# 华为云阿根廷 PDPL 合规性说明

**文档版本** 1.0

**发布日期** 2020-12-16

**华为技术有限公司**

**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，华为公司对本文档内容不做任何明示或默示的声明或保证。

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。

# 华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： https://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

# 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国际站在阿根廷开放的产品和服务。

## 1.2 发布目的

本文档旨在帮助客户了解：

1. 华为云隐私保护责任模型；
2. 《阿根廷第25,326号个人数据保护法》（Argentina Personal Data Protection Act 25,326，以下简称“**PDPL**”）及相关法律要求；
3. 基于责任模型，华为云自身对PDPL的遵循；
4. 华为云在隐私管理上已实现的控制和成效；
5. 基于责任模型，PDPL管辖下的客户须遵循的责任与义务；
6. 如何利用华为云的安全产品或服务实现隐私保护合规。

## 1.3 基本定义

- **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。

- **个人数据**

  可识别到明确自然人或法人的任何类型的信息。

- **敏感数据**

  揭示数据拥有者的种族和族裔血统、政治观点、宗教、哲学或道德信仰、工会会员资格以及有关健康状况、性习惯、性行为的个人数据。

- **数据处理**

无论是通过电子或其他方式，包含收集、保存、组织、存储、修改、关联、评估、分区、销毁的个人数据处理行动，以及与第三方之间的报告、查询、互联、传输等通讯的系统操作和流程。

- **数据拥有者**

  凡是在阿根廷境内有法定住所、办事机构、分支机构的自然人或者法人，且其数据以PDPL所规定的形式进行处理的，皆定义为的数据拥有者。

- **数据使用者**

  可以自行决定如何处理存储在其拥有或可能通过连接访问的文件、寄存器或数据银行中（此处指华为云提供的平台、系统或其他云服务）的个人数据的个人或法人。

- **数据分离**

  可使所获得的信息不能与任何特定或可确定的人相关的个人数据处理方式。

- **帐户信息**

  指客户在创建或管理其华为云帐户时向华为云提供的数据，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。对于帐户信息中的个人信息，华为云是数据使用者。

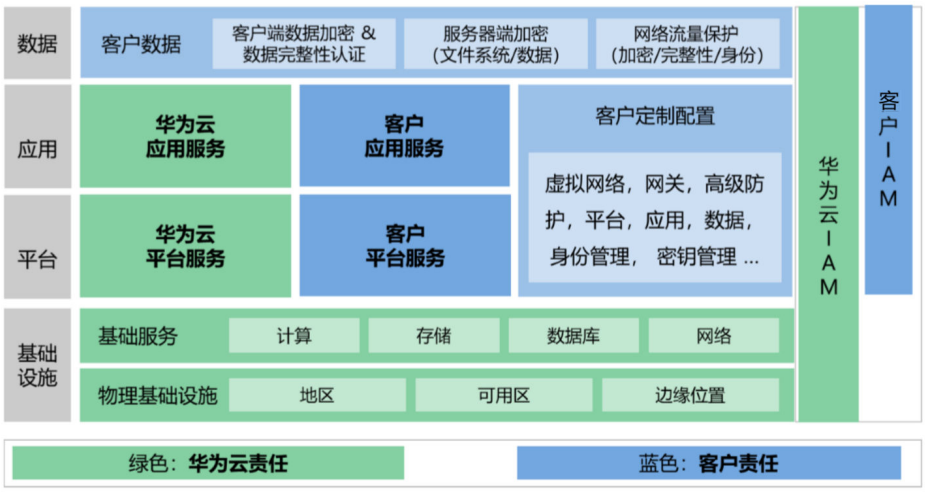
- **内容数据**

  指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。内容数据中可能会包含个人信息，对于内容数据中的个人信息，客户是数据使用者。

# 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，需要客户与华为云共同努力。基于此，华为云为帮助客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。在模型中客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，华为云与客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客户个人数据安全与合规，另一方面负责为客户提供安全、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**。

- **客户隐私保护**：华为云识别并保护客户的个人数据。从公司政策、流程、操作层面制定了隐私保护策略，并采取数据分离、数据加密、系统及平台安全防护等措施，全面保护客户隐私的安全。
- **平台安全及客户安全支持**：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，提升华为云的应用安全、平台安全水平以遵从适用的隐私保护法规的要求。同时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隐私保护。

**客户**：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，因此客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**：客户应正确、全面地识别云端的个人数据，制定可保护个人数据的安全性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**：客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 阿根廷隐私法规概述

## 3.1 法规背景介绍

PDPL于2000年10月30日经阿根廷国会批准生效，适用于位于阿根廷境内就个人或法律实体（后者需位于阿根廷或在阿根廷设有办事处、分支机构）个人数据的处理行为，目的是全面保护记录在数据文件、寄存器、数据库或数据银行或其他数据处理技术手段中的个人数据。

由于法规已经发布了较长时间，而云计算的概念在立法通过后的6年，即2006年才被首次提出，云服务与PDPL中提及的数据文件、寄存器、数据库或数据银行具有一定的相似性。因此华为云依据PDPL的要求对收集的客户个人数据或存储的客户内容数据中包含的个人数据进行适当地保护。

除PDPL之外，阿根廷监管机构发布了多份具体化的规则与指引帮助数据使用者更好地符合PDPL的要求，其中较为核心的一份文件为2018年7月23日由阿根廷获取公众信息局（以下简称“AAPI”）颁布的第47/2018号决议(Resolution 47/2018，以下简称“第47号决议”)。第47号决议旨在促进数据使用者对PDPL相关要求的进一步遵循，为管理、规划、控制和持续改善信息安全提供了安全措施的建议。

## 3.2 PDPL 的核心监管要求

PDPL规定了如下有关个人数据处理的核心监管要求：

- **保障个人数据的质量**

  为了确保个人数据的质量，PDPL第4条做出了相关的规定，主要内容包括目的适当性、合法正当、目的限定、数据准确、数据更正、数据访问及数据保留限制。

- **通知和获取同意**

  每当数据使用者要求数据拥有者提供个人数据时，数据使用者应事先以清晰和明确的方式通知数据所有者数据处理的目的、数据使用人身份及类型、提供数据不准确或不提供数据的后果及数据所有者享有的数据访问、更正和删除的权利。发送给数据所有者的通知须以书面形式或其他类似形式作出，在获得数据所有者的明示同意后，数据使用者才能对数据进行处理。

