# 华为云新加坡 PDPA 隐私遵从性说明

文档版本 3.1

发布日期 2023-12-20

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新加坡共和国（简称“新加坡”）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. 新加坡隐私相关的法律要求；
3. 基于责任模型，华为云自身关于新加坡隐私法规的遵循性；
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，新加坡隐私法规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合规。

## 1.3 基本定义

- **数据控制者/组织：**包括任何个人、公司、协会或团体，无论法人或非法人，无论是否在新加坡法律下成立或认可、是否是新加坡居民或是否在新加坡设有办事处或营业地点。以上描述来自《新加坡个人数据保护法》（以下简称“PDPA”），亦指代本文中的“数据控制者”。
- **数据处理者/数据中介：**代表另一个组织处理个人数据的组织，但不包括该组织的员工。以上描述来自 PDPA，亦指代本文中的“数据处理者”。
- **内容数据：**指客户在使用华为云服务期间存储或处理的数据，包括但不限于数据、文件、软件、图像、音频、视频等类型的数据。
- **收集：**指组织获得对个人数据的控制权或拥有个人数据涉及的任何单独或一系列行为。

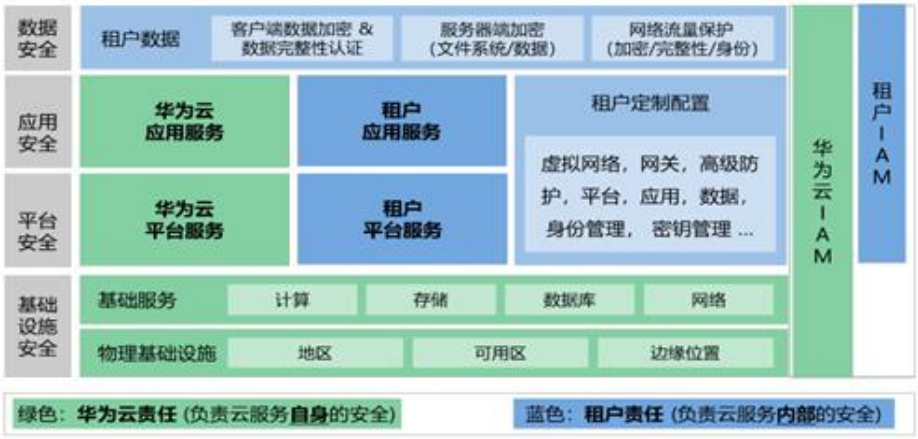
- **处理**：就个人数据而言，指与个人数据有关的任何操作或一系列操作，包括记录、持有、整理、调整或更改、恢复、组合、传输、删除或销毁。
- **使用**：指组织应用个人数据的任何行为或一系列行为。
- **披露**：指组织披露、转移或以其他方式向其他任何组织提供其控制或拥有的个人数据的任何单独的或一系列行为。
- **个人数据**：与一个身份已被识别或者身份可被识别的自然人（“数据主体”）相关的任何信息。身份可识别的自然人是指其身份可以通过诸如姓名、身份证号、位置数据等识别码或者通过一个或多个与自然人的身体、生理、精神、经济、文化或者社会身份相关的特定因素来直接或者间接地被识别。个人数据包括自然人的email 地址、电话号码、生物特征（指纹）、位置数据、IP 地址、医疗信息、宗教信仰、社保号、婚姻状态等。
- **华为云**：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。

# 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 华为云责任共担模型




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。
- **数据主体权利响应：**客户应保障数据主体的权利，响应数据主体的请求，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、通知数据主体、采取缓解措施等。

# 3 新加坡隐私法规概述

## 3.1 法规背景介绍

《个人数据保护法》（PDPA），为新加坡的个人数据提供了数据保护的基线标准，整体规范了组织对个人数据的收集、使用和披露，保障个人数据保护的权利，既承认个人数据保护的权力，也承认数据控制者出于合理目的收集、适用和披露个人数据的必要性。2020 年 11 月，首次全面修订《个人数据保护法》，并正式颁布《2020 年个人数据保护（修订）法》。该修订案的要求分阶段生效，2021 年 2 月生效的修正案包括数据泄露的通知要求、扩大明示同意的范围和明示同意的例外情况等。2022 年 10 月生效的修正案包括提高组织违反 PDPA 要求的罚款数额。

