华为云墨西哥隐私遵从性指南

文档版本 1.0

发布日期 2022-06-07

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 概述

1.1 适用范围

本文档提供的信息适用于华为云在墨西哥合众国（以下简称“墨西哥”）开放的产品和服务。

1.2 发布目的

本文档旨在帮助客户了解：

- 华为云隐私保护责任模型；
- 墨西哥隐私相关的法律法规；
- 基于责任模型，华为云自身关于墨西哥隐私法律法规的遵循性；
- 华为云在隐私管理上已实现的控制和成效；
- 基于责任模型，墨西哥隐私法律法规管辖下的客户须遵循的责任与义务；
- 如何利用华为云的安全产品或服务实现对墨西哥隐私相关的法律法规的遵从。

1.3 基本定义

- **个人数据**

  有关已识别或可识别的自然人的任何信息。当一个人的身份可以通过任何信息直接或间接地确定时，他或她的身份就被认为是可识别的。

- **敏感个人数据**

  涉及其数据拥有者最私密领域的数据，或其不当使用可能引起歧视或给数据拥有者带来严重风险。包括但不限于可能揭示种族或民族血统、目前或未来的健康状况、遗传信息、宗教、哲学和道德信仰、政治观点和性取向等方面的个人数据。

- **数据控制者**
  - 决定处理个人数据的个人或私人法人实体。（《保护私人持有的个人数据联邦法》中的定义）
  - 决定处理个人数据的义务主体，即行政、立法和司法部门、自治机构、政党、信托机构和公共基金的任何当局、实体、机关和机构。（《保护义务主体持有的个人数据联邦法》中的定义）。

- **数据处理者**
  - 代表数据控制者单独或与他人共同处理个人数据的个人或法人实体。（《保护私人持有的个人数据联邦法》中的定义）
  - 在数据控制者组织之外，代表控制者单独或与他人共同处理个人数据的自然人或公共或私人法律实体。（《保护义务主体持有的个人数据联邦法》中的定义）。
- **数据拥有者**

  个人数据所对应的自然人。
- **ARCO权利**

  访问、更正、取消和反对处理个人数据的权利。
- **取消**

  是指数据控制者停止对个人数据的处理，取消的动作会导致一段时间的封锁期。
- **封锁**

  一旦收集个人数据的目的已经完成，就仅对这些数据进行识别和保留，封锁期间唯一的目的是确定与其处理有关的可能责任，直到法律或合同规定的时效期限。在此期间，个人数据可能不会被处理，一旦过了这个期限，这些数据将从相应数据库中抑制。
- **抑制**

  根据适用的保留规定，在数据控制者事先制定的安全措施下，消除、清理或销毁个人数据的活动。
- **华为云**

  华为云是华为的云服务品牌，致力于提供稳定可靠、安全可信、可持续创新的云服务。
- **客户**

  与华为云达成商业关系的注册用户。
- **帐户信息**

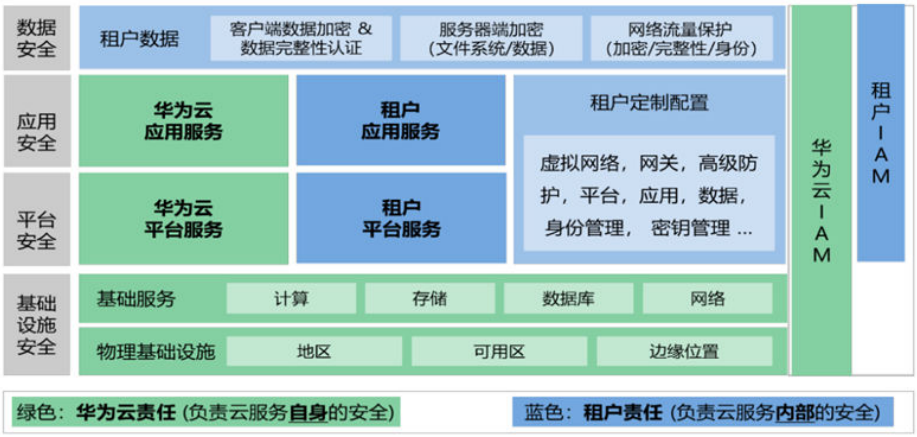
  客户在创建或管理其华为云帐户时向华为云提供的个人数据，例如客户的姓名、电话号码、电子邮件地址、银行账户信息和账单信息等。对于账户信息中的个人数据，华为云是数据控制者。
- **内容数据**

  客户使用华为云服务过程中存储或处理的内容，包括但不限于数据、文件、软件、图像、音频、视频等类型的数据。

2 云服务的隐私保护责任界定

在复杂的云服务业务模式中，隐私保护不再是某一方单一的责任，需要租户与华为云共同努力。基于此，华为云为帮助租户理解双方的隐私保护责任边界、避免出现隐私保护真空区而提出了责任共担模型。在模型中租户与华为云具体负责的区域可参见下图。

图 2-1 责任共担模型



基于责任共担模型，华为云与租户主要承担如下的隐私保护责任：

华为云：作为云产品、云服务提供商（Cloud Service Provider，简称CSP），一方面负责自身运营过程中收集和处理的租户个人数据的安全与合规，另一方面负责为租户提供安全、合规的云服务相关的基础设施、云平台以及软件应用，也就是负责**平台安全**。

- **租户隐私保护：**华为云识别并保护租户的个人数据。从公司政策、流程、操作层面制定了隐私保护策略，并采取匿名化、数据加密、系统及平台安全防护等措施，全面保护租户个人数据的安全。
- **平台安全及租户安全支持：**华为云负责在云服务中涉及到的基础平台及设施的安全与合规，并确保华为云的应用安全、平台安全水平遵从适用的隐私保护法规的要求。同时华为云为租户提供多种隐私保护技术及服务，包括访问控制和身份认证、数据加密、日志和审计等功能，帮助租户根据业务需求进行隐私保护。

租户：作为云产品、云服务的购买方，将决定如何使用相关产品或服务，也决定如何利用云产品或服务存储和处理内容数据，包括其中可能的个人数据，因此租户负责内容数据的安全与合规，也就是负责内容安全。

- **内容数据保护：**租户应正确、全面地识别云端的个人数据，制定可保护个人数据的安全及隐私的策略并选择恰当的隐私保护措施。具体措施包括根据业务和隐私保护的需求进行安全配置工作，例如操作系统配置、网络设置、安全防护、数据库加密策略等，设置恰当的访问控制策略和密码策略。
- **数据拥有者权利响应：**租户应保障数据拥有者的权利，响应数据拥有者的请求，当发生个人数据泄露事件时，应遵循法规要求采取恰当的行动，例如通知监管部门、通知数据拥有者、采取缓解措施等。

3 墨西哥隐私法律法规概述

3.1 立法背景介绍

2009年，墨西哥宪法修正案中承认了保护个人数据是一项基本权利。随即，国会颁布了《保护私人持有的个人数据联邦法》（《私人数据保护法》），该法于2010年7月6日生效，《私人数据保护法》是一部综合性的数据保护法，规定了所有私人主体在处理任何个人数据时应遵循的原则和最低标准。随后在2011年12月22日颁布了《保护私人持有的个人数据联邦法的条例》，条例旨在澄清《私人数据保护法》中规定的原则和义务的范围。

2017年1月27日颁布了《保护义务主体持有的个人数据联邦法》（《义务主体数据保护法》）。该法为在联邦、州和市一级行政、立法和司法部门、自治机构、政党、信托机构和公共基金的任何当局、实体、机关和机构保护个人数据制定了法律框架。

3.2 华为云在墨西哥隐私法律法规下的角色

墨西哥两部个人数据保护法主要的区别在于受其监管的主体不同。《保护私人持有的个人数据联邦法》及其条例适用于处理个人数据的私人主体，包括个人及私人法人实体。《保护义务主体持有的个人数据联邦法》适用于联邦、州和市一级行政、立法和司法部门、自治机构、政党、信托机构和公共基金的任何当局、实体、机关和机构。法律监管的行为为在物理或电子媒体中的个人数据的任何处理，无论其创建的形式或方法、媒体类型、处理、存储或组织。

华为云作为在墨西哥提供公有云服务的法人实体，符合《私人数据保护法》定义的私人主体，需要遵循《私人数据保护法》及其条例中的要求。同时根据《义务主体数据保护法》中规定的数据处理者的义务，当华为云的客户属于义务主体时华为云需要遵循该法对数据处理者的要求。

华为云处理的个人数据主要包括客户内容数据中的个人数据和客户在使用华为云进行包括但不限于注册、购买服务、实名认证、服务支持等操作时提供的个人数据。客户有内容数据的控制权，在处理内容数据中的个人数据时，华为云一般作为数据处理者。在处理客户创建或管理华为云帐号时提供的个人数据时，华为云作为数据控制者。

- **华为云作为数据控制者**

当客户使用华为云进行包括但不限于注册、购买服务、实名认证、服务支持等操作时，华为云会基于客户服务的目的向客户收集个人数据，包含姓名、地址、证件号

码、银行账户信息等内容。华为云将负责该部分客户个人数据的安全及隐私保护，确保个人数据的收集、处理、存储过程符合法律规定，响应数据拥有者权利申请，基于墨西哥个人数据保护法要求的有限度披露以及努力避免个人数据泄露事件的发生。

- **华为云作为数据处理者**

当客户为负责处理个人数据的实体而使用华为云服务或应用处理其内容数据中的个人数据时，华为云的角色为数据处理者。华为云代表客户根据个人数据处理协议或负责处理个人数据的实体指令处理个人数据。

4 华为云如何遵从墨西哥隐私法律法规的要求

4.1 华为云隐私承诺

华为云以网络安全和隐私保护作为最高纲领，将网络安全和隐私保护融入到云服务中，承诺尊重和保护客户隐私的同时为客户提供稳定、可靠、安全、值得信赖及可持续的服务。

华为云郑重对待并积极承担相应责任，以遵守全球隐私保护法律法规。华为云建立专业的隐私保护团队、建立并优化流程、积极开发新技术、不断构建隐私保护能力以实现华为云的隐私保护目标：遵守严格的服务边界保护客户个人数据安全，助力客户实现隐私保护。

4.2 华为云隐私保护基本原则

- **合法、正当、透明**

  华为云以合法、正当、对个人数据拥有者透明的方式处理个人数据。

- **目的限制**

  华为云基于具体、明确、合法的目的收集个人数据，不以与此目的不相符的方式做进一步处理。

- **数据最小化**

  华为云在处理个人数据时应遵循数据处理目的，且是必要的、适当的。华为云尽可能对个人数据进行匿名或化名处理，降低对个人数据拥有者的风险。

- **准确性**

  华为云确保个人数据的准确性，并在必要的情况下及时更新。根据数据处理的目的，采取合理的措施确保及时删除或修正不准确的个人数据。

- **存储期限最小化**

  华为云在存储个人数据时不超过实现数据处理目的所必要的期限。

- **完整性与保密性**

  华为云根据现有技术能力、实现成本、隐私风险程度和概率采取适度的技术和组织措施确保个人数据的安全性，包括防止个人数据被意外或非法损毁、丢失、篡改、未授权访问或披露。