- **有条件地收集和处理敏感数据与医疗数据**

  数据使用者不能强迫数据拥有者提供敏感数据。仅当在出于公共利益的考虑被法律所授权或无法识别数据所有者时出于统计及科研的需求，才可收集与处理敏感

数据。同时，PDPL禁止储存可能直接或间接透露敏感数据的信息也禁止被存储。当医疗机构、医学研究机构以提供患者医疗服务为目的时，可以收集患者的医疗数据。

- **保障数据安全**

  数据使用者必须采取必要的技术和组织措施，保护个人数据免受更改、丢失、未经授权的访问或处理，充分保障个人数据的安全性和机密性。

- **保密义务**

  数据使用者以及参与个人数据处理任何阶段的所有人员均对个人数据负有保密责任。即使不再作为数据使用者或参与个人数据处理，其仍然需要承担保密责任。

- **数据传输相关的同意**

  仅在与数据使用者和个人数据接收者的合法利益直接相关的前提下，且告知数据拥有者此类数据传输的目的并获得同意后，才能传输处理的个人数据。接收者与数据使用者负有相同的义务。

  数据拥有者就数据传输的同意是可撤销的。当数据传输直接在政府之间进行或采取了数据分离措施，则数据使用者无需获得数据拥有者的同意。

- **有条件的跨境传输**

  除国际司法合作、流行病学调查需要、为打击犯罪进行国际合作以及阿根廷就相关传输规定有专门的国际条约等例外情况之外，PDPL禁止将任何类型的个人数据传输到没有提供足够保护水平的国家或国际组织或超国家实体。

- **信息登记要求**

  PDPL要求数据使用者或负责个人数据文件、数据库或寄存器的个人，必须向当地的监管机构建立的登记处登记相关信息，包括：负责人姓名和住址、收集个人数据的目的、收集个人数据的特质、收集和更新个人数据的方法、保证数据安全性的手段以及可能传输个人数据的目的地等。

- **数据留存时间限制**

  数据使用者在履行合同义务后，应及时删除存储的个人数据。在合理推测未来可能提供服务的情况下，个人数据可留存时间最长不超过2年。

- **直接促销的数据处理限制**

  数据使用者仅可在特定情况下向数据拥有者发送电子营销的商业信息，例如个人数据可以在公共文档中获取、数据拥有者主动提供、已获取数据使用者的同意等情况。

## 3.3 第 47 号决议的安全措施要求

AAPI作为阿根廷数据保护的监管机构，在2018年发布了第47号决议。第47号决议规定数据使用者应采取必要技术和组织措施，保障个人数据的安全性和机密性，该决议从数据收集、访问控制、变更管理、备份和恢复、漏洞管理、销毁信息、安全事件及开发环境八个控制领域出发，依据国际标准提出了共30个具体安全保护目标以及相对应的建议安全控制措施。

## 3.4 PDPL 的角色划分

PDPL规定了数据拥有者和数据使用者两种角色。

数据拥有者是个人数据的所有者，享有PDPL赋予的知情权、访问权、撤回权、更正、更新和限制处理权等。

数据使用者需对收集的个人数据负责，基于PDPL的核心要求（见3.2章）收集、处理、保护、传输数据拥有者的个人数据，并应遵从如第47号决议等监管机构发布的条例、良好实践指南等官方文件。

## 3.5 华为云在 PDPL 下的角色

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创建或管理华为云帐号时提供的个人数据。

在处理客户的内容数据中的个人数据时，客户作为数据使用者，需承担PDPL中对数据使用者设定的义务。华为云仅依从客户指令对内容数据进行处理并保密，同时会采取恰当的安全措施保护客户的内容数据安全。

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，华为云会基于为客户提供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。此时华为云作为客户个人数据的数据使用者，将负责该部分客户个人数据的安全性及隐私保护，按照法律规定对个人数据进行收集、处理、存储，并对数据拥有者权利申请进行响应。

# 4 华为云如何响应阿根廷 PDPL 及其实施细则

## 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、对数据拥有者，即数据拥有者，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 华为云响应 PDPL 的合规措施

基于华为云业务的特性，根据PDPL的要求，**在管理客户账户信息时，**华为云作为数据使用者，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阿根廷PDPL规定个人数据使用的核心要求。

| PDPL核心要求 | 华为云适用的具体要求 | 华为云采取的措施 |
| --- | --- | --- |
| **保障个人数据的质量** | **目的适当性：**收集和处理的个人数据必须出于确定的、适当的和相关的处理目的。<br>**合法正当：**不得使用不忠实或欺诈手段或违反PDPL规定的方式进行数据收集。<br>**目的限定：**不得把收集和处理的个人数据用于与收集目的不符或超出范围的目的。<br>**数据准确：**数据应准确并在必要时进行更新。<br>**数据更正：**对于所有不准确或不完整的数据，数据使用者在收到有关情况后进行禁用/删除或替换。<br>**数据访问权：**数据使用者应保证数据拥有者可以访问到其被收集或处理中的个人数据。<br>**数据保留限制：**一旦不再需要或与收集目的无关时，应销毁这些数据。 | 华为云以为客户提供云服务为核心，基于《隐私政策声明》中披露的目的收集和处理个人数据，并且华为云针对涉及个人数据的产品及服务会定期进行隐私影响评估，以防产品及服务涉及的个人数据收集、处理超出实际目的所需范围。<br>华为云为客户提供便捷的行使数据拥有者权利的渠道，客户可以通过《隐私政策声明》中的邮箱发起访问、修改其不正确或不完整个人信息的请求，华为云将在验证请求者身份信息后为客户提供所查询的个人数据副本或根据请求对不完整或不准确的信息进行更新、替换或废除等处理。<br>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数据分离或删除等安全处理。 客户可以使用官网关闭帐号功能删除保存在华为云中的数据。 |