## 3.2 角色划分及基本义务

新加坡隐私法规规定了组织（数据控制者）、数据中介（数据处理者）两种关键角色。

**组织（数据控制者）：**包括任何个人、公司、协会或团体，无论法人或非法人，无论是否在新加坡法律下成立或认可、是否是新加坡居民或是否在新加坡设有办事处或营业地点。

**数据中介（数据处理者）：**代表另一个组织处理个人数据的组织，但不包括该组织的员工。

**数据控制者**的基本义务主要包括：

1. **通知及同意：**数据控制者事先通知个人收集、使用或披露个人数据的目的。数据控制者只能出于个人同意的目的，或在 PDPA 或新加坡任何其他成文法律授权的情况下收集、使用或披露个人数据。如果个人撤回同意，则该数据控制者必须停止收集、使用或披露个人数据。
2. **目的限制：**目的限制义务规定数据控制者仅可以出于合理的并已经通知个人的目的收集、使用或披露个人数据。
3. **访问及更正：**个人有权要求访问其个人数据并更正其由数据控制者拥有或控制的个人数据。
4. **准确性：**PDPA 要求数据控制者确保数据控制者或代表数据控制者收集的个人数据是准确和完整的，以保证可能需要使用个人数据以做出会对个人产生影响的决策时，所有相关且准确的个人数据均能被考虑在内。

5. **保护：**在收集、使用、披露个人数据之前，数据控制者应进行评估确保该行为不会对个人产生不利的影响。通过做出合理的安全规划以保护其拥有或控制的个人数据，以防止未经授权的访问、收集、使用、披露、复制、修改、处置以及存储个人数据的介质或设备的丢失或类似风险。
6. **保留限制：**当数据控制者不再能满足个人数据当初被收集的目的，并且个人数据不再需要出于法律或商业的目的被保留时，停止保留个人数据，或保证数据无法识别个人身份。
7. **转移限制：**数据控制者不得将任何个人数据转移到新加坡境外的国家或地区，除非转移的个人数据受到的保护符合 PDPA 规定的数据保护标准。
8. **泄露通知：**数据控制者必须以合理和迅速的方式评估数据泄露是否应通知，在评估为应通知的情况下，通知受影响的个人和/或委员会。
9. **问责义务：**问责义务主要指数据控制者需要制定和执行 PDPA 义务所必需的政策和实践并对公众可知，与此相关的要求在 PDPA 中统称为问责义务。

## 3.3 华为云在新加坡隐私法规下的角色

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，华为云一般作为个人数据处理者。在处理客户创建或管理华为云帐号提供的个人数据时，华为云作为个人数据的数据控制者。

- **华为云作为个人数据的控制者**

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。华为云将基于新加坡隐私法规的要求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、传输过程符合法律规定，响应个人数据主体权利申请。

- **华为云作为客户内容数据的个人数据的处理者/服务提供商**

当客户为个人数据的控制者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，华为云的角色为个人数据处理者/服务提供商。华为云代表客户根据个人数据处理协议或个人数据控制者的指令处理个人数据。

# 4 华为云如何响应新加坡隐私合规要求

## 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、对数据主体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，降低对数据主体的风险。

- **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数据控制者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 华为云响应新加坡《个人数据保护法》《个人数据保护条例》和《个人数据保护（数据泄露通知）条例》的合规措施

基于华为云业务的特性，根据新加坡《个人数据保护法》《个人数据保护条例》《个人数据保护（数据泄露通知）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的角色。

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新加坡《个人数据保护法》《个人数据保护条例》和《个人数据保护（数据泄露通知）条例》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。