- **可归责**
  华为云负责且能够对外展示遵从上述原则。

4.3 华为云遵从墨西哥《保护私人持有的个人数据联邦法》及其条例的措施

基于华为云业务的特性，根据墨西哥《保护私人持有的个人数据联邦法》及《保护私人持有的个人数据联邦法的条例》的要求，华为云作为处理个人数据的法人实体，在不同场景下承担数据控制者和数据处理者两种角色。华为云积极响应并履行自身的义务，采取了如下隐私保护机制及技术以遵循墨西哥《保护私人持有的个人数据联邦法》的要求。以下华为云适用的具体要求融合了法律的要求以及条例的补充说明。

核心要求	华为云适用的具体要求 （作为数据控制者）	华为云采取的措施

遵守个人数据处理原则的措施	华为云必须遵守法律规定的合法性、同意、信息、质量、目的、忠诚、相称性和问责制等原则。为实现此目的，华为云可使用标准、最佳国际惯例、公司政策、自我规管安排或任何其他被认为足以实现这一目的的机制。 措施应至少包括： 1. 编制在华为云组织内具有约束力和可执行性的隐私策略和方案。 2. 实施培训计划，旨在培养、更新和提高人员对保护个人数据义务的认识。 3. 建立内部监督和监测系统，并进行外部检查或审计，以核实对隐私策略的遵守情况。 4. 为实施隐私方案和策略提供专门的资源。 5. 实施一个程序，以处理因实施新产品、服务、技术和商业模式而对个人数据保护造成的风险，并减轻这些风险。 6. 定期审查安全策略和方案，以确定所需的修改。 7. 建立接受和回应数据拥有者问题和投诉的程序。 8. 建立遵守隐私策略和计划的机制，以及对违反策略和计划的制裁机制。 9. 建立保护个人数据的措施，即一组技术和管理行动，使华为云能够确保遵守法律和条例规定的原则和义务。 10. 建立个人数据的追踪措施，即允许在处理个人数据时进行追踪的行动、措施和技术程序。	华为云已根据ISO 27701国际标准要求建立了隐私信息管理体系（PIMS）用于组织范围内的隐私管理，实施文档化的隐私政策和程序为个人数据处理提供指导。华为云至少每年审查一次信息安全及隐私信息管理体系文档，并根据需要予以更新，以反映业务目标或风险环境的变更情况。信息安全及隐私保护政策和程序的变更需要获得高级管理层的审批。 为有效地识别和控制隐私风险，华为云在云服务各项业务中广泛地开展隐私风险分析和管理工作。华为云要求在所有业务处理个人数据前必须开展隐私风险分析（PIA），主要包括识别业务涉及的个人数据项、业务场景及处理过程、合规分析、对数据拥有者可能产生的影响、风险分析并制定风险控制措施和计划等，只有将隐私风险降低至可接受的水平后才能开展业务。 对于云服务，我们要求在云服务规划阶段即开展PIA，并在设计活动中对隐私风险进行详细的分析，并将所有隐私风险控制需求落入设计方案中。 华为云建立了正式的、定期的审计计划，包括持续的、独立的内部和外部评估，内部评估持续追踪控制措施的有效性，外部评估以独立审核员身份进行审计，以验证华为云控制环境的实施和运行有效性。同时华为云每年定期开展管理评审，识别体系运行过程中的问题并实施整改，推动管理体系的持续改进。 华为云制定了自上而下的治理结构，由领导层决策和审批信息安全及隐私保护策略和目标、信息安全及隐私保护相关角色和职责，制定相应的信息安全计划、分配执行信息安全活动所需的资源，同时为体系内其他角色提供支持，促进体系持续改进。 在个人数据处理的追踪方面，华为云通过日志记录和审计技术对关键系统的访问操作进行监控和审计。

		华为云建立了自己的培训机制，根据不同的角色、岗位为员工设计合适的培训方案。新员工转正前必须通过有关信息安全与隐私保护的上岗培训和考试；在岗员工需根据不同业务角色，选择相应课程进行学习与考试，其中一般员工的培训频率为至少每年一次，核心岗位员工培训频率更高。管理者需参加网络安全培训和研讨。针对安全及隐私意识，华为云对全员进行相关培训，以帮助员工了解组织信息安全及隐私保护方针及政策等，同时员工须承诺遵守公司各项政策和制度要求。 华为云已制定并实施违规政策，可供所有员工进行查看学习，并定期组织培训提升员工对违规行为、违规后果、惩罚措施的了解。 华为云对外提供了**统一的沟通接口**，负责收集并处理客户的投诉。任何用户均可通过多种渠道进行服务咨询、意见反馈和投诉建议，除了站内**在线客服**和投诉建议热线电话外，客户也可以通过华为云官网**提交工单**提出问题或进行投诉，华为云将根据内部制定的客户投诉处理流程及时处理客户的投诉。

隐私声明	华为云应在收集个人数据前通过隐私声明向数据拥有者告知向其收集的个人数据以及处理目的，尤其是有关于营销、广告或商业探索的处理以及被用于无需人工干预的决策的处理。隐私声明中还应该包括华为云的公司名称及地址、对个人数据进行的任何传输、以及当华为云使用远程或本地电子、光学或其他技术手段的通信机制自动获得个人数据时，这种技术的使用和数据拥有者反对其使用的方式。允许数据拥有者对隐私声明中所述内容表示拒绝、限制数据使用或披露以及撤回同意的机制、行使数据拥有者权利的方式、向数据拥有者通知隐私声明变更的方法、对敏感个人数据的处理等也应通过隐私声明传达。 可通过口头、纸质、电子化、视频或音频格式或任何其他技术将隐私声明提供给数据拥有者。隐私声明必须简单且包含必要信息，语言、结构和设计清晰且利于理解。 如果个人数据不是直接从数据拥有者处获得的，华为云必须将隐私声明的更改通知数据拥有者。在无法向数据拥有者提供隐私声明的情况下，或者由于数据拥有者的数量过大或数据的年限过长而付出不成比例的付出的情况下，华为云可以向监管机构（国家透明度、获取信息和个人数据保护研究所INAI）提出请求，在获得授权后利用大众传播媒体实施补偿措施。	在客户注册帐号时，华为云会向客户展示**《隐私政策声明》**，客户可自愿主动勾选同意。**《隐私政策声明》**中包含包括发送营销信息在内的数据处理目的以及对敏感数据的处理及其目的，且向用户告知其数据拥有者权利，包括反对处理及撤回同意的权利，以及行使权利的方式。 如果购买服务或者售后服务涉及隐私声明中以外的个人数据收集或者个人数据使用目的，将在该产品的产品协议中提供额外的隐私声明，并获得数据拥有者的同意。当产品或服务收集的个人数据范围或使用目的发生变化时，将对隐私声明进行更新，并重新获取数据拥有者的同意。 华为云收集个人数据基于提供服务的必要性。收集个人数据的目的原则包括：用户同意、合同执行、法务合规、保护组织的合法利益、保护数据拥有者或他人的重要利益。

数据拥有者的同意	所有个人数据的处理均应获得经数据拥有者同意。除非法律要求数据拥有者明确表示同意，否则默许同意一般情况下是有效的。如果数据拥有者没有对隐私声明表示反对，可视为其对数据处理的默许同意，前提是隐私声明中包含足够的信息。 如果华为云打算处理数据用于与隐私声明中所述目的之外的不相容或类似的其他目的，则必须再次获得数据拥有者的同意。数据拥有者可以拒绝或随时撤销对数据处理的同意，也可以反对为不必要的目的处理其数据。但数据拥有者的拒绝、撤销同意或反对处理不会终止基于必要目的的处理以及以华为云和数据拥有者之间的法律关系为基础的处理。	在客户注册帐号时，华为云会向客户展示**《隐私政策声明》**，客户可自愿主动勾选同意。**《隐私政策声明》**中包含包括发送营销信息在内的数据处理目的以及对敏感数据的处理及其目的，且向用户告知其数据拥有者权利，包括反对处理及撤回同意的权利，以及行使权利的方式。 如果购买服务或者售后服务涉及隐私声明中以外的个人数据收集或者个人数据使用目的，将在该产品的产品协议中提供额外的隐私声明，并获得数据拥有者的同意。当产品或服务收集的个人数据范围或使用目的发生变化时，将对隐私声明进行更新，并重新获取数据拥有者的同意。
建立安全措施的要求	华为云必须建立和维护不低于管理其组织内部信息的物理和技术管理安全措施，以保护个人数据免受损坏、丢失、更改、破坏或未经授权的使用、访问或处理。安全措施可由控制者自行采取或外包给个人或法人机构。同时应考虑数据类型划分的固有风险、个人数据的敏感性、技术发展、数据违规行为对数据拥有者可能造成的后果、所涉数据拥有者的数量、处理系统中的以往违规行为、个人数据对外界的潜在价值所带来的风险以及其他影响风险水平的因素如法律法规所导致的风险等。	华为云采取严格的管理和技术控制，确保个人数据在访问、传输、存储、处理等各生命周期阶段的安全。 • 在身份认证方面，采用严格的密码策略和多因素认证； • 在权限管理方面，对运维人员实行基于角色的访问控制和权限管理； • 在数据处理方面，采用加密技术对敏感数据进行加密并通过日志记录和审计技术对关键系统的访问操作进行监控和审计。 客户也可以通过华为云认证和报告验证华为云环境中的隐私安全控制。华为云获得了多个隐私合规相关国际标准的认证，以保障华为云的隐私安全，包括ISO 27701、ISO 29151、ISO 27018、BS 10012、SOC隐私原则的审计报告等（详细的认证介绍见第6章），其中ISO 27018是专注于云中个人数据保护的国际行为准则，ISO 27018的通过，表明华为云已拥有完备的个人数据保护管理系统。

