锡捷翻译p21-42

(四）数据出境方确保数据安全的能力

1. 数据安全管理能力，包括管理和组织体系、制度建设、全流程管理、分类分级、应急响应、风险评估、个人信息权益保护规则及其实施等；

锡捷上海和锡捷新加坡以及整个锡捷组织都有一个确定的数据安全计划，由法律部门的数据治理部门和IT部门中的信息安全部门为其提供支持。IT部门的信息安全部负责实施和执行全球企业基础设施的系统安全、网络安全和相关IT安全。此外，信息安全部的职责还包括：

- 在公司内部进行研究，制定网络安全和数字运行的原则和准则。

- 为网络安全政策和数据管理的实施提供指导。

- 协调和解决与网络安全、数字运营和其他相关事宜有关的重要问题。

- 采取措施防止数据泄露，将数据泄露的风险降到最低。

锡捷上海已指定副总裁、首席合规官兼公司秘书Laurie Webb担任数据保护官，负责管理法律合规，包括数据治理、数据保护和隐私。锡捷采取以下政策：

1. 维持数据保护合规管理体系，明确数据处理合规的责任主体和责任，梳理管理流程，制定相关合规准则；

2. 明确数据分类和分级的原则和标准，并开展数据分类工作；

3. 在主动防御、持续监测、事后审计、安全宣传教育等方面加强网络与信息安全防护。

这些政策包括：

11-9001 数据治理原则政策： 锡捷的数据保护和隐私原则的目的是建立一个统一的全球隐私合规和锡捷数据保护的方针。

11-9002 隐私审查政策： 本政策的目的是让业务请求者和工作人员了解隐私审查程序和要求，并使业务请求者能够进行隐私审查程序。

11-9003 数据主体权利请求政策： 本政策正式确定了处理数据主体请求的全球通用的程序，以行使适用法律所赋予他们的个人数据有关的权利。

11-9200 数据分类政策： 该政策为保护锡捷和锡捷合作伙伴创建、使用、存储、处理和/或传输的信息提供了一个分类方案和框架。

07-600.07 IT分类数据处理标准：本标准的目的是确定如何对锡捷所处理的的信息进行分类。

06-8006 员工记录和个人数据隐私：概述了如何维护员工信息以及对信息访问和发布的要求。

适用于锡捷上海和锡捷新加坡以及锡捷组织结构中其他锡捷实体的隐私声明在<https://www.seagate.com/cn/zh/>中，并包含在附录A中。

2. 数据安全技术能力，包括从数据收集、存储、使用、处理、传输、提供、披露和删除的整个过程中所采用的安全技术和方法；

锡捷上海和锡捷新加坡以及整个锡捷组织的信息系统都是根据严格的权限控制策略来管理的。系统操作人员必须通过内网登录系统，并在规定的操作权限内进行操作。

锡捷上海，作为一个较大的锡捷组织，设立一个跨职能的企业安全风险管理小组，每季度召开一次会议，针对信息安全和数据治理等领域进行职能问责。该小组在锡捷董事会审计委员会的监督下，找出公司在技术、流程和培训方面需要进行改进的地方。

网络名称、服务提供商和其他相关细节在第二节所列的表格中提供。5. 向外传输数据的链接。

锡捷上海在执行某些必要的处理流程时会保留用户的个人信息。在完成处理流程后，个人信息将会被保留到相关法律法规所规定的时间，或为了锡捷的某些法律行为(例如适用的时效、诉讼或监管调查)进行保留。

锡捷在全球范围内遵循一个统一的记录保留政策，其定义如下：

11-160 记录保留政策： 该政策正式确定并概述了各种数据集类别、记录保留说明和相关的代码。在此基础上，我们将尽职调查数据销毁情况。

3. 对数据安全保障措施的有效性进行认证，包括已进行的数据安全风险评估、数据安全能力认证、数据安全检查和评估、数据安全合规性审计和网络安全分级保护评估。

锡捷通过适用于锡捷新加坡公司的常规审计来维持可信商业联盟(Responsible Business Alliance，RBA)认证。RBA认证包含与数据安全有关的领域，以及其他领域。RBA认证的数据安全领域包括：