| 法规基本义务 | 华为云适用的具体要求<br>（作为个人数据控制者） | 华为云采取的措施 |
| --- | --- | --- |
| **通知及同意** | 1. 数据控制者应事先通知个人收集、使用或披露个人数据的目的。<br>2. 数据控制者只能出于个人同意的目的，或在 PDPA 或新加坡任何其他成文法律授权的情况下收集、使用或披露个人数据。<br>3. 如果个人撤回同意，数据控制者必须停止收集、使用或披露个人数据。 | 1. 在客户与华为云互动过程中，如要收集客户个人数据，华为云会主动通知所收集的个人数据类型、目的、处理方式、时间等内容，如在官网提供的华为云**《隐私政策声明》**。对于各类线下市场营销活动中需收集个人数据时，在显著的位置提供隐私通知，并在收集个人数据时提供同意选项。<br>对于涉及个人数据处理的云服务，华为云会在云服务用户资料中提供个人数据清单，说明相关个人数据处理的业务场景、目的、个人数据范围及处理方式等，以帮助您评估相关业务的合规风险和隐私管控措施。必要时云服务中提供了配置隐私通知的功能，您可根据业务合规需求自行配置隐私通知。<br>2. 针对客户的内容数据，华为云不会使用或披露，除非是客户授权，或者是为遵守当 |

| 法规基本义务 | 华为云适用的具体要求（作为个人数据控制者） | 华为云采取的措施 |
| --- | --- | --- |
| | | 地适用的法律法规或政府机关的约束性命令。 |
| **目的限制** | 1. 数据控制者仅可以出于合理的并已经通知个人的目的收集、使用或披露个人数据。 | 1. 华为云仅在获得客户同意后，收集提供服务所必须的客户个人数据，并在《隐私政策声明》中限定的目的范围内处理客户个人数据。<br>2. 在华为云产品设计阶段，华为云会梳理涉及的所有个人数据类型并进行隐私影响评估(Privacy Impact Assessment，简称 PIA），确保华为云各产品涉及的个人数据的收集不超出实现目的所需。在运营运维过程中，华为云会基于工作人员的角色，设置其对个人数据不同的访问权限，确保工作人员可访问或使用的个人数据仅为其工作所必须。 |
| **访问及更正** | 1. 个人有权要求访问其个人数据并更正其由数据控制者拥有或控制的个人数据。 | 1. 华为云保障客户行使其作为数据主体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，华为云建立了数据主体权利请求响应机制，以保障数据主体的权利请求得到合理、及时的响应。<br>2. 华为云将准确完整地回应数据主体请求内容，以文件形式向其提供个人数据使用和披露信息的副本。 |
| **准确性** | 1. 数据控制者收集的个人数据是准确和完整的，以保证可能需要使用个人数据以做出会对个人产生影响的决策时，所有相关且准确的个人数据均能被考虑在内。 | 1. 对于客户个人数据，华为云采取了不同的措施确保其准确性。例如，华为云在客户输入个人数据时会对数据进行有效性检验，增强数据输入的规范性和准确性。华为云还要求客户输入通过客户提供的电子邮件地址或手机号码获取的验证码，以确认客户的身份及相关联系信息的准确性。对于客户的内容数据，华为云为客户提供了 |

| 法规基本义务 | 华为云适用的具体要求（作为个人数据控制者） | 华为云采取的措施 |
| --- | --- | --- |
| | | 多种数据安全和隐私保护功能，帮助客户保证其内容数据的准确性。 |
| 保护 | 1. 在收集、使用、披露个人数据之前，数据控制者应进行评估确保该行为不会对个人产生不利的影响。通过做出合理的安全规划以保护其拥有或控制的个人数据，以防止未经授权的访问、收集、使用、披露、复制、修改、处置以及存储个人数据的介质或设备的丢失或类似风险。 | 1. 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，要求在其处理个人数据前必须开展隐私影响评估（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、对数据主体可能产生的影响、风险分析并制定风险控制措施和计划等，将所有隐私风险控制需求落入设计方案中。只有将隐私风险降低至可接受的水平后才能开展业务。<br>2. 针对客户个人数据，华为云通过一系列的技术保障个人数据的安全。例如，通过身份认证和访问控制技术，实施基于角色所需最小权限的策略，防止未授权处理个人数据的行为；广泛采用加密技术对客户个人数据进行加密存储和传输，确保个人数据存储和传输中的安全；通过日志记录和审计技术，及时发现潜在的安全隐患以便及时迅速的做出反馈，解决问题。<br>3. 针对客户的内容数据，华为云使用各种数据安全技术和相关管控措施如身份认证和访问控制、数据传输及存储加密技术、日志记录等手段保障华为云服务自身的安全性。 |
| 保留限制 | 1. 当数据控制者不再能满足个人数据当初被收集的目的，并且个人数据不再需要出于法律或商业的目的被保留时，停止保留个人数据，或保证数据无法识别个人身 | 1. 对于客户个人数据，华为云将会在达成隐私声明所述目的所需的期限内保留客户的个人数据，除非按照法律要求需要延长保留期。保留期可能基于处理的目的以及相 |

