更多的公司收购以共同使用等，并在早期阶段理清与相关业务伙伴的关系。(应该注意的是，如果在这个阶段不能确定项目的方案，则要改变要承担的责任，不仅从隐私的角度，也从法律的角度。)

[38] 审议并发布《照相机图像利用指导手册 ver2.0》（经济产业省、总务省、物联网推进联盟，2018）等。

图 11 个人数据生命周期的例子



在将目标企业的个人数据生命周期可视化的过程中，我们可以看到一些消费者容易识别的领域和一些难以识别的领域。

特别是物联网设备（如摄像头和传感器）获取的个人数据，以及通过分析推断的数据的使用等，都有可能造成隐私问题，因此有必要仔细解释个人数据的处理及其目的。

5.2. 识别隐私风险（识别隐私问题）

识别个人数据生命周期中出现隐私问题的地方，并考虑如何解决这些问题。

这里的关键点有以下几点[39][40]：

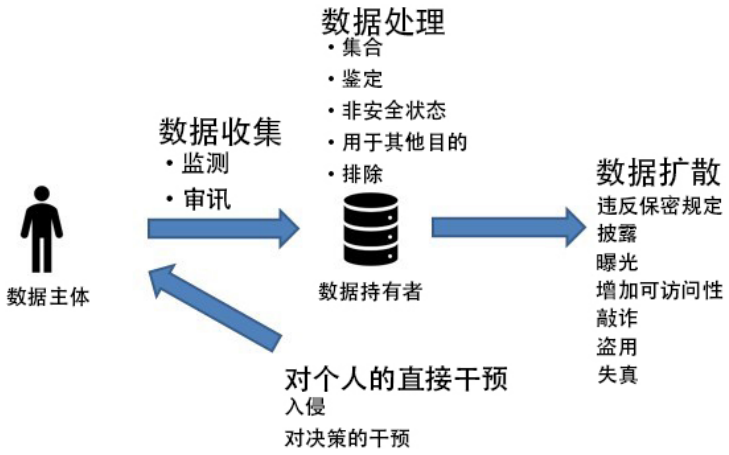
- 应采用基于风险的方法考虑隐私问题；
- 根据业务性质对隐私问题进行系统的组织；
- 使用适合组织的目标、能力和隐私问题的工具和技术来识别隐私风险。

以下是在个人数据生命周期的每个阶段可能出现的隐私问题类型的一个例子。当你确定你的项目的系统要求和操作时，你可能希望使用以下内容来确定隐私问题并考虑如何解决这些问题。

[39] 这一概念是为了确定与隐私问题相关的风险，并采取灵活的措施来应对风险。它包括对确定的风险和相关的系统和流程进行隐私影响评估，以及实施隐私风险管理实践。

[40] "ISO/IEC 29134:2017 "提供了关于进行 PIA 的过程以及 PIA 报告的结构和内容的指导手册。

图 12 造成隐私问题的活动类型



(来源：译自《隐私分类学》的图 1，DANIEL J. SOLOVE，2005。

图 13 隐私问题的例子

数据收集	监测	由于持续的监测，你是否让个人感到不安和不适?
	质询	你是否对个人施加压力，从他们手中撬出信息？这些深入的问题是否使个人是否感到被迫和焦虑?
数据处理[41]	集合	通过收集有关个人的信息碎片，揭示出个人没有想象到的新事实，从而使个人的期望落空。
	鉴定	通过将所有数据与个人联系起来，对个人有害的信息也会与数据联系起来，这是否给个人带来焦虑和挫折?
	非安全问题	个人数据是否受到不适当的保护而损害了个人利益?
	用于其他目的	在未经个人同意的情况下，你是否将数据用于原定用途之外的其他目的?
	排除	重要的决定是否是由个人控制，例如不给予披露或更正个人数据的权利吗?
数据扩散	破坏了保密关系	通过特定信任关系获得的个人数据，通过向其他公司披露，会给个人一种被背叛的感觉吗?