| PDPL核心要求 | 华为云适用的具体要求 | 华为云采取的措施 |
| --- | --- | --- |
| **通知和获取同意** | **通知：**收集个人数据时，应事先以清晰和明确的方式向数据拥有者通知，通知的内容包括：数据处理的目的、数据接收者的身份、提供数据不准确或不提供数据的后果及数据拥有者享有的权利。<br>**明示同意：**通知必须通过明示或突出的方式以书面或其他等同方式呈现给数据拥有者，在获得数据拥有者的同意后才能对数据进行收集和处理。 | **《隐私政策声明》**中介绍了华为云将如何收集和处理客户的个人数据、告知其是否必须提供数据、拒绝提供数据的后果、数据使用目的、数据转移对象的类别以及数据拥有者享有的权利。<br>在客户注册帐号时，华为云会在官网明显处向客户展示**《隐私政策声明》**，客户需点击“确认”按钮以表示同意**《隐私政策声明》**。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。<br>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，并重新获取客户的同意。 |

| PDPL核心要求 | 华为云适用的具体要求 | 华为云采取的措施 |
| --- | --- | --- |
| **保障数据安全** | 数据使用者必须实施合理和适当的组织和技术措施，以保护个人数据免受更改、丢失以及未经授权的访问和处理。数据使用者应把个人数据存储在符合技术完整性和安全性的环境中。 | 华为云采取多种管理和技术控制，保护个人信息的安全性。<br>**组织安全措施：**华为集团已设置全球网络安全与用户隐私保护官，负责华为隐私保护政策的制定及推行。华为云设置了隐私保护专家团队，包括隐私保护领域专家、法务人员以及网络和信息安全专职人员，为华为云隐私保护战略和实践上提供专业的支撑。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，帮助华为云在当地开展的各类活动满足适用的隐私法律法规要求。<br>华为云建立了覆盖各业务的隐私保护治理框架，并通过一系列的隐私保护流程，保障业务活动开展符合隐私保护的要求，如数据拥有者权利保障、数据泄露应急响应、个人数据留存等。<br>华为云对于个人信息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。<br>**物理安全措施：**华为云已制定并实施完善的物理和环境安全防护策略、规程和措施，同时，华为云运维运营团队严格执行访问控制、安保措施、例行监控审计、应急响应等措施，以保障华为云数据中心的物理和环境安全。<br>**技术安全措施：**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；在数据存储和传输方面，采用加密技术对敏感数据进行加密；在风险监测方面，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。<br>**安全性认证：**此外，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，以保证华为云的隐私安全，包括ISO 27701、ISO 29151、ISO |

| PDPL核心要求 | 华为云适用的具体要求 | 华为云采取的措施 |
| --- | --- | --- |
| | | 27018、BS 10012、SOC2 Type1隐私原则的审计报告等（详细的认证介绍见第6章），其中ISO27018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。 |
| **保密义务** | 参与个人数据处理的所有人员或数据使用者应对接触过的个人数据严格保密。即使不再参与处理个人数据，这一义务也应继续履行。 | 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。当员工不再负责当前工作时，相关权限会被删除。 |
| **数据传输相关的同意** | 仅在数据使用者和个人数据接收者的合法利益直接相关的前提下，且告知数据拥有者此类数据传输的目的并获得同意后，才能传输处理的个人数据。 | 华为云在**《隐私政策声明》**中说明了个人数据使用的情形（目的、第三方的信息等）并获得了数据拥有者的同意。为向客户提供必须的交易支持、服务支持、安全支持，华为云可能将部分个人数据分享给关联公司、分公司、服务提供商、分包商、合作伙伴等第三方。<br>当传输个人数据给第三方时，华为云将使用加密传输并对数据进行数据分离操作，保护数据传输过程的安全。 |
| **跨境传输的同意** | 除例外情况外，应在确认传输的国家或国际组织有足够的水平保护个人数据时才能进行个人数据的跨境传输。 | 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。 |
| **信息登记要求** | 在处理内容数据前，应向当地的监管机构建立的登记处登记相关信息，包括：负责人姓名和住址、收集个人数据的目的、收集个人数据的特质、收集和更新个人数据的方法、保证数据安全性的手段以及可能传输个人数据的目的地等。 | 根据ISO27001标准的要求，华为云配备了专人与行业机构、风险和合规组织、地方当局和监管机构保持联系并建立联络点。<br>华为云设立了专岗同外部各方保持积极的联系，以关注法律、法规的动态。 |

| PDPL核心要求 | 华为云适用的具体要求 | 华为云采取的措施 |
| --- | --- | --- |
| **数据留存时间限制** | 在履行合同义务后，应及时删除存储的个人数据。在合理推测未来可能提供服务的情况下，个人数据可留存时间最长不超过2年。 | 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，华为云会严格遵循数据销毁标准和与客户之间的协议约定，对存储的客户数据进行清除。 |
| **直接促销的数据处理限制** | 应仅可在特定情况下向数据拥有者发送电子营销的商业信息，例如个人数据可以在公共文档中获取、数据拥有者主动提供、已获取数据使用者的同意等情况。 | 客户注册华为云官网帐号时可以选择是否同意将个人数据用于促销，在获得客户，即数据拥有者同意后，华为云才会向客户推送促销信息。<br>在客户同意促销后，华为云通过短信或者邮件方式发送促销信息给客户。<br>如果客户需要停止将其个人数据用于直接促销，可以在用户中心的消息接收配置中进行修改。 |

# 4.4 华为云响应第 47 号决议（Resolution 47/2018）的合规措施

华为云积极采取多种类型及维度的管控措施保障数据的安全，并根据第47号决议的要求，履行数据使用者在收集、访问、变更、开发、销毁和安全事件发生时保护个人数据安全的义务，具体措施如下：