| 法规基本义务 | 华为云适用的具体要求（作为个人数据控制者） | 华为云采取的措施 |
| --- | --- | --- |
| | 份。 | 关服务而有所差异。在客户注销帐户后，华为云将停止向客户提供服务并删除客户的相关个人数据。<br>2. 对于客户内容数据，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。 |
| **转移限制** | 1. 数据控制者不得将任何个人数据转移到新加坡境外的国家或地区，除非转移的个人数据受到的保护符合 PDPA 规定的数据保护标准。 | 1. 华为云在全球多个国家建立数据中心，在运营运维过程中涉及需要进行数据跨境传输的场景时，遵循当地隐私保护法律法规并经过内部严格评审。如在签订数据转移协议或获得数据主体的明确同意之后进行数据跨境转移，保证个人数据将被合法、正当、透明地处理。 |
| **泄露通知** | 1. 数据控制者必须以合理和迅速的方式评估数据泄露是否应通知，在评估为应通知的情况下，通知至客户，由客户通报受影响的个人和/或委员会。 | 1. 华为云内部制定了完善的关于个人数据泄露事件的管理制度，相关人员将依据流程分析事件的影响，若事件已对或即将对云服务客户产生影响时，华为云将启动通知通报机制，将事件通知委员会和客户。通知的内容包括但不限于：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。同时为配合客户满足法规要求，为配合客户满足个人数据信息泄露事件上报的要求，华为云设置 7*24h 的专业安全事件响应团队以及专家资源池，依照法律法规要求，对相关事件及时披露，及时知会客户，同时执行应急预案及恢复流程，降低业务影响。 |
| **问责义务** | 1. 数据控制者需要制定和执行 PDPA 义务所必需的政策和实践并对公众可知。具体有 | 1. 华为公司制定并实施了关于个人数据保护的政策及规定，华为云遵循与华为公司 |

| 法规基本义务 | 华为云适用的具体要求<br>（作为个人数据控制者） | 华为云采取的措施 |
| --- | --- | --- |
| | 关此义务的要求包括：<br>员工应了解此类政策和实践；数据控制者应建立响应《个人数据保护法》相关投诉的流程，投诉方式应对公众可知；数据控制者应有专人负责对 PDPA 的合规并将其相关联系方式公开等。 | 同样的政策，建立了全面的隐私保护流程体系，通过一系列科学、严格的流程，确保业务活动开展符合隐私保护的要求，如隐私流程框架、保护政策、隐私保护设计规范等。华为公司个人数据保护的政策及规定在华为内网对每个员工均可见，若有任何关于政策的更改，华为公司会向员工发出通告，确保员工知晓并遵守相关政策，从内部管理保障客户个人数据的安全。 |

# 5 华为云协助客户响应新加坡隐私合规要求

## 5.1 客户的隐私保护责任

当客户利用华为云的服务为其他电子系统使用者提供新加坡隐私法规管辖范围下的服务时，华为云将协助客户履行其相应的义务。

| 法规基本义务 | 客户适用的具体要求<br>（作为个人数据控制者） | 华为云采取的措施 |
| --- | --- | --- |
| 通知及同意 | 1. 数据控制者应事先通知个人收集、使用或披露个人数据的目的。<br>2. 数据控制者只能出于个人同意的目的，或在 PDPA 或新加坡任何其他成文法律授权的情况下收集、使用或披露个人数据。<br>3. 如果个人撤回同意，则数据控制者必须停止收集、使用或披露个人数据。 | 1. 客户在华为云中的内容数据包含个人数据，客户应将个人数据收集的目的告知数据主体并获得其同意；数据主体可以发送合理请求撤回已被视为给予的同意。同时，客户可使用华为云产品和服务提供的功能或自身构建的能力，更好地践行个人数据保护法中关于通知及同意的原则。例如在华为云的融合视频云服务（Convergent Video Cloud Service，简称 CVCS）中，客户可通过华为云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的功能，将个人数据处理的政策告知其用户。针对涉及个人数据处理相关特性的云服务，客户可根据华为云在其产品资料中提供的关于个人数据的种类、处理和存储的方式等相关信息，采取相应的隐 |