* 合理保护与他们有业务往来的相关人员（包括供应商、客户、消费者和员工）的个人隐私信息。
* 在收集、储存、处理、传输和共享个人信息时遵守隐私和信息安全法律和监管要求。
* 管理系统需要具有以下要素：

o公司承诺

o管理责任和义务

o法律和客户要求

o风险评估和风险管理

o改进目标

o培训

o沟通

o员工反馈、参与、申诉

o审计和评估

o纠正措施流程

o文件和报告

4. 遵守有关数据安全和网络安全的法律法规

锡捷上海在过去两年中没有受到数据和网络安全监管部门的任何行政处罚，也没有受到任何个人或企业

根据数据和网络安全法律法规做出的有效司法裁决的司法索赔。

锡捷上海坚持遵守有关数据安全和网络安全的适用法律和法规。

请参阅附录B，了解锡捷公司为《中华人民共和国个人信息保护法》中规定的数据主体权利而提供的受理表截图。

(V) 境外接收方

1. 境外接收方的基本信息；

锡捷新加坡国际有限公司总部成立于1997年1月3日，注册地址为90 Woodlands Avenue 7, Singapore 737911(兀兰7道90号，新加坡邮区737911)。注册号码为199700025H。

2. 境外接收方处理数据的目的和方法；

1. 目的

锡捷上海有必要将通过锡捷上海的业务运营所收集的消费者个人信息转移到锡捷新加坡总部支持的管理系统，以确保质量、服务、可用、数据安全的有效性和一致性。

锡捷上海也有必要将通过锡捷上海的人力资源管理活动所收集到的雇员个人信息转移到锡捷新加坡总部的综合人力资源管理系统中，以用于锡捷的全球人力资源管理，包括评估雇员的表现、控制人事的费用、协调人员的工作安排以及为雇员提供薪资和福利。这些综合系统提供了一个高效的全球企业平台，消费者服务和人力资源管理活动可以在这个平台上进行统一操作和管理。整合后的系统和数据降低了数据的分散性，通过集中式的应用技术和组织方法，提升了数据安全和风险处置方面的能力。

2. 方法

锡捷使用Consumer Identity Access Management（CIAM）、Product Registration、Salesforce和Oracle Eloqua应用程序来接收和处理消费者的个人信息。它们为消费者提供一系列相关服务，包括用于保修服务的产品注册、可选的营销电子邮件、以及为中国消费者提供的用以确保质量、服务、可用、数据安全的有效性和一致性的客户服务票据追踪服务。

锡捷使用SAP SuccessFactors应用程序来接收与员工有关的个人信息。该系统用来进行中国的人力资源管理工作，包括员工入职和离职管理、职位管理、工资管理和福利计划管理，以确保质量、服务、可用、数据安全的有效性和一致性。

3. 境外接收方的数据安全保障措施；

1. 数据安全管理能力

锡捷上海，作为一个较大的锡捷组织，设立一个跨职能的企业安全风险管理小组，每季度召开一次会议，针对信息安全和数据治理等领域进行职能问责。该小组在锡捷董事会审计委员会的监督下，找出公司在技术、流程和培训方面需要进行改进的地方。

锡捷新加坡和整个锡捷组织都有一套固定的由法律部门的数据治理团队和IT部门的信息安全团队支持的数据安全体系。其中IT部门的信息安全团队负责保障全球范围内企业基础设施的系统安全、网络安全和相关IT安全。此外，信息安全部的职责还包括：

* 在公司内部研究并制定用于网络安全和数字操作的准则。
* 对网络安全政策和数据管理的实施提供指导。
* 协调和解决与网络安全、数字运营和其它安全事项有关的关键问题。
* 采取措施防止数据泄露，并尽量减少数据泄露的风险。