[41] 在以人工智能为基础的社会中，可能会从个人的行为等数据中高度准确地估计出个人的政治立场、经济状况、爱好等。以个人不希望的方式分配和使用这些数据可能会造成侵犯个人自由、尊严和平等等问题。然而，这些问题将在 "聚合 "和 "识别 "等隐私问题的背景下被感知。(《以人为本的人工智能社会原则》（促进全面创新战略理事会，2019 年）也包括一项隐私原则。)

	披露	向第三方披露个人数据是否会给二级用户带来额外的隐私问题?
	揭秘	将生活的方方面面暴露给他人，是否会造成严重的耻辱并阻碍个人参与社会的能力?
	提高可及性	它是否通过增加他人对个人数据的可及性来增加 "披露"的风险?
	恫吓	是不是有在权力的控制，威胁下，个人数据被公开，并透露给其他人的情况呢?
	剽窃行为	我们是否应该为他人的目的使用他人的身份和个性，由此使个人失去了其自己的身份，影响了其参与社会的能力?
	失真	个人是否有可能操纵他人的看法和判断方式，做出虚假和误导性的行为，从而导致耻辱、污名和名誉受损? 是不是应该限制我们自己和如何控制信息的能力? 是不是应该扭曲对自我认同和参与公共生活的能力至关重要的声誉和个性吗? 是否存在任意和不成比例地扭曲社会关系的风险?
对个人的直接干预	入侵	是不是不必要地接近个人电子邮件，电话等，妨碍个人的日常习惯，会造成不舒服和焦虑感?
	对决策的干预	当人工智能被用于个人生活中的重要决策时，决策方法不明，个人是否有寒蝉效应。

(资料来源：秘书处参照"隐私分类学"编写，DANIEL J. SOLOVE, 2005)

另一个可以参考的框架是 Fivesafe 模型，它是一种适合于隐私问题的识别隐私风险的工具。自 2003 年以来，英国国家统计局 (ONS) 一直在运作，以规范使用敏感信息的研究，作为确保数据有用和安全的一种方式。"五安全模式"在欧盟和其他国家已被广泛使用，不仅是个人统计数据使用的安全规则，也是数据使用的安全规则，在考虑隐私问题和对策时可以作为参考。

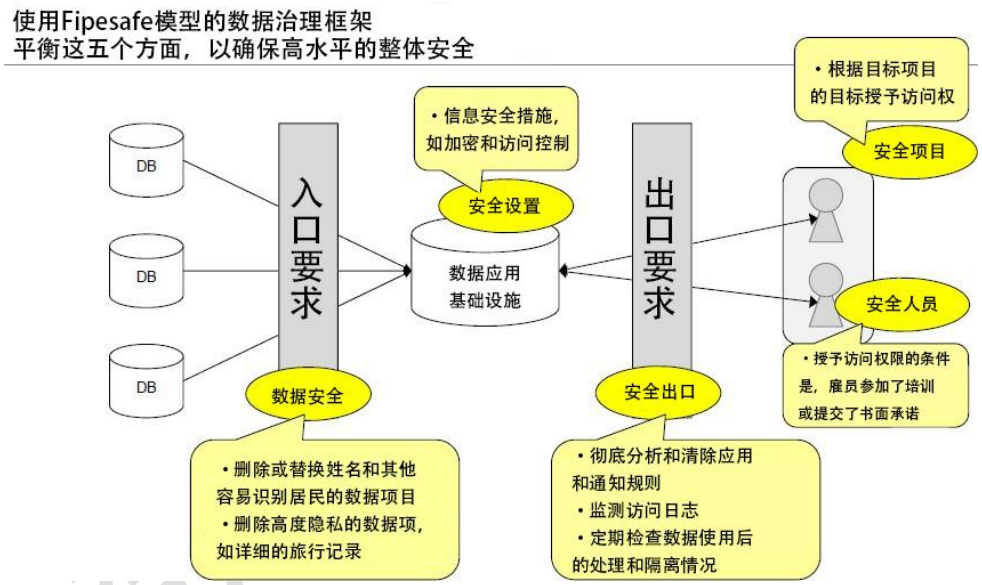
图 14 （参考）Fivesafe 模式的概述

项目	描述
安全项目	分析结果是否有保密披露的风险?
安全用户	设施环境是否限制了非批准的使用?
安全数据	数据本身是否有保密披露的风险?
安全的设备环境	能否相信研究人员会以适当的方式使用个人数据?
安全分析结果	从法律和社会的角度来看，使用数据的目的和处理数据的方式是否合适?