| 法规基本义务 | 客户适用的具体要求<br>（作为个人数据控制者） | 华为云采取的措施 |
| --- | --- | --- |
| | | 私保护措施。 |
| **目的限制** | 1. 数据控制者仅可以出于合理的并已经通知个人的目的收集、使用或披露个人数据。 | 1. 如果客户在华为云中的内容数据包含个人数据，客户可依托华为云提供的相关服务或自身构建的能力，确保仅出于合理的以及在数据主体已经同意的目的范围内处理个人数据。客户可通过华为云提供的数据安全中心（Data Security Center，简称DSC），从自己拥有的海量数据中迅速识别出个人数据，并进行相应的数据保护处理，客户可基于识别的个人数据分析已经收集的个人数据是否为满足业务目的所必需的，数据收集的目的是否已经对数据主体进行告知并符合相关个人数据处理要求。若存在不合规之处，可及时采取整改措施，避免违法风险。 |
| **访问及更正** | 1. 客户有权要求访问其个人数据并更正其由数据控制者拥有或控制的个人数据。<br>2. 客户向数据控制者提出的请求必须以书面形式提出，并且必须包括足够的细节，以使数据控制者能够判断：提出请求的申请人；申请人要求的个人数据以及使用和披露信息；申请人要求的个人数据更正请求等信息。 | 1. 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。<br>2. 数据主体享有访问权、更正权、删除或限制权、可携带权以及撤回同意等隐私权利，客户应形成个人数据管理机制。华为云的大部分产品或服务中具备数据处理功能，用户可自主访问、更正、删除、导出个人数据。 |
| **准确性** | 1. 确保数据控制者收集的个人数据是准确和完整的，以保证可能需要使用个人数据以做出会对个人产生影响的决策时，所有相关且准确的个人数据均能被考虑在内。 | 1. 华为云提供的多种数据安全和隐私保护功能，保证其内容数据的准确性。例如，在数据存储阶段，华为云在云硬盘、对象存储、镜像服务和关系型数据库等多个服务均提供数据加密（服务端加密）功 |

| 法规基本义务 | 客户适用的具体要求<br>（作为个人数据控制者） | 华为云采取的措施 |
| --- | --- | --- |
| | | 能，采用高强度的算法对存储的数据进行加密，且服务端加密功能集成了**数据加密服务**（Data Encryption Workshop，简称 DEW），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。<br>2. 在数据使用阶段，客户可通过华为云提供的**统一身份认证服务**（Identity and Access Management，简称 IAM），采取适合企业的用户管理、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。在数据传输阶段，客户可通过华为云提供的多种加密传输机制，保证数据传输过程中的完整性，如当客户通过互联网提供 Web 网站业务时，可以使用华为云的证书管理服务，实现网站的可信身份认证以及基于加密协议的安全传输；针对客户业务混合云部署和全球化布局的场景，可以使用华为云提供的**虚拟专用网络**（Virtual Private Network，简称 VPN）、**云专线服务**（Direct Connect，简称 DC）、**云连接**（Cloud Connect，简称 CC）等服务。 |
| **保护** | 1. 在收集、使用、披露个人数据之前，数据控制者应进行评估确保该行为不会对个人产生不利的影响。通过做出合理的安全规划以保护其拥有或控制的个人数据，以防止未经授权的访问、收集、使用、披露、复制、修改、处置以及存储个人 | 1. 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，并设置恰当的访问控制策略和密码策略。同时，客户可通过华为云提供的多种安全服 |