为保护个人数据安全而采取的措施	为了建立和维护个人数据的安全，华为云必须将以下行动考虑在内： 1. 准备一份个人数据和处理系统的清单。 2. 确定个人数据处理人员的责任和义务。 3. 对个人数据进行风险分析，包括识别危险和估计对个人数据的风险。 4. 建立适用于个人数据的安全措施，并确定那些有效实施的措施。 5. 分析现有的安全措施和那些为保护个人数据而缺少的安全措施之间的差距。 6. 为实施差距分析中产生的缺失的安全措施准备一份工作计划。 7. 进行审查和审计。 8. 培训个人数据处理人员，以及 9. 保存个人数据存储介质的记录。 华为云应确保参与个人数据处理任何阶段的人员必须对此类数据保密，即使在其与数据拥有者或与华为云的关系结束后，该义务仍将继续存在。	华为云的信息资产分类由专门的工具进行监控和管理，形成资产清单，每个资产均被指定所有者。对于个人数据，华为云通过隐私影响评估（PIA）定期梳理个人数据资产清单，并识别对应的资产负责人。 华为云高度重视用户的数据信息资产，把数据保护作为华为云安全策略的核心。华为云遵循数据安全生命周期管理的业界先进标准，在身份认证、权限管理、访问控制、数据隔离、传输安全、存储安全、数据删除、物理销毁等方面，采用优秀技术、实践和流程，为用户提供最切实有效的数据保护能力，保证客户对其数据的隐私权、所有权和控制权不受侵犯。 华为云制定了隐私风险评估（PIA）及数据保护风险评估（DPIA）方法，从多个维度识别隐私及个人数据保护风险。各业务部门根据要求定期自行通过识别是否涉及个人数据、梳理数据清单与信息流、识别华为云在数据处理中的角色、识别DPIA及PIA需求、识别对检查清单的符合情况等步骤执行风险评估。风险评估涵盖隐私及个人数据保护的各方面，包括通知，选择和同意，个人数据收集、使用、保留和处置，数据拥有者访问，第三方披露，跨境转移等各方面对适用法律法规的符合情况。风险评估的目的是识别华为云隐私及个人数据保护方面的风险，基于风险发生的可能性和影响性为风险评级，通过风险评估报告对评估进行正式记录并制定风险消减措施及计划。 华为云有专门的审计团队定期评估策略、规程及配套措施和指标的符合性和有效性。此外，独立第三方评估机构也提供独立保证，这些评估员通过执行定期安全评估和合规性审计或检查（例如SOC、ISO标准、PCIDSS审计）来评估信息和资源的安全性、完整性、机密性和可用性，

		从而对风险管理内容/流程进行独立评估。 华为云从多方面使员工资质、能力和行为符合隐私保护的需求，要求员工每年应通过隐私保护的相关考核。在此基础上，华为云识别隐私保护相关岗位，明确定义岗位职责。华为云对新员工进行背景调查和技能考帮助员工符合要求；所有员工在职期间需要参加隐私保护意识相关培训，并通过考核。 华为云制定了介质管理标准，要求存储介质必须保存在受控访问区，所有存储介质都必须纳入介质管理流程来管理。 华为云与员工签署的保密协议中约定了保密内容和保密期限，即使职务终止后仍有保密义务。
安全措施文件	华为云应编写一份安全措施文件，列出上述安全措施。 当发生以下情况时，华为云必须更新安全措施文件： 1. 因华为云的安全策略的修订而对安全措施或流程进行修改，以持续改进。 2. 由于风险程度的变化，在处理过程中进行了实质性的修改。 3. 个人数据处理过程中发生违规。 4. 发生了其他对个人数据的造成影响的情况。 如涉及敏感个人数据，华为云应每年审查一次并在必要时更新安全措施文件。	华为云已根据ISO 27701国际标准要求建立了隐私信息管理体系（PIMS）用于组织范围内的隐私管理，实施文档化的隐私政策和程序为个人数据处理提供指导。 华为云至少每年审查一次隐私信息管理体系文档，并根据需要予以更新，以反映业务目标或风险环境的变更情况。

个人数据保存期限	当个人数据不再是向数据拥有者提供的隐私声明或适用法律中规定的目的所必需的或处理个人数据的目的已实现时，华为云应将其取消，然后将其封锁，以便随后进行抑制。 为履行合同义务收集的个人数据应在不再履行合同义务之日起的72个月后进行移除。 华为云必须建立并记录个人数据的保存、封锁和抑制程序，包括保存期限。个人数据的保存期限不得超过实现处理目的所需的期限，并应遵守适用于相关事项的法律，同时考虑到有关信息的行政、会计、税务、法律和历史方面。	华为云定期对收集、使用、披露个人数据的目的进行审核，对不再需要的个人数据进行匿名化或删除等安全处理。 华为云制定了个人数据保留机制，将会在达成隐私声明中所述目的或履行适用法律中规定的目的所需的期限内保留客户的个人数据，除非按照法律要求或客户的要求需要延长保留期。在客户的个人数据超出保留期限且没有法律要求华为云继续处理客户的特定个人数据的情况下，华为云将会根据适用法律的要求删除客户的个人数据，或进行匿名化处理。 华为云对于个人数据处理活动留存完整的记录，各服务通过开展隐私影响评估，在评估记录中列出数据拥有者类别、个人数据类型、收集个人数据的目的、个人数据流转情况、保存期限及采取的安全措施。
数据处理者或其他第三方	若个人数据由数据处理者或其他第三方进行处理，华为云应采取必要措施确保该数据处理者遵守本法确立的个人数据保护原则且始终遵守向数据拥有者提供的隐私声明。 华为云和数据处理者之间的关系必须通过合同或其他法律文书来确立，并允许其存在、范围和内容得到证明。 华为云应提请数据处理者注意数据拥有者对其个人数据的更正、取消或同意的撤销请求，并确保处理者执行相应请求。	华为云对所有供应商按要求进行尽职调查及隐私安全能力评估，合同中明确供应商作为处理者/子处理者的隐私保护义务及适用法律法规的要求，确保供应商满足客户的隐私保护要求。其他华为云可能依法向第三方披露数据的场景可详见**《隐私政策声明》**。

安全违规事件的更正措施及通知	在每个处理阶段发生的个人数据安全违规行为包括丢失或未经授权的破坏；盗窃、误置或未经授权的复制；未经授权的使用、访问或处理，以及未经授权的损坏、改变或修改。在个人数据发生安全违规行为的情况下，华为云必须分析其发生的原因，并实施更正、预防和改进措施，使安全措施充分，以避免再次发生违规事件。 在发生信息安全违规事件时，华为云必须在确认事件并已采取行动进行对事件规模的详尽审查后，立刻将那些严重损害数据拥有者财产或非金钱权利的安全事件通知数据拥有者，以便受损害的数据拥有者可以采取适当措施。通知应至少包含以下内容：安全事件的性质、被泄露的个人数据、向数据拥有者提出建议，说明其可以采取哪些措施来保护其利益、立即实施更正措施、数据拥有者可以通过什么方式获得更多信息。 华为云在个人数据处理的任何阶段，如发生对数据拥有者的财产或精神权利有重大影响的安全违规行为，华为云应立即报告给数据拥有者，以便后者可以采取适当的行动来维护其权利。	华为云设置7*24小时专业安全事件响应团队，按照适用法律法规要求，对个人数据泄露事件及时披露，同时执行应急预案及恢复流程，以降低对客户的影响。 华为云制定安全事件的定级原则和升级原则，根据安全事件对个人数据拥有者业务的影响程度进行事件定级，并根据安全事件的通报机制启动通知流程，将事件通知个人数据拥有者。当发生严重的安全事件，已经或可能对大量客户造成严重影响时，华为云会在最快的时间内将事件的相关信息通知客户，至少包括事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等，并根据当地法规要求进行必要的监管报备。

数据拥有者权利的响应	华为云应建立机制，向数据拥有者提供远程或本地电子通信手段或其认为适当的其他手段，确保数据拥有者可随时行使访问、更正、取消及反对的权利（ARCO权利），同时应指定个人数据人员或部门负责处理数据拥有者为行使本法所述权利而提出的请求。 华为云应在收到ARCO权利请求之日起20个工作日内通知数据拥有者其做出的是否受理的决定。该决定在发出通知之日起15个工作日内生效。如果由于数据拥有者在其权利请求中提供信息不充分或不准确而无法处理其请求，华为云应在收到请求后的5个工作日内要求数据拥有者补充信息。 若华为云不持有请求者的个人数据，也应在收到请求的20个工作日内予以回复。 当数据拥有者要求确认对其个人数据的处理是否已经停止时，华为云应明确回复。 遵守访问权的方式可以是现场访问（华为云规定的访问期限不得少于15个工作日），或通过发放副本或使用磁性、光学、声音、视觉或全息媒体，以及隐私声明中考虑的其他信息技术，华为云应确保格式的可读性。 华为云应在确认数据拥有者身份后免费提供个人数据，且不得将任何带有费用的服务或手段作为提出行使ARCO权利请求的唯一途径。 如数据拥有者提出取消其个人数据的请求，华为云应在接到请求的20个工作日内进行答复，在答复中将封锁期通知数据拥有者，并在答复受理数据拥有者的取消权后的15个工作日内开始对数据进行封锁。在封锁期，华为云应避免除存储和访问之外的处理，并对数据采取适当的安全措施。封锁期的长度为根据适用法律关系产生的诉讼的时效期或合同规定的期限，封锁期结束后华为云应正式停止对个人数据的任何处理并对个人数据进行抑制。	华为云保障客户行使其作为数据拥有者访问和更正其个人数据的权利。针对客户行使访问和更正其个人数据的权利，华为云提供专门的渠道接收客户相关请求，并配备专业团队响应客户关于个人数据和隐私保护相关的请求。针对客户的合理请求，华为云专业团队在符合法律规定及内部规范规定时间内完成处理并将结果反馈给客户。 当个人数据拥有者要求删除其个人数据时，华为云将响应个人数据拥有者的权利，除为遵循适用法律法规要求之外，对其个人数据进行匿名化或删除等安全处理。 当客户注销华为云账号后，除为遵循适用法律法规要求之外，存储期限结束后，华为云会对不再需要的个人数据进行匿名化或删除等安全处理。

	在处理的目的实现后，华为云必须在封锁期后停止处理收集到的数据，并随后消除、清理或销毁这些数据。 若数据拥有者认为华为云在响应数据拥有者权利方面违反了本法规定，其有权向监管机构提交申请以启动权利保护程序。在监管机构收到请求并将其发送给华为云后，华为云应在15个工作日内作出书面回应，提供证据。监管机构将在分析证据后对权利保护请求作出决定，如果该决定有利于数据拥有者，华为云将被命令在收到通知后10个工作日内或决定中规定的更长时间内，采取必要行动响应受保护的数据拥有者权利，并应在10个工作日内以书面形式向监管机构报告决定的遵守情况。	
个人数据的国内及跨境传输	任何个人数据的传输，无论是国内的还是国际的，除了本法规定的例外情况如法律规定、医疗健康原因、传输给相关公司、合同必要、维护公共利益、司法原因等，都必须征得数据拥有者的同意。 如果华为云打算将个人数据传输给除数据处理者以外的国内或国外第三方，则必须向该第三方提供隐私声明以及数据拥有者限制数据处理的目的。 数据处理将按照隐私声明中的约定进行，第三方接收方将承担与传输数据的华为云相同的义务。 国内及跨境传输都应通过一种正式化机制，如传输个人数据时华为云可以使用合同和其他法律文书，其中至少包含与华为云所受义务相同的义务，以及数据拥有者同意处理其个人数据的条件。	华为云设置了隐私保护专家团队来评估数据传输涉及的国家提供的个人数据保护水平，针对业务所在国家和地区，华为云还配备了法务和隐私保护专职人员，帮助华为云根据适用的隐私法规要求采取必要的措施。