(来源：Tanvi Desai, et al, "Five Safes: designing data access for research")

(西英格兰大学)，2016 年

图 15 （参考）基于 Fivesafe 模型的数据治理框架



5.3. 隐私影响评估（PIA）

隐私影响评估（PIA）是一种分析、评估和应对与个人信息和隐私有关的风险的方法。

企业需要有一个机制来评估其组织内的隐私风险。当考虑一个企业时，重要的是知道“谁”和“什么时候”应该评估隐私风险。例如，如果在一项服务发布之前发现隐私风险很高，就没有时间采取行动了。反之，如果发现得太早，隐私风险可能不会出现。

下图说明了一个业务部门在发布产品或服务时可以采取的步骤。如果假设目标业务的隐私风险很高，可能会在业务审查的早期阶段和发布决定时与管理层评估隐私风险。解决隐私

风险的方法是在确定系统需求之前评估隐私风险，并采取措施确保在做出发布决定时风险已经得到缓解，如果有任何剩余风险，应提前考虑发布后的措施。在引入外部服务或从外部来源购买数据而不是在内部获取个人数据时，与你的法律部门或隐私组织在合同的法律和采购审查中评估隐私风险也可能是有用的。

图 16 （示例）发布产品或服务的步骤

何时和何人应纳入隐私风险评估机制，将因企业规模、业务性质和所处理的个人数据的性质而有很大不同，但重要的是，例如，对每种模式进行分类并制定规则[42][43]。

也可以通过整合一段时间内获得的知识，制定评估隐私风险的模板或检查单。然而，重要的是要确保团队成员理解这些原则，这样检查表和模板才不会导致一刀切的做法。它们还需要不断地被维护和审查。

ISO/IEC 29134:2017 为开展 PIA 的过程以及 PIA 报告的结构和内容提供了指导手册。

它分为三个部分："确定 PIA 的必要性"、"进行 PIA"和"跟进 PIA"，并包括"目标"、"投入"、"预期产出"和"行动"。

"实施指导手册"有详细规定[44][45]。

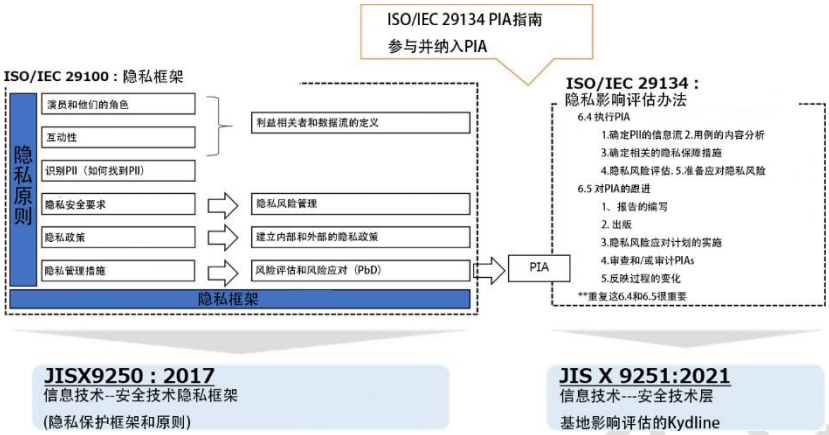
[42] 公司已经建立的系统和操作流程，以评估其他风险，如安全。在某些情况下，通过更好地利用数据管理系统（例如，通过使用 "数据管理系统"），或者优先考虑使用个人数据最多的部门，可以实现高效运作。

[43] 在敏捷开发而不是瀑布开发的情况下，产品所有者和其他利益相关者有必要不断意识到隐私问题并采取行动。同样重要的是，确保在作出决定时，风险已经得到了缓解。

[44] ISO/IEC 29134:2017 于 2021 年 1 月作为 JIS 标准发布，成为 JIS X 9251:2021。

[45] 在《个人信息保护法：所谓的三年期审查：系统性修正纲要》第三章第 2.(2)节中指出："为了促进私营部门的自愿努力，委员会还将考虑在未来采取的措施，如编写关于 PIA 的案例研究和建立一个奖励制度。报告中指出了这一点。