| 法规基本义务 | 客户适用的具体要求<br>（作为个人数据控制者） | 华为云采取的措施 |
| --- | --- | --- |
| | 数据的介质或设备的丢失或类似风险。 | 务，满足其不同安全级别的要求，详情可参考华为云已发布的《华为云安全白皮书》和《华为云数据安全白皮书》 。 |
| **保留限制** | 1. 当数据控制者不再能满足个人数据当初被收集的目的，并且个人数据不再需要出于法律或商业的目的被保留时，停止保留个人数据，或保证数据无法识别个人身份。 | 1. 华为云不会触碰客户的内容数据，客户享有数据自主权，华为云提供多处可用区供客户自主选择数据存储区域。<br>2. 为满足法规中对于数据保留的目的、期限要求，客户应制定相应的数据保留政策，并借助华为云提供的相关服务设置保留期限，在个人数据不再被法律或商业目的需要时删除个人数据或将其匿名化。客户可通过华为云提供的相关服务，对敏感个人数据进行脱敏，让数据无法再识别个人身份。比如，客户可使用华为云数据安全中心（Data Security Center，简称 DSC）发现存储在各类数据库中的个人数据，根据规则识别出个人数据，并依据脱敏策略对个人数据进行实时隐藏。<br>3. 针对客户的内容数据，用户可在已开服的节点自定义选择留存位置、留存时间，华为云使用各种数据安全技术和相关管控措施如身份认证和访问控制、数据传输及存储加密技术、日志记录等手段保障华为云服务自身的安全性 |
| **转移限制** | 1. 数据控制者不得将任何个人数据转移到新加坡境外的国家或地区，除非转移的个人数据受到的保护符合 PDPA 规定的数据保护标准。 | 1. 客户在购买华为云产品或服务时，应根据自身业务的合规需要，选择存储内容数据的可用区并合理配置虚拟私有云（VPC）策略。如果在华为云存储个 |

| 法规基本义务 | 客户适用的具体要求<br>（作为个人数据控制者） | 华为云采取的措施 |
| --- | --- | --- |
| | | 人数据，告知数据主体其个人数据所存储的区域。客户与其个人用户之间有关数据跨境传输的事项的定义为客户的责任。<br>2. 客户可以指定内容所存储的区域，未经客户同意，华为云不会将客户内容从选择的区域中迁移。此外，客户可通过华为云提供的 VPC 服务搭建私有网络环境，通过子网规划、路由策略配置等进行网络区域划分，将存储放置在指定可用区域的内部子网。 |
| **泄露通知** | 1. 数据控制者必须以合理和迅速的方式评估数据泄露是否应通知，在评估为应通知的情况下，通知受影响的个人和/或委员会。 | 1. 当发生数据泄露事件后，客户必须以合理和迅速的方式评估数据泄露是否为应报告的数据泄露事件。如发生导致对个人造成重大伤害或是大规模的数据泄露事件，客户必须在做出评估后的 72h 内通知委员会和受影响的个人。向委员会提交数据泄露发生的日期和情况、已经采取的控制措施、数据泄露的原因等信息；同时应向受影响的个人发出通知，包含：数据泄露的情况、对个人的潜在伤害，已采取的控制措施、业务代表联系方式等信息。<br>2. 华为云内部制定了完善的关于个人数据泄露事件的管理制度，相关人员将依据流程分析事件的影响，若事件已对或即将对云服务客户产生影响时，华为云将启动通知通报机制，将事件通知委员会和客户。通知的内容包括但不限于：事件的描述、起因、影响、华为云已采取 |

| 法规基本义务 | 客户适用的具体要求<br>（作为个人数据控制者） | 华为云采取的措施 |
| --- | --- | --- |
| | | 的措施、建议客户采取的措施等。同时为配合客户满足法规要求，为配合客户满足个人数据信息泄露事件上报的要求，华为云设置 7*24h 的专业安全事件响应团队以及专家资源池，依照法律法规要求，对相关事件及时披露，及时知会客户，同时执行应急预案及恢复流程，降低业务影响。 |
| 问责义务 | 1. 数据控制者需要制定和执行 PDPA 义务所必需的政策和实践并对公众可知。具体有关此义务的要求包括：员工应了解此类政策和实践；数据控制者应建立响应《个人数据保护法》相关投诉的流程，投诉方式应对公众可知；数据控制者应有专人负责对 PDPA 的合规并将其相关联系方式公开等。 | 1. 客户内容中包含的个人数据由客户自行收集，若客户选择使用华为云服务并将包含个人数据的客户内容存储在华为云上，客户有责任建立个人数据保护政策和实践，确保其政策和实践符合 PDPA 的要求，并使数据主体知晓。<br>2. 客户可通过华为云官网信任中心公开的资料了解华为云隐私保护的相关信息，如有需要，可获取华为云第三方审计报告以了解华为云内部管理控制情况。 |