核心要求	华为云适用的具体要求 （作为数据处理者）	华为云采取的措施

处理个人数据的义务	对于代表数据控制者进行的处理，华为云应承担以下义务： 1. 仅根据数据控制者的指示处理个人数据。 2. 不得为数据控制者指示以外的目的处理个人数据。 3. 执行法律、本条例和其他适用法律和法规要求的安全措施。 4. 对需要处理的个人数据进行保密。 5. 在与数据控制者的法律关系结束后或根据数据控制者的指示消除个人数据，前提是没有法律要求保存这些个人数据。 6. 不传输个人数据，除非基于数据控制者的决定、分包或者如果主管当局的要求。	华为云作为数据处理者，仅遵循客户的指令进行个人数据处理操作，内容数据收集的目的和范围由客户自行管理。 华为云高度重视客户的数据信息资产，把数据保护作为华为云安全策略的核心。华为云遵循数据安全生命周期管理的业界先进标准，在身份认证、权限管理、访问控制、数据隔离、传输安全、存储安全、数据删除、物理销毁等方面，采用优秀技术、实践和流程，为用户提供最切实有效的数据保护能力，保证客户对其数据的隐私权、所有权和控制权不受侵犯。 华为云向客户提供计算、存储、数据库、网络或其他服务，客户在使用服务时有许多选项可以加密其内容数据，华为云未经客户同意不得访问或使用客户内容数据。 针对客户内容数据，当客户主动进行数据删除操作或因服务期满需要对数据进行删除时，华为云会严格遵循适用的法律法规，以及与客户之间的协议约定，按照数据销毁标准清除客户的数据并保证数据不可恢复。 客户能够控制其在华为云上内容数据的整个生命周期，并根据自己的特定需求管理其内容数据。

4.4 华为云遵从墨西哥《保护义务主体持有的个人数据联邦法》的措施

根据墨西哥《保护义务主体持有的个人数据联邦法》的要求，当客户属于该法定义的义务主体范畴并进行数据处理时，华为云作为云服务提供商，承担了数据处理者的角色，受该法针对数据处理者的规定所监管。华为云积极响应并履行自身的义务，采取了如下隐私保护机制及技术以遵循墨西哥隐私法律法规的要求。

核心要求	华为云适用的具体要求 （作为数据处理者）	华为云采取的措施
处理个人数据的义务	华为云对个人数据处理活动的范围和内容没有任何决策权，其行为应限于数据控制者规定的条款。	华为云作为数据处理者，仅遵循客户的指令进行个人数据处理操作，内容数据收集的目的和范围由客户自行管理。

保护个人数据	华为云应承诺按照本法规定的原则和义务以及适用的规定保护个人数据，此为数据控制者将个人数据传输到本国领土之外的前提。	华为云采取严格的管理和技术控制，确保个人数据在访问、传输、存储、处理等各生命周期阶段的安全。 • 在身份认证方面，采用严格的密码策略和多因素认证； • 在权限管理方面，对运维人员实行基于角色的访问控制和权限管理； • 在数据处理方面，采用加密技术对敏感数据进行加密并通过日志记录和审计技术对关键系统的访问操作进行监控和审计。 客户也可以通过华为云认证和报告验证华为云环境中的隐私安全控制。华为云获得了多个隐私合规相关国际标准的认证，以保障华为云的隐私安全，包括ISO 27701、ISO 29151、ISO 27018、BS 10012、SOC隐私原则的审计报告等（详细的认证介绍见第6章），其中ISO 27018是专注于云中个人数据保护的国际行为准则，ISO 27018的通过，表明华为云已拥有完备的个人数据保护管理系统。

5 华为云协助客户遵从墨西哥隐私法律法规的要求

5.1 客户在《保护私人持有的个人数据联邦法》及其条例下的隐私保护责任

当客户是决定处理个人数据的私人主体并使用华为云的服务为他人提供服务时，客户属于《保护私人持有的个人数据联邦法》及其条例中定义的数据控制者，应遵循该法及其条例中针对数据控制者的合规要求。当客户是受数据控制者委托对个人数据进行处理并使用华为云服务的私人主体时，客户属于本法定义的数据处理者，应遵循其针对数据处理者的合规要求。针对客户的两种不同角色，华为云作为云服务提供商会在以下领域为客户提供合规支持，协助客户通过华为云的服务遵从监管要求。以下列举的具体要求融合了《保护私人持有的个人数据联邦法》以及对应的《保护私人持有的个人数据联邦法的条例》的补充说明。

核心要求	客户适用的具体要求 （作为数据控制者）	华为云为客户提供的服务支持

遵守个人数据处理原则的措施	客户须遵守法律规定的合法性、同意、信息、质量、目的、忠诚、相称性和问责制等原则。为实现此目的，客户可使用标准、最佳国际惯例、公司政策、自我规管安排或任何其他被认为足以实现这一目的的机制。 措施应至少包括： 1. 编制在客户组织内具有约束力和可执行性的隐私策略和方案。 2. 实施培训计划，旨在培养、更新和提高人员对保护个人数据义务的认识。 3. 建立内部监督和监测系统，并进行外部检查或审计，以核实对隐私策略的遵守情况。 4. 为实施隐私方案和策略提供专门的资源。 5. 实施一个程序，以处理因实施新产品、服务、技术和商业模式而对个人数据保护造成的风险，并减轻这些风险。 6. 定期审查安全策略和方案，以确定所需的修改。 7. 建立接受和回应数据拥有者问题和投诉的程序。 8. 建立遵守隐私策略和计划的机制，以及对违反策略和计划的制裁机制。 9. 建立保护个人数据的措施，即一组技术和管理行动，使客户能够确保遵守法律和条例规定的原则和义务。 10. 建立个人数据的追踪措施，即允许在处理个人数据时进行追踪的行动、措施和技术程序。	华为云为客户提供多种隐私保护技术及服务，包括访问控制和身份认证、数据加密、日志和审计等功能，帮助客户根据业务需求进行个人数据保护。 华为云有专门的团队支持和客户的沟通联系，客户可以通过工单服务寻求华为云的帮助。

隐私声明	客户应在收集个人数据前通过隐私声明向数据拥有者告知收向其收集的个人数据以及处理目的，尤其是有关于营销、广告或商业探索的处理以及被用于无需人工干预的决策的处理。隐私声明中还应该包括客户的公司名称及地址、对个人数据进行的任何传输、以及当客户使用远程或本地电子、光学或其他技术手段的通信机制自动获得个人数据时，这种技术的使用和数据拥有者反对其使用的方式。允许数据拥有者对隐私声明中所述内容表示拒绝、限制数据使用或披露以及撤回同意的机制、行使数据拥有者权利的方式、向数据拥有者通知隐私声明变更的方法、对敏感个人数据的处理等也应通过隐私声明传达。 可通过口头、纸质、电子化、视频或音频格式或任何其他技术将隐私声明提供给数据拥有者。隐私声明必须简单且包含必要信息，语言、结构和设计清晰且利于理解。 如果个人数据不是直接从数据拥有者处获得的，客户必须将隐私声明的更改通知数据拥有者。在无法向数据拥有者提供隐私声明的情况下，或者由于数据拥有者的数量过大或数据的年限过长而付出不成比例的付出的情况下，客户可以向监管机构（国家透明度、获取信息和个人数据保护研究所INAI）提出请求，在获得授权后利用大众传播媒体实施补偿措施。	华为云提供的部分产品和服务中为客户提供嵌入隐私声明的接口以及记录相关操作的功能，客户可在隐私声明中告知数据拥有者将收集的个人数据的种类、使用目的、保存期限等信息。 建议客户对其产品和服务进行评估，若满足通知的条件，建议客户按照法律要求执行通知。
处理敏感个人数据	客户可在以下情况下收集敏感个人数据：当法律有要求；涉及国家安全、公共秩序、健康和安全以及第三方权利的保护等情况；根据明确的活动或目的，为合法、具体的目的而需要时。 客户在处理敏感个人数据、财务或资产相关个人数据时需要获得通过数据拥有者的签名、电子签名或为此目的建立的任何认证机制传达的明示同意。	华为云向客户提供的**数据安全中心服务（DSC）**可以帮助客户进行数据分级分类，数据安全风险识别，数据水印溯源，数据脱敏等基础数据安全操作。可精准高效识别敏感数据并根据敏感数据发现策略精准识别数据库中的敏感数据，基于多种预置脱敏算法和用户自定义脱敏算法，实现全栈敏感数据防护。

数据拥有者的同意	所有个人数据的处理均应获得经数据拥有者同意。除非法律要求数据拥有者明确表示同意，否则默许同意一般情况下是有效的。如果数据拥有者没有对隐私声明表示反对，可视为其对数据处理的默许同意，前提是隐私声明中包含足够的信息。 如果客户打算处理数据用于与隐私声明中所述目的之外的不相容或类似的其他目的，则必须再次获得数据拥有者的同意。数据拥有者可以拒绝或随时撤销对数据处理的同意，也可以反对为不必要的目的的处理其数据。但数据拥有者的拒绝、撤销同意或反对处理不会终止基于必要目的的处理以及以客户和数据拥有者之间的法律关系为基础的处理。	华为提供的部分云产品和服务中提供的功能或自身构建的能力更好地践行隐私保护法规明确告知数据拥有者的要求。例如客户可通过华为云提供的接口嵌入客户的隐私政策，建议客户在隐私政策中明确说明个人数据处理的目的和满足的合法依据，华为云可为客户提供记录数据拥有者同意的操作记录能力。
为保护个人数据安全而采取的措施	为了建立和维护个人数据的安全，客户必须将以下行动考虑在内： 1. 准备一份个人数据和处理系统的清单。 2. 确定个人数据处理人员的责任和义务。 3. 对个人数据进行风险分析，包括识别危险和估计对个人数据的风险。 4. 建立适用于个人数据的安全措施，并确定那些有效实施的措施。 5. 分析现有的安全措施和那些为保护个人数据而缺少的安全措施之间的差距。 6. 为实施差距分析中产生的缺失的安全措施准备一份工作计划。 7. 进行审查和审计。 8. 培训个人数据处理人员，以及 9. 保存个人数据存储介质的记录。 客户应确保参与个人数据处理任何阶段的人员必须对此类数据保密，即使在客户或数据拥有者与其关系结束后，该义务仍将继续存在。	华为云为客户提供多种隐私保护技术及服务，包括**统一身份认证服务（IAM）**、**数据加密服务（DEW）**、**云日志服务（LTS）**和**云审计服务（CTS）**等，为客户提供访问控制和身份认证、数据加密、日志和审计等功能。帮助客户根据业务需求进行个人数据保护。
个人数据保存期限	当个人数据不再是向数据拥有者提供的隐私声明或适用法律中规定的目的所必需的或处理个人数据的目的已实现时，客户应将其取消，然后将其封锁，以便随后进行抑制。 为履行合同义务收集的个人数据应在不再履行合同义务之日起的72个月后进行移除。 客户必须建立并记录个人数据的保存、封锁和抑制程序，包括保存期限。个人数据的保存期限不得超过实现处理目的所需的期限，并应遵守适用于相关事项的法律，同时考虑到有关信息的行政、会计、税务、法律和历史方面。	华为云的大部分产品或服务中提供了数据删除功能，对于客户内容数据，客户可以主动进行数据删除操作。