## A. 个人数据的收集

| 目的 | 控制简述 | 华为云采取的措施 |
| --- | --- | --- |
| A.1 数据完整性 | A.1.1确保完整性 | 华为云内部制定了数据安全规范，规范了数据在收集传输过程中的分级管控要求，对传输通道采用合理的加密技术手段，检测重要数据传输过程中的完整性。华为云按照数据分级标准，对不同级别的数据采用对应的加密技术机密数据，保护了数据的完整性。 |
| | A.1.2 最小化输入错误 | 华为云针对收集的数据类型设计了不同的数据输入策略，限制了用户输入数据的格式、位数及所含字符要求，降低的输入错误的可能性。 |
| | A.1.3确保数据准确性 | 华为云具有数据校验机制，对输入的数据例如手机号、邮箱通过验证码进行校验，验证收集的数据是准确有效的。 |

| 目的 | 控制简述 | 华为云采取的措施 |
| --- | --- | --- |
| A.2 保密性 | A.2.1 确保收集过程中的机密性 | 华为云建立了一套科学有效的管理体系， 能够系统的、持续的管理安全风险，具备保障自身及客户的数据保密性、完整性和可用性的能力，并且通过了**CSA STAR金牌认证**。 |
| | A.2.2 限制对数据收集的访问 | 华为云制定严格的密码策略和启用多因素认证，对访问收集过程的权限进行严格控制。<br>同时，华为云使用了IAM访问控制和身份认证技术管理访问收集过程的权限控制，并对传输通道采用了加密技术，来限制对收集过程的非授权访问。 |
| | A.2.3限制收集过程中的未授权访问 | |

## B. 访问控制

| 目的 | 控制简述 | 华为云采取的措施 |
| --- | --- | --- |
| B.1 资产识别 | B.1.1 识别资产 | 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。<br>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。<br>华为云通过内外部审计检查控制效果，内部审计持续追踪安全控制措施的有效性，外部审计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。 |
| | B.1.2 定义责任人及定义责任范围 | |
| | B.1.3 验证控制措施的应用 | 华为云具有访问控制机制，为每一位员工提供了唯一的身份标识并根据工作职责划分权限并通过日志记录和审计技术记录对各关键系统的访问，定时进行监控和审计来管理特权账户。 |
| B.2 数据访问 | B.2.1 管理对系统的访问 | 华为云依据ISO27001的要求建立了访问控制管理要求，遵循权限最小化原则、权限分离原则，定期对员工的权限范围进行审核，避免出现超出其工作范围应覆盖的权限。<br>员工在每一次登陆时华为云对其身份进行验证，出现事故时可及时追溯日志进行问责。<br>当员工在岗状态发生变化时，及时对其权限进行清理与修改。员工的登陆、操作等日志将留存需要的时间以响应审核需求。 |
| | B.2.2分配权限 | 华为云已制定并实施完善的物理和环境安全防护策略、规程和措施。华为云数据中心严格管理人员及设备进出，在数据中心园区及建筑的门口设置7×24小时保安人员进行登记盘查，限制并监控来访人员授权活动范围。门禁控制系统在不同的区域采取不同安全策略的门禁控制 |

| 目的 | 控制简述 | 华为云采取的措施 |
| --- | --- | --- |
| | B.2.3 验证身份和授权 | 系统，严格审核人员出入权限。华为云数据中心采用当前通用的机房安保技术监测，并消除物理隐患。对机房外围、出入口、走廊、电梯、机房等进行7×24小时闭路电视监控，并与红外感应、门禁等联动。保安人员对数据中心定时巡查，并设置在线巡更系统。对非法闯入和其他安保事件及时进行声光报警。<br>华为云对员工按工作需要的最小范围分配权限，并对其信息安全管理系统、敏感信息的访问、修改等操作进行监控和记录。所有的端口、应用、系统组件等的访问均仅向授权的个人和应用程序开放。 |
| | B.2.4 控制对数据中心的物理访问 | 华为云严格遵从国际相关标准要求，对数据中心进行统一垂直管理，实施分层分级的安全防护，从围栏到 DC 建筑，从 DC 建筑到模块，从模块到机柜，从机柜到服务器，安全防护措施逐级增强，确保数据中心的物理和环境安全。在严格执行物理访问控制的同时，通过智能的 7×24 小时监控，及时发现并修复安全隐患，维护数据中心稳定运行。 |
| | B.2.5 监测活动 | 华为云具有访问权限管理机制，对于访问个人数据的权限进行了严格控制，并在不需要时立刻删除该权限。同时华为云通过日志记录和审计技术监控对敏感数据的访问。 |
| | B.2.5监测活动（敏感数据） | |

## C. 变更管理

| 目的 | 控制简述 | 华为云采取的措施 |
| --- | --- | --- |
| C.1 变更管理 | C.1.1 确认变更 | 华为云有配置和变更管理的机制，对生产环境的各要素，如机房设施、网络、系统平台软硬件和应用等的更改采取统一的变更管理流程，经过申请、环境测试等验证测试和安全评审后才能进行变更，提升数据的完整性、可用性和机密性。 |
| | C.1.1确认变更（敏感数据） | |

## D. 备份和恢复

| 目的 | 控制简述 | 华为云采取的措施 |
| --- | --- | --- |
| D.1 备份副本和恢复过程 | D.1.1 确保正式的备份和恢复流程 | 华为云具有备份策略，会对个人数据定期进行备份，并且会定期对系统内的个人数据的备份有效性进行测试，并保留备份测试的记录。 |

| 目的 | 控制简述 | 华为云采取的措施 |
| --- | --- | --- |
| | D.1.2 确保对存储介质的访问控制 | 华为云具有访问控制机制，对存储个人数据备份的服务器或机房和进行备份恢复测试的环境进行了访问权限控制和物理访问控制，并且通过与数据加密服务集成对存储的备份进行了加密。 |
| | D.1.2 确保对存储介质的访问控制（敏感数据） | |