## 5.2 华为云产品和服务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新加坡隐私法规。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 | 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 | 个人数据收集<br>个人数据合法处理 |

| 产品名称 | 产品介绍 | 对应的核心要求及控制措施 |
| --- | --- | --- |
| Identity and Access Management (IAM) | 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。 | 保障数据主体的权利<br>数据安全 |
| 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，保障数据主体的知情权、实现快速查找。 | 个人数据合法处理<br>个人数据处理原则<br>保障数据主体的权利 |
| 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。 | 个人数据合法处理<br>个人数据处理原则<br>个人数据泄露通知<br>数据安全 |
| 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，保障数据主体的知情权。 | 个人数据处理原则<br>个人数据泄露通知<br>数据安全<br>保障数据主体的权利 |

- 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。 | 数据安全 |
| 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。 | 个人数据处理原则<br>数据安全 |

| | | |
|---|---|---|
| **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。 | 个人数据处理原则<br>数据安全 |
| **DDoS 高防**<br>(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。 | 数据安全 |
| 数据安全中心<br>Data Security Center (DSC) | DSC 是新一代的云原生数据安全平台，提供数据分类分级，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能力。<br>客户可通过 DSC 整合数据安全生命周期各阶段状态，构建云服务全景图，保护数据采集、存储/传输、使用、交换/销毁的安全。 | 数据安全 |
| 云堡垒机<br>Cloud Bastion Host (CBH) | CBH 是华为云的一款 4A 统一安全管控平台，为企业提供集单点登录、统一资产管理、多终端访问协议、文件传输、会话协同等功能于一体的运维管理服务。<br>客户可通过 CBH 对云主机进行远程运维，提高客户的访问控制安全能力，保护资源运维和系统管理的安全性，降低系统和运维资源被非法入侵的风险。 | 数据安全 |
| 云证书管理服务<br>Cloud Certificate Manager (CCM) | CMM 是一个为云上海量证书颁发和全生命周期管理的服务，提供 SSL 证书管理和私有证书管理服务。<br>客户可通过 CCM 提高对 SSL 证书和私有证书的保密性和安全性，提升访问和传输通道的安全，降低数据在传输和访问过程中被非法入侵、访问或盗取的风险。 | 数据安全 |

- **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<br>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。 | 数据安全 |

| 产品名称 | 产品介绍 | 对应的核心要求及控制措施 |
| --- | --- | --- |
| | 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。 | |
| 虚拟私有云<br>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，各客户之间 100%隔离，增强云上数据的安全性。 | 数据安全 |

- **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。 | 数据安全 |
| 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。 | 数据安全 |

# 6 华为云隐私保护相关认证资质

华为云继承了华为公司完备的管理体系以及 IT 系统的建设和运营经验，对华为云各项服务的集成、运营及维护进行主动管理，并持续改进。截至目前，华为云已获得众多全球性、区域性和行业特定的安全合规的权威认证，全力保障客户部署业务的安全。

关于更多华为云的安全合规信息以及获取相关合规证书，可参见华为云官网“信任中心-合规中心”

**华为云部分标准类认证/鉴证示例：**

| 认证 | 描述 |
| --- | --- |
| ISO27001:2022 | ISO27001 是目前国际上被广泛接受和应用的信息安全管理体系认证标准。该标准以风险管理为核心，通过定期评估风险和对应的控制措施来有效保证组织信息安全管理体系的持续运行。 |
| ISO27017:2015 | ISO27017 是针对云计算信息安全的国际认证。ISO27017 的通过，表明华为云在信息安全管理能力达到了国际公认的最佳实践。 |
| ISO27018:2019 | ISO27018 是专注于云中个人数据保护的国际行为准则。ISO27018 的通过，表明华为云已满足国际认可的公有云个人数据保护措施的要求，可保证客户个人数据安全。 |
| TL 9000& ISO 9001 | ISO 9001 是 ISO 9000 族标准所包括的一组质量管理体系核心标准之一，用于证实组织具有提供满足顾客要求和适用法规要求的产品的能力。<br>TL 9000 是一个建立在 ISO9001 基础上的，由全球电信业优质供应商联盟（QuEST Forum）针对全球信息和通讯技术（ICT）行业特定设计的、为 ICT 产品和服务供方提供的一套通用的质量管理体系要求。它包括了 ISO9001 的所有要求，ISO9001 将来的任何改动也会导致 TL9000 的改动。 |