数据处理者或其他第三方	若个人数据由数据处理者或其他第三方进行处理，客户应采取必要措施确保该数据处理者遵守本法确立的个人数据保护原则且始终遵守向数据拥有者提供的隐私声明。 客户和数据处理者之间的关系必须通过合同或其他法律文书来确立，并允许其存在、范围和内容得到证明。 客户应提请数据处理者注意数据拥有者对其个人数据的更正、取消或同意的撤销请求，并确保处理者执行相应请求。	客户可通过华为云部分产品和服务中提供的签署和查询隐私通知的接口，嵌入同意或撤销隐私通知并记录相关操作记录的功能，将个人数据处理的政策告知其用户。

云计算中的个人数据处理	对于云计算中的服务、应用和基础设施中的个人数据处理，其中客户通过一般合同条件或条款遵守同样的要求，此类服务只能在云提供商满足以下要求时被使用: 至少遵守以下规定： 1. 拥有并应用符合本法和条例规定的适用原则和义务的个人数据保护策略。 2. 对分包所涉及所提供的服务信息的透明化。 3. 不得在提供服务时附加获得服务所涵盖数据的所有权的条件。 4. 对其提供服务的个人数据进行保密。 至少具有以下机制： 1. 公布其隐私策略或其提供服务的条件的变化。 2. 允许客户限制其提供服务的个人数据的处理类型。 3. 建立和维护适当的安全措施，以保护其提供服务的个人数据。 4. 一旦向客户提供的服务终止，则确保抑制个人数据，并且控制者能够恢复此等个人数据。 5. 阻止没有适当权限的人访问个人数据，如主管当局正式提出访问要求，应通知客户。 客户应确保在任何情况下使用能确保适当保护个人数据的服务。	为保护客户个人数据并帮助客户构建云上业务的隐私保护，持续有效地开展隐私保护管理工作，华为云已建立并持续完善华为云业务隐私保护管理体系。华为云在“尊重和保护隐私，让人们放心地使用便捷可信的云服务”愿景指导下，参考被业界广泛认可的隐私保护原则，采用隐私融入设计PbD的理念，将隐私保护融入到每一个业务活动，形成华为云特有的隐私保护管理体系。 为配合客户行使对服务提供商监管，华为云线上的**《华为云用户协议》**对客户和华为云的安全职责进行划分，**《华为云服务等级协议》**规定了华为云提供的服务水平。同时，华为云也制定了线下合同模板，可根据客户的具体要求，在其中规定华为云若聘用分包商，需通知客户，并对分包的服务负责。 华为云深刻理解客户的内容数据对客户业务的重要程度，华为云秉承中立态度，保障客户数据为客户所有、为客户所用、为客户创造价值。客户使用华为云的过程中，拥有对其内容数据的全面控制权。 华为云与员工签署的保密协议中约定了保密内容和保密期限，即使员工职务终止后仍有保密义务。 华为云在其官网提供**《隐私声明政策》**并

		在其发生变化时重新获得用户同意。 华为云提供不同类型的服务和产品供客户自行选择，提供包括存储、分析等个人数据处理功能。 华为云的大部分产品或服务中提供了数据删除功能，对于客户内容数据，客户可以主动进行数据删除操作。 客户可通过华为云的**统一身份认证服务（IAM）**对使用云资源的用户账号进行管理。每一位华为云客户在华为云都拥有唯一可辨识的用户ID，此外，华为云还提供多种用户身份验证机制，包括账号密码、多因素认证等。
安全违规事件的更正措施及通知	在每个处理阶段发生的个人数据安全违规行为包括丢失或未经授权的破坏；盗窃、误置或未经授权的复制；未经授权的使用、访问或处理，以及未经授权的损坏、改变或修改。在个人数据发生安全违规行为的情况下，客户必须分析其发生的原因，并实施更正、预防和改进措施，使安全措施充分，以避免再次发生违规事件。 在发生信息安全违规事件时，客户必须在确认事件并已采取行动进行对事件规模的详尽审查后，立刻将那些严重损害数据拥有者财产或非金钱权利的安全事件通知数据拥有者，以便受损害的数据拥有者可以采取适当措施。通知应至少包含以下内容：安全事件的性质、被泄露的个人数据、向数据拥有者提出建议，说明其可以采取哪些措施来保护其利益、立即实施更正措施、数据拥有者可以通过什么方式获得更多信息。 客户在个人数据处理的任何阶段，如发生对数据拥有者的财产或精神权利有重大影响的安全违规行为，客户应立即报告给数据拥有者，以便后者可以采取适当的行动来维护其权利。	建议客户考虑如何管理和保护个人数据安全，防止出现个人数据泄露，如有泄露事件，应依据相应的法律法规及时通知数据拥有者及监管机构。 华为云有专门的团队保证和客户的沟通和联系，当在客户侧发生数据泄露事件时，华为云将配合客户进行个人数据泄露调查和响应流程。 华为云提供的**云日志服务（LTS）**及**云审计服务（CTS）**可用于对安全违规行为的发现，也可以在安全违规事件的取证、调查、分析及处置环节协助客户。

数据拥有者权利的响应	客户应建立机制，向数据拥有者提供远程或本地电子通信手段或其认为适当的其他手段，确保数据拥有者可随时行使访问、更正、取消及反对的权利（ARCO权利），同时应指定个人数据人员或部门负责处理数据拥有者为行使本法所述权利而提出的请求。 客户应在收到ARCO权利请求之日起20个工作日内通知数据拥有者其做出的是否受理的决定。该决定在发出通知之日起15个工作日内生效。如果由于数据拥有者在其权利请求中提供信息不充分或不准确而无法处理其请求，客户应在收到请求后的5个工作日内要求数据拥有者补充信息。 若客户不持有请求者的个人数据，也应在收到请求的20个工作日内予以回复。 当数据拥有者要求确认对其个人数据的处理是否已经停止时，客户应明确回复。 遵守访问权的方式可以是现场访问（客户规定的访问期限不得少于15个工作日），或通过发放副本或使用磁性、光学、声音、视觉或全息媒体，以及隐私声明中考虑的其他信息技术，客户应确保格式的可读性。 客户应在确认数据拥有者身份后免费提供个人数据，且不得将任何带有费用的服务或手段作为提出行使ARCO权利请求的唯一途径。 如数据拥有者提出取消其个人数据的请求，客户应在接到请求的20个工作日内进行答复，在答复中将封锁期通知数据拥有者，并在答复受理数据拥有者的取消权后的15个工作日内开始对数据进行封锁。在封锁期，客户应避免除存储和访问之外的处理，并对数据采取适当的安全措施。封锁期的长度为根据适用法律关系产生的诉讼的时效期或合同规定的期限，封锁期结束后客户应正式停止对个人数据的任何处理并对个人数据进行抑制。 在处理的目的实现后，客户必须在封锁期后停止处理收集到的数据，并随后消除、清理或销毁这些数据。 若数据拥有者认为客户在响应数据拥有者权利方面违反了本法规定，其有权向监管机构提交申请以启动权利保护程序。在监管机构收到请求并将其发送给客户后，客户应在15个工作日内作出书面回应，提供证据。监管机构将在分析证据后对权利保护请求作出决定，如果该决定有利于数据拥有者，客户将被命令在收到通知后10个工作日内或决定中规定的更长时间内，采取必要行动响应受保护的数据拥有者权利，并应在10个	华为云有专门的团队负责和客户的沟通联系，客户可以通过工单服务寻求华为云的帮助。

	工作日内以书面形式向监管机构报告决定的遵守情况。	
个人数据的国内及跨境传输	任何个人数据的传输，无论是国内的还是国际的，除了本法规定的例外情况如法律规定、医疗健康原因、传输给相关公司、合同必要、维护公共利益、司法原因等，都必须征得数据拥有者的同意。 如果客户打算将个人数据传输给除数据处理者以外的国内或国外第三方，则必须向该第三方提供隐私声明以及数据拥有者限制数据处理的目的。 数据处理将按照隐私声明中的约定进行，第三方接收方将承担与传输数据的客户相同的义务。 国内及跨境传输都应通过一种正式化机制，如传输个人数据时客户可以使用合同和其他法律文书，其中至少包含与客户所受义务相同的义务，以及数据拥有者同意处理其个人数据的条件。	建议客户评估数据传输涉及的国家提供的个人数据保护水平，并通过正式化机制进行个人数据跨境传输。

法规基本义务	客户适用的具体要求 （作为数据处理者）	华为云为客户提供的服务支持
处理个人数据的义务	对于代表数据控制者进行的处理，客户应承担以下义务： 1. 仅根据数据控制者的指示处理个人数据。 2. 不得为数据控制者指示以外的目的处理个人数据。 3. 执行法律、本条例和其他适用法律和法规要求的安全措施。 4. 对需要处理的个人数据进行保密。 5. 在与数据控制者的法律关系结束后或根据数据控制者的指示消除个人数据，前提是没有法律要求保存这些个人数据。 不传输个人数据，除非基于数据控制者的决定、分包或者如果主管当局的要求。	建议客户仅按照数据控制者的指示，在数据控制者规定的目的下处理个人数据。 华为云向客户提供计算、存储、数据库、网络或其他服务，客户在使用服务时有许多选项可以加密其内容数据，华为云未经客户同意不得访问或使用客户内容数据。 华为云的大部分产品或服务中提供了数据删除功能，对于客户内容数据，客户可以主动进行数据删除操作。