## E. 漏洞管理

| 目的 | 控制简述 | 华为云采取的措施 |
| --- | --- | --- |
| E.1 漏洞管理 | E.1.1 预防安全事件的设计 | 华为云构建了统一的分析和预警平台，全面掌握数据安全态势，快速识别、响应安全事件，同时通过对告警、事件、资产等信息的关联分析进行风险评估以及安全态势预测，由此可预先制定安全防护策略，做到防范于未然。 |
| | E.1.2 确保充分保护 | 华为云在互联网边界部署 Anti-DDoS设备，来完成对异常和超大流量攻击的检测和清洗。同时在关键网络分区边界部署入侵防御设备，识别来自互联网以及客户间的攻击行为，并能够进行自动化、精确的阻断。<br>华为云所有云平台主机均安装安全防护软件，进行主机层面的弱密码检测、配置管理、入侵检测、应急响应等，构建合规、安全的主机环境。<br>华为云对生产、测试和开发环境进行了物理间隔和加密，并且有完善的访问权限控制机制来管理对不同环境的访问。<br>华为云拥有完善的安全事件管理机制，并建立了事件管理平台。通过安全日志监控和审计日志监控，华为云对安全事件进行预警和追踪所有的信息安全事件的进展、处置措施与落实，对事件处置后的影响进行分析。<br>针对日常多样化的攻击告警事件，华为云有专业的安全事件管理系统对安全事件进行端到端的跟踪闭环，整个处置过程可回溯。 |
| | E.1.2 确保充分保护（敏感数据） | |

| 目的 | 控制简述 | 华为云采取的措施 |
| --- | --- | --- |
| | E.1.3检测潜在的安全事件 | 华为云使用IPS入侵防御系统、Web应用防火墙、防病毒软件以及HIDS主机型入侵检测系统对系统组件及网络进行漏洞管理。IPS入侵防御系统可以检测并预防潜在的网络入侵活动；Web应用防火墙部署在网络边界以保护应用软件的安全，使其免于受到来自外部的SQL注入、CSS、CSRF等面向应用软件的攻击；防病毒软件提供病毒防护及Windows系统内的防火墙；HIDS主机型入侵检测系统保护云服务器的安全，降低账户被窃取的风险，提供弱密码检测、恶意程序检测、双因子认证、脆弱性管理、网页防篡改等功能。<br>华为云通过内外部审计相结合的方式，持续追踪安全控制措施、系统安全配置的有效性。 |
| | E.1.4 保证有效和持久的措施（敏感数据） | 华为云拥有统一的分析和预警平台，全面掌握数据安全态势，快速识别、响应安全事件，同时通过对告警、事件、资产等信息的关联分析进行风险评估以及安全态势预测，由此可预先制定安全防护策略，做到防范于未然。 |

## F. 销毁信息

| 目的 | 控制简述 | 华为云采取的措施 |
| --- | --- | --- |
| F.1 确保销毁信息 | F.1.1设置销毁模型/格式 | 华为云支持根据客户要求对数据进行安全删除，安全删除的方式包括删除加密存储的加密密钥、底层存储回收并覆写、对报废的物理介质进行消磁/折弯/粉碎。 |
| | F.1.2 建立安全处置机制 | 华为云有建立数据安全处理机制，其中规定了数据的安全销毁处置要求，对不再需要的个人数据进行匿名化或删除等安全处理，并保留数据销毁、删除记录。<br>根据ISO27001标准，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，且删除介质或数据资产都会形成相应的删除记录。 |
| | F.1.3 指定负责销毁 | |
| | F.1.4 监控流程 | 华为云建立信息系统安全和个人数据处理监控的管理办法，并对处理个人数据的信息安全管理系统、数据访问、修改和销毁等操作进行监控和记录。 |
| | F.1.5丢弃磁性介质（敏感数据） | 华为云支持根据客户要求对数据进行安全删除，安全删除的方式包括删除加密存储的加密密钥、底层存储回收并覆写、对报废的物理介质进行消磁/折弯/粉碎。 |

## G. 安全事件

| 目的 | 控制简述 | 华为云采取的措施 |
| --- | --- | --- |
| G.1 安全事件通知 | G.1.1 建立责任和程序 | 华为云制定了完善的安全日志管理要求、安全事件定级处置流程和7*24小时的专业安全事件响应团队以及对应的安全专家资源池来应对突发安全事件。华为云秉承快速发现、快速定界、快速隔离与快速恢复的安全事件响应原则。同时，华为云根据安全事件对整网、客户的危害刷新事件定级标准以及响应时限和解决时限等要求。详情请参考华为云发布的**《华为云安全白皮书》**。<br>当安全事件发生后，华为云有专人将安全事件的影响范围、性质、受影响的个人数据类型等内容总结为报告，遵循要求通知AAPI安全事件响应组织及受影响的数据拥有者。 |
| | G.1.2 准备报告 | |
| | G.1.3 发送通知 | |

## H. 开发环境

| 目的 | 控制简述 | 华为云采取的措施 |
| --- | --- | --- |
| H.1 安全的开发环境 | H.1.1 部署安全的开发环境 | 华为云使用DevOps以及DevSecOps 模式进行开发，实现开发、测试和QA环境分离，并制定了相应管理制度与流程对开发、变更活动进行控制。<br>华为云及相关云服务遵从安全及隐私设计原则和规范、法律法规要求，在安全需求分析和设计阶段根据业务场景、数据流图、组网模型进行威胁分析，并指定威胁削减方案。同时，所有云服务发布前均需通过多轮安全测试以及代码审查。 |

# 5 华为云协助客户响应 PDPL 的合规要求

## 5.1 客户关于 PDPL 的隐私保护责任

当客户的内容数据中包含其他数据拥有者的个人数据时，客户有可能需要受到PDPL的管辖。如若满足，客户应遵循PDPL中对于数据使用者的要求，同时华为云尽可能帮助客户响应其应承担的要求和义务。