锡捷的政策是

1. 维持数据保护合规管理体系，明确数据处理合规的责任主体和相关责任，梳理管理流程，制定相关合规指引；

2. 明确数据分类分级的原则和标准，并开展数据分类工作；

3. 在主动防御、持续监测、事后审计、安全宣传教育等方面加强网络与信息安全保护。

这些政策包括：

11-9001 数据治理原则政策： 锡捷的数据保护和隐私原则的目的是建立一个统一的全球隐私合规和锡捷数据保护的方针。

11-9002 隐私审查政策： 本政策的目的是让业务请求者和工作人员了解隐私审查程序和要求，并使业务请求者能够进行隐私审查程序。

11-9003 数据主体权利请求政策： 本政策正式确定了处理数据主体请求的全球通用的程序，以行使适用法律所赋予他们的个人数据有关的权利。

11-9200 数据分类政策： 该政策为保护锡捷和锡捷合作伙伴创建、使用、存储、处理和/或传输的信息提供了一个分类方案和框架。

07-600.07 IT分类数据处理标准：本标准的目的是确定如何对锡捷所处理的的信息进行分类。

06-8006 员工记录和个人数据隐私：概述了如何维护员工信息以及对信息访问和发布的要求。

2. 数据安全技术能力

锡捷新加坡公司作为更大的锡捷组织的一部分，执行一个由专门团队领导的内部数据保护计划，该团队维持一个数据分类框架，为锡捷内部所有数据实施适当的保护协议。通过对整个数据生命周期（创建、存储、使用、共享、归档和销毁）的常规评估，数据保护团队实时关注新出现的风险和提供额外保护措施的机会。数据保护团队通过严格的政策、精确的流程和强大的技术，以保护锡捷的数据免受未经授权的访问、破坏和损失。

锡捷利用市面上的设备和行业内的标准技术来维护网络安全，包括防火墙、入侵检测和预防系统、访问控制技术。

例如，对锡捷网络的网络防火墙基础设施的访问必须根据 "按需知密(need-to-know) "和 "最小权限(least-privilege)"的原则进行限制。只有在获得首席信息安全官的明确批准后，才能访问网络防火墙的基础设施文件。防火墙的运行必须通过全天候的监控和寻呼来维护为每个网络区域定义的可用性要求。

另一个例子是，所有包含人力资源数据的系统必须限制只允许被授权的个人访问。必须进行充分的认证以确保访问数据的人的身份。必须保持足够的日志记录，以记录访问的时间和范围。

锡捷在相关系统上安装和维护最新的终端保护软件，并进行定期的终端保护监控和系统扫描，以保护规定范围内的信息免受潜在的威胁和风险，并防止对信息的未经授权的访问或使用。

3. 数据安全认证

锡捷通过适用于锡捷新加坡公司的常规审计来维持可信商业联盟(Responsible Business Alliance，RBA)认证。RBA认证包含与数据安全有关的领域，以及其他领域。RBA认证的数据安全领域包括：

* 合理保护与他们有业务往来的相关人员（包括供应商、客户、消费者和员工）的个人隐私信息。
* 在收集、储存、处理、传输和共享个人信息时遵守隐私和信息安全法律和监管要求。
* 管理系统需要具有以下要素：

o公司承诺

o管理责任和义务

o法律和客户要求

o风险评估和风险管理

o改进目标

o培训

o沟通

o员工反馈、参与、申诉

o审计和评估

o纠正措施流程

o文件和报告

(以下未修订)

4. 数据安全保护政策和法规以及海外接收方所在国家或地区的网络安全环境；以及

海外接收方--希捷新加坡位于新加坡，新加坡有自己的《2012年个人数据保护法》（"PDPA"），也有《2018年网络安全法》（"CSA"）。

4.1 《PDPA》和《CSA》的出台

4.1.1 《个人数据保护法

PDPA包含两套主要条款，涉及数据保护和拒收电话登记处。它于2012年首次颁布，并于2020年修订，修正案于2021年2月1日开始生效。除《个人隐私法》外，包括《2021年个人数据保护条例》在内的附属立法的修正案也于2021年2月1日开始生效。