使用分包服务	客户的任何分包服务意味着对个人数据的处理，必须得到数据控制者的授权，并应以后者的名义和代表进行。 在获得授权后，客户必须通过合同或其他允许证明其存在、范围和内容的文书，正式确定与分包商的关系。 被分包的个人或法人团体将承担法律、本条例和其他适用法律和法规为客户规定的相同义务。 客户有义务证明该分包是在数据控制者的授权下进行的。 当正式确定数据控制者和客户之间关系的合同或法律文书考虑到后者可以分包服务时，控制者对客户的授权将被理解为通过这些文件中的条款给予。 如果数据控制者和客户之间的合同或法律文书中没有考虑到分包，则客户必须在分包之前获得数据控制者的授权。	建议客户在使用分包服务前得到控制者的授权同意，并与分包商签订正式合同。

5.2 客户在《保护义务主体持有的个人数据联邦法》下的隐私保护责任

当客户是受《保护义务主体持有的个人数据联邦法》管辖的义务主体，即行政、立法和司法部门、自治机构、政党、信托机构或公共基金的任何当局、实体、机关或机构，且决定个人数据的处理时，其角色为数据控制者，应满足本法针对数据控制者的合规要求。当客户是受数据控制者委托对个人数据进行处理并使用华为云的服务的义务主体时，客户属于本法定义的数据处理者，应满足其针对数据处理者的合规要求。针对客户的两种不同角色，华为云会在以下领域为客户提供合规支持。

核心要求	客户适用的具体要求 （作为数据控制者）	华为云为客户提供的服务支持

遵守个人数据处理原则的措施	客户在处理个人数据时应遵守合法、目的、忠诚、同意、质量、比例、信息和责任的原则，遵守适用法规赋予的权力或义务。同时客户进行的所有个人数据处理必须有具体、合法、明确和正当的目的，且为充分的、相关的和对处理目的严格必要的。客户仅能在拥有法律赋予的权力或数据拥有者同意或数据拥有者为报告失踪的人员的情况下为隐私声明中规定的目的以外的目的处理个人数据。 客户为遵守本法规定的责任原则而采取的机制中，至少应包括以下内容： 1. 为实施个人数据保护方案和政策分配为此目的而授权的资源。 2. 制定个人数据保护政策和方案，在客户的组织内具有强制性和可执行性。 3. 实施培训和更新计划，让员工了解有关个人数据保护的义务和其他职责 4. 定期审查个人数据安全政策和方案，以确定可能需要的修改。 5. 建立一个内部和/或外部监督和监测系统，包括审计，以核实对个人数据保护政策的遵守情况。 6. 建立接收和响应数据拥有者提出的询问和投诉的程序。 7. 根据本法规定的条款和有关该事项的其他适用条款，设计、开发和实施其公共政策、计划、服务、计算机系统或平台、电子应用程序或任何其他涉及处理个人数据的技术；和 8. 保证其公共政策、计划、服务、计算机系统或平台、电子应用或任何其他涉及个人数据处理的技术，默认遵守本法规定的义务和关于该事项的任何其他适用规定。	华为云为客户提供多种隐私保护技术及服务，包括访问控制和身份认证、数据加密、日志和审计等功能，帮助客户根据业务需求进行个人数据保护。 华为云有专门的团队支持和客户的沟通联系，客户可以通过工单服务寻求华为云的帮助。

隐私声明	客户必须通过隐私声明告知数据拥有者其个人数据将受到的处理的存在和主要特征，以便其可以在这方面做出知情决定。 一般来说，隐私声明应通过客户可用的电子和物理手段进行传播。 为了使隐私声明有效地履行其告知功能，它必须以清晰和简单的方式起草和组织。 当不可能直接通知需提供隐私声明的数据拥有者，或者这需要不相称的努力时，客户可以根据国家透明度、获取信息和个人数据保护系统为此目的发布的标准，实施大众传播的补偿措施。 隐私声明应以两种方式提供给数据拥有者：简化和详细。 简化隐私声明应包含以下信息： 1. 客户的名称。 2. 获取个人数据的处理目的，区分那些需要数据拥有者同意的目的。 3. 在传输需要同意的个人数据时，必须告知以下人员及内容： 1. 三级政府的主管部门、权力机构、实体、机关和政府机构，以及接受个人数据的自然人或法人；以及 2. 传输的目的。 1. 可用的机制和手段，以便数据拥有者在适当情况下可以对以需要其同意的目的处理和传输其个人数据表示反对，以及 2. 可以访问详细隐私声明的网站。 详细的隐私声明应包含以下信息： 1. 客户的地址。 2. 将被处理的个人数据，并识别其中的敏感个人数据。 3. 授权客户进行处理的法律依据。 4. 获取个人数据的处理目的，区分那些需要得到数据拥有者同意的目的。 5. 可用于行使ARCO权利的机制、手段和程序。 6. 透明度部门的地址，以及 7. 客户将以何种方式向数据拥有者传达对隐私声明的修改。	华为云提供的部分产品和服务中为客户提供嵌入隐私声明的接口以及记录相关操作的功能，客户可在隐私声明中告知数据拥有者将收集的个人数据的种类、使用目的、保存期限等信息。 建议客户对其产品和服务进行评估，若满足通知的条件，建议客户按照法律要求执行通知。
处理敏感个人数据	本法中针对数据控制者处理敏感个人数据的规定与《保护私人持有的个人数据联邦法》相同。	见5.1“处理敏感个人数据”部分

数据拥有者的同意	本法中针对数据控制者获得数据拥有者同意的规定与《保护私人持有的个人数据联邦法》相同。	见5.1“数据拥有者的同意”部分
为保护个人数据安全而采取的措施	为了建立和维护保护个人数据的安全措施，客户应至少开展以下相互关联的活动： 1. 建立管理和处理个人数据的内部政策，其中考虑到处理发生的背景和个人数据的生命周期，即其收集、使用和随后的抑制。 2. 界定参与处理个人数据的人员的职能和义务。 3. 编制个人数据和处理系统的清单。 4. 对个人数据进行风险分析，考虑到个人数据的现有威胁和脆弱性，以及涉及处理这些数据的资源，如但不限于硬件、软件、客户的人员等。 5. 分析现有的安全措施与客户组织中缺乏的措施的差距。 6. 为实施缺失的安全措施以及日常遵守管理和处理个人数据的政策的措施制定工作计划。 7. 监督并定期审查所实施的安全措施，以及个人数据所受到的威胁和破坏，以及 8. 根据人员在处理个人数据方面的作用和责任设计和实施不同级别的培训。 客户必须建立控制或机制，其目的是确保所有参与处理个人数据的任何阶段的人对这些数据进行保密，这一义务即使在他们与控制者的关系结束后也应持续存在。	华为云为客户提供多种隐私保护技术及服务，包括**统一身份认证服务（IAM）**、**数据加密服务（DEW）**、**云日志服务（LTS）**和**云审计服务（CTS）**等，为客户提供访问控制和身份认证、数据加密、日志和审计等功能。帮助客户根据业务需求进行个人数据保护。
安全、检察和司法机构拥有的数据库	根据本法的规定，安全、执法和司法行政机构的主管部门对个人数据的收集和处理，仅限于那些为行使国家安全、公共安全方面的职能，或为防止或起诉犯罪所必需和相称的情况和数据类别。它们必须储存在专门为此目的而建立的数据库中。应对该数据库建立高水平的安全措施，以保证数据的完整性、可用性和保密性，以保护个人数据免受损害、损失、更改、破坏或未经授权的使用、访问或处理。 在安全、执法和司法行政机构的主管监管实体对个人数据的处理以及使用数据库存储数据时，必须遵守本法规定的数据处理原则。私人通信是不可侵犯的。只有联邦司法当局，应法律授权的联邦当局或相应联邦实体的检察官办公室负责人的要求，才能授权截获任何私人通信。	华为云产品中提供访问控制，网络隔离等安全配置。华为云提供专门的安全产品，助力客户提高某一方面的安全能力，如**数据库安全服务（DBSS）**、**DDoS高防（AAD）**、**漏洞扫描服务（VSS）**等。 华为云获得了多个隐私合规相关国际标准的认证，以证明华为云在数据处理的技术能力和组织能力方面有足够保障措施。

个人数据保存期限	如果不再需要个人数据来实现隐私声明所述的目的，应将个人数据进行封锁，并在封锁期结束后予以抑制。客户必须制定并记录个人数据的保存、封锁和抑制程序，其中应包括其保留期限。相关程序中必须包括允许客户遵守为抑制个人数据而设定的最后期限的机制，并对保留个人数据的必要性进行定期审查。个人数据的保存期限不得超过为实现其处理目的所必需的期限，并应遵守适用于有关事项的规定，考虑到个人数据的行政、会计、税务、法律和历史方面。	华为云的大部分产品或服务中提供了数据删除功能，对于客户内容数据，客户可以主动进行数据删除操作。
数据处理者或其他第三方	客户和数据处理者之间的关系应通过合同或客户根据适用法规决定的任何其他法律文书来正式确定，并允许对其存在、范围和内容进行认证。由客户决定的合同或法律文书必须至少包括与数据处理者提供的服务有关的下列一般条款： 1. 按照客户的指示进行个人数据的处理。 2. 避免为客户指示以外的目的处理个人数据。 3. 根据适用的法律文书实施安全措施。 4. 当其根据指示处理的个人数据出现安全违规行为时，通知客户。 5. 对所处理的个人数据进行保密。 6. 一旦与客户的法律关系履行完毕，删除或归还正在处理的个人数据，只要没有法律规定要求保留个人数据；以及 7. 避免传输个人数据，除非客户决定这样做，或传输由于分包，或由主管部门明确授权。 客户和处理者之间与个人数据处理有关的协议不得违反本法和其他适用的规定，以及相应的隐私声明的规定。	客户可通过华为云部分产品和服务中提供的签署和查询隐私通知的接口，嵌入同意或撤销隐私通知并记录相关操作记录的功能，将个人数据处理的政策告知其用户。
云计算中的个人数据处理	本法中针对数据控制者使用云计算进行个人数据处理的规定与《保护私人持有的个人数据联邦法》相同。	见5.1“云计算中的个人数据处理”部分