| PDPL核心要求 | 客户的隐私保护责任 | 华为云为客户提供的服务支持 |
| --- | --- | --- |
| **保障个人数据的质量** | 客户应对其收集个人数据的质量负责，满足以下要求：<br>**目的适当性：**收集和处理的个人数据必须出于确定的、适当的和相关的处理目的。<br>**合法正当：**不得使用不忠实或欺诈手段或违反PDPL规定的方式进行数据收集。<br>**目的限定：**不得把收集和处理的个人数据用于与收集目的不符或超出范围的目的。<br>**数据准确：**数据应准确并在必要时进行更新。<br>**数据更正：**对于所有不准确或不完整的数据，数据使用者在收到有关情况后进行禁用/删除或替换。<br>**数据访问权：**数据使用者应保证数据拥有者可以访问到其被收集或处理中的个人数据。<br>**数据保留限制：**一旦不再需要或与收集目的无关时，应销毁这些数据。。 | 华为云仅依从客户的指令进行数据处理操作，客户应通过公平透明的原则收集个人数据并保障目的的适当性，不将个人数据用于约定以外的目的。<br>客户可自行修订、提取存储在华为云上的个人数据。当个人数据不再需要时，可自行删除数据。<br>同时华为云成立了专门的团队支持和客户的沟通联系，客户遇到困难时，可以通过工单服务寻求华为云的帮助。 |

| PDPL核心要求 | 客户的隐私保护责任 | 华为云为客户提供的服务支持 |
| --- | --- | --- |
| **通知和获取同意** | 客户应确保收集个人数据的通知和获取同意符合适用的法律法规：<br>**通知：**收集个人数据时，都应事先以清晰和明确的方式通知数据拥有者数据处理的目的、其数据收件人身份、提供数据不准确或不提供数据的后果及数据拥有者享有的权利。<br>**明示同意：**通知必须通过明示或突出的方式以书面或其他等同方式呈现给数据拥有者并获得数据拥有者的同意后才能对数据进行收集和处理。 | 华为云仅遵循客户的指令进行数据处理操作，内容数据收集的目的和范围由客户自行管理。<br>部分华为云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，帮助客户实现将个人数据处理的政策告知其数据拥有者。 |
| **有条件地收集和处理敏感数据与医疗数据** | 客户应根据自身的业务性质判断是否可收集个人敏感数据或医疗数据。若为可合法收集、处理敏感数据或医疗数据的个人或实体，则应获取客户的同意，并使用一定的技术对敏感数据进行数据分离或脱敏后再进行存储。 | 华为云产品中提供了动态数据脱敏及敏感数据发现策略，帮助客户生成脱敏规则和审计规则，对处理的个人敏感数据和处理记录中可能包含的个人敏感数据进行脱敏。 |
| **保障数据安全** | 客户须采取必要的技术和组织措施以保证个人数据的安全性和机密性、保护数据免受更改，丢失、未经授权的访问或处理。 | 华为云为客户提供了多种安全产品及服务，包括网络安全防护、事件监控及响应、访问控制、数据加密等功能的产品。详情请见本文档第5.3章节。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、DDoS高防AAD、漏洞扫描服务等。 |
| **保密义务** | 客户以及参与个人数据处理任何阶段的所有人员均对个人数据负有保密义务。即使不再作为数据使用者或参与个人数据处理，其仍然需要承担保密义务。 | 华为云与其员工均签署了保密协议，约定了对于数据处理过程中的保密义务，并对员工的遵循情况进行定期审计。 |
| **数据传输相关的同意** | 客户应在传输个人数据之前，向数据拥有者提供有关传输目的、相关个人数据类别、数据传输的性质的信息，并得到数据拥有者对传输的同意。 | 部分华为云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，客户可以在隐私声明中告知数据拥有者其有关转让目的、相关个人数据类别、数据共享的性质的信息。 |
| **有条件地跨境传输** | 客户应在确认传输的国家或国际组织有足够的水平保护个人数据时才能进行个人数据的跨境传输。 | 部分华为云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，客户可以在隐私声明中告知数据拥有者个人数据可能被传输、存储至其他国家与地区。 |

| PDPL核心要求 | 客户的隐私保护责任 | 华为云为客户提供的服务支持 |
| --- | --- | --- |
| **信息登记要求** | 在处理内容数据前，客户应向当地的监管机构建立的登记处登记相关信息，包括：负责人姓名和住址、收集个人数据的目的、收集个人数据的特质、收集和更新个人数据的方法、保证数据安全性的手段以及可能传输个人数据的目的地等。 | - |
| **数据留存时间限制** | 在履行合同义务后，客户应及时删除存储的个人数据。在合理推测未来可能提供服务的情况下，个人数据可留存时间最长不超过2年 | 客户应形成内容数据中的个人数据的删除机制，并可通过云数据库产品对于指定数据进行删除操作。 |
| **直接促销的数据处理限制** | 应仅可在特定情况下向数据拥有者发送电子营销的商业信息，例如个人数据可以在公共文档中获取、数据拥有者主动提供、已获取数据使用者的同意等情况。 | 部分华为云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，客户可以在隐私声明中告知数据拥有者其个人数据将用于营销目的。 |

# 5.2 客户关于第 47 号决议（Resolution 47/2018）的合规责任

当客户作为数据使用者，应依据Resolution 47/2018的管控要求完善数据安全保护相关措施。

<table>
<tr><th>目的</th><th>控制简述</th><th>数据安全保护责任</th></tr>
<tr><td colspan="3">A. 个人数据的收集</td></tr>
<tr><td rowspan="3">A.1 数据完整性</td><td>A.1.1 确保完整性</td><td rowspan="6">客户的隐私保护责任：<br>作为数据使用者，客户应确保收集的个人数据在传输过程中的完整性，并采取适当的加密方法来保护传输过程中的个人数据。<br>客户应确保收集个人数据的准确性，以及对数据拥有者提供的数据进行数据校验。<br>客户应设置访问权限控制和身份管理，限制对收集的个人数据的非授权访问。<br>华为云为客户提供的服务支持：<br>华为云产品中提供统一身份认证IAM、云专线DC、虚拟专用网络VPN以及数据加密服务DEW等安全产品及服务来帮助客户保障个人数据收集过程中的保密性和访问权限控制，避免因未经授权访问带来的风险。</td></tr>
<tr><td>A.1.2 最小化输入错误</td></tr>
<tr><td>A.1.3 确保数据准确性</td></tr>
<tr><td rowspan="3">A.2 保密性</td><td>A.2.1 确保收集过程中的机密性</td></tr>
<tr><td>A.2.2 限制对数据收集的访问</td></tr>
<tr><td>A.2.3限制收集过程中的未授权访问</td></tr>
<tr><td colspan="3">B. 访问控制</td></tr>
</table>