虽然《个人信息保护法》没有使用 "个人信息处理者 "的概念，而是在定义受《个人信息保护法》义务约束的实体时使用了更广泛的术语 "组织"，但《个人信息保护法》将 "组织 "定义为 "任何个人、公司、协会或法人或非法人团体，无论是否（a）根据新加坡法律成立或认可；或（b）在新加坡居住、拥有办事处或营业场所。同样，PDPA没有使用 "受托方 "一词，而是使用 "数据中介 "一词，PDPA将其定义为 "代表另一组织处理个人数据的组织，但不包括该另一组织的雇员。

组织的主要义务是：

各组织必须遵守PDPA第三部分至第五部分所规定的PDPA的十项数据保护条款。这十条数据保护条款如下：

同意的义务

目的限制

通知

提供信息

数据主体访问和纠正个人数据的权利

数据准确性义务

 数据安全义务

数据保留限制义务

数据传输限制

数据泄露通知义务

问责义务

组织机构必须实施合理的技术和安全措施，以防止未经授权的访问、收集、使用、披露、复制、修改或处置，以及存储个人数据的任何存储介质或设备的丢失。

然而，《隐私保护法》并没有为数据主体提供删除的权利。关键概念咨询准则》阐明，个人可以撤回对收集、使用或披露其个人数据的同意，但《隐私保护法》并不要求组织应要求删除或销毁个人数据。相反，只有在以下情况下，组织才需要删除个人数据：(i)收集数据的目的已不再需要保留，以及(ii)保留数据对商业或法律目的来说是不必要的。

根据《隐私保护法》，所有组织都必须任命一名DPO，其业务联系信息必须公开。虽然DPO不需要在新加坡实际存在，但他们应该可以从新加坡随时联系到，并在新加坡的工作时间内运作。

PDPA规定，对于数据中介为其目的而处理的个人数据，一个组织将承担与该组织本身处理的个人数据相同的义务。此外，如果数据中介位于海外（即新加坡以外），转移限制义务将适用，要求该组织确保（接收方）数据中介受法律上可执行的义务（如合同）的约束，以提供与《隐私保护法》规定的保护标准相当的保护。

PDPA规定，一个组织不得将个人数据转移到新加坡以外的国家或地区，除非符合PDPA和PDPR 2021规定的要求，其中规定了一个组织可以将个人数据转移到海外的条件。

如果一个组织已经采取了适当的步骤，确保海外接收方受到法律上可执行的义务或指定的认证的约束，为被转移的个人数据提供与《隐私保护法》规定的保护标准相当的保护，则该组织可以向海外转移个人数据。

对不遵守《隐私保护法》的惩罚：

PDPA规定，在不遵守规定的情况下，PDPC可能会发出行政和货币处罚。根据违规情况，刑事检控局可处以最高100万新元（约5,353,319日元）的罚款，或该组织在新加坡的年营业额的10%（如果该组织在新加坡的年营业额超过1,000万新元（约53,533,190日元），以高者为准。修订后的经济处罚上限将不早于2022年10月1日生效。

4.1.2 CSA

2018年网络安全法》（"CSA"）和《2018年网络安全（关键信息基础设施）条例》（"网络安全条例"）规定了新加坡网络安全的监管框架。

CSA规定任命一位网络安全专员，他是新加坡网络安全监管机构--新加坡网络安全局的官员，拥有广泛的权力来监管新加坡的网络安全。虽然网络安全局拥有适用于所有计算机或计算机系统的权力，但CSA特别对在新加坡提供基本服务的关键信息基础设施（'CII'）的所有者规定了网络安全义务，例如在能源、信息通信、水、医疗保健以及银行和金融等部门。

CSA还为某些网络安全服务提供商提供了一个许可框架。

除了CSA之外，1993年《计算机滥用法》（"CMA"）将某些涉及未经授权访问、修改或阻碍使用计算机和计算机材料的行为定为犯罪。

关于网络安全的监管机构，除了网络安全局，还有其他对网络安全事务有权力或法律责任的监管机构，如个人数据保护委员会（'PDPC'）、监管新加坡信息通信和媒体部门的信息通信媒体发展局（'IMDA'）、作为金融监管机构和中央银行的新加坡金融管理局（'MAS'）、监管新加坡电力和天然气行业以及地区冷却服务的能源市场管理局（'EMA'）。