安全违规事件的更正措施及通知	在数据处理的任何阶段发生的个人数据安全违规行为包括未经授权的丢失或破坏；盗窃、误置或未经授权的复制；未经授权的使用、访问或处理；未经授权的损坏、改变或修改等情况。在出现安全违规行为时，客户应分析违规的原因，并在其工作计划中实施预防和更正措施，以调整安全措施和个人数据的处理，以防止安全违规行为再次发生。客户应将安全违规记录在案，说明违规情况、发生日期、原因以及立即和最终实施的更正措施。 客户必须在确认发生违规行为且已开始采取行动以启动对违规行为的严重程度进行详尽审查后，立即将严重影响经济或精神权利的违规行为通知数据拥有者，并酌情通知监管机构和联邦实体的担保机构，以便受影响的数据拥有者能够采取相应措施来维护其权利。通知应至少包含以下内容：事件的性质、受影响的个人数据、就数据拥有者为保护其利益可能采取的措施向其提出建议、立即进行的更正行动以及在这方面可以获得更多信息的途径。	建议客户考虑如何管理和保护个人数据安全，防止出现个人数据泄露，如有泄露事件，应依据相应的法律法规及时通知数据拥有者及监管机构。 华为云有专门的团队保证和客户的沟通和联系，当在客户侧发生数据泄露事件时，华为云将配合客户进行个人数据泄露调查和响应流程。 华为云提供的**云日志服务（LTS）**及**云审计服务（CTS）**可用于对安全违规行为的发现，也可以在安全违规事件的取证、调查、分析及处置环节协助客户。

数据拥有者权利的响应	数据拥有者或其代表可在任何时候要求访问、更正、取消或反对处理其个人数据。为行使ARCO的权利，客户有必要确认数据拥有者或其代表的身份和人格。在法律规定、法院命令或在适当的特殊情况下，由数据拥有者或其代表以外的人行使ARCO的权利是可能的。 根据民法，在未成年人或处于禁治状态或无行为能力的人行使ARCO权利时，应适用同一立法中规定的代表规则。 对于涉及已故人员的个人数据，根据适用的法律，证明具有合法权益的人可以行使本法所赋予的权利，但条件是权利持有者已正式表达了他或她的意愿，或者有法院的命令表明这一点。 ARCO权利的行使应是免费的。根据适用的规定，只能为收回复制、认证或提供的成本而收费。就获取个人数据而言，确定复制和认证费用的法律在确定时应考虑该金额允许或有利于行使该权利。当数据拥有者提供复制个人数据所需的磁性或电子手段或机制时，应免费向数据拥有者提供。当信息涉及的交付不超过20个简单的页面时，应免费提供。透明度部门可以根据数据拥有者的社会经济情况，免除复制和提供的费用。客户不得为提交行使ARCO权利的请求设立任何意味着数据拥有者需要付费的服务或手段。 客户应建立简单的程序，以使ARCO权利得到行使，其响应时间从收到请求的次日起不应超过20个工作日。响应期限在有正当理由的情况下可以延长一次，最多不超过10个工作日，且必须在答复期限内通知数据拥有者。如果ARCO权利的行使是可接受的，客户必须在不超过15个工作日的期限内使其生效，该期限从数据拥有者收到答复通知之日的次日算起。 对于行使ARCO权利的请求，客户不得提出比下列更高的要求： 1. 数据拥有者的姓名及其住所或任何其他接收通知的方式。 2. 证明数据拥有者身份的文件，以及在适当情况下证明其代表的人格和身份的文件。 3. 如果可能的话，负责处理个人数据并向其提交请求的地区。 4. 对个人数据的清晰和准确描述，该请求旨在行使ARCO的任何权利，但访问权的情况除外。	华为云有专门的团队负责和客户的沟通联系，客户可以通过工单服务寻求华为云的帮助。

	5. 对要行使的ARCO权利的描述，或数据拥有者要求的内容，以及 6. 任何其他有助于查找个人数据的要素或文件。 在要求访问个人数据的情况下，客户必须以数据拥有者要求的形式遵守请求，除非存在物理或法律上的不可能性，限制其以这种形式复制个人数据，在这种情况下，必须以其他形式提供个人数据并说明这种行动的理由和原因。 如果数据保护请求不符合本条所述的任何要求，而监管机构或担保机构不具备补救的要素，则将在提出行使ARCO权利的请求后的5个工作日内，一次性通知数据拥有者，让其在通知之日的次日起的10个工作日内补充遗漏信息。 当客户没有能力处理行使ARCO权利的请求时，它应在提出请求后的3个工作日内将这种情况告知数据拥有者，如果可以确定，它应引导数据拥有者向有能力的数据控制者提出请求。如果客户声明其档案、记录、系统或文件中不存在个人数据，这种声明应记录在透明委员会的决议中，以确认个人数据的不存在。如果客户注意到行使ARCO权利的请求与本法规定的权利不同，它必须通过通知数据拥有者以重新确定路径。 如果适用于某些个人数据处理的条款规定了申请行使ARCO权利的具体流程或程序，客户应在请求行使ARCO权利后5个工作日内通知数据拥有者是否存在ARCO权利，以便后者决定是通过具体流程行使其权利，还是通过客户根据本法规定为处理行使ARCO权利的请求而制度化的程序行使其权利。	

个人数据保护影响评估	当要处理的个人数据存在固有的风险、处理敏感的个人数据及已进行或打算进行个人数据的传输，应视为对个人数据进行了密集或相关处理。当客户打算实施或修改公共政策、计算机系统或平台、电子应用程序或任何其他技术，而其认为这意味着对个人数据的密集或相关处理时，客户必须进行个人数据保护的影响评估，并酌情提交给监管机构或担保机构，这些机构可以发布专门保护个人数据的非约束性建议。 个人数据保护影响评估的内容应由国家透明度、信息获取和个人数据保护体系决定。 开展个人数据保护影响评估的客户应在其打算实施或修改公共政策、计算机系统或平台、电子应用程序或任何其他技术的日期前30个工作日，向监管机构或担保机构提交影响评估，以发便后者发布相应的非约束性建议。当客户认为，由于可能实施或修改公共政策、计算机系统或平台、电子应用程序或涉及密集或相关的个人数据处理的任何其他技术，或在紧急情况或紧急情况下，可能会损害其预期效果，则不需要进行个人数据保护影响评估。	建议客户根据评估个人数据是否涉及密集或相关处理，如涉及则根据国家透明度、信息获取和个人数据保护体系进行个人数据保护影响评估，并在指定期限内向监管机构或担保机构提交影响评估。
个人数据的国内及跨境传输	任何国内或国际的个人数据传输都应征得数据拥有者的同意，但法律规定、法院命令、主管部门的合理授权等本法规定的例外情况除外。只有当接收的第三方或数据处理者承诺按照本法规定的原则和义务以及适用的规定保护个人数据时，客户才可以将个人数据传输或转发到本国领土之外。 在任何个人数据的传输中，客户应向个人数据的接收者传达隐私声明，根据该隐私声明处理个人数据。所有的传输必须根据符合适用于客户的规定，通过执行合同条款、合作协议或任何其他法律文书来正式确定，以证明个人数据的处理范围，以及各方承担的义务和责任。	建议客户评估数据传输涉及的国家提供的个人数据保护水平，并通过正式化机制进行个人数据跨境传输。

核心要求	客户适用的具体要求 （作为数据处理者）	华为云为客户提供的服务支持
处理个人数据的义务	客户对个人数据处理活动的范围和内容没有任何决策权，其行为应限于数据控制者规定的条款。	见5.1“处理个人数据的义务”部分
使用分包服务	本法中针对数据处理者使用分包服务的规定与《保护私人持有的个人数据联邦法》相同。	见5.1“使用分包服务”部分

保护个人数据	客户应承诺按照本法规定的原则和义务以及适用的规定保护个人数据，此为数据控制者将个人数据传输到本国领土之外的前提。	华为云为客户提供多种隐私保护技术及服务，包括访问控制和身份认证、数据加密、日志和审计等功能，帮助客户根据业务需求进行个人数据保护。

5.3 华为云的产品和服务如何助力客户实现内容数据的隐私安全

华为云理解客户的隐私保护需求，并结合自身丰富隐私保护实践及技术能力，通过华为云产品或服务帮助客户遵循墨西哥隐私法律法规。华为云为客户提供的产品及服务范围涵盖网络产品、数据库产品、安全产品、管理与部署工具等产品，产品的数据保护、数据删除、网络隔离、权限管理等功能可帮助客户实现内容数据的隐私安全。

- **管理与部署产品**

产品名称	产品介绍	对应的核心要求及控制措施
统一身份认证服务 Identity and Access Management (IAM)	提供身份认证和权限管理功能，可以管理用户（比如员工、系统或应用程序）帐号，并且可以控制这些用户对其名下资源的操作权限。 客户可通过IAM采取适合的用户管理、身份认证和细粒度的云上资源访问控制等措施，防止对内容数据进行的未授权修改。	保护私人持有的个人数据联邦法（第19、21、22、23、24、25条） 保护私人持有的个人数据联邦法律的条例（第50、52、59、61、87、90条） 保护义务主体持有的个人数据联邦法（第31、42、43、44、45、46、51、64、82条）
云审计服务 Cloud Trace Service(CTS)	为客户提供云帐户下资源的操作记录，实现安全分析、合规审计、问题定位等场景。 客户可以通过配置CTS对象存储服务，将操作记录实时同步保存至CTS，以便保存更长时间的操作记录，保障个人数据拥有者的知情权、实现快速查找。	保护私人持有的个人数据联邦法（第20、22条） 保护私人持有的个人数据联邦法律的条例（第50、52、59、61条） 保护义务主体持有的个人数据联邦法（第31、43、44、45、46、51、64条）

云监控服务 Cloud Eye Service(CES)	为客户提供一个针对弹性云服务器、带宽等资源的立体化监控平台。 客户可通过CES全面了解华为云上的资源使用情况、业务的运行状况，并及时收到异常报警做出反应，保证业务顺畅运行。	保护私人持有的个人数据联邦法（第20、21条） 保护私人持有的个人数据联邦法律的条例（第50、52、59、61、64条） 保护义务主体持有的个人数据联邦法（第31、40、42、82条）
云日志服务 Log Tank Service(LTS）	提供日志收集、实时查询、存储等功能，无需开发即可利用日志做实时决策分析，提升日志处理效率，帮助用户轻松应对日志实时采集、查询分析等日常运营、运维场景。 客户可通过LTS保留对个人数据的操作记录，保障个人数据拥有者的知情权。	保护私人持有的个人数据联邦法（第20条） 保护私人持有的个人数据联邦法律的条例（第50、52、59、61、64条） 保护义务主体持有的个人数据联邦法（第40条）
云数据库MySQL MySQL RDS for MySQL（RDS）	RDS为客户提供稳定可靠、可弹性伸缩的云数据库部署服务。 客户可通过RDS实现完全托管软硬件部署、补丁升级、自动备份、监控告警、弹性扩容、故障转移等功能，并在业务高负载情况下保证数据不丢失。	保护私人持有的个人数据联邦法（第21条） 保护私人持有的个人数据联邦法律的条例（第50、52、59、61条） 保护义务主体持有的个人数据联邦法（第31、42、82条）
文档数据库服务 Document Database Service（DDS）	文档数据库服务（Document Database Service）完全兼容MongoDB协议，提供安全、高可用、高可靠、弹性伸缩和易用的数据库服务。 客户可通过DDS实现一键部署、弹性扩容、容灾、备份、恢复、监控和告警等功能。	保护私人持有的个人数据联邦法（第21条） 保护私人持有的个人数据联邦法律的条例（第50、52、59、61条） 保护义务主体持有的个人数据联邦法（第31、42、82条）