| 目的 | 控制简述 | 数据安全保护责任 |
| --- | --- | --- |
| B.1 资产识别 | B.1.1 识别资产 | **客户的隐私保护责任：**<br>作为数据使用者，客户应对处理的个人数据资产进行识别，形成响应的数据资产清单并确认资产的负责人。<br>客户应对个人数据以及处理个人数据的系统设置访问权限控制和身份认证机制，对处理个人数据的系统和个人数据进行加密，分配对应的访问权限，防止对系统或个人数据的非授权访问。<br>并且客户应该对系统进行监控，开启访问日志对系统用户访问个人数据的活动进行记录和监控。<br>**华为云为客户提供的服务支持：**<br>华为云为客户提供的弹性云服务器ECS产品中包含添加标签的功能，标签用于标记云资源，如实例、镜像和磁盘等。如果客户的帐户下有多种云资源，并且不同云资源之间有多种关联，可以为云资源添加标签，实现云资源的分类和统一管理，便于客户识别和管理信息资产。<br>此外，华为云的IAM服务可以对员工的权限按角色进行管理，通过多因素验证等方式验证员工身份。并协同云日志LTS、云审计CTS服务，记录员工的操作并进行审计，监控异常行为的发生。 |
| | B.1.2 定义责任人及定义责任范围 | |
| | B.1.3 验证控制措施的应用 | |
| B.2 数据访问 | B.2.1 管理对系统的访问 | |
| | B.2.2分配权限 | |
| | B.2.3 验证身份和授权 | |
| | B.2.4 控制对数据中心的物理访问 | |
| | B.2.5 监测活动 | |
| | B.2.5监测活动（敏感数据） | |
| **C. 变更管理** | | |
| C.1 变更管理 | C.1.1 确认变更 | **客户的隐私保护责任：**<br>客户应在生产环境进行变更过程中验证生产环境的维护以及保护个人数据的完整性。应该对生产环境进行隔离、设置访问控制以及验证个人数据的完整性、可用性和机密性并保留相应的记录。<br>**华为云为客户提供的服务支持：**<br>客户可使用主机安全服务HSS对镜像文件进行完整性校验，对比的方法来确定当前文件状态是否不同于上次扫描该文件时的状态，利用这种对比来确定文件是否发生了有效或可疑的修改。当发现潜在风险，将及时提醒客户。 |
| | C.1.1 确认变更（敏感数据） | |
| **D. 备份和恢复** | | |
| D.1 备份副本和恢复过程 | D.1.1 确保正式的备份和恢复流程 | **客户的隐私保护责任：**<br>客户应该设置适当的备份策略和备份恢复流程，并且对备份副本进行加密，设置访问控制措施来保护备份的安全。<br>**华为云为客户提供的服务支持：** |
| | D.1.2 确保对存储介质的访问控制 | |

| 目的 | 控制简述 | 数据安全保护责任 |
| --- | --- | --- |
| | D.1.2 确保对存储介质的访问控制（敏感数据） | 华为云为客户提供云备份CBR、云硬盘备份VBS、云服务器备份CSBS服务。客户可根据需求对于数据及服务器进行备份，并通过IAM设置对于备份数据的访问权限。 |
| **E. 漏洞管理** | | |
| E.1 漏洞管理 | E.1.1 预防安全事件的设计<br>E.1.2 确保充分保护<br>E.1.2 确保充分保护（敏感数据）<br>E.1.3检测潜在的安全事件<br>E.1.4 保证有效和持久的措施（敏感数据） | **客户的隐私保护责任：**<br>客户应建立完善的安全事件管理机制来预防和监测安全事件的发生。客户应该通过漏洞扫描、环境隔离、外来入侵防护、审计日志以及持续的设备/硬件/程序更新等措施来预防和监测安全事件。<br>**华为云为客户提供的服务支持：**<br>华为云有专门的产品安全事件响应团队帮助客户建立成熟的漏洞响应机制，降低漏洞带来的风险。<br>同时客户也可使用华为云提供的漏洞扫描服务VSS中的 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，自动发现网站或服务器暴露在网络中的安全风险。<br>华为云拥有企业主机安全HSS服务提供资产管理、漏洞管理、基线检查、入侵检测等功能，降低主机安全风险，提升整体安全保障能力。 |
| **F. 数据销毁** | | |
| F.1 确保销毁信息 | F.1.1设置销毁模型/格式<br>F.1.2 建立安全处置机制<br>F.1.3 指定负责销毁<br>F.1.4 监控流程<br>F.1.5丢弃磁性介质（敏感数据） | **客户的隐私保护责任：**<br>客户应建立数据销毁机制，在数据拥有者提出删除请求或不再需要个人数据时对个人数据执行擦除程序，确保销毁的安全、保密和不可逆转性，并且保留相应的销毁记录。<br>客户应对存储个人数据的介质设置销毁机制，通过消磁、分解、焚烧、粉碎或复写技术实施物理销毁过程。<br>**华为云为客户提供的服务支持：**<br>华为云仅遵循客户的指令进行数据销毁操作，销毁的数据类别、数量和介质由客户自行决定。 |
| **G. 安全事件** | | |
| G.1 安全事件通知 | G.1.1 建立责任和程序<br>G.1.2 准备报告 | **客户的隐私保护责任：**<br>客户建立完善的安全事件报告机制，在安全事件发生后迅速形成安全事件报告并报告给相关方。<br>**华为云为客户提供的服务支持：** |

| 目的 | 控制简述 | 数据安全保护责任 |
| --- | --- | --- |
| | G.1.3 发送通知 | 客户可使用华为云云监控服务CES对服务器的运行状态、云上资源进行实时监控，当出现硬件故障时，云监控将会通过邮件、短信、HTTP/S通知客户。 |
| **H. 开发环境** | | |
| H.1 安全的开发环境 | H.1.1 部署安全的开发环境 | **客户的隐私保护责任：**<br>客户应该负责制定和实施安全开发策略，以满足法规定义的对开发环境的安全要求。并且客户应对其开发环境中的个人数据进行加密或匿名化操作。<br>**华为云为客户提供的服务支持：**<br>华为云支持客户使用虚拟私有云VPC服务在云上建立隔离的生产与测试环境流程。 |