图 17 （参考）隐私框架（ISO/IEC 29100）和隐私影响评估（ISO/IEC 29134）



六、设计中的隐私

有一个全球标准可以作为基本隐私保护的参考，那就是隐私设计（PbD）的概念。这是一个想法，即隐私应该从一开始就建立在商业模式、技术和组织中，而不是在企业或组织中出现隐私问题时作为一种一刀切的解决方案。

1. 对隐私问题的认识以及解决这些问题的必要性
2. 应用公平信息实践（FIPs）的原则
3. 在信息技术和系统的开发过程中，在整个信息生命周期中尽早识别和缓解隐私问题
4. 信息需要由隐私领导和专家提供。
5. 除了纳入和整合隐私保护技术（PET）外，还规定了七项原则。

图 18 七项隐私设计原则的概述

原则	行动
主动/预防	要主动而不是被动，要预防而不是补救。其目的是在隐私泄露事件发生之前就加以预防。隐私设计的方法是主动的而不是被动的。 这是隐私保护和应对的一个特点。
将隐私作为默认设置	隐私保护必须在默认情况下启用。这也被称为默认隐私。隐私保护从一开始就建立在系统中。个人无需采取任何行动就能保护隐私。个人不需要采取步骤来改变他们的个人设置。
整合到你的设计中	隐私保护机制应被纳入企业或系统的设计和结构中。它不应该作为一个额外的功能在事后添加。隐私机制是企业或系统的一个组成部分。这是公司的一项核心职能。
正和，而不是零和	争取采用正和方法，为所有功能产生合法的利益和目标，而不是采用零和方法，通过建立隐私保护机制，造成权衡，如失去便利性。对于公司来说，尊重隐私可以带来各种形式的激励（例如，增加客户满意度）。此外，还可能有其他方面的激励（如声誉、商业利益）。

(来源：秘书处根据"隐私设计的七项原则"编写)

隐私设计不是一种零和的方法，即隐私保护机制会产生权衡，如失去便利性，而是一种正和的方法，即实现所有合法的利益和目标，包括对公司尊重隐私的各种形式的激励，这可以带来企业价值的增加。其目的是实现一个正和的方法，实现合法的利益和目标。

另一方面，商业和社会环境的变化可能会引起意料之外的隐私问题。另一方面，商业或社会环境的变化可能会引起最初未曾预料的隐私问题。因此，既要考虑建立隐私设计系统，也要考虑不断审查和改进该系统的过程。

七、总结

在未来，包括预期的社会 5.0，数据的使用有望成为创新的源泉，将成为未来商业活动的核心部分。

个人数据是业务的来源，但它也给公司带来了隐私方面的挑战。隐私保护是数字转型（DX）议程的一个组成部分，信任也是如此。当然，在日本，企业已经认真对待隐私保护，但大多是针对个别案例。在未来，随着数据处理的扩大，隐私问题可能会变得更加多样化和复杂，传统的方法将受到限制。隐私是社会越来越关注的问题，社会，包括消费者，开始从隐私的角度来评估和区分不同的公司。因此，如果一家公司在其任何活动中提出隐私问题，这可能会对整个公司产生严重后果。另一方面，适当处理隐私问题的公司将获得公众的信任，这将使公司获得商业优势。换句话说，虽然隐私对企业来说是必不可少的，但它不一定是一种成本。相反，它是提高产品和服务质量的一种方式，也是区别于竞争对手的一个重要因素。

本指导手册是为企业高管和负责企业战略和支持的人准备的。该指导手册确定了公司需要解决的要求和组织结构。隐私问题不能只靠企业来解决，还要处理好与社会，包括消费者的关系，比如公众对企业隐私行为的了解以及与消费者的沟通。

该指导手册将帮助公司改善其隐私做法，从而提高其产品和服务的价值，以及其自身的经济和社会价值。

应该注意的是，隐私问题不仅取决于有关的产品或服务，而且随着技术的进步和公众的兴趣而变化。在这个意义上，预计本指导手册将在必要时进行修订和更新。