弹性云服务器 Elastic Cloud Server（ECS）	ECS可以根据客户需要自定义服务器配置，灵活地选择所需的计算资源，打造可靠、安全、灵活、高效的应用环境。客户可以通过ECS实现Web应用防火墙、漏洞扫描等多种维度的安全服务，实现对自身云环境的安全评估，实现基于可定制的白名单机制的智能化进程管理， 实现通用Web漏洞检测、第三方应用漏洞检测等多项扫描服务。	保护私人持有的个人数据联邦法（第21条） 保护私人持有的个人数据联邦法律的条例（第50、52、59、61条） 保护义务主体持有的个人数据联邦法（第31、42、82条）

- **安全产品**

产品名称	产品介绍	对应的核心要求及控制措施
数据库安全服务 Database Security Service(DBSS)	DBSS是一款智能的数据库安全服务，基于机器学习机制和大数据分析技术，提供数据库审计，SQL注入攻击检测，风险操作识别等功能。 客户可通过DBSS检测潜在风险，保障云上数据库的安全。	保护私人持有的个人数据联邦法（第21条） 保护私人持有的个人数据联邦法律的条例（第50、52、59、61条） 保护义务主体持有的个人数据联邦法（第31、42、82条）
数据加密服务 Data Encryption Workshop(DEW)	DEW是一款综合的云上数据加密服务，提供专属加密、密钥管理、密钥对管理等功能。其密钥由硬件安全模块保护，并与华为云其他服务集成。 客户也可以借此服务开发自己的加密应用。 客户可采用DEW进行密钥全生命周期集中管理，保障数据存储过程中的完整性。	保护私人持有的个人数据联邦法（第21条） 保护私人持有的个人数据联邦法律的条例（第50、52、59、61条） 保护义务主体持有的个人数据联邦法（第31、42、82条）
Web应用防火墙 Web Application Firewall(WAF)	WAF可对网站业务流量进行多维度检测和防护，结合深度机器学习智能识别恶意请求特征和防御未知威胁，阻挡诸如SQL注入或跨站脚本等常见攻击。 客户可使用WAF保护其网站或服务器免受外部攻击，避免这些攻击影响Web应用程序的可用性、安全性或过度消耗资源，降低数据被篡改、失窃的风险。	保护私人持有的个人数据联邦法（第21条） 保护私人持有的个人数据联邦法律的条例（第50、52、59、61条） 保护义务主体持有的个人数据联邦法（第31、42、82条）

漏洞扫描服务 Vulnerability Scan Service(VSS)	VSS是一款多维度的安全检测服务，具有Web漏洞扫描、操作系统漏洞扫描、资产内容合规检测、配置基线扫描、弱密码检测五大核心功能。 客户可通过VSS可自动识别网站或服务器暴露在网络中的安全威胁，从而保护数据的完整性。	保护私人持有的个人数据联邦法（第21条） 保护私人持有的个人数据联邦法律的条例（第50、52、59、61条） 保护义务主体持有的个人数据联邦法（第31、42、82条）
DDoS高防 (AAD)	AAD是一款保护互联网服务器免受大流量DDoS攻而击导致不可用的增值服务。 客户可以通过AAD产品配置高防IP，将攻击流量引流到高防IP清洗，确保源站业务稳定可靠。	保护私人持有的个人数据联邦法（第21条） 保护私人持有的个人数据联邦法律的条例（第50、52、59、61条） 保护义务主体持有的个人数据联邦法（第31、42、82条）

- **网络产品**

产品名称	产品介绍	对应的核心要求及控制措施
虚拟专用网络 Virtual Private Network(VPN)	VPN用于搭建客户本地数据中心与华为云VPC之间便捷、灵活，即开即用的IPsec加密连接通道。 客户可通过VPN实现灵活一体，可伸缩的混合云计算环境，并且由于VPN的加密特性，提高了客户的安全防护能力。	保护私人持有的个人数据联邦法（第21条） 保护私人持有的个人数据联邦法律的条例（第50、52、59、61条） 保护义务主体持有的个人数据联邦法（第31、42、82条）
虚拟私有云 Virtual Private Cloud(VPC)	VPC是客户在华为云上的隔离的、私密的虚拟网络环境。客户可以自由配置VPC内的IP地址段、子网、安全组等子服务，也可以申请弹性带宽和弹性IP搭建业务系统。 VPC是客户的云上私有网络，各客户之间100%隔离，增强云上数据的安全性。	保护私人持有的个人数据联邦法（第21条） 保护私人持有的个人数据联邦法律的条例（第50、52、59、61条） 保护义务主体持有的个人数据联邦法（第31、42、82条）

API网关 API Gateway（APIG）	APIG是为客户提供高性能、高可用、高安全的API托管服务，轻松构建、管理和部署不同规模的API。 客户可通过APIG提供的身份认证和权限管理来保护API，并实施灵活而精细的配额管理、流控管理来保护后端服务，灵活、安全的开放服务能力。	保护私人持有的个人数据联邦法（第21条） 保护私人持有的个人数据联邦法律的条例（第50、52、59、61条） 保护义务主体持有的个人数据联邦法（第31、42、82条）

- **数据存储产品**

产品名称	产品介绍	对应的核心要求及控制措施
云硬盘备份 Volume Backup Service(VBS)	VBS为云硬盘创建在线永久增量备份，并对加密盘发备份数据自动加密，并可将数据恢复到任意备份点，增强数据可用性。 VBS可降低病毒入侵、人为误删除、软硬件故障等事件的发生的可能性，保护数据安全可靠，降低数据被非法篡改的风险。	保护私人持有的个人数据联邦法（第21条） 保护私人持有的个人数据联邦法律的条例（第50、52、59、61条） 保护义务主体持有的个人数据联邦法（第31、42条）
云服务器备份 Cloud Server Backup Service(CSBS)	CSBS可同时为云服务器下多个云硬盘创建一致性在线备份。 CSBS可降低病毒入侵、人为误删除、软硬件故障等事件的发生的可能性，保护数据安全可靠，降低数据被非法篡改的风险。	保护私人持有的个人数据联邦法（第21条） 保护义务主体持有的个人数据联邦法（第31、42条）
对象存储服务 Object Storage Service（OBS）	OBS是一款稳定、安全、高效、易用的云存储服务，可存储任意数量和形式的非结构化数据。 客户可通过OBS加密上传数据，对访问用户的身份进行鉴权，结合多种方式和技术确保数据传输与访问的安全，且可以针对敏感操作开启身份验证保护。	保护私人持有的个人数据联邦法（第21条） 保护私人持有的个人数据联邦法律的条例（第50、52、59、61条） 保护义务主体持有的个人数据联邦法（第31、42条）

云硬盘 Elastic Volume Service（EVS）	EVS是一种为ECS等计算服务提供持久性块存储的服务，提供高可用性、持久性，稳定的低时延性能。 客户可通过EVS加密系统盘和数据盘，且应用无感知，安全便捷，可利用分布式多副本技术，保证任何一个副本故障时快速进行数据迁移恢复，避免单一硬件故障造成数据丢失。	保护私人持有的个人数据联邦法（第21条） 保护私人持有的个人数据联邦法律的条例（第50、52、59、61条） 保护义务主体持有的个人数据联邦法（第31、42条）

6 华为云隐私保护相关认证资质

华为云遵守业务开展地所有适用的隐私相关法律法规。华为云投入专业的法律团队紧密关注法律法规更新情况，对海内外法律法规保持持续跟踪并进行快速分析，确保遵循法律法规的要求。

华为云隐私保护和个人资料安全的能力和成效在全球范围得到广泛认可，截至目前为止，华为云共取得海内外十余家机构的相关认证，获得20余项认证证书，主要包括适用于全球的隐私安全标准类认证、数据安全标准类以及适用于部分地区的数据安全认证。

隐私标准类认证，包括：

- **ISO 27701**

  隐私信息管理体系认证。通过ISO 27701认证表明华为云在隐私数据保护领域建立了完善的管理体系。

- **ISO 29151**

  国际个人身份信息保护实践指南。通过ISO 29151认证表明华为云实施了国际认可的、贯穿个人资料处理全生命周期的管理措施。

- **ISO 27018**

  云平台个人资料保护的国际行为准则。通过ISO 27018认证表明华为云满足国际认可的公有云平台个人资料保护措施的要求，可保障客户个人资料安全。

- **BS 10012**

  英国标准协会（BSI）发布的个人信息数据管理体系标准。通过BS 10012认证表明华为云在个人资料保护上拥有完善的体系以保障个人资料安全。

- **SOC审计**

  由第三方审计机构根据美国注册会计师协会（AICPA）制定的相关准则，针对外包服务商的系统和内部控制情况出具的独立审计报告。目前华为云已通过SOC 1 Type II、SOC 2 Type II审计并发布了SOC 3报告。

数据安全标准类认证，包括：

- ISO 27001信息安全管理体系认证
- ISO 27017云服务信息安全管理体系
- ISO 20000信息技术服务管理体系认证
- ISO 22301业务连续性管理体系

- CSA STAR云安全国际金牌认证
- PCI DSS第三方支付行业数据安全标准认证
- 国际通用准则CC EAL3+安全评估标准
- PCI 3DS支持3DS实施的安全标准
- TISAX可信信息安全评估交换

地区性安全认证，包括：

- MTCS Level3多层云计算安全规范（新加坡）
- OSPAR新加坡银行业公会(ABS)外包服务提供商审计报告（新加坡）
- 云服务用户数据保护能力认证（中国）
- 可信云服务评估（中国）
- 网络安全等级保护（中国）
- 可信云金牌运维专项评估（中国）
- 网信办网络安全审查（中国）
- 工信部云计算服务能力（中国）

7 结语

华为云始终秉持着华为公司“以客户为中心”的核心价值观，积极践行信息安全实践，为此华为云构建了信息安全管理体系，应用业界通用的信息安全保护技术，通过第三方机构的认证与审核检查安全控制的有效落实，致力于保护客户的数据安全。同时，为帮助客户应对日益复杂和开放的网络环境及日益发展的信息安全技术，华为云不断开发各种数据保护领域的工具、服务和方案，支持客户提升数据保护能力，降低风险。本白皮书仅供客户作为参考，不具备任何法律效力或构成法律建议，也不作为任何客户在云上环境一定合规的依据。客户应酌情评估自身业务和安全需求，选用适合的云产品及服务。

8 版本历史

日期	版本	描述
2021年11月	1.0	首次发布