| 认证 | 描述 |
| --- | --- |
| | 华为云取得了 ISO9001 / TL9000 认证证书，表明华为云可以为您提供更快，更好和更具成本效益的服务。 |
| ISO20000-1:2018 | ISO20000 是针对信息技术服务管理领域的国际标准，提供设计、建立、实施、运行、监控、评审、维护和改进服务管理体系的模型以保证服务供应商可提供有效的 IT 服务来满足客户和业务的需求。 |
| ISO22301:2019 | ISO22301 是国际公认的业务连续性管理体系标准，通过对风险的识别、分析和预警来帮助组织规避潜在事件的发生，并且制定完备的“业务连续性计划”，有效地应对中断发生后的快速恢复，保持核心功能正常运行，将损失和恢复成本降至最低。 |
| CSA STAR 认证 | CSA STAR 认证是由标准研发机构 BSI（英国标准协会）和 CSA（云安全联盟）合作推出的国际范围内的针对云安全水平的权威认证，旨在应对与云安全相关的特定问题，协助云计算服务商展现其服务成熟度的解决方案。 |
| ISO27701:2019 | ISO27701 规定了建立、实施、维护和持续改进隐私相关所特定的管理体系的要求。华为云通过 ISO27701 表明了其在个人数据保护具有健全的体制。 |
| BS 10012:2017 | BS10012 是 BSI 发布的个人信息数据管理体系标准，BS10012 认证的通过表明华为云在个人数据保护上拥有完整的体系以保证个人数据安全。 |
| ISO 29151:2017 | ISO29151 是国际个人身份信息保护实践指南。ISO29151 的通过，表明华为云实施国际认可的个人数据处理的全生命周期的管理措施。 |
| PCI DSS | 支付卡行业数据安全标准（PCI DSS）是由 JCB、美国运通、Discover、万事达和 Visa 等五家国际信用卡组织共同建立的一套支付卡行业数据安全标准，由支付卡行业安全标准委员会管理。它是世界上最权威、最严格的金融机构认证。 |
| PCI 3DS | PCI 3DS 标准，旨在保护执行特定 3DS 功能或者存储 3DS 数据的 3DS 环境，支持 3DS 的实施。PCI 3DS 的评估对象为 3D 协议执行环境，包括访问控制服务器、目录服务器或 3DS 服务器功能；以及 3D 执行环境内和连接到环境所需要的系统组件，如防火墙、虚拟服务器、网络设备、应用等；除此之外，还会评估 3D 协议执行环境的过程、流程、人员管理等。 |

| 认证 | 描述 |
| --- | --- |
| ISO 27799:2016 | ISO/IEC 27799 是专注于医疗行业的信息安全管理体系，为医疗行业和其相关机构提供了关于如何更好地保护个人健康信息的保密性、完整性、可审计性和可用性的指导。<br>华为云是全球首个获得该认证的云服务商，表明华为云对医疗行业的理解和实践，对医疗行业信息安全的防护能力得到国际权威认可，能够更可靠的保障您的信息安全。 |
| ISO 27034 | ISO/IEC 27034 是国际标准化组织 ISO 通过的第一个关注建立安全软件程序流程和框架的标准，它清晰地定义了实际应用中软件系统面临的风险，同时为不同类型的软件开发组织提供了一套可以灵活应用的方法。华为云是全球首家获得 ISO/IEC 27034 认证的云服务提供商，表明华为云具备在云服务中保持持续安全和合规的能力。 |
| SOC 审计报告 | SOC 审计报告是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。 |

# 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新加坡隐私要求的遵从。

# 8 版本历史

| 日期 | 版本 | 描述 |
| --- | --- | --- |
| 2023 年 12 月 | 3.1 | 合规要求更新 |
| 2023 年 02 月 | 3.0 | 合规要求更新 |
| 2022 年 04 月 | 2.0 | 合规要求更新 |
| 2019 年 11 月 | 1.0 | 首次发布 |