# 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PDPL及相关规章要求。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**<br>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。<br>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。 | PDPL-保障个人数据的质量<br>PDPL-保障数据安全；<br>PDPL-保密义务;<br>第47号决议-A.2 保密性；<br>第47号决议-B.1 资产识别；<br>第47号决议-B.2 数据访问； |

| 产品名称 | 产品介绍 | 对应的核心要求及控制措施 |
| --- | --- | --- |
| 云审计服务<br>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。<br>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，保障数据拥有者的知情权、实现快速查找。 | PDPL-保障数据安全；<br>PDPL-保密义务;<br>第47号决议-A.2 保密性；<br>第47号决议-B.1 资产识别；<br>第47号决议-B.2 数据访问； |
| 云监控服务<br>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。<br>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。 | PDPL-保障个人数据的质量<br>PDPL-保障数据安全；<br>第47号决议-E.1 漏洞管理；<br>第47号决议-G.1 安全事件通知； |
| 云日志服务<br>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。<br>客户可通过LTS保留对个人信息的操作记录，保障数据拥有者的知情权。 | PDPL-保障数据安全；<br>PDPL-保密义务;<br>第47号决议-A.2 保密性；<br>第47号决议-B.1 资产识别；<br>第47号决议-B.2 数据访问；<br>第47号决议-G.1 安全事件通知； |

- **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<br>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。<br>客户可通过DBSS检测潜在风险，保障云上数据库的安全。 | PDPL-保障个人数据的质量<br>PDPL-保障数据安全；<br>第47号决议-A.1 数据完整性；<br>第47号决议-E.1 漏洞管理；<br>第47号决议-G.1 安全事件通知； |
| 数据加密服务<br>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。<br>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。 | PDPL-保障个人数据的质量<br>PDPL-保障数据安全；<br>第47号决议-A.1 数据完整性；<br>第47号决议-A.2 保密性；<br>第47号决议-E.1 漏洞管理； |
| Web应用防火墙<br>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。<br>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。 | PDPL-保障个人数据的质量<br>PDPL-保障数据安全；<br>第47号决议-A.1 数据完整性；<br>第47号决议-E.1 漏洞管理；<br>第47号决议-G.1 安全事件通知； |
| 漏洞扫描服务<br>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。<br>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。 | PDPL-保障个人数据的质量<br>PDPL-保障数据安全；<br>第47号决议-A.1 数据完整性；<br>第47号决议-E.1 漏洞管理；<br>第47号决议-G.1 安全事件通知； |

| 产品名称 | 产品介绍 | 对应的核心要求及控制措施 |
| --- | --- | --- |
| 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。<br>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。 | PDPL-保障个人数据的质量<br>PDPL-保障数据安全；<br>第47号决议-A.1 数据完整性；<br>第47号决议-E.1 漏洞管理；<br>第47号决议-G.1 安全事件通知； |

- **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。<br>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。 | PDPL-保障个人数据的质量<br>PDPL-保障数据安全；<br>第47号决议-A.1 数据完整性；<br>第47号决议-A.2 保密性；<br>第47号决议-E.1 漏洞管理； |
| 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。<br>VPC是客户的云上私有网络，各租户之间100%隔离，增强云上数据的安全性。 | PDPL-保障个人数据的质量<br>PDPL-保障数据安全；<br>第47号决议-A.1 数据完整性；<br>第47号决议-A.2 保密性；<br>第47号决议-B.1 资产识别；<br>第47号决议-B.2 数据访问；<br>第47号决议-H.1 安全的开发环境； |

- **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**<br>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。<br>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。 | PDPL-保障个人数据的质量<br>PDPL-保障数据安全；<br>第47号决议-D.1 备份副本和恢复过程； |
| **云服务器备份**<br>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。<br>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。 | PDPL-保障个人数据的质量<br>PDPL-保障数据安全；<br>第47号决议-D.1 备份副本与恢复过程； |

# 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，以遵循法律法规的要求。

华为云隐私保护和个人数据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近20个，主要包括适用于全球的隐私标准类、数据安全标准类证书以及区域性数据安全认证。

**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、贯穿个人数据处理全生命周期的管理措施。

- **ISO 27018**

  云平台隐私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隐私保护措施的要求，可保证客户个人数据安全。

- **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 认证表明华为云在隐私保护上拥有完善的体系以保证个人数据安全。

- **SOC2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SOC2 Type1隐私原则的审计，证明其在管理和技术上设计了合理的控制措施。

**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
- ISO 27799 健康信息安全管理体系认证

- 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
- 全球顶级数据中心基础设施运维认证(M&O认证)
- NIST网络安全框架
- PCI 3DS标准认证

**地区性安全认证**，包括：

- MTCS Level3多层云计算安全规范（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

华为云始终秉持华为公司“以客户为中心”的核心价值观，充分理解客户个人数据安全的重要性，尊重和保护客户隐私权利。华为云使用业界通用的安全及隐私保护技术，并通过云服务和解决方案的方式向客户提供相关能力，帮助客户应对日益复杂和开放的网络环境及日趋严格的隐私保护法律法规要求。

为实现各地区开展的业务符合当地隐私保护法规的要求，华为云持续洞察相关法律法规的更新，并将法规的新要求转换为华为云内部的规定，优化内部流程，以保证华为云开展的各类活动满足法律法规的要求。华为云根据更新的法律法规要求不断发展和持续推出隐私保护相关的服务和方案，帮助客户满足的隐私保护法律法规的新要求。

遵循隐私保护法律法规的要求是一项长期和多方位的活动，华为云愿意在未来持续提升能力，致力满足相关法律法规的要求，为客户构建安全、可信的云平台。

本白皮书仅供参考，不具备法律效应或构成法律建议。客户应酌情评估自身使用云服务的情况，并确保在使用华为云时对阿根廷PDPL及其他监管要求的遵从。

# 8 版本历史

| 日期 | 版本 | 描述 |
| --- | --- | --- |
| 2020年12月 | 1.0 | 首次